Sirja Virolainen

IDENTITEETIN- JA PÄÄSYNHALLINTAAN LIITTYVÄT RISKIT ASIANTUNTIJAORGANISAATIOISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Virolainen, Sirja
Identiteetin- ja pääsynhallintaan liittyvät riskit asiantuntijaorganisaatioissa
Jyväskylä: Jyväskylän yliopisto, 2020, 91 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Halttunen, Veikko

Nykypäivänä asiantuntijaorganisaatioissa käsitellään suurta määrää tietoa, kuten heidän asiakkaisiinsa ja työntekijöihin liittyvää sensitiivistä tietoa. Erityisesti asiantuntijaorganisaatiot ovat hyvin riippuvaisia heidän maineestaan ja luotettavuudesta asiakkaiden silmissä, koska koko organisaation liiketoiminta perustuu asiakkaiden luottamukseen. Tietoturva on suurimpia organisaatioiden kohtaamia haasteita, ja monet yritykset vastaavat tähän haasteeseen erilaisin teknologiaratkaisuin. Identiteetin- ja pääsynhallinta on tärkeä osa organisaation tietoturvaa, koska sen avulla voidaan taata organisaatioresursseihin pääsy vain valtuutetuille käyttäjille. Tämän tutkimuksen tavoitteena oli selvittää identiteetin- ja pääsynhallintaan liittyviä riskejä asiantuntijaorganisaatioissa. Tutkimus toteutettiin kirjallisuuskatsauksena ja empiirisenä tutkimuksena, jolle kirjallisuuskatsaus muodostaa teoreettisen perustan. Tutkielma toteutettiin toimeksiantona kohdeorganisaatiolle. Kirjallisuuskatsauksen perusteella luotiin teemahaastattelurunko, jolla pyrittiin selvittämään erilaisia identiteetin- ja pääsynhallintaan liittyviä riskejä. Haastateltavina toimivat kohdeorganisaation asiantuntijat, joita tutkimukseen haastateltiin kymmenen. Haastateltavia valittiin kolmesta eri asiantuntijaryhmistä, joita olivat tietohallinnon asiantuntijat, identiteetin- ja pääsynhallinnan asiantuntijat ja sisäisen tietoturvan asiantuntijat. Haastattelun perusteella selvisi identiteetin- ja pääsynhallintaan liittyvän runsaasti erilaisia riskejä. Tutkimuksessa esiin nousseet riskiteemat olivat manuaalisuus, hajautuneisuus, pilvipalveluihin liittyvät riskit, keskitetyn identiteetin- ja pääsynhallinnan riskit, automaation riskit ja organisaation sisäiset riskit. Jokaiseen riskiteemaan tunnistettiin niin kirjallisuuskatsauksessa, kuin empiirisessäkin tutkimuksessa runsaasti riskejä. Identiteetin- ja pääsynhallintaan voidaan siis tutkielman perusteella liittyvän runsaasti erilaisia riskejä, joita asiantuntijaorganisaatioiden tulee ottaa huomioon heidän identiteetin- ja pääsynhallinnassa, etenkin pohdittaessa uuden ratkaisun valintaa ja hankintaa.

Asiasanat: identiteetin- ja pääsynhallinta, riskit, identiteetinhallinta, pääsynhallinta, keskitetty identiteetinhallinta, automaatio

ABSTRACT

Virolainen, Sirja
The identity and access management risks in expert organizations
Jyväskylä: University of Jyväskylä, 2020, 91 pp.
Information Systems, Master's Thesis
Supervisor(s): Halttunen, Veikko

Today's expert organizations manage great amount of their clients and employee's sensitive data. Especially expert organizations are highly dependent on their reputation, because their business is strictly based on customers trust. Information security is one of the biggest challenges for organizations and many of them utilize variety of technology solutions. Identity and access management is important part of organizations information security, because it gives access only for authorized users. Aim of this thesis is to find out what different kind of risks are related to expert organizations identity and access management. This thesis consists literature review and empirical research. Semi-structured interview frame was created based on literature reviews findings. The interviewees were employees of the case organization with different roles; Information Management specialist, Identity and Access Management specialist and Information Security specialist. Based on interviews it can be said that identity and access management contain great amount of risks. Based on this study there are six risk themes related to identity and access management: manual work, decentralization, risks related to cloud services, risks of centralized identity and access management, risks of automation and internal risks of the organization. The results of the empirical study mostly supported literature review results. Based on these findings it can be said that identity and access management contain variety of risks, and expert organizations should consider these risks in their identity and access management related decision-making.

Keywords: identity and access management, risks, identity management, access management, centralized access management, automation

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Maailman väestön kasvaessa myös Internetin, matkapuhelimien ja sähköpostien käyttäjien määrä kasvaa jatkuvasti (Kumar & Bhardwaj, 2018). Päivittäin miljoonat ihmiset kommunikoivat, tekevät ostoksia, keräävät tietoa ja suorittavat lukemattomia muita tehtäviä verkon välityksellä (Gauthier & Merlo, 2012).

Myös nykypäivän yritysten toiminta perustuu merkittävissä määrin tiedon käsittelyyn, ja organisaatioissa käsitellään jatkuvasti kasvavaa määrää tietoa (Bodkin, 2004). Sensitiivisen tiedon käsittely tuo mukanaan monia riskejä, kuten tietovuodot, jotka voivat aiheuttaa mittavia taloudellisia vahinkoja, sekä maineen ja uskottavuuden menettämisen asiakkaiden, median ja sidosryhmien silmissä (Bodkin, 2004; Bulgurcu, Cavusoglu & Benbasat, 2010; Gauthier & Merlo, 2012).

Organisaatiot ovat voimakkaasti riippuvaisia tietojärjestelmistä, mikä vaatii niitä huolehtimaan tietojärjestelmiin liittyvistä riskeistä (Bulgurcu ym., 2010; Gauthier & Merlo, 2012). Tietojärjestelmien turvallisuus on suurin haaste, jonka globaalit organisaatiot kohtaavat nykypäivänä (Bradford, Earp & Grabski, 2014). Tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus ja vähentää liiketoimintaan kohdistuvia vahinkoja, tietoturvaan liittyviä riskejä minimoimalla (Von Solms & Van Niekerk, 2013). Monet organisaatiot luottavat tietoturvaasioissa teknologiaan pohjautuviin ratkaisuihin, kuten identiteetin ja pääsyhallintaan liittyvissä ratkaisuissa (Bulgurcu ym., 2010).

Identiteetin- ja pääsynhallinnalla organisaatiokontekstissa tarkoitetaan käyttäjien oikeuksien hallintaa erilaisissa tietojärjestelmissä (Anilkumar & Sumathy, 2018; Dunphy & Petitcolas, 2018; Kumar & Bhardwaj, 2018). Käsite jaetaan identiteetinhallintaan ja pääsynhallintaan. Identiteetinhallinta kattaa käyttäjien identiteetin tallentamiseen ja säilytykseen liittyvät toiminnot, kun taas pääsynhallintaan kuuluu käyttäjän tunnistus, todennus ja varmennus eri organisaatioresursseihin pääsemiseksi (Kumar & Bhardwaj, 2018; Linden, 2012).

Identiteetin- ja pääsynhallinta ovat kriittisessä osassa yrityksen tietoturvaa, koska sen avulla voidaan minimoida monia riskejä, jotka ovat hyvin kriittisiä koko yrityksen liiketoiminnan kannalta (Feng, Lin, Peng & Li, 2008; Hummer, Kunz, Netter, Fuchs & Pernul, 2016; Khan, 2012; Kumar & Bhardwaj, 2018).

Identiteetin- ja pääsynhallintaan on tarjolla useita erilaisia malleja, joista yleisimmin käytettäviin perehdytään luvussa 3 (Anilkumar & Sumathy, 2018; Dos Santos, Westphall & Westphall, 2014; Hummer ym., 2016; Kunz, Fuchs, Hummer & Pernul, 2015b). Jokaisessa mallissa on omat etunsa ja rajoitteensa (Bradford ym., 2014; Hummer ym., 2016). Malli tulee valita yrityksen tarpeiden ja strategian mukaisesti (Hummer ym., 2016).

Tämän pro gradu -tutkielman tavoitteena on kartoittaa laajasti identiteetin- ja pääsynhallintaan liittyviä potentiaalisia riskejä asiantuntijaorganisaatioissa. Näkökulmana on organisaation sisäinen, eli työntekijöiden identiteetin- ja pääsynhallinta organisaation näkökulmasta. Tutkimusongelma muotoiltiin seuraavasti

> Millaisia potentiaalisia riskejä identiteetin- ja pääsynhallintaan liittyy asiantuntijaorganisaatioiden näkökulmasta?

Ennen varsinaiseen tutkimusongelmaan vastaamista tulee selvittää mitä identiteetin- ja pääsynhallinnalla tarkoitetaan organisaatiokontekstissa. Tutkimusongelman selvittämiseksi tutkimukselle laadittiin kaksi varsinaista tutkimuskysymystä:

1. Mitä identiteetin- ja pääsynhallinta tarkoittaa organisaatiokontekstissa?
2. Millaisia riskejä identiteetin- ja pääsynhallintaan liittyy asiantuntijaorganisaatioiden näkökulmasta?

Tutkielma koostuu kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta. Kirjallisuuskatsauksen tavoitteena on selvittää mitä identiteetin- ja pääsynhallinta tarkoittaa organisaatiokontekstissa sekä muodostaa teemahaastattelupohja, jolla voidaan selvittää vastaus tutkimuskysymykseen kaksi.

Kirjallisuuskatsaus perustuu aiempiin tieteellisiin tutkimuksiin ja artikkeleihin. Valittu tutkimusaineisto koostuu suurimmaksi osin vertaisarvioiduista tutkimusartikkeleista. Käytetty aineisto on kerätty käyttämällä universaaleja tieteellisten julkaisujen hakukoneita Google Scholaria sekä Scopusta. Muita lähdemateriaalien valinnalle asetettuja kriteerejä ovat seuraavat:

- tutkimusaineisto on kirjoitettu joko suomeksi tai englanniksi
- tutkimusaineisto vastaa tutkimuskysymyksiin ja/tai sisältää muuten tutkimuksen kannalta relevanttia informaatiota
- tutkimusaineisto on vapaasti luettavissa tai saatavilla Jyväskylän yliopiston verkon kautta
- tutkimusaineisto on julkaistu vuosina 2012-2020 (muutamia poikkeuksia lukuun ottamatta)
- tutkimusaineistoon on viitattu useita kymmeniä kertoja Google Scholar -palvelussa
- tutkimusaineisto on Julkaisufoorumi-luokitukseltaan 1-3.

Lähdemateriaalien haut toteutettiin käyttämällä erilaisia aiheeseen liittyviä englanninkielisiä hakusanoja sekä niiden yhdistelmiä. Hakutermeinä käytettiin: *digital identity, identity and access management, identity and access management risks, identity and access management risk, IAM, access control, access control models, role-based access control, attribute based access control, centralized access control* ja *decentralized access control.*

Tutkielman lähdeaineistoksi valikoitui tutkimusartikkeleita identiteetin- ja pääsynhallinnasta, digitaalisesta identiteetistä ja erilaisista digitaalisen identiteetin- ja pääsynhallinnan malleista. Myös muutamia hajautettuja järjestelmiä, kuten pilvipalveluiden pääsynhallintaa koskevia tutkimuksia valikoitui mukaan. Lähdemateriaalin valinnassa pyrittiin valitsemaan korkeintaan kahdeksan vuotta vanhoja julkaisuja, mutta myös muutamia vanhempia hyväksyttiin mukaan niiden relevanttiuden vuoksi.

Tutkielman empiirinen tutkimusosuus toteutettiin tapaustutkimuksena. Tapaustutkimuksen kohdeorganisaationa oli asiantuntijaorganisaatio, joka toimii Suomessa useilla paikkakunnilla, ja sen palveluksessa työskentelee yli 1000 henkilöä. Tapaustutkimus toteutettiin teemahaastatteluiden avulla, joissa haastateltiin kymmentä henkilöä, jotka ovat tutkimusaiheen asiantuntijoita. Tutkimuksen empiirisessä osuudessa pyritään selvittämään teemahaastatteluiden avulla, millaisia riskejä organisaatioiden identiteetin- ja pääsynhallintaan liittyy. Kirjallisuuskatsauksessa muodostettiin teemahaastattelulle rakenne kirjallisuudessa esiintyneiden identiteetin- ja pääsynhallinnan riskien perusteella. Tutkielmassa on tarkoitus vastata ensimmäiseen tutkimuskysymykseen kirjallisuuskatsauksen perusteella ja toiseen sekä kirjallisuuskatsauksen että empiirisen tutkimuksen avulla.

Tutkielman toinen luku käsittelee identiteetin- ja pääsynhallintaan yleisellä tasolla organisaatioissa. Kolmannessa luvussa perehdytään identiteetin- ja pääsynhallinnan malleihin, koska ne ovat hyvin merkittävä osa identiteetin- ja pääsynhallintaa, ja sen vuoksi tärkeä osa myös tätä tutkielmaa. Luvut kaksi ja kolme muodostavat tutkielman kirjallisuuskatsausosan. Luvussa neljä esitellään empiirisen tutkimuksen toteutus kokonaisuudessaan suunnittelusta toteutusvaiheeseen. Luvussa viisi esitellään empiirisen tutkimuksen tulokset. Luvussa kuusi ovat tutkimuksen johtopäätökset, arvioidaan tutkimuksen luotettavuutta ja esitellään relevantteja jatkotutkimusaiheita. Viimeisenä lukuna on koko tutkielman yhteenveto.

2 IDENTITEETIN- JA PÄÄSYNHALLINTA

Tietojärjestelmien turvallisuus on suurin haaste, jonka globaalit organisaatiot kohtaavat tänä päivänä (Bradford ym., 2014). Monet nykypäivän organisaatiot toimivat lukuisien tietojärjestelmien varassa, ja ovat voimakkaasti riippuvaisia niiden toimivuudesta (Bulgurcu ym., 2010; Gauthier & Merlo, 2012). Identiteetin- ja pääsynhallinnan merkitystä tärkeimpien liiketoimintaprosessien käsittelyssä ei voida sivuuttaa, koska sen avulla voidaan vähentää merkittäviä riskejä liiketoiminnalle, kuten minimoida sensitiivisen datan pääseminen organisaation ulkopuolelle (Popescu, Barbu, & Popescu, 2015).

Yhä useampi organisaatiosovellus ja -tietojärjestelmä käsittelee yksityisyyteen tai turvallisuuteen liittyviä arkaluontoisia tietoja (Gauthier & Merlo, 2012). Valitettavasti verkkopohjaiset sovellukset ja tietojärjestelmät joutuvat usein myös verkkourkinnan eli tietojenkalastelun ja erilaisten muiden tietoturvahyökkäysten kohteiksi (Bradford ym., 2014; Sun, Xu, & Su, 2011). Tietoturva on kuitenkin myös kilpailutekijä tällä digitalisaation aikakaudella (Popescu, Barbu, & Popescu, 2015).

Identiteetin- ja pääsynhallinnan haavoittuvuudet ovat kaikkein vaarallisimpia haavoittuvuuksia verkkosovelluksissa ja tietojärjestelmissä, koska sen pettäessä ovat tuhot merkittäviä niin kooltaan kuin skaalaltaankin (Sun ym., 2011). Monet organisaatiot luottavat tietoturva-asioissaan teknologiapohjaisiin ratkaisuihin, kuten erilaisiin identiteetin- ja pääsynhallinnan ratkaisuihin (Bulgurcu ym., 2010).

Tässä luvussa tutustutaan identiteetin- ja pääsynhallinnan kahteen kokonaisuuteen, identiteetinhallintaan ja pääsynhallintaan, sekä esitellään niihin liittyviä keskeisimpiä käsitteitä. Tämän lisäksi luvussa kerrotaan identiteetin- ja pääsynhallinnasta organisaatiokontekstissa, identiteetin- ja pääsynhallinnan automaatiosta sekä yleisesti riskeistä.

2.1 Identiteetinhallinta

Identiteetin- ja pääsynhallinta *(IAM, Identity and Access Management)* voidaan jakaa kahteen erilliseen kokonaisuuteen, identiteetinhallintaan (IdM) ja pääsynhallintaan (AM) (Taulukko 1). Identiteetinhallinta tarkoittaa prosessia, jonka perusteella tietojärjestelmissä esitetään kohteita erilaisina digitaalisina identiteetteinä (Anilkumar & Sumathy, 2018; Dunphy & Petitcolas, 2018; Linden, 2012). Pääsynhallinta taas tarkoittaa toimintoja, joilla käyttäjä tunnistetaan tietojärjestelmässä (Linden, 2012). Pääsynhallintaa esitellään paremmin luvussa 2.2. Identiteetinhallintaan siis kuuluu käyttäjien hallinta ja käyttäjäarkistot, ja pääsynhallinta kattaa käyttäjän identiteettiin liittyvät tunnistautumis- ja varmentamistoimet. Nykyisin nämä kaksi termiä ovat hyvin tiiviisti liitetty yhteen, ja muodostavat identiteetin- ja pääsynhallinnan.

Taulukko 1 Identiteetinhallinnan ja pääsynhallinnan toimintojen luokittelu

Identiteetinhallinta	**Pääsynhallinta**
Digitaalinen identiteetti	Tunnistus
Käyttäjän ja roolin hallinta	Todennus
Salasanojen hallinta	Valtuutus
Automaatio	Kertakirjautuminen
Hakemistot	Pääsynhallinnan mallit
Tiedon synkronointi	Monivaiheinen tunnistautuminen

Identiteetti koostuu persoonallisuuden määrittelevistä ominaisuuksista (Camp, 2004). Chadwickin (2009) mukaan identiteetti (*eng. identity*) tarkoittaa kokonaisuutta, jossa on yksi tai useampi tietoelementti, joiden avulla yksilö voidaan tunnistaa yhteisössä siinä määrin kuin on välttämätöntä. Tietoelementeillä tarkoitetaan tässä yhteydessä yksilöiviä tai henkilökohtaisesti tunnistettavia tietoja, jotka kuvaavat henkilöä ja mahdollistavat kyseisen henkilön tunnistamisen niiden perusteella. Tällaisia tietoja ovat myös sellaiset, jotka eivät yksinään kuvaa tunnistettavasti henkilöä, mutta yhdessä muiden tietojen kanssa muodostavat tällaisen kokonaisuuden. (Chadwick, 2009.)

Identiteetti on siis mikä tahansa yksittäisen henkilön ominaisuusarvojen joukko, joiden avulla tämä voidaan tunnistaa riittävästi missä tahansa (Kumar & Bhardwaj, 2018; Pfitzmann & Hansen, 2010). Tietojärjestelmätieteessä identiteetti on eri käsite, kuin identiteettikäsite psykologiassa, ja siitä käytetäänkin usein sekaannusten välttämiseksi käsitettä digitaalinen identiteetti (Kumar & Bhardwaj, 2018).

Digitaalinen identiteetti (*eng. digital identity*) tarkoittaa Kumarin ja Bhardwajin (2018) mukaan yksilön identiteettiä erilaisissa sähköisissä järjestelmissä. Digitaalinen identiteetti muodostuu henkilön ominaisuuksista järjestelmässä, joita voivat olla esimerkiksi henkilön vastuualue, toimipaikka tai tehtävä (Kumar & Bhardwaj, 2018; Popescu ym., 2015).

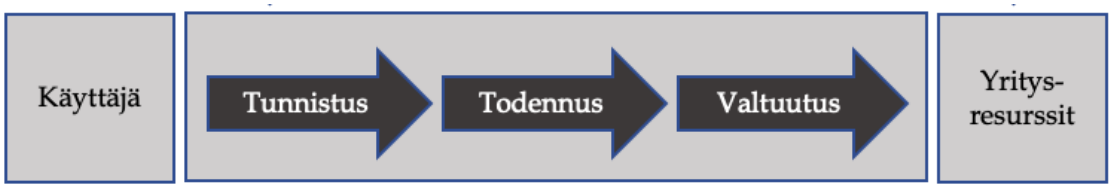
Digitaalinen identiteetti on toimiva kokonaisuus, johon liittyy pysyviä tai pitkäaikaisia stabiileja ominaisuuksia järjestelmissä (Camp, 2004). Cameronin

(2005) mukaan digitaalinen identiteetti on henkilö tai asia, joka on edustettuna tai olemassa digitaalisessa ympäristössä ja jota kuvataan tai käsitellään siinä (Cameron, 2005). Kunzin, Puchtan, Grollin, Fuchsin ja Pernulin (2019) mukaan digitaalinen identiteetti on ihminen edustettuna jossakin järjestelmässä. Identiteetinhallinnan tavoitteena on luoda jokaiselle käyttäjälle vain yksi digitaalinen identiteetti, jota ylläpidetään, modifioidaan sekä seurataan koko käyttöoikeuden elinkaaren ajan (Kumar & Bhardwaj, 2018). Joissakin yrityksissä käytetään moni-identiteettimalleja, jolloin henkilö voi edustaa useampia digitaalisia identiteettejä (Kunz ym., 2019).

Useimmiten identiteetinhallintaratkaisujen toiminnot koskevat käyttäjien henkilöllisyyden, heidän käyttäjäprofiiliensa ja niihin liittyvän arkaluontoisen tiedon tallennusta, käsittelyä, paljastamista ja hävittämistä (Baldwin ym., 2010). Identiteetinhallinta voidaan nähdä prosessien ja työkalujen joukoksi, joiden avulla pystytään selvittämään käyttäjän identiteetti, kuten työntekijä tai asiakkaan erilaisissa järjestelmissä (Kumar & Bhardwaj, 2018). Baldwinin ym. (2010) mukaan identiteetin- ja pääsynhallinnan ydintoimintoja ovat identiteettitietojen tallennus, niiden indeksointi ja hakutoiminnot. Identiteetinhallinnan mahdollistamia toimintoja ovat erilaiset itsepalvelutoiminnot, kuten käyttäjien omatoiminen rekisteröityminen järjestelmään, käyttäjätilin hallinta sekä omatoiminen salasanan resetointi. (Baldwin ym., 2010.)

2.2 Pääsynhallinta

Identiteetin- ja pääsynhallinnan toinen osa pääsynhallinta (AM) tarkoittaa erilaisia toimintoja, joiden avulla käyttäjä tunnistetaan järjestelmään (Kumar & Bhardwaj, 2018; Linden, 2012). Kolme päätoimintoa (Kuvio 1) ovat tunnistaminen, todennus sekä valtuuttaminen, jotka ovat peräkkäisiä toimintoja (Anilkumar & Sumathy, 2018; Bradford ym., 2014; Gunter, Liebovitz & Malin, 2011; Khan, 2012; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016). Tunnistamisella (*eng. identification*) tarkoitetaan yksilön kuvaamista järjestelmään (Bradford ym., 2014; Dos Santos ym., 2014).



Kuvio 1 Pääsynhallinnan rakenne

Todennus (*eng. authentication*) on toiminto, jonka avulla järjestelmä määrittää pääsyn tason käyttäjälle erilaisissa suojatuissa resursseissa (Kumar & Bhardwaj, 2018). Todennusvaiheessa varmistetaan, että pyydetty toiminto on oikeutettu

sekä se, että resursseihin pääsevät vain tunnistetut ja todennetut käyttäjät (Bradford ym., 2014; Petrovksa ym., 2019).

Valtuuttaminen (*eng. authorization*) kertoo, millaiset oikeudet tietyllä käyttäjällä on järjestelmän hallinnoimiin kohteisiin (Bradford ym., 2014; Petrovksa ym., 2019). Sitä käytetään määrittelemään pääsykäytäntö, sekä oikeudet eri resursseihin, jotka liittyvät tietoon ja tietoturvaan (Kumar & Bhardwaj, 2018). Valtuuttaminen myös varmistaa, että resurssit ovat vain valtuutettujen käyttäjien käytettävissä (Petrovksa ym., 2019).

Pääsynhallinta mahdollistaa monia erilaisia toimintoja, kuten kertakirjautumisen ja vahvan tunnistautumisen, jotka helpottavat käyttäjän toimintaa, lisäävät järjestelmän turvallisuutta sekä mahdollistavat automatisoituja toimintoja (Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016).

Kertakirjautuminen eli SSO (*eng. single-sign on*) tarkoittaa, että käyttäjä kirjautuu sisään vain kerran, jonka jälkeen kaikki yrityksen sisäiset verkkopalvelut ovat hänen käytettävissään, mikäli käyttäjällä on niihin vaadittavat käyttöoikeudet (Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016). Kertakirjautuminen mahdollistaa sujuvan käyttäjäkokemuksen ja työnkulun, sekä nostaa käyttäjän kokemaa tyytyväisyyttä järjestelmää kohtaan (Kumar & Bhardwaj, 2018). Kertakirjautuminen on yksi identiteetin- ja pääsynhallinnan järjestelmien keskeisimmistä toiminnallisuuksista (Anilkumar & Sumathy, 2018).

Monivaiheinen tunnistautuminen eli MFA (*eng. Multi-Factor authentication*) on tunnistautumismenetelmä, jossa käyttäjälle annetaan pääsy järjestelmään tai laitteeseen kahden tai useamman todennusfaktorin antamisen jälkeen (Bradford ym., 2014; Kim & Hong, 2011). Monivaiheisen tunnistautumisen faktoreita on kolmen tyyppisiä: jotain, mitä käyttäjä tietää (*something you know*), jotain käyttäjän hallussa olevaa *(something you have)* ja jotain, mitä käyttäjä on *(something you are) (*Bradford ym., 2014; Khan, Akbar, Shahzad, Farooq & Khan, 2015*).* Monivaiheisesta tunnistautumisesta käytetään myös yleensä termiä vahva tunnistautuminen, jota Suomessa esimerkiksi pankit käyttävät.

Jotain mitä käyttäjä tietää tarkoitetaan jotakin, jonka vain käyttäjä yksin tietää, kuten salasana tai PIN-koodi. *Jotain käyttäjän hallussa olevaa* tarkoittaa, että tunnistautumiseen vaaditaan jotakin, joka käyttäjällä on hallussaan, kuten puhelin, muun laitteen avainlukusovellus tai erillinen avainlukulaite. *Jotain mitä käyttäjä on* tarkoittaa jotakin ominaisuutta, jota käyttäjä itse on, kuten erilaiset biometriset ominaisuudet, kuten sormenjälki tai kasvontunnistus. (Khan ym., 2015.)

Tehtävien hajauttaminen eli SoD (*eng. Segregation of dutie*s *tai separation of dutie*s) tarkoittaa, että jonkin tehtävän toteuttamiseen vaaditaan enemmän kuin yksi henkilö (Baracaldo & Joshi, 2013; Bradford ym., 2014). Tehtävien hajauttaminen laskee käyttäjien tahallisten väärinkäytösten riskiä huomattavasti, koska sen seurauksena esimerkiksi kaikkein kriittisimpien toimintojen toteuttamiseen vaaditaan enemmän kuin yksi tunnistettu käyttäjä (Baldwin, Casassa Mont, Beres & Shiu, 2010).

Itsenäinen salasanan resetointi eli SSPR (*eng. Self service password reset*) tarkoittaa prosessia, jonka avulla käyttäjät voivat nollata oman salasanansa, mikäli salasana unohtuu tai lukkiutuu (Kumar & Bhardwaj, 2018). Tämä nostaa yrityksen toiminnan tehokkuutta, koska käyttäjät pystyvät itse resetoimaan unohtuneen salasanan, eikä tähän tarvita teknisen asiakaspalvelun apua, jolloin tilanne ratkeaa todennäköisesti nopeammin ja pienemmillä resursseilla (Bradford ym., 2014).

Identiteetin- ja pääsynhallintaan liittyy myös identiteetin varmentaminen (*eng. identity assurance*), jolla tarkoitetaan, että pystytään tunnistamaan varmasti, että identiteettiä käyttää joka hetki juuri oikea ja siihen valtuutettu henkilö (Baldwin ym., 2010; Dos Santos ym., 2014; Petrovksa ym., 2019). Organisaation tulee myös kyetä todistamaan ja demonstroimaan ulkoisille ja sisäisille auditoijille heidän identiteetin varmentamisprosessinsa (Baldwin ym., 2010; Kumar & Bhardwaj, 2018).

2.3 Identiteetin- ja pääsynhallinta organisaatioissa

Tehokas identiteetin- ja pääsynhallinta, joka liittyen työntekijöiden pääsyyn sensitiivisiin sovelluksiin ja dataan on nykypäivän yritysten suurimpia turvallisuushaasteita (Hummer ym., 2016). Organisaatioiden identiteetin- ja pääsynhallinnassa on otettava huomioon tietoturva ja yksityisyys, sekä pyrkiä parhaaseen mahdolliseen käyttäjäkokemukseen (Kumar & Bhardwaj, 2018).

Identiteetin- ja pääsynhallinta on keskeinen tekijä organisaation informaatioteknologian infrastruktuurissa (Bradford ym., 2014), ja se koostuu monista eri osa-alueista ja teemoista (Kuvio 2). Kumarin ja Bhardwajin (2018) mukaan identiteetin - ja pääsynhallinnalla tarkoitetaan yksilöllisten identiteettien hallintaa, niiden todennusta ja valtuutusta. Identiteetin- ja pääsynhallinta kattaa erilaisia yrityksen sisäisiä sekä ulkoisia rooleja ja oikeuksia. Organisaatioissa identiteetin- ja pääsynhallintaa käytetään verkon ja järjestelmien yksittäisten käyttäjien roolien ja käyttöoikeuksien määrittelemiseen, luomiseen ja hallintaan. (Kumar & Bhardwaj, 2018.)

Kuvio 2 Identiteetin- ja pääsynhallinnan osa-alueet

Identiteetin- ja pääsynhallinta on joukko liiketoimintaprosesseja sekä sitä tukeva infrastruktuuri, joka mahdollistaa digitaalisen identiteetin luomisen, ylläpidon ja käyttämisen (Anilkumar & Sumathy, 2018; Kumar & Bhardwaj, 2018; Kunz ym., 2019). Identiteetin- ja pääsynhallinnan prosesseja ovat muun muassa sellaiset, jotka sallivat, kieltävät tai rajoittavat käyttäjien pääsyä johonkin tiettyyn järjestelmään erilaisten käytäntöjen perusteella (Khan, 2012; Maesa, Mori & Ricci, 2017). Prosessi voi olla esimerkiksi käyttäjän luominen järjestelmään, ja käytäntö sääntö, jonka mukaan työntekijälle annetaan työsuhteen alussa tietty joukko oikeuksia (Anilkumar & Sumathy, 2018; Kumar & Bhardwaj, 2018; Kunz ym., 2019).

Identiteetin- ja pääsynhallinnan järjestelmien data ja toiminnot luottavat käytäntöihin niiden toiminnan ohjaamiseksi (Hummer ym., 2016; Kunz ym., 2019). Tapa, jolla nämä käytännöt määritetään ja hallitaan, muodostaa identiteetin- ja pääsynhallintamallin (Dos Santos ym., 2014). Hummerin ym. (2016) mukaan identiteetin- ja pääsynhallinnan käytännöt ovat usein huonosti määriteltyjä ja heikosti dokumentoituja, näin ollen ne vanhenevat nopeasti, niitä ei noudateta tai ne jätetään kokonaan huomioimatta. (Hummer ym., 2016.) Identiteetin ja pääsynhallinnan malleihin keskitytään luvussa kolme.

Identiteetin- ja pääsynhallinta käsittää myös prosessit, jotka liittyvät identiteettien ominaisuuksien elinkaaren hallintaan (Anilkumar & Sumathy, 2018; Dunphy & Petitcolas, 2018). Identiteetin elinkaarenhallinta kattaa kaikki toiminnot käyttäjän digitaalisen identiteetin järjestelmään luomisesta sen täydelliseen tuhoamiseen (Bradford ym., 2014; Kumar & Bhardwaj, 2018). Toiminnot tulee olla kontrolloitu prosessin jokaisessa vaiheessa sekä mahdolliset riskit tunnistettuina (Bradford ym., 2014; Gunter ym., 2011). Identiteetin- ja pääsynhallinnan tarkoituksena on suojata yritysresursseja, sekä hallita käyttäjiä, tiedostoja ja muita resursseja (Gunter ym., 2011; Khan, 2012; Maesa ym., 2017). Identiteetin- ja pääsynhallinnan prosessien toimivuus on tärkeää organisaation tuloksenkin kannalta. Mikäli työntekijällä ei ole tehtäviensä hoitamiseen tarvit-

tavaa oikeutta, johtaa se välittömiin tuottavuuden menetyksiin muiden epäsuorien tappioiden ohella. (Popescu ym., 2015).

Identiteetin- ja pääsynhallinta on olennaisen tärkeä tietojen yksityisyyden, luottamuksellisuuden ja eheyden varmistamisessa (Dos Santos ym., 2014; Gunter ym., 2011). Kumarin ja Bhardwajin (2018) mukaan identiteetin- ja pääsynhallinnan tärkein tehtävä on lisätä tietoturvaa ja tuottavuutta vähentämällä samalla kustannuksia, seisokkeja ja toistuvia tehtäviä erilaisten automaatioiden avulla. Automatisoitavissa olevia toistuvia identiteetin- ja pääsynhallinnan tehtäviä ovat esimerkiksi käyttäjän luominen järjestelmään, käyttäjän poistaminen järjestelmästä, käyttäjän käyttöoikeuden lukitseminen, käyttäjän käyttöoikeuden lukituksen poistaminen, käyttäjän käyttöoikeuden myöntäminen organisaatioresursseihin sekä käyttäjän käyttöoikeuden peruminen. (Kumar & Bhardwaj, 2018.)

Identiteetin- ja pääsynhallinta edellyttää organisaatioilta identiteettitietojen analysointia, raportointia ja niiden jatkuvaa seurantaa, mallintamista sekä tehokkaita päätöksentekoprosesseja (Popescu ym., 2015). Baldwinin ym. (2010) mukaan identiteettitiedot eivät koskaan ole staattisia, vaan käyvät läpi erilaisia käsittelyvaiheita, kuten tiedonhankinta, -käsittely ja -julkistaminen. Tiedon dynaaminen luonne vaatii organisaatioilta jonkin tyyppistä identiteetinhallintaratkaisua. (Baldwin ym., 2010.)

Erilaiset identiteetin- ja pääsynhallinnan järjestelmät ovat organisaatioissa tyypillisesti sääntöpohjaisia, mikä tarkoittaa, että resurssien käyttöyritykset sallitaan tai evätään sen perusteella, onko pääsy sallittu jonkin ennakkoon määritellyn säännön mukaan (Chen & Crampton, 2011). Identiteetin- ja pääsynhallinnan järjestelmän tehtävä on päättää, sallitaanko pääsy pyydettyyn resurssiin vai evätäänkö se (Chen & Crampton, 2011; Kunz ym., 2019; Maesa ym., 2017). Nykyiset identiteetin- ja pääsynhallinnan järjestelmät toimivat yleensä liittämällä tietoihin subjektin (esim. työntekijädata), objektin (käyttöoikeudet ja sovellukset) ja myöntäen tai eväten pääsyn niiden suhteen perusteella (Hummer ym., 2016 ; Kunz ym., 2019; Khan 2012). Identiteetin- ja pääsynhallinnan järjestelmät voivat tallentaa tietoja evätyistä pääsy-yrityksistä (Khan, 2012; Popescu ym., 2015).

Kumarin ja Bhardwajin (2018) mukaan identiteetin- ja pääsynhallintaan on erilaisia järjestelmiä, jotka tarjoavat organisaatioille välineitä ja tekniikoita, joilla hallita käyttäjien pääsyä kriittiseen tietoon yrityksen sisällä. Identiteetin- ja pääsynhallinnan hallintajärjestelmien tarkoituksen on lisätä yrityksen tietoturvaa sekä liiketoiminnan tuottavuutta vähentämällä samalla kustannuksia, häiriöaikoja sekä rutiinitehtäviä automaation avulla. (Kumar & Bhardwaj, 2018.) Erilaisia identiteetin- ja pääsynhallinnan malleja käsitellään luvussa kolme.

2.4 Automaatio identiteetin- ja pääsynhallinnassa

Laajasti automatisoitu ja mukautuva infrastruktuuri ovat yritykselle erinomainen kilpailuvaltti (Bradford ym., 2014; Hummer ym., 2016). Nykypäivän identiteetin- ja pääsynhallinnan ratkaisut mahdollistavat jo useimpien identiteetin- ja

pääsynhallinnan tehtävien onnistuneen automatisoinnin (Kunz ym., 2019). Huolimatta identiteetin- ja pääsynhallinnan käytäntöjen tärkeydestä, usein juurikaan mitään käytäntöjä automatisointiin ja prosessin tehostamiseen tai käytäntöjen hallintaan ei ole (Hummer ym., 2016). Yhtenäisten, huolella määriteltyjen käytäntöjen ja prosessien puute aiheuttaa käytäntöjen vanhentumisen, jonka seurauksena tehottomuus sekä tietoturva haavoittuvuuksien todennäköisyys kasvaa (Bradford ym., 2014; Hummer ym., 2016).

Manuaalinen identiteetin- ja pääsynhallinta altistaa yrityksen erilaisille riskeille (Bradford ym., 2014; Bulgurcu ym., 2010; Hummer ym., 2016; Kumar & Bhardwaj, 2018). Manuaalisen identiteetin- ja pääsynhallinnan ongelmia ovat esimerkiksi inhimilliset virheet, monimutkaisuus ja oikeuksien kokonaisvaltaisen näkemyksen puute (Bradford ym., 2014).

Manuaalinen identiteetin- ja pääsynhallinta voi olla lisäksi hajautettuna eri vastuuhenkilöille, joka monimutkaistaa oikeuksien hallintaa entisestään ja pahimmillaan jokaiselle erilliselle sovellukselle on omat pääsynhallinnan ratkaisut ja niistä vastaavat henkilöt. Manuaalisesta identiteetin- ja pääsynhallinnasta aiheutuu käyttäjille virheellisiä ja liiallisia oikeuksia. Käyttäjillä ei tulisi olla laajempia käyttöoikeuksia, kuin mitä heidän työtehtävänsä vaativat. (Bradford ym., 2014).

Manuaaliset prosessit kuluttavat henkilöstön aikaa, luovat inhimillisiä virheitä, laskevat yrityksen ja yksittäisten työntekijöiden tehokkuutta sekä häiritsee strategisempia tehtäviä (Bradford ym., 2014; Hummer ym., 2016). Kustannukset nousevat, mikäli järjestelmien käyttäjien elinkaaressa olevat rutiininomaiset tehtävät tehdään käsin (Bradford ym., 2014).

Suurin osa etenkin keskisuurista ja suurista organisaatioista käyttää standardoituja identiteetin- ja pääsynhallinnan käytäntöjä sekä infrastruktuuria automaation tason parantamiseksi (Kumar & Bhardwaj, 2018). Automaatio nostaa tehokkuutta ja auttaa vähentämään virheitä identiteetin- ja pääsynhallinnan toiminnoissa. Erilaiset rutiinitehtävät etenkin ovat helposti automatisoitavissa, kuten erilaiset käyttöoikeuksien elinkaareen liittyvät toiminnot (Bradford ym., 2014; Hummer ym., 2016). Automaation avulla identiteetin- ja pääsynhallinnasta saadaan huomattavasti tehokkaampaa ja virheettömämpää (Bradford ym., 2014; Kumar & Bhardwaj, 2018).

Bradfordin ym. (2014) mukaan keskitetty identiteetin- ja pääsynhallinta mahdollistaa automaation jokaiselle identiteetin- ja pääsynhallinnan osa-alueelle. Automaation tekemät tehtävät ja päätökset perustuvat ennakkoon määriteltyihin sääntöihin. Automaatio parantaa tietoturvallisuutta ja vähentää kustannuksia. Automaatio laskee kustannuksia, koska sen avulla ihmisen ei enää tarvitse toteuttaa identiteetin- ja pääsynhallinnan rutiinitoimenpiteitä, minkä lisäksi automaatio toteuttaa ne nopeammin. (Bradford ym., 2014.)

Automatisoitu identiteetin- ja pääsynhallinta mahdollistaa kaikki identiteetin elinkaaren tehtävät (Hummer ym., 2016). Automatisointi antaa käyttäjille käyttöoikeudet, avustaa salasanan palauttamiseessa (*SSPR*), mahdollistaa monivaiheisen tunnistautumisen (*MFA*) sekä kertakirjautumisen (*SSO*) (Bradford ym., 2014; Kumar & Bhardwaj, 2018). Kaikki automaation avulla toteutettavat

toiminnot vaativat taustalleen toimivat ja huolella määritellyt säännöt ja prosessit (Hummer ym., 2016). Identiteetin- ja pääsynhallinnan tulisi olla automatisoitu, nopeuttaa toimintojen toteuttamista sekä yksinkertaistaa käyttöoikeuksien antamista (Bradford ym., 2014).

Automaatio ei kuitenkaan mahdollista ainoastaan etuja organisaatioille, vaan se tuo mukanaan myös riskien mahdollisuuksia. Identiteetin- ja pääsynhallinnan järjestelmä on kytketty verkkoon, joka taas tuo lukuisia uusia riskejä (Godha, Prateek & Kataria, 2014). Järjestelmään voidaan murtautua, jolloin rikollinen pääsee käsiksi organisaation resursseihin (Godha ym., 2014). Tästä syystä tietojen luottamuksellisuuden ja palvelun turvallisuuden varmistamiseksi organisaatioiden tulee suorittaa tehokasta pääsynhallintaa, jotta voidaan varmistaa kaikkien järjestelmään pyrkivien olevan valtuutettuja käyttäjiä (Deng, Deng, Li & Yang, 2010; Godha ym., 2014).

Luottamuskysymykset ovat erittäin tärkeitä harkitessa automaatiota identiteetin- ja pääsynhallinnassa. Voidaanko automaation virheettömään ja oikeelliseen toimintaan luottaa? Automaatioon liittyvät luottamushuolet ovat ymmärrettäviä ottaen huomioon niiden rajallisen ymmärryksen (Hoffman, Johnson, Bradshaw & Underbrink, 2013). Organisaatioissa ei myöskään aina ymmärretä automaation tuomien mahdollisuuksien määrää (Hoffman ym., 2013). Ihmisten luottamus teknologiajärjestelmiin edustaa jossain määrin heidän luottamustaan tällaisten järjestelmien kehittäjiin (Hoff, & Bashir, 2015; Hoffman ym., 2013).

Automaatio voidaan siis nähdä yhtenä onnistuneen identiteetin- ja pääsynhallinnan tuomana mahdollisuutena. Sen avulla saavutetaan merkittäviä etuja liiketoiminnalle sekä kyetään minimoimaan useita riskejä, joilla saattaisi olla tuhoisia seurauksia. Automaatioon liittyy kuitenkin myös monia luottamuskysymyksiä, kuten voidaanko teknologiaan täysin luottaa ja voiko se tunnistaa luvattoman käyttöoikeuspyynnön järjestelmässä.

2.5 Riskit

Identiteetin- ja pääsynhallinta on erittäin tärkeä osa yrityksen toimintaa, koska sen avulla voidaan välttää monia tietoturvariskejä, kasvattaa tehokkuutta sekä vastata nykypäivän turvallisuusvaatimuksiin (Bradford ym., 2014; Gauthier & Merlo, 2012; Kumar & Bhardwaj, 2018). Toimiva identiteetin- ja pääsynhallinta on elintärkeä erityisesti organisaatioissa, joissa työskennellään useiden erilaisten teknologioiden, tietojärjestelmien ja sovellusten kanssa, koska identiteetin- ja pääsynhallinta ohjaa käyttäjien toimintaa todentamalla ja valtuuttamalla pääsyn niihin verkon välityksellä (Anilkumar & Sumathy, 2018; Kumar & Bhardwaj, 2018; Maesa ym., 2017). Identiteetin- ja pääsynhallintaan liittyy monia mahdollisuuksia, mutta myös erilaisia riskejä. Jatkuvasti kehittyvällä, teknologian hallitsemalla aikakaudella organisaatioiden on tärkeää tunnistaa erilaisia keinoja hallita liiketoiminnan ja kasvun riskejä (Kumar & Bhardwaj, 2018). Identiteetin- ja pääsynhallinnan avulla pystytään estämään muun muassa auk-

torisoimattoman henkilön pääsy organisaation tietojärjestelmiin ja sitä kautta sensitiivisiin yritystietoihin (Bradford ym., 2014).

Vaikka identiteetin- ja pääsynhallinnan avulla yritys pystyy saavuttamaan monia etuja, kuten kasvaneen tietoturvan, on siinä kuitenkin myös erilaisia riskejä. Nykypäivän yritykset ovat voimakkaasti riippuvaisia maineestaan sekä asiakkaidensa luottamuksesta, koska niiden menettäminen voi johtaa pahimmillaan koko liiketoiminnan tuhoon (Bradford ym., 2014). Identiteetin- ja pääsynhallinnan tärkeyden, sekä niihin liittyvien riskien merkityksellisyyden takia, on tärkeää perehtyä organisaation mahdollisiin uhkiin identiteetin- ja pääsynhallinnassa. Erilaisten sisäisten ja ulkoisten säädösten sekä tietoturvavaatimusten vuoksi, organisaation sisäinen identiteetin- ja pääsynhallinta on saanut merkittävän roolin niin tutkimuksessa kuin käytännössäkin viime vuosina (Hummer ym., 2016). Identiteetin- ja pääsynhallintaan liittyy erilaisia käyttäjä- sekä organisaatiotason haasteita, jotka vaikuttavat hyvin monenlaisiin toimintoihin jokaisessa organisaatiossa (Kumar & Bhardwaj, 2018).

Identiteetin- ja pääsynhallintaan liittyviä riskejä ovat erilaiset organisaation sisäiset riskit, kuten sisäpiirihyökkäykset, liialliset ja vanhentuneet käyttöoikeudet, käyttäjien toimien jäljettömyys sekä monimutkaisuus (Baracaldo & Joshi, 2013; Bradford ym., 2014; Chen & Crampton, 2011; Hummer ym., 2016). Riskien kartoittaminen on tärkeää onnistuneen identiteetin- ja pääsynhallinnan varmistamiseksi ja kokonaisvaltainen näkemys riskeihin johtaa erinomaisiin ja pitkäkestoisiin tuloksiin (Baldwin ym., 2010; Popescu ym., 2015).

Suurimpina riskeinä identiteetin- ja pääsynhallinnan osa-alueella on käyttäjien liialliset oikeudet. Liiallisilla oikeuksilla varustetut käyttäjät voivat aiheuttaa vahingossa tai tahallisella toiminnallaan yritykselle menetyksiä (Kumar & Bhardwaj, 2018). Nämä menetykset voivat olla muun muassa taloudellisia tai maineeseen liittyviä (Bulgurcu ym., 2010; Gauthier & Merlo, 2012; Kumar & Bhardwaj, 2018).

Tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus ja minimoida liiketoiminnan vahingot rajoittamalla tietoturvatapausten vaikutusta sen toimintaan (Von Solms & Van Niekerk, 2013). Ihminen on usein tietoturvan kannalta epävarmin tekijä (Bulgurcu ym., 2010). Kun väärillä oikeuksilla varustettu käyttäjä pääsee yrityksen tietojärjestelmiin, voivat seuraukset olla todella tuhoisia (Feng ym., 2008). Verkkopohjaisten sovellusten ja järjestelmien jatkuvasti kasvava suosio on luonut uuden mahdollisuuden tietoturvahyökkäyksille ja kyberrikollisille (Sun ym., 2011). Järjestelmän turvallisuus on merkittävä haaste nykypäivän organisaatioille, jotka toimivat erilaisten tietojärjestelmien varassa (Bradford ym., 2014).

Automaatio tuo identiteetin- ja pääsynhallintaan omat riskinsä. Vaikka automaatio tuo monia etuja organisaatioille identiteetin- ja pääsynhallintaan, tuo se mukanaan kuitenkin myös riskejä. Identiteetin- ja pääsynhallinnan järjestelmä on kytketty verkkoon, joka aiheuttaa riskejä (Godha ym., 2014). Verkkoon kytkettyyn järjestelmään voidaan murtautua helpommin, kuin kytkemättömään, jolloin rikollinen voi päästä käsiksi organisaation resursseihin (Godha ym., 2014). Toinen automaatioon liittyvä riskikokonaisuus ovat luottamukseen liit-

tyvät asiat (Godha ym., 2014; Hoff, & Bashir, 2015; Hoffman ym., 2013). Käyttäjät voivat olla epävarmoja teknologian luotettavuudesta, ja tutkijoiden mukaan huolet ovat ymmärrettäviä, koska organisaatioissa saattaa olla melko rajallinen ymmärrys teknologiasta sekä sen tuomista mahdollisuuksista organisaatioille (Hoffman ym., 2013).

Sovellusten ja palveluiden kehittäjät kohtaavat kaksi merkittävää infrastruktuuriongelmaa, jotka ovat turvallisen ja luotettavan identiteetin- ja pääsynhallinnan toimintojen tarjoaminen sekä integrointi käyttäjille sopivalla tavalla muihin riippumattomien osapuolten kehittämiin palveluihin (Tuecke ym., 2016). Nämä ovat tärkeää huomioida sovelluskehityksessä, koska myöhemmissä vaiheissa sovellusten integroiminen samaan identiteetin- ja pääsynhallinnan järjestelmään voi olla haastavaa (Tuecke ym., 2016). Tällöin uhkana on hajautettu identiteetin- ja pääsynhallinnan malli, joka monimutkaistaa ja hankaloittaa käytäntöjä huomattavasti (Bradford ym., 2014; Hummer ym., 2016; Tuecke ym., 2016). Hajautuneessa identiteetin- ja pääsynhallinnassa on mahdotonta tai vähintään hyvin hankalaa todistaa, hallita ja seurata kenellä käyttäjistä pääsy mihinkin informaatioon, sekä ovatko nämä käyttöoikeudet linjassa organisaation sisäisten ja ulkoisten määräysten sekä sääntöjen kanssa (Bradford ym., 2014). Lisää hajautetusta identiteetin- ja pääsynhallinnan mallista luvussa 3.

3 IDENTITEETIN- JA PÄÄSYNHALLINNAN MALLIT

Identiteetin- ja pääsynhallinnan päätökset ovat erittäin tärkeitä kaikissa organisaatiojärjestelmissä (Hummer ym., 2016). Laajalle hajautetuissa järjestelmissä, kuten pilvijärjestelmissä, identiteetin- ja pääsynhallintaan liittyvien päätösten tulee olla joustavampia ja skaalautuvampia kuin perinteisissä on-premise -ratkaisuissa (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Hummer ym., 2016; Kunz ym., 2015b; Kunz, Fuchs, Hummer & Pernul, 2015a). Tämän ja muiden erilaisten vaatimusten ja tarpeiden vuoksi on olemassa useita erilaisia identiteetin- ja pääsynhallinnan malleja (Bradford ym., 2014; Hummer ym., 2016).

Identiteetin- ja pääsynhallinnan mallin valinta tulee tehdä huolella ja ottaa huomioon organisaation tulevaisuuden suunnitelmat, koska esimerkiksi organisaation koko voi kasvaa huomattavasti vuosien varrella, jonka seurauksena aiemmin valittu identiteetin- ja pääsynhallinnan malli voi myöhemmin olla epäsopiva organisaation tarpeisiin (Hummer ym., 2016). Organisaation käytössä aluksi hyvin toiminut identiteetin- ja pääsynhallinnan malli, voi myöhemmin olla liian yksinkertainen ja aiheuttaa järjestelmän monimutkaisuutta ja muita ongelmia (Bradford ym., 2014; Hummer ym., 2016). Yksittäisessä identiteetin- ja pääsynhallinnan järjestelmässä voi olla jopa miljoonia yksittäisiä rooleja ja objekteja (Hummer ym., 2016). Malleja suositellaan arvioitavaksi hallinnollisten kustannusten, käytäntöjen kattavuuden, skaalautuvuuden sekä suorituskyvyn perusteella (Dos Santos ym., 2014).

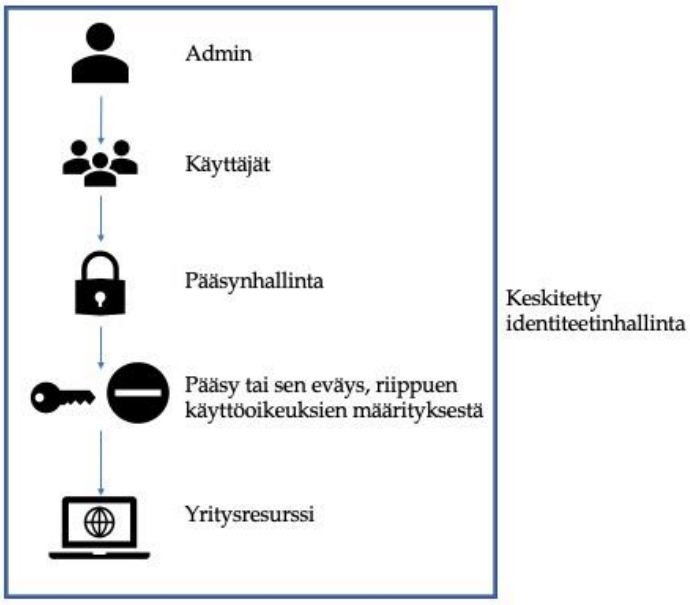
Tässä luvussa esitellään identiteetin- ja pääsynhallinnan malleja, ja niiden vahvuuksia ja heikkouksia. Luvussa esitellyt mallit ovat valikoituneet niiden yleisyyden takia, ja kaikki esiteltävät mallit ovat hyvin standardeja nykypäivän organisaatioissa.

3.1 Identiteetinhallinnan mallit

Identiteetin- ja pääsynhallinnan mallit voidaan jakaa identiteetinhallinnan malleihin sekä pääsynhallinnan malleihin. Identiteetinhallinnan mallit keskittyvät identiteetin- ja pääsynhallinnan infrastruktuuriin ja arkkitehtuuriin, ja voivat olla toteutettu joko keskitetysti tai hajautetusti. Tämä tarkoittaa organisaation identiteetin- ja pääsynhallinnan toimintojen olevan hallittu joko keskitetysti yhden järjestelmän kautta tai hajautetusti useamman eri järjestelmän toimesta (Bradford ym., 2014; Dos Santos ym., 2014; Hummer ym., 2016; Kumar & Bhardwaj, 2018; Kunz ym., 2019). Viime vuosina keskitetystä, koko organisaation laajuisesta identiteetin- ja pääsynhallinnan järjestelmästä on tullut keskeinen elementti käyttöoikeuksien hallinnoimiseen suurissa ja keskisuurissa yrityksissä (Hummer ym., 2016).

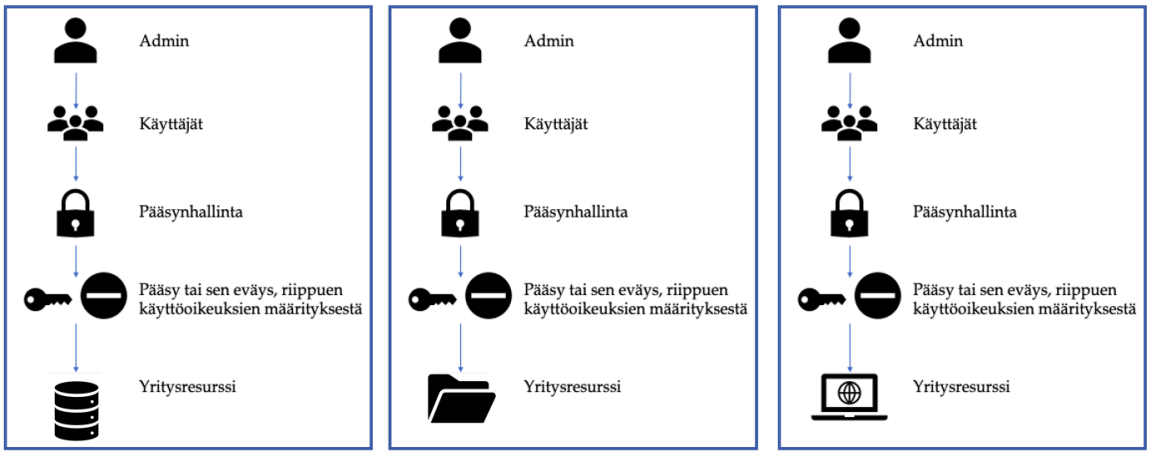
Identiteetinhallinnan malli siis kertoo, kuinka identiteetin- ja pääsynhallintaa hallinnoidaan kokonaisuutena, eli hallinnoidaanko kaikkia käyttäjien identiteettejä sekä käyttöoikeuksia yhdestä hallintajärjestelmästä vai hajautetusti useammasta. Useammasta järjestelmästä hallinnoitavaa identiteetinhallintaa kutsutaan hajautetuksi, koska siinä eri sovellusten ja järjestelmien käyttöoikeuksia ja käyttäjien identiteettejä niissä joudutaan hallitsemaan useammasta eri kanavasta. Kun käyttäjien identiteetit sekä käyttöoikeudet hallinnoidaan yhdestä järjestelmästä, puhutaan silloin keskitetystä identiteetinhallinasta.

Pääsynhallinnan malli kertoo, millaiset sääntöjä käyttäjien oikeuksien määräämiseen ja antamiseen on. Yleisimpiä pääsynhallinnan malleja ovat rooliperustaisessa pääsynhallintamalli sekä ominaisuusperustainen pääsynhallintamalli (Petrovksa ym., 2019). Pääsynhallinta on osa identiteetinhallintaa, riippumatta siitä onko identiteetinhallinta toteutettu hajautetusti vai keskitetysti (Kuvio 3). Pääsynhallinnan malleja käsitellään luvussa 3.2.



Kuvio 3 Identiteetin- ja pääsynhallinnan rakenne keskitetyssä identiteetinhallissa

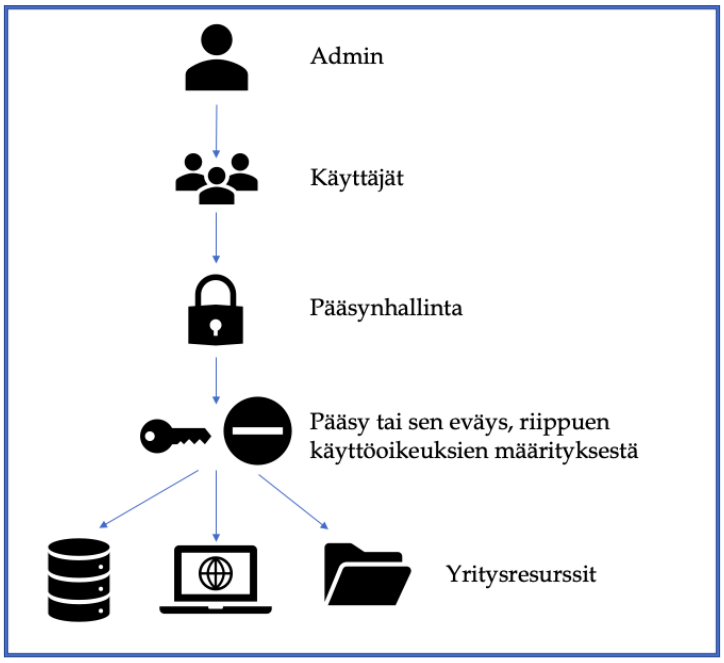
Identiteetinhallinnan mallit voidaan jakaa hajautettuun ja keskitettyyn malliin (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kunz ym., 2015b). Hajautettu pääsynhallintamalli (Kuvio 4) tarkoittaa (*eng. decentralized access management*), että organisaation käyttäjien identiteetin- ja pääsynhallinta hallitaan useammasta eri järjestelmästä, eli organisaatiolla ei ole yhtä keskitettyä identiteetin- ja pääsynhallintajärjestelmää (Baracaldo & Joshi, 2013). Tämä tarkoittaa, että jokaisen uuden tietojärjestelmän implementointi voi aiheuttaa kokonaan uuden identiteetin- ja pääsynhallinnan infrastruktuurin, jossa käyttäjien identiteetit sekä käyttöoikeudet hallitaan erillään muista jo olemassa olevista järjestelmistä (Bradford ym., 2014). Usean eri identiteetin- ja pääsynhallinnan järjestelmän käyttö aiheuttaa monimutkaisuutta, virheellisiä käyttöoikeuksia sekä hankaloittavat ylläpitoa (Baracaldo & Joshi, 2013; Bradford ym., 2014; Feng ym., 2008).



Kuvio 4 Hajautettu identiteetinhallinta

Keskitetyssä identiteetinhallintamallissa (*eng. centralized identity and access management, CIAM*) käyttäjien käyttöoikeuksia ja identiteettejä hallinnoidaan keskitetysti yhden järjestelmän kautta, jonka prosessit ovat selkeästi kuvattu ja johdettu (Bradford ym., 2014; Dos Santos ym., 2014; Hummer ym., 2016; Kumar & Bhardwaj, 2018; Kunz ym., 2019). Keskitetyssä identiteetinhallinnassa käyttäjien identiteetit, oikeuksien pyytäminen ja antaminen tapahtuvat yhden keskitetyn järjestelmän kautta, kaikkiin organisaation resursseihin ja järjestelmiin.

Monien yritysten tavoitteena on siirtyä keskitettyyn pääsynhallintamalliin (Bradford ym., 2014; Dos Santos ym., 2014). Keskitetty pääsynhallintamalli (Kuvio 5) on laajasti automatisoitavissa ja on mukautuva identiteetin- ja pääsynhallinnan infrastruktuuri sisältäen kaikki kolme avainaktiviteettiä; tunnustuksen, todennukset ja valtuutuksen (Bradford ym., 2014; Kumar & Bhardwaj, 2018).



Kuvio 5 Keskitetty identiteetinhallinta

On tärkeää luoda identiteetin- ja pääsynhallinnan järjestelmä, joka mahdollistaa keskitetyn hallinnoinnin, itsenäiset toiminnot käyttäjille, toimivan pääsynhallinnan mallin ja integroidun identiteetin- ja pääsynhallinnan järjestelmän (Baldwin ym., 2010; Bradford ym., 2014; Hummer ym., 2016; Kumar & Bhardwaj, 2018). Organisaatiot pyrkivät keskitettyyn identiteetinhallinnan mallin, koska hajautetussa identiteetinhallinnassa kokonaisvaltainen hallinnointi on vaikeaa, monimutkaista ja lähestulkoon mahdotonta, jonka vuoksi se aiheuttaa järjestelmien monimutkaisuutta, virheitä sekä altistaa erilaisille tietovuodoille (Bradford ym., 2014). Hajautetussa mallissa käyttäjillä voi olla useita eri käyttäjätunnuksia ja salasanoja, jotka nostavat taas työnmäärää organisaatiossa, kuten teknisessä tuessa muun muassa unohtuneiden salasanojen takia, ja laskee käyttäjän kokemaa tyytyväisyyttä (Kumar & Bhardwaj, 2018).

Lisäksi hajautetuissa identiteetin- ja pääsynhallinnan järjestelmissä käyttäjillä on helposti virheellisiä, liiallisia tai vanhentuneita oikeuksia (Bradford ym., 2014; Feng ym., 2008). Kuten aiemmin sanottu, kun virheellisillä käyttöoikeuksilla oleva käyttäjä pääsee organisaation verkkoon ja -järjestelmiin, seuraukset voi olla tuhoisia (Feng ym., 2008). Virheelliset käyttöoikeudet ovat vaarallisia organisaatioille, koska verkon sekä järjestelmien tietoturvallisuus laskee merkittävästi ja samalla riskien todennäköisyys kasvaa (Feng ym., 2008; Tuecke ym., 2016). Hajautettu pääsynhallintamalli nostaa riskien mahdollisuuksia myös siksi, koska se on usein hankalasti hallittavissa (Bradford ym., 2014).

Keskitetyn identiteetinhallinnan avulla organisaatiot ja käyttäjät kokevat merkittäviä etuja, kuten kertakirjautumisen (SSO), kasvaneen tietoturvallisuuden, kasvaneen tietosuojan, yritystoiminnan tehokkuuden kasvun, tehokkaan salasanahallinnan sekä auditointiprosessien parantumisen (Anilkumar & Su-

mathy, 2018; Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016).

Bradfordin ym. (2014) mukaan keskitetyssä identiteetinhallintamallissa järjestelmän perustana on prosessi, joka suorittaa identiteetin- ja pääsynhallinnan kolme keskeistä tehtävää: tunnistuksen, todennuksen sekä varmentamisen. Keskitetty pääsynhallintamalli parantaa IT-johtamista ja vähentää pääsynhallintaan liittyviä riskejä, koska toimintaperiaatteita ja käytänteitä sovelletaan johdonmukaisesti kaikissa organisaation liiketoimintajärjestelmissä. (Bradford ym., 2014.)

Hajautetussa identiteetinhallinnassa on haastavaa auditoida oikeuksia tai laittaa organisaation ohjeita ja käytäntöjä toteutukseen, jonka seurauksena käyttäjillä on helposti liian laajat tai vanhentuneet käyttöoikeudet (Feng ym., 2008; Hummer ym., 2016). Keskitetty identiteetinhallintamalli mahdollistaa kontrolloidut identiteetin- ja pääsynhallinnan toiminnot jokaisessa prosessin vaiheessa, jolloin myös sen riskit ovat tunnistettu (Bradford ym., 2014). Keskitetyn identiteetinhallinnan avulla on mahdollista toteuttaa standardisoidut käyttöoikeuksien elinkaaren prosessit, vähentää tietoturvariskejä ja noudattaa voimassa olevia kansallisia ja kansainvälisiä määräyksiä (Hummer ym., 2016).

Koko organisaation kattava, keskitetty identiteetin- ja pääsynhallinta on kasvattanut suosiotaan organisaatioiden ja tutkijoiden keskuudessa, koska sen avulla erilaisten määräysten ja tietoturvavaatimusten noudattaminen on huomattavasti helpompaa (Hummer ym., 2016). Keskitetty identiteetinhallinta kasvattaa datan ja resurssien yksityisyyttä ja turvallisuutta ja samalla nopeuttaa eri toimintoja, esimerkiksi käyttäjien kirjaamista järjestelmiin, käyttöoikeuksien perustamista sekä salasanojen nollaamista (Bradford ym., 2014).

Keskitetty identiteetinhallinta täyttää monet yksityisyydensuojaa ja tietoturvaan liittyvät tavoitteet ja helpottaa niiden toteuttamista organisaatioissa (Bradford ym., 2014; Dos Santos ym., 2014; Hummer ym., 2016). Bradfordin ym. (2014) mukaan automatisoimalla identiteetin- ja pääsynhallinnan prosesseja saadaan auditointiprosessista paljon tehokkaampaa. Parannukset auditointiprosesseissa ja kasvanut sääntöjen noudattaminen ovat keskitetyn identiteetin- ja pääsynhallinnan etuja. Keskitetty identiteetinhallinta antaa myös standardikäytännöt käyttöoikeushallintaa sekä mahdollistaa paremman jäljitettävyyden käyttäjien toiminnalle. Tämä tarkoittaa, että on mahdollista selvittää, kuka käyttäjä on tehnyt mitä toimenpiteitä järjestelmässä ja milloin (Bradford ym., 2014).

Keskitetyistä identiteetinhallinnasta on tullut kuitenkin myös yksi yritysten suurimmista haasteista, jotta organisaatiot voivat tarjota turvallinen ja vaatimustenmukainen pääsyn IT-resursseihin (Kunz ym., 2019). Kun keskitetty identiteetinhallintamalli on implementoitu organisaation käyttöön, voidaan hallita lukuisien järjestelmien käyttöoikeuksia ja käyttäjien identiteettejä yhdestä keskitetystä hallintajärjestelmästä (Bradford ym., 2014). Keskitetyn identiteetinhallinnan mallin saavuttaminen ei ole kuitenkaan helppoa tai yksinkertaista, vaan toteuttaminen sekä käyttöönotto ovat erittäin kallista ja aikaa vievää (Bradford ym., 2014; Kunz ym., 2019).

Bradfordin ym. (2014) mukaan monet yritykset ovat epäonnistuneet käyttöönottoyrityksissään, koska implementointiprosessi on hyvin pitkä ja monimutkainen, etenkin suurissa yrityksissä, joissa on paljon käyttäjiä, sovelluksia ja erilaisia käyttöoikeuksia. Keskitetty identiteetinhallinta vaatii uusien käytänteiden ja toimintatapojen luomisen, jotta mahdollistetaan uusien hallintajärjestelmien käyttö ja ylläpito. Lisäksi implementoinnin keston vuoksi se toteutetaan todennäköisesti vaiheittain, jolloin sekä vanhan että uuden identiteetin- ja pääsynhallinnan järjestelmän tulee toimia yhtä aikaa. Keskitetyn identiteetinhallinnan käyttöönottoon vaikuttavat myös tietyt rajoitteet, kuten tekniset rajoitteet, organisaatiolliset rajoitteet, ja ympäristölliset rajoitteet, jotka haittaavat keskitetyn identiteetinhallinnan käyttöönottoa, mikäli niitä ei osata ottaa huomioon ja johtaa oikein. (Bradford ym., 2014.)

Lukuisien hajautettuun malliin liittyvien ongelmien, kuten monimutkaisuuden, ohjeiden ja käytäntöjen toimeenpanon hankaluuden sekä virheellisten käyttöoikeuksien takia monet yritykset ovat toteuttaneet tai haluavat toteuttaa keskitetyn identiteetin- ja pääsynhallinnan mallin digitaalisen identiteetin hallintaa varten, vaikka keskitetyssä identiteetinhallinnassa on myös omat riskinsä (Hummer ym., 2016).

Keskitetyn identiteetin- ja pääsynhallinnan saavuttaminen tarjoaa monia etuja ja poistaa hajautetun identiteetinhallinnan ongelmakohtia. Organisaatio saa kattavan edun, kun sen tietoturvaan liittyvät riskit pienenevät merkittävästi, sekä organisaation kokonaiskustannukset laskevat säästetyn työajan vuoksi (Bradford ym., 2014; Hummer ym., 2016; Kunz ym., 2019). Luvattoman pääsyn todennäköisyys pienenee, koska oikeuksien ylläpito ja auditointi helpottuu keskitetyn hallintajärjestelmän ansiosta, minkä lisäksi käytäntöjen ja määräysten käyttöönotto toteutuu helpommin ja nopeammin (Bradford ym., 2014). Näiden merkittävien etujen (Taulukko 2) vuoksi monet yritykset ovat päätyneet keskitettyyn identiteetinhallintaan, huolimatta sen implementoinnin mahdollisista haasteista (Bradford ym., 2014; Kunz ym., 2019). Keskitetty identiteetinhallinta on nykypäivänä yleisesti tavoiteltu tilanne organisaatioiden identiteetinhallinnassa (Bradford ym., 2014; Kunz ym., 2019).

Taulukko 2 Keskitetyn identiteetinhallinnan edut

Edut	Automatisoituvuus	Bradford ym., 2014; Hummer ym., 2016; Kumar & Bhardwaj, 2018
	Itsepalvelut toiminnot	Baldwin ym., 2010; Bradford ym., 2014; Hummer ym., 2016K Kumar & Bhardwaj, 2018
	Kertakirjautuminen (SSO)	Anilkumar & Sumathy, 2018; Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016
	Tietoturvallisuus	Anilkumar & Sumathy, 2018; Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016
	Tietosuoja	Bradford ym., 2014; Dos Santos ym., 2014; Hummer ym., 2016
	Tehokas salasanahallinta	Baldwin ym., 2010; Bradford ym., 2014; Kumar & Bhardwaj, 2018; Petrovksa ym., 2019; Tuecke ym., 2016
	Tehokkuus	Anilkumar & Sumathy, 2018; Bradford ym., 2014; Hummer ym., 2016; Kumar & Bhardwaj, 2018; Popescu ym., 2015
	Auditointiprosessin parantuminen ja tehostuminen	Bradford ym., 2014; Kumar & Bhardwaj, 2018; Kunz ym., 2019
	Parantunut IT-johtaminen	Bradford ym., 2014
	Järjestelmien ja käytäntöjen yhtenäisyys	Bradford ym., 2014; Hummer ym., 2016
	Määräysten noudattaminen	Hummer ym., 2016; Kunz ym., 2019
Ongelmat	Monimutkainen ja hidas käyttöönotto	Bradford ym., 2014; Kunz ym., 2019
	Toteutuksen korkeat kustannukset	Bradford ym., 2014; Kunz ym., 2019
	Runsaasti implementoinnin epäonnistumisen mahdollisuuksia	Bradford ym., 2014; Hummer ym., 2016; Kunz ym., 2019

3.2 Pääsynhallinnan mallit

Työntekijöillä tulee olla työtehtävien tekemiseen vaaditut oikeudet, jotta he voivat tehdä työtään. Tehokas ja tietoturvallinen pääsynhallinta on yksi nykypäivän organisaation suurimmista turvallisuushaasteista (Kunz ym., 2019). Erilaiset pääsynhallinnan mallit (*eng. access control models*) ovat olennainen osa organisaatioiden identiteetin ja pääsynhallintaa. Kuten aiemmin kerrottua, pääsynhallinnan malli kertoo, millä perustein käyttäjälle joko annetaan tai evätään oikeus yritysresursseihin, kuten tiettyyn sovellukseen (Feng, 2008; Kunz ym., 2015b). Käyttäjälle voidaan myöntää oikeus esimerkiksi tälle ennakkoon määritellyn roolin perusteella (rooliperustainen pääsynhallinnan malli) tai jonkin dynaamisesti muuttavan ominaisuuden tai niiden yhdistelmän perusteella, kuten vuorokauden ajan tai tittelin mukaan (ominaisuusperustainen pääsynhallinnan malli).

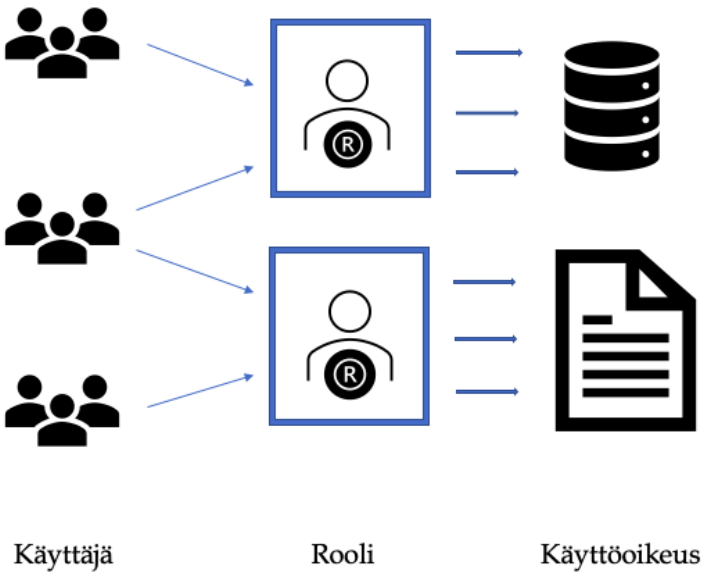
Pääsynhallintaan on olemassa monia eri malleja, ja valitessa organisaation pääsynhallinnan mallia tulee olla huolellinen ja miettiä organisaation strategiaa useamman vuoden päähän (Hummer ym., 2016), koska lyhytkatseisesti valittu pääsynhallinnan malli voi myöhemmin olla organisaation tarpeisiin liian monimutkainen tai muuten epäsopiva (Dos Santos ym., 2014; Hummer ym., 2016). Yleisimpiä pääsynhallinnan malleja ovat rooliperustainen pääsynhallinnan malli sekä ominaisuusperustainen pääsynhallinnan malli (Petrovksa ym., 2019), joita tässä luvussa käsitellään yksityiskohtaisemmin.

3.2.1 Rooliperustainen pääsynhallinnan malli

Rooliperustainen pääsynhallinnan malli (*eng. role-based access control, RBAC)* on yleisin käytettävä pääsynhallinnan malli (Dos Santos ym., 2014; Feng, 2008; Kunz ym., 2019; Kunz ym., 2015b). Perinteinen pääsynhallinnan lähestymistapa perustuu roolien käsitteeseen, ja sitä hallitaan tyypillisesti hierarkkisesti, ylhäältä alas -lähestymistavalla (Gunter ym., 2011). Rooliperustainen pääsynhallinnan malli on käyttöoikeuden hallintatekniikka, joka perustuu nimensä mukaisesti käyttäjän rooliin (Anilkumar & Sumathy, 2018; Gunter ym., 2011). Rooliperustaisesta mallista on tullut standardoitunut malli nykypäivän organisaatioiden pääsynhallintaan (Kunz ym., 2019).

Rooliperustaisessa pääsynhallintamallissa käytetään käyttöoikeuksien määrittelyssä apuna yksilön organisaatiollista roolia pääsyn myöntämiseksi tietojärjestelmiin ja muihin organisaation resursseihin (Baracaldo & Joshi, 2013; Bradford ym., 2014; Chen & Crampton, 2011; Khan, 2012; Kunz ym., 2019). Käyttöoikeudet annetaan rooleille ja roolit käyttäjille (Kuvio 6). Tämän vuoksi se on luonnollinen pääsynhallinnan malli organisaatioille, joissa käyttäjän rooli yrityksessä määrittelee myös tämän digitaalisen identiteetin ja käyttöoikeudet järjestelmissä (Baracaldo & Joshi, 2013; Sun ym., 2011). Organisaatioissa käyttäjälle määritellään rooli perustuen työntekijän rooliin työpaikalla, kuten ase-

maan, jaostoon tai muuhun suurempaan kokonaisuuteen perustuen (Baracaldo & Joshi, 2013; Khan, 2012; Sun ym., 2011).



Kuvio 6 Rooliperustainen pääsynhallinnan malli

Jokainen rooli rooliperustaisessa pääsynhallintamallissa vastaa jotakin käyttöoikeutta (Khan, 2012; Kunz ym., 2019). Kun käyttäjälle osoitetaan jokin rooli, samalla hänelle myönnetään käyttöoikeuksia, jotka roolille on annettu (Baracaldo & Joshi, 2013; Chen & Crampton, 2011; Feng ym., 2008; Khan, 2012; Kunz ym., 2019). Käyttäjät ja käyttöoikeudet liitetään rooliin, ja rooleja on huomattavasti vähemmän kuin käyttäjiä tai käyttöoikeuksia, minkä vuoksi rooli tarjoaa käytännöllisen tavan yhdistää käyttäjäryhmiä joihinkin käyttöoikeusjoukkoihin (Baracaldo & Joshi, 2013; Chen & Crampton, 2011). Rooliperustainen pääsynhallinnan malli mahdollistaa monimutkaisuuden vähentämisen, yhdistämällä käyttöoikeudet ja työntekijät rooliin (Khan, 2012; Kunz ym., 2019).

Rooliperustainen pääsynhallinnan malli on osoittautunut lupaavaksi lähestymistavaksi erityyppisille organisaatioille (Baracaldo & Joshi, 2013), ja sitä käytetään laajasti eri sovelluksissa (Feng, 2008; Kunz ym., 2015b). Rooliperustainen pääsynhallinnan malli mahdollistaa uudet automaatiotasot, jonka vuoksi se on parantunut käyttöoikeushallinnan tehokkuutta merkittävästi (Gunter ym., 2011). Rooleista on tullut käytännöllinen pääsynvalvonnan standardi yrityksen identiteetin- ja pääsynhallintajärjestelmissä (Kunz ym., 2015b). Roolit on otettu laajasti käyttöön organisaatioissa ja ne tarjoavat erilaisia hallinnollisia sekä turvallisuuteen liittyviä etuja (Coyne & Weil, 2013).

Useimmissa verkkosovelluksissa ja tietojärjestelmissä on ainakin kolmen tyyppisiä rooleja: järjestelmänvalvojien rooli eli admin-rooli, normaalien kirjautuneiden käyttäjien rooli ja julkisten tai anonyymien käyttäjien rooli (Sun ym., 2011). Rooliperusteinen pääsynhallinta ryhmittelee käyttöoikeudet rooleihin ja vaatii kaikkien käyttöoikeuksien määräytyvän rooliperusteinen mallin mukai-

sesti (Coyne & Weil, 2013). Kunzin ym. (2015) mukaan hallintajärjestelmä pääasiassa keskittyy roolikokoonpanojen päivittämiseen ja siivoamiseen sekä käyttämättömien roolien hävittämiseen ja uusien roolien määrittelemiseen. Päivittäisen hallinnan lisäksi on strateginen ylläpito, johon kuuluu roolimallien suunnittelu ja strateginen johtaminen. (Kunz ym., 2015b.)

Roolit on suunniteltava huolellisesti ja standardoidusti, ennen kuin rooliperusteinen pääsynhallintamalli voidaan ottaa käyttöön, minkä lisäksi yrityksen roolit on suunniteltava tukemaan organisaation turvallisuus- ja yrityssääntöjä (Coyne & Weil, 2013). Käyttäjän rooli määritetään vähimmillä tarvittavilla oikeuksilla, joita käyttäjä tarvitsee työnsä suorittamiseksi (Khan, 2012). Käyttöoikeuksia voidaan myöhemmin lisätä tai poistaa, mikäli käyttäjän roolin käyttöoikeustarpeet muuttuvat. (Khan, 2012; Kunz ym., 2015b.)

Pääsynhallinnan mallit voidaan jakaa kahteen ryhmään, perinteisiin ja dynaamisiin (Dos Santos ym., 2014). Rooliperustainen pääsynhallinnan malli kuuluu perinteisiin pääsynhallinnan malleihin (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014). Dos Santosin ym. (2014) mukaan perinteiset pääsynhallinnan mallit luottavat staattiseen valtuutukseen, eli jokainen käyttöoikeuspäätös on ennakkoon vahvistettu käytäntöjen perusteella. Perinteiset pääsynhallintamallit eivät riitä varmistamaan esimerkiksi erilaisiin pilviratkaisuihin perustuvien ympäristöjen turvallisuutta, koska pilviympäristöissä on tarpeen lisätä joustavuutta tehokkaan tiedon jakamisen mahdollistamiseksi kriittisissä tilanteissa. (Dos Santos ym., 2014.)

Vaikka rooliperustainen pääsynhallinnan malli on laajasti käytetty, sen ongelma on roolimallien dynaaminen muuttuminen ajan saatossa (Anilkumar & Sumathy, 2018; Kunz ym., 2015b). Rooliperustainen pääsynhallinnan malli ei siis pysty käsittelemään dynaamisesti muuttuvia ominaisuuksia, kuten esimerkiksi kellonaika ja sijainti (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013). Rooliperustainen pääsynhallinnan malli on kallis toteuttaa, eikä se kykene reagoimaan reaaliaikaisesti ympäristötekijöihin (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Kunz ym., 2015b). Roolien kehittyessä ajan myötä yritykset kuitenkin pyrkivät kehittämään ja ylläpitämään johdonmukaista roolimallia (Kunz ym., 2015b). Käyttäjien roolit yrityksessä muuttuvat ajan myötä, minkä vuoksi yritykset kamppailevat kehittääkseen ja ylläpitääkseen jatkuvaa roolimallia koko ajan muuttuvissa olosuhteissa (Kunz ym., 2015b). Ongelma on myös, että käyttäjän käyttöoikeuksien muuttaminen on monimutkaista muuttamatta käyttäjän roolia (Anilkumar & Sumathy, 2018).

Kunzin ym. (2015) mukaan roolien muuttumisen lisäksi ongelmana rooliperustaisessa pääsynhallinnan mallissa on ajan myötä kasvava roolien määrä. Suuri roolien määrä johtaa järjestelmän monimutkaisuuteen, ja aiheuttaa lisää työtä niiden ylläpitoon ja hallintaan. Riskien minimoimiseksi yksi olennainen tekijä on pyrkiä ylläpitämään roolien korkeaa laatua arvioimalla säännöllisesti roolimallikomponenttien, kuten käyttäjäroolimääritysten, käyttöoikeuksien määritysten tai roolihierarkiarakenteiden oikeellisuus. (Kunz ym., 2015b.)

Kunzin ym. (2015) mukaan nopeasti muuttuvat liiketoimintaprosessit, organisaatiorakenteelliset muutokset ja erilaiset tietoturvapolitiikat sekä uusina

määrätyt säännöt pakottavat järjestelmäylläpitäjiä nopeasti päivittämään pääsynhallinnan kuntoon. Tämä johtaa kasvavaan roolien määrään, kokonaisvaltaiseen roolien laadun laskuun sekä altistaa tietoturvahaavoittuvuuksille virheellisesti myönnettyjen tai vanhentuneiden oikeuksien seurauksena. (Kunz ym., 2015b.)

Kunzin ym., (2015b) mukaan rooleja tulee auditoida ja käydä läpi säännöllisesti, jotta organisaatio voi karsia käyttämättömiä ja tarpeettomia rooleja ja oikeuksia, minkä avulla taas voidaan varmistaa tietoturvallisuus ja roolien oikeellisuus. Samalla voidaan välttää järjestelmän monimutkaisuus ja roolien määrän tarpeeton kasvu. (Kunz ym., 2015b).

Baracaldon & Joshin (2013) mukaan rooliperustainen pääsynhallinnan malli toimii hyvin ympäristöissä, joissa käyttäjät ovat hyväkäytöksisiä ja heidän toimintaansa voi täysin luottaa. Tämän takia rooliperustainen pääsynhallinnan malli ei pysty estämään sisäpiirin hyökkäyksiä, joissa työntekijä toimii tahallaan tai epähuomiossaan vahingollisesti organisaatiota kohtaan. Sisäpiirin hyökkäykset ovat valitettavan todellinen ongelma yritysmaailmassa. (Baracaldo & Joshi, 2013.)

On kuitenkin olemassa keinoja, joilla rooliperustaisen pääsynhallinnan mallin riskejä voidaan minimoida. Järjestelmässä tulisi olla käytössä tehtävien hajauttaminen (SoD), jossa ennakkoon määriteltyjen tehtävien toteuttamiseen vaaditaan useamman henkilön tunnistautuminen (Baracaldo & Joshi, 2013; Bradford ym., 2014). Baracaldon & Joshin (2013) mukaan tämä vähentää merkittävästi tahallisen tai tahattoman sisäpiirin hyökkäyksen ja muiden tietoturvauhkien toteutumista. Tämän lisäksi järjestelmän tulisi automaattisesti reagoida epätavalliseen toimintaan, jonka lisäksi henkilöihin voitaisiin liittää esimerkiksi erilaisia luottamustasoja. (Baracaldo & Joshi, 2013.)

Rooliperustainen pääsynhallinnan malli ei myöskään kykene selviytymään käyttäjien muuttuvasta käyttäytymisestä (Anilkumar & Sumathy, 2018; Baracaldo & Joshi, 2013). Mikäli käyttäjällä on oikeus johonkin resurssiin, hänelle myös myönnetään pääsy tietoihin ja järjestelmään, vaikka käyttäjän toiminta olisi epäilyttävää tai voimakkaasti normaalista poikkeavaa (Baracaldo & Joshi, 2013). Rooliperustainen pääsynhallinnan malli ei kykene reagoimaan poikkeuksiin, jonka vuoksi siinä on suuri todennäköisyys tiedon vuotamiseen (Anilkumar & Sumathy, 2018; Baracaldo & Joshi, 2013)

Kasvanut tarve jakaa tietoa dynaamisissa ympäristöissä on luonut tarpeen riskitietoisemmille pääsynhallintamalleille rooliperustaisen pääsynhallinnan rinnalle tai korvaajaksi (Anilkumar & Sumathy, 2018; Chen & Crampton, 2011). Standardi rooliperustainen pääsynhallinnan malli on suunniteltu toimimaan suhteellisen vakaassa, suljetussa ympäristössä ja se ei tue muuttuvia dynaamisia olosuhteita (Chen & Crampton, 2011). Rooliperustainen pääsynhallinnan malli sisältää kattavasti hyviä asioita, mutta siinä on myös rajoitteita (Taulukko 3).

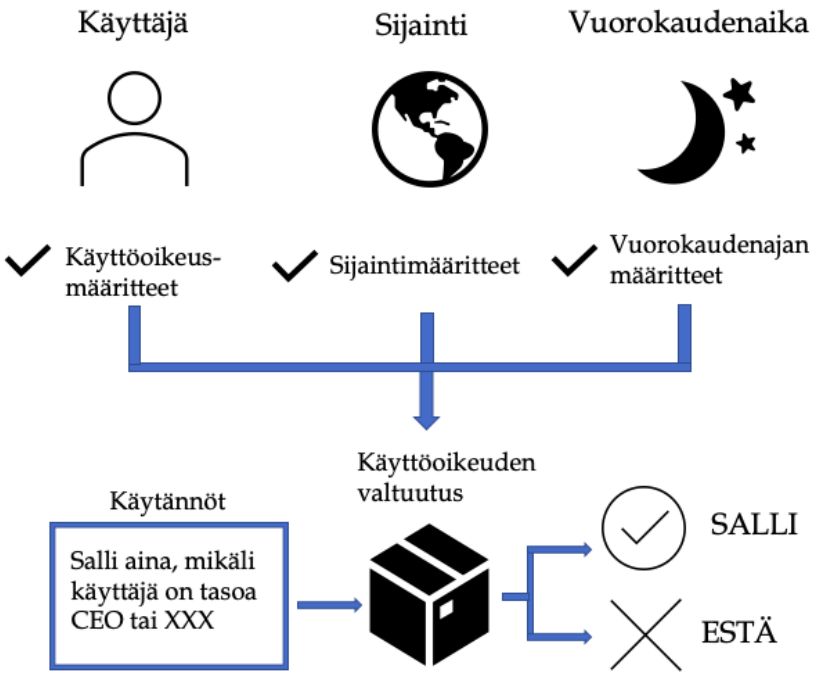
Taulukko 3 Rooliperustaisen pääsynhallinnan mallin edut ja ongelmat

Edut	Luonnollinen organisaatioille	Anilkumar & Sumathy, 2018; Baracaldo & Joshi, 2013; Gunter ym., 2011; Kunz ym., 2019; Sun ym., 2011
	Monimutkaisuuden väheneminen	Baracaldo & Joshi, 2013; Chen & Crampton, 2011; Coyne & Weil, 2013; Khan, 2012; Kunz ym., 2019
	Automaatio	Gunter ym., 2011
	Tietoturva	Coyne & Weil, 2013
	Tehtävien hajauttaminen	Baracaldo & Joshi, 2013; Bradford ym., 2014
Ongelmat	Dynaamisuuden ja joustavuuden puute	Anilkumar & Sumathy, 2018; Baracaldo & Joshi, 2013; Coyne & Weil, 2013; Dos Santos ym., 2014; Kunz ym., 2015b
	Aloituskustannukset	Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Kunz ym., 2015b
	Työläs ylläpitää	Anilkumar & Sumathy, 2018; Kunz ym., 2015b
	Sisäpiirin hyökkäykset	Baracaldo & Joshi, 2013

3.2.2 Ominaisuusperustainen pääsynhallinnan malli

Uusien järjestelmäarkkitehtuurien syntyminen on johtanut uusien pääsynhallinnan mallien kehittämiseen (Dos Santos ym., 2014; Maesa ym., 2017). Tällaisia uusia järjestelmäarkkitehtuureja ovat esimerkiksi hajautetut ja pilvipohjaiset järjestelmät (Dos Santos ym., 2014; Maesa ym., 2017). Organisaatioissa on tunnistettu tarve rooliperustaista pääsynhallintamallia laajemmalle käyttöoikeusmallille, joka huomioi dynaamisesti muuttuvia määritteitä, kuten vuorokaudenajan ja käyttäjän sijainnin (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Hu ym., 2013; Khan, 2012; Kunz ym., 2019).

Ominaisuusperustainen pääsynhallinnan malli (*eng. Attribute Based Access Control, ABAC*) on looginen pääsynhallinnan malli, jossa valtuutus resursseihin määritetään arvioimalla käyttäjään, kohteeseen, pyydettyihin toimintoihin ja joissain tapauksissa ympäristöolosuhteisiin liittyvät ominaisuudet suhteessa ennakkoon määriteltyihin ehtoihin ja käytäntöihin (Kuvio 7) (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Hu ym., 2013; Khan, 2012; Kunz ym., 2019; Maesa ym., 2017).



Kuvio 7 Ominaisuusperustainen malli

Kuten aiemmin mainittua, pääsynhallinnan mallit voidaan jakaa dynaamisiin ja perinteisiin malleihin (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kunz ym., 2015b). Dynaamiset mallit ovat kykeneväisiä reagoimaan ympäristön muuttuviin ominaisuuksiin, kuten käyttäjän sijaintiin (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kunz ym., 2015b). Ominaisuusperustainen malli kuuluu dynaamisiin malleihin. Dynaamisten pääsynhallinnan mallien taustalla on dynaamisen pääsynhallinnan toiminnot, jotka analysoivat reaaliaikaisesti jokaisen käyttöoikeuspyynnön ottaen huomioon käytäntöjen lisäksi erilaisia tilannesidonnaisia tietoja, kuten tietoturvariskin, operatiivisen tarpeen ja siitä saatavan hyödyn sekä kontekstin (Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kunz ym., 2015b).

Ominaisuusperustainen pääsynhallinnan malli käyttää rooliin perustuvien käyttöoikeuksien sijasta merkittyjä objekteja ja käyttäjämääreitä tarjotakseen joustavan pääsynhallinnan (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Maesa ym., 2017). Mallin käytännöt koostuvat joukosta ominaisuuksille osoitettuja ehtoja, jotka kuvaavat käyttöoikeuspyyntöön osallistuvien kohteiden, resurssien ja ympäristön ominaisuuksia (Maesa ym., 2017).

Ominaisuuksia voivat olla esimerkiksi käyttäjän henkilönumero yrityksessä, sen yrityksen tunnus, jonka palveluksessa käyttäjä työskentelee, käyttäjän rooli yrityksessä, käyttäjälle osoitettujen projektien nimet, käyttäjän fyysinen sijainti tai resurssien lukumäärä, joita hän tällä hetkellä käyttää (Maesa ym., 2017). Käytännössä mikäli käyttäjällä on ominaisuuksia, jotka heijastuvat objekteihin, joita käyttäjä haluavat käyttää, tullaan käyttöoikeus myöntämään (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Maesa ym., 2017).

Erona rooliperustaiseen malliin on, että oikeuksia ei määritellä absoluuttisesti etukäteen, vaan ne muodostuvat riippuen erilaisista dynaamisista ominaisuuksista (Coyne & Weil, 2013; Maesa ym., 2017). Toisin sanoen käyttäjälle on etukäteen annettu joukko rooleja (ja siten myös käyttöoikeuksia) rooliperustaisella pääsynhallinnan avulla, kun taas ominaisuusperustaisen mallin käyttöoikeudet voidaan hankkia dynaamisesti käyttäjän määritteiden avulla (Coyne & Weil, 2013).

Viimeaikainen suuntaus on ominaisuusperustaisen pääsynhallinnan soveltaminen oikeuksien automaattiseen myöntämiseen työntekijöille (Gunter ym., 2011; Kunz ym., 2019). Ominaisuusperustainen pääsynhallinnan malli poistaa rooliperustaisen mallin rajoitteita, kuten roolien määrän kasvaminen, jonka lisäksi se on joustavampi ja mahdollistaa sekä yksityiskohtaisen että yksinkertaisemman ominaisuusmallin. (Gunter ym., 2011; Kunz ym., 2019).

Malli on joustavampi kuin rooliperustainen, koska se pystyy reagoimaan reaaliaikaisesti käyttäjän käyttöoikeuspyyntöihin, ja ei aiheuta seisauksia käyttäjän työssä. Käyttäjällä tulee olla työtehtäviensä toteuttamiseen vaaditut käyttöoikeudet (Kumar & Bhardwaj, 2018). Ominaisuusperustaisen pääsynhallinnan mallin menestys riippuu kuitenkin suuresti ominaisuusmääritelmien ja ominaisuusarvojen jäsennellyn hallinnan taustalla olevista prosesseista ja niiden laadusta (Kunz ym., 2019).

Ominaisuusperustainen pääsynhallinnan malli tarkistaa subjektien, esineiden tai ympäristöominaisuuksien arvot ennalta määriteltyjen sääntöjen perusteella ja sallii tai evää pääsyn resursseihin näiden noudattamisen perusteella (Kunz ym., 2019). Virheellisesti määritetyt ominaisuusarvot voivat johtaa eitoivottuun pääsyyn, joka altistaa erilaisille tietoturvallisuusuhille ja mahdollistaa lopulta sisäpiiriläisten tahallisen tai tahattoman väärinkäytöksen organisaatioresursseissa (sisäpiirin hyökkäykset) (Baracaldo & Joshi, 2013; Kunz ym., 2019). Tämän lisäksi ominaisuuksien laaduttomuus voi johtaa virheellisiin pääsynhallinnan päätöksiin ja siten tietoturvaheikkouksiin (Kunz ym., 2019).

Coynen ja Weilin (2013) mukaan ominaisuusperustaisessa pääsynhallinnan mallissa tulee ymmärtää ja hallita suurta määrää ominaisuusattribuutteja ja jonkun ulkopuolisen identiteetin- ja pääsynhallinnan asiantuntijan tulee valikoida ne. Ulkopuolinen identiteetin- ja pääsynhallinnan asiantuntija pystyy objektiivisesti katsomaan mitä rooleja yrityksessä tarvitaan, ja näin voidaan välttää roolien päällekkäisyydet tai liian laajat kuvaukset. Ominaisuusmääritteillä ei ole yksinään merkitystä, ennen kuin ne on liitetty johonkin käyttäjään, esineeseen tai relaatioon. Ongelmana ominaisuusperustaisessa pääsynhallinnan mallissa on, että käyttöoikeuksien katselmointi on haastavaa ja epäkäytännöllistä, koska käyttöoikeudet muodostuvat ominaisuuksien mukaan, eikä käyttäjälle ole määritelty vain yhtä merkitsevää ominaisuutta, jonka lisäksi ominaisuudet muuttuvat dynaamisesti, eivätkö ole stabiileja. (Coyne & Weil, 2013.)

Ominaisuusperustainen pääsynhallinnan malli poistaa rooliperustaisen pääsynhallinnan mallin ongelmia, kuten dynaamisuuden puutteen ja riskitiedottomuuden (Coyne & Weil, 2013; Kunz ym., 2019). Ominaisuusperustaisessa pääsynhallinnan mallissa on monia etuja, mutta se ei kuitenkaan ole ongelma-

ton (Taulukko 4). Ominaisuusperustainen pääsynhallinnan malli vaatii toimiakseen huolellisesti määritellyt käytännöt eikä oikeuksien auditointi ole käytännössä mahdollista monimutkaisten ja dynaamisesti myönnettävien oikeuksien vuoksi (Baracaldo & Joshi, 2013; Coyne & Weil, 2013; Kunz ym., 2019).

Taulukko 4 Ominaisuusperustaisen pääsynhallinnan mallin edut ja ongelmat

Edut	Dynaamisuus	Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kumar & Bhardwaj, 2018; Kunz ym., 2015b
	Reaaliaikaisuus	Anilkumar & Sumathy, 2018; Dos Santos ym., 2014; Kunz ym., 2015b
	Riskitietoisuus	Anilkumar & Sumathy, 2018; Dos Santos ym., 2014
	Automaatio	Gunter ym., 2011; Kunz ym., 2019
Ongelmat	Laaduttomat ominaisuudet	Baracaldo & Joshi, 2013; Kunz ym., 2019
	Hankala auditointiprosessi	Coyne & Weil, 2013

4 TUTKIMUKSEN TOTEUTUS

Tässä luvussa käsitellään pro gradu -tutkielman empiiristä tutkimusosaa ja sen toteuttamista. Luvussa kuvataan, kuinka tutkimusprosessi on suunniteltu ja toteutettu. Ensimmäisessä alaluvussa kerrotaan tutkimusmenetelmästä ja sen valinnasta. Toisessa alaluvussa tutustutaan tiedonkeruumenetelmään ja sen toteutukseen. Kolmannessa alaluvussa esitellään tutkimuksen analysointimenetelmää ja neljännessä esitellään tämän tutkielman tapaustutkimuksen kohdeorganisaatio.

4.1 Tutkimusmenetelmä

Työn empiirinen osuus on toteutettu kvalitatiivisena eli laadullisena tutkimuksena. Laadullinen tutkimusote on toinen yleisimmistä tutkimusstrategioista, ja toinen niistä on kvantitatiivinen eli määrällinen tutkimusote. Laadullisessa tutkimuksessa kohteen ominaisuuksia kuvataan, kun taas määrällisessä kohteen ominaisuuksia mitataan. Laadullista tutkimusaineistoa voidaan kerätä erilaisilla menetelmillä, kuten haastatteluilla, dokumentteihin perehtymällä tai tutkimukseen osallistuvien kohdehenkilöitä seuraamalla (Myers, 1997). Laadullisen tutkimuksen avulla tutkimuksesta voidaan saada syvällisiä yksityiskohtia, joiden avulla pystytään ymmärtämään johtopäätösten merkitys (Hirsjärvi & Huttunen, 1995).
Laadullisen tutkimuksen tarkoituksena on ymmärtää mahdollisimman tarkasti tutkimuksen kohteena oleva ilmiö (Hirsijärvi, Remes & Sajavaara, 2009), jonka vuoksi laadullinen tutkimus soveltuu tähän tutkimukseen parhaiten, koska tutkimuksen tavoitteena on ymmärtää jokin tietty ilmiö ja kuvata sitä mittaamisen sijaan (Hirsjärvi & Huttunen, 1995). Tässä tutkielmassa on tarkoitus ymmärtää, millaisia riskejä identiteetin- ja pääsynhallintaan liittyy, jolloin pyritään kuvaamaan niitä mittaamisen sijaan.

Laadullinen tutkimus mahdollistaa kokonaisvaltaisemman ja syvällisemmän käsityksen tutkittavasta ilmiöstä, kuin mitä määrällinen tutkimus tarjoaisi

(Hirsjärvi, Remes & Sajavaara, 2009). Tämän lisäksi laadullinen tutkimustapa soveltuu hyvin tutkimukseen, jossa informaatioteknologian ja organisaatioiden välistä vuorovaikutusta halutaan ymmärtää (Darke, Shanks & Broadbent, 1998). Laadullinen tutkimus sopii myös näistä syistä tämän tutkimuksen menetelmäksi, koska tapaustutkimuksen tutkimuskohteena on kohdeorganisaation identiteetin- ja pääsynhallinta.

Laadullinen tutkimus antaa enemmän mahdollisuuksia tutkittavien henkilöiden omille kokemuksille, näkökulmille, ajatuksille ja tunteille tutkittavan ilmiön ympärillä (Hirsjärvi & Huttunen, 1995), joka oli tässä tutkimuksessa erityisen tärkeää, koska haluttiin tunnistaa todellisia identiteetin- ja pääsynhallintaan liittyviä riskejä asiantuntijoiden omien kokemusten ja näkökulmien perusteella.

Tutkimus toteutettiin tapaustutkimuksena, jossa kiinnostuksen kohteena oli kohdeorganisaatio. Tapaustutkimus on yksi laadullisen tutkimusmenetelmän yleisimpiä tutkimusstrategioita (Darke ym., 1998). Tapaustutkimuksen avulla tutkitaan ilmiöitä yhdestä tai useammasta entiteetistä, eikä sillä pyritä laajaan, tilastolliseen tutkimukseen (Benbasat, Goldsteinin & Meadin, 1987; Yin, 2003). Tapaustutkimuksen tarkoituksena ei ole löytää tyypillisiä piirteitä tai syy-seuraussuhteita, vaan kuvailla ilmiötä ja tehdä siitä uusia havaintoja (Yin, 2003). Tähän tutkielmaan tapaustutkimus oli sopiva tutkimusmuoto, koska tutkimuksessa tavoiteltiin syvällistä ymmärrystä erilaisiin identiteetin- ja pääsynhallinnan riskeihin sekä haluttiin saada näkemys aiempien tutkimusten, ja tämän tapaustutkimuksen tulosten yhtäläisyyksiin ja eroavaisuuksiin. Tutkimus toteutettiin toimeksiantona kohdeorganisaatiolle.

Tapaustutkimuksen tarkoituksena on ymmärtää tutkittavaa ilmiötä syvällisesti, joten se sopii hyvin tämän tutkimuksen tutkimusmuodoksi, koska tutkimuksessa keskitettiin melko rajattuun tutkimuskohteeseen laajemman tutkimuksen sijaan. Tämän lisäksi tapaustutkimuksen tekemistä perustelee se, että tutkimuskohteena on jokin reaalimaailman ongelma (Eriksson & Koistinen, 2005). Tapaustutkimus valikoitui tämän tutkielman tutkimustavaksi, koska sen tavoitteena on ratkaista reaalimaailman ongelma.

4.2 Tiedonkeruumenetelmä

Tapaustutkimuksessa tietoja voidaan kerätä haastatteluilla, dokumenteista, havainnoinnilla sekä fyysisiä artefakteja tutkimalla (Myers, 1997; Yin, 2003). Empiirinen tutkimus toteutettiin haastatteluiden avulla, joilla pyrittiin selvittämään, millaisia erilaisia riskejä identiteetin- ja pääsynhallintaan organisaatioissa liittyy. Tavoitteena oli löytää yhtäläisyyksiä ja eroavaisuuksia kirjallisuuden ja tapaustutkimuksen tulosten välillä. Haastattelututkimus on yleisin tiedonkeruumenetelmä laadullisen tutkimuksen toteutuksessa (Myers & Newman, 2007). Haastattelututkimus mahdollistaa tarkentavien kysymysten esittämisen ja antaa haastateltavalle enemmän mahdollisuuksia kuvailuun vastauksissaan (Metsämuuronen, 2008), jonka vuoksi se on tähän tutkimukseen parempi toteutus-

muoto verrattuna esimerkiksi kyselytutkimukseen, jossa on hyvin tiukkaan strukturoitu rakenne.

Haastattelut toteutettiin teemahaastatteluina. Teemahaastattelut antavat mahdollisuuden haastattelijan ja haastateltavan väliselle monipuoliselle vuorovaikutukselle (Näpärä, 2017). Teema ja kysymysrunko ovat ennakkoon suunniteltuja, mutta haastattelun on muuten tarkoitus olla hyvin vapaamuotoinen. Teemahaastattelu antaa mahdollisuuden keskittyä haastattelutilanteessa tarvittaessa tiettyihin aiheisiin tarkemmin, ja käsitellä tarvittaessa joitakin aiheita kevyemmin (Hirsjärvi & Hurme, 2015). Teemahaastattelussa kysymysten järjestystä ja muotoilua voidaan muuttaa haastattelun aikana, eikä se ole muutenkaan yksityiskohtaisesti ennakkoon määritelty (Hirsjärvi & Hurme, 2015).

Tutkimus toteutettiin teemahaastatteluina, koska teemahaastatteluiden rakenne on joustava, mikä mahdollisti haastattelun personoinnin tarvittaessa jokaiselle haastateltavalle. Haastateltavien tietämys identiteetin- ja pääsynhallinnasta kohdeorganisaation ulkopuolella vaihteli, jonka vuoksi joidenkin haastateltavien kanssa keskitettiin tarkemmin kysymyksiin, kun taas joidenkin kanssa käsiteltiin aihetta yleisemmällä tasolla. Teemahaastattelut mahdollistavat haastattelukysymysten järjestyksen muuttamisen, jolloin voitiin esittää kysymyksiä haastattelun etenemisen mukaan loogisessa järjestyksessä, esimerkiksi jos jokin aihe tuli esiin ennalta suunniteltua aiemmin. Haastatteluilta haluttiin saada myös sellaisia havaintoja, joita kirjallisuus ei tarjonnut, minkä vuoksi teemahaastattelut sopivat tutkimusmuodoksi, koska niiden avulla tutkija voi esittää tarkentavia kysymyksiä, jotka eivät ole valmiissa kysymysrungossa.

Teemahaastattelun runko muodostettiin perusten kirjallisuuskatsauksessa esiin tulleisiin riskiteemoihin. Haastattelututkimusta varten laadittiin sellaisia haastattelukysymyksiä (Liite 1), joihin ei voisi vastata ainoastaan yhdellä sanalla, kuten ”kyllä” tai ”ei”, koska haluttiin saada kuvailevia ja laajempia vastauksia. Tällä voitiin varmistaa, että haastattelututkimuksesta saatiin kattavaa materiaalia analysointia varten.

Empiirisen tutkimusaineiston keruu toteutettiin heinäkuussa 2020. Haastattelututkimuksessa haastateltiin kohdeorganisaation työntekijöitä yksilöhaastatteluilla. Haastateltavat valittiin heidän tehtäviensä sekä vastuualueensa perusteella kohdeorganisaatiossa. Laadullisessa tutkimuksessa on olennaista, että haastateltavat ovat henkilöitä, joilla on tietämystä tutkittavasta ilmiöstä tai aiheesta, tai heillä on kokemusta siitä (Tuomi & Sarajärvi, 2017). Haastatteluun osallistui henkilöitä kohdeorganisaation tietohallinnosta, tietoturva-asiantuntijoita, identiteetin- ja pääsynhallinnan asiantuntijoita sekä IT-arkkitehti. Näillä henkilöillä on paras käsitys kohdeorganisaation identiteetin- ja pääsynhallinnasta, jonka vuoksi he olivat kaikkein sopivampia haastateltavia tutkimukseen. Identiteetin- ja pääsynhallinnan asiantuntijoilla on lisäksi kokemusta identiteetin- ja pääsynhallinnasta oman työnsä kautta eri asiakasprojekteista.

Haastateltavien motivoimisena toimi tutkielman hyödyllisyys molemmille toimeksiannon osapuolille. Tutkielma vastaa kohdeorganisaation todelliseen ongelmaan ja tarpeeseen, minkä vuoksi kaikki haastateltavat osallistuivat mie-

lellään tutkimukseen. Haastateltaville kerrottiin ennakkoon tutkielman tavoitteet kohdeorganisaatiolle, ja että heidän osallistumisensa tarjoaisi tärkeää osaamista ja näkökulmaa myös opinnäytetyöhön.

Haastattelut toteutettiin etähaastatteluina Microsoft Teams -palvelulla, koska COVID-19 pandemiasta johtuvien poikkeusolojen takia kasvotusten tapaaminen ei ollut kohdeorganisaation suositusten mukaista. Haastatteluajat sovittiin sähköpostitse, ja samalla haastateltaville lähetettiin haastattelukysymykset, joihin he pystyivät halutessaan tutustumaan. Haastattelukysymyksiin ennakkoon perehtyminen ei kuitenkaan ollut vaatimus haastattelun onnistumiselle.

Haastattelukutsuja lähetettiin yhteensä 13 henkilölle, ja lopulta 10 heistä haastateltiin lopulliseen tutkimukseen. Haastateltavien määrä valikoitui kymmeneen sen takia, että haastateltavien vastaukset olivat hyvin saman tyylisiä jo, eikä enää merkittävää lisäarvoa saatu tutkimukseen lisäämällä haastateltavien määrää. Laadullisessa tutkimuksessa sopiva haastateltavien määrä voidaan määritellä juuri kyllääntymisen, eli saturaation avulla (Eskola & Suoranta 1998; Hirsjärvi & Hurme, 2015). Saturaatio tarkoittaa, että haastatteluissa ei enää saada tutkimuksen kannalta olennaista uutta tietoa, eli aineisto alkaa toistamaan itseään (Eskola & Suoranta 1998; Hirsjärvi & Hurme, 2015).

Kaikki haastattelut äänitettiin, ja jokaiselta haastateltavalta kysyttiin lupa siihen ennen haastattelun aloittamista. Jokaiselle haastateltavalle äänittäminen sopi. Äänitteitä käytettiin vain haastattelun litterointia varten eli puhtaaksikirjoittamisen apuna (Hirsjärvi & Hurme, 2015). Haastateltavilla oli myös halutessaan mahdollisuus käydä läpi puhtaaksikirjoitettu haastattelu, jolloin heillä oli mahdollisuus tehdä korjauksia tai jättää jotain halutessaan pois.

Teemahaastatteluiden avulla kerätty aineisto on yleensä runsas (Hirsjärvi & Hurme, 2015). Litteroinnissa haastatteluaineistosta jätettiin toistoja pois ja muita täytesanoja, kuten *tota*, *niin kuin* ja *noh*. Toistojen ja pikkusanojen poistaminen tehtiin aineiston selkeyden parantamiseksi. Lisäksi litteroinnissa lisättiin selittäviä sanoja sulkuihin, jotta voitiin tehdä tulosten esittelystä selkeämpi. Tällaisia selittäviä sanoja käytettiin, mikäli haastateltava oli viitannut aiheeseen esimerkiksi sanalla *se* tai *tämä*. Litteroimisen jälkeen haastattelulitteroinnit kategorisoitiin haastateltavien profiilin perusteella ja nimettiin niiden mukaan anonymiteetin säilyttämiseksi. Tämän jälkeen haastatteluiden analysointi voitiin aloittaa.

4.3 Analysointi

Kvale (1996 Hirsjärven ja Hurmeen, 2015, s.136-138, mukaan) esittää teemahaastatteluiden analysointiin kuusi erilaista lähestymistapaa. Analysointitavat poikkeavat toisistaan eniten siinä, missä vaiheessa analysointi tapahtuu ja kuka sen tekee. Ensimmäinen tapa on spontaani, jossa haastateltavat kuvaavat elämäänsä ja elämismaailmaansa haastattelun kuluessa. Haastateltava kertoo aiheeseen liittyvistä kokemuksista ja tuntemuksista, eikä kuvausta erityisesti tulkita. Toi-

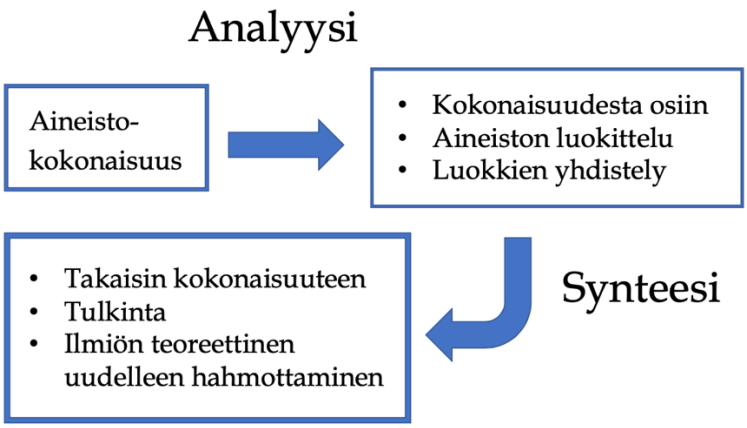
sessa analysointitavassa haastateltava itse tunnistaa yhteyksiä asioiden välillä tai huomaavat uusia merkityksiä. Haastattelija ei tässä tavassa luo tulkintoja. Kolmannessa analysointitavassa haastattelija tiivistää ja tulkitsee haastateltavan kuvausta jo haastattelun aikana ja kertoo tulkinnoistaan myös haastateltavalle. Tapa antaa haastateltavalle mahdollisuuden kumota tai vahvistaa tulkinta. Dialogia voidaan käydä, kunnes päästään oikeaan tulkintaan. Tätä haastattelumuotoa voidaan kutsua ”itseäänkorjaavaksi” haastatteluksi. (Kvalen, 1996 viitattu lähteessä Hirsjärvi & Hurme, 2015.)

Kvalen (1996 Hirsjärven ja Hurmeen, 2015, s.137-138) mukaan neljännessä tavassa haastattelija tulkitsee litteroitua aineistoa yksin tai yhdessä muiden tutkijoiden kanssa. Analysoinnissa voidaan käyttää kolmea menettelyä: Aineistoa järjestetään ja tuodaan esiin sen rakentuminen, aineiston selventäminen sekä varsinainen analyysi. Viides lähestymistapa on uudelleen haastattelu, jossa tutkija ensimmäisen analysoinnin perusteella pyytää haastateltavaa kertomaan näkemyksensä tulkinnan oikeellisuudesta. Kuudes tapa kattaa kuvaukseen ja tulkintaan liittyvän toiminnan, jolloin haastateltavat alkavat toimia haastattelussa ilmenneiden seikkojen mukaisesti. Tällöin tutkimushaastattelu voi muistuttaa jopa terapeuttista haastattelua. (Kvalen, 1996 viitattu lähteessä Hirsjärvi & Hurme, 2015.)

Tämän tutkimuksen analysointiin sopi parhaiten neljäs lähestymistapa aineiston analysointiin, eli analysointi, jossa haastattelija tulkitsee litteroitua aineistoa joko yksin tai yhdessä muiden tutkijoiden kanssa (Hirsjärvi & Hurme, 2015). Tämä pro gradu -tutkielma on tehty yksin, joten myös analysoinnin teki tutkija yksin.

Valitussa analysointimenetelmässä voidaan käyttää kolmea erilaista menetelmää. Ensimmäinen niistä on aineiston järjestäminen ja aineiston rakentumisen esiintuominen. Tämä on tarpeen etenkin laajempien aineistojen kanssa. Toisessa vaiheessa eliminoidaan aineistosta kaikki asiaan kuulumattomat osat, kuten toistot ja epäolennaisuudet. Kolmannessa vaiheessa, eli varsinaisessa analyysissä muun muassa tiivistetään, luokitellaan ja tulkitaan. (Hirsjärvi & Hurme, 2015.)

Laadullisen aineiston käsittely sisältää monia eri vaiheita, ja keskeisimmiltä osilta se on sekä analyysiä että synteesiä (kuvio 8) (Hirsjärvi & Hurme, 2015). Analyysissä aineistoa eritellään ja luokitellaan. Synteesissä pyritään luomaan näkemystä kokonaisuudesta ja nähdä tutkimuksen kohde uudesta näkökulmasta.



Kuvio 8 Haastatteluaineiston käsittely analyysistä synteesiin (Hirsjärvi & Hurme, 2015)

Analysointi aloitettiin lukemalla koko litteroitu aineisto läpi useaan kertaan pitäen mielessä tutkimuksen tavoitteet. Tutkimuksen tavoitteena oli tutustua erilaisiin identiteetin- ja pääsynhallinnan malleihin organisaatiokontekstissa sekä erityisesti tunnistaa siihen liittyviä riskejä. Johdannossa esitetty päätutkimuskysymys oli ”Millaisia riskejä identiteetin- ja pääsynhallintaan liittyy organisaatioissa?” Koska laadullisessa tutkimuksessa analysoitavaa materiaalia on usein runsaasti, on tärkeää olla selkeä käsitys siitä, mitkä asiat ovat tämän tutkimuksen kannalta olennaisia (Hirsjärvi & Hurme, 2015; Sarajärvi & Tuomi, 2017). Litteroituun haastattelumateriaaliin merkittiin kohdat tekstinkäsittelyohjelman korostustyökalulla, joissa saatiin tutkimuksen kannalta merkittäviä tuloksia, kuten vastauksia tutkimusongelmaan. Erityisen mielenkiintoisina pidettiin erilaisia haastatteluissa esiin nousseita riskejä ja haavoittuvuuksia sekä millaisia riskejä tiettyihin ominaisuuksiin voi liittyä.

Eskolan ja Suorannan (1998) mukaan analyysissä aineistoa tiivistetään, jotta sen informaatioarvo kasvaa. Kommentoinnin jälkeen aineisto voidaan ryhmitellä haastateltavien henkilöiden taustatietojen perusteella (Sarajärvi & Tuomi, 2017). Haastateltavat ryhmiteltiin kolmeen kategoriaan heidän tehtävien mukaan kohdeorganisaatiossa: tietohallinnon asiantuntijat, identiteetin- ja pääsynhallinta ja sisäisen tietoturvan asiantuntijat. Valitut ryhmät eroavat asemansa ja erityisosaamisensa takia toisistaan merkittävästi, joten analysointi ja sen tulokset ovat mielekkäämpiä erillään.

Aineiston analyysitavaksi valittiin teemoittelu, joka on aineiston pilkkomista ja ryhmittelyä erilaisten aihepiirien mukaan (Sarajärvi & Tuomi, 2017). Aineistoon tehtyjen merkintöjen jälkeen löydetyt asiat merkittiin teemoittain Excel-taulukkoon. Aineiston analyysiä helpotti kysymysten teemoittelu. Aineisto käytiin läpi teemoittain ja pyrittiin löytämään haastattelumateriaalista vastaavia riskejä, mitä kirjallisuuskatsauksessa oli kirjallisuudesta löydetty. Yhtäläisyyksien lisäksi oltiin kiinnostuneita tapaustutkimuksen sekä kirjallisuuskatsauksen tulosten eroavaisuuksista. Excel-taulukkoon merkittiin eri teemojen alle sekä kirjallisuuskatsauksen löydökset että tapaustutkimuksen tulokset jokaisesta teemasta. Analysointi toteutettiin ikään kuin vuoropuheluna teorian ja

empirian välillä pyrkien nostamaan esiin sekä yhtäläisyyksiä, mutta myös eroavaisuuksia, jolloin voitiin luoda synteesiä näiden kahden tuloksista.

4.4 Tutkimuskohde

Tutkimus toteutettiin toimeksiantona organisaatiolle, joka tarjoaa erilaisia asiantuntijapalveluita yrityksille. Kohdeorganisaatio on eräs Suomen johtavista asiantuntijaorganisaatioista. Organisaation palveluihin kuuluu laajasti erilaisia asiantuntija- ja konsulttipalveluita. Kohdeorganisaatio toimii Suomessa useilla paikkakunnilla, ja sen palveluksessa työskentelee yli 1000 henkilöä.

Luottamus asiantuntijaorganisaatioon on merkittävä tekijä valittaessa asiantuntijaa (Van Swol & Sniezek, 2005). Kohdeorganisaatiossa käsitellään paljon sensitiivistä dataa, ja koko yrityksen liiketoiminta on riippuvainen asiakkaiden luottamuksesta. Sensitiivisen tiedon käsittely tuo mukanaan monia riskejä ja tietoturva on tärkeä ja käytännössä vaadittava osa tällaisen datan käsittelyä (King & Raja, 2012). Tietovuodoista on vakavia seurauksia yrityksille, kuten maineriski, taloudelliset menetykset sekä erilaisia oikeustoimia (Bodkin, 2004; King & Raja, 2012).

Organisaation tietoturvassa tärkeä tekijä on turvallinen ja luotettava identiteetin- ja pääsynhallinta. Identiteetin- ja pääsynhallinta on erittäin kriittisessä osassa koko organisaation tietoturvaa, koska sen avulla pyritään minimoimaan lukuisia riskejä, joilla voisi olla tuhoisia seurauksia organisaatiolle (Feng ym., 2008; Hummer ym., 2016; Khan, 2012; Kumar & Bhardwaj, 2018). Identiteetin- ja pääsynhallinnan avulla huolehditaan muun muassa, ettei yrityksen verkkoon ja muihin resursseihin pääse valtuuttamattomia ulkopuolisia henkilöitä, tai ettei yrityksen hallussa olevat sensitiiviset tiedot pääse vuotamaan organisaation ulkopuolelle.

Kohdeorganisaation tavoitteena on lähitulevaisuudessa siirtyä uuteen identiteetin- ja pääsynhallinnan ratkaisuun sisäisessä identiteetin- ja pääsyhallinnassa, eli työntekijöiden identiteetinhallinnassa. Tällä hetkellä organisaation identiteetin- ja pääsynhallintaa hallinnoidaan hajautetusti, mutta keskeisimmät käyttöoikeudet hallinnoidaan keskitetysti. Nykyinen ratkaisu on osittain automatisoitu tavanomaisten käyttöoikeuksien elinkaaren prosessien osalta, mutta vaatii kuitenkin edelleen merkittävästi manuaalista työtä. Manuaalinen työ lisää inhimillisten virheiden mahdollisuutta sekä tekee prosessista riippuvaisen käyttäjästä. Nykyinen ratkaisu sisältää erilaisia riskejä ja sen on todettu olevan vanhanaikainen.

Uudelta identiteetin- ja pääsynhallinnalta toivotaan mahdollisimman pitkälle keskitettyä hallintaa, perusprosessien automatisointia, lisäoikeuksien pyytämisen automatisointia sekä selkeää näkymää kokonaisuudesta. Uuden ratkaisun halutaan olevan helppokäyttöisempi ja tietoturvallisempi verrattuna nykyiseen toteutukseen.

5 TUTKIMUSTULOKSET

Tässä luvussa esitellään empiirisen tutkimuksen tuloksia. Tulokset esitellään riskiteemoittain, jotka ovat muodostettu kirjallisuuskatsauksen perusteella. Kirjallisuuskatsauksessa esiin tulleiden riskiteemojen lisäksi on nostettu yksi riskiteema empiriasta, koska se koettiin merkittäväksi riskikokonaisuudeksi ja toistui useimmissa haastatteluissa.

Pilvipalveluriskit ovat empirian pohjalta nostettu riskiteema, jota ei käsitelty erikseen kirjallisuuskatsauksen lähdemateriaaleissa, mutta koettiin olennaiseksi osaksi tätä tutkielmaa, koska pilvipalvelut ovat laajalti käytössä nykypäivänä, ja myös monet pilvipalveluidentarjoajat tarjoavat erilaisia identiteetin- ja pääsynhallinnan ratkaisuja organisaatioille, joten tutkimuksessa koettiin olennaiseksi kartoittaa myös pilvipohjaisen identiteetin- ja pääsynhallinnan ratkaisun mahdollisia riskejä ja ongelmakohtia. Kirjallisuuskatsauksessa kuitenkin käsiteltiin yleisellä tasolla verkkoon kytkettyjen ratkaisuiden riskejä.

Esitettävät riskiteemat ovat: manuaalityön riskit, hajautuneisuudesta johtuvat riskit, pilvipalveluihin liittyvät riskit, keskitetyn identiteetin- ja pääsynhallinnan riskit, automaation riskit sekä organisaation sisäiset riskit. Tulokset käydään läpi asiantuntijaryhmittäin aiemmin jaetun mukaan: tietohallinnon asiantuntijat, identiteetin- ja pääsynhallinnan asiantuntijat ja sisäisen tietoturvan asiantuntijat. Tulokset on esitetty taulukoissa teemoittain aina teeman lopussa. Liitteessä 2 on koonti kaikista tämän luvun taulukoista.

Analyysin tulosten läpikäynnissä esitellään suoria otteita haastateltujen henkilöiden tarkistamista haastatteluaineistoista. Haastatteluotteissa näkyvät huomiot sulkujen sisällä ovat tutkijan lisäämiä tarkentavia huomioita, jotta kokonaisuus olisi mahdollisimman ymmärrettävä.

5.1 Manuaalityö

Tietohallinto
Tietohallinnon yksikön henkilöiden haastatteluissa nousi esiin yhtenä suurena teemana manuaalisen työn riskit. Kohdeorganisaatiossa identiteetin- ja pääsynhallinta toteutetaan tällä hetkellä suurilta osin manuaalisesti, joten haastateltavat tunnistivat siitä useita erilaisia ongelmia ja uhkakuvia. Haastateltavat kuvasivat manuaalisen työn riskeiksi pienet virheet, kuten kirjoitusvirheet ja niiden tuomat ongelmat prosesseissa sekä yleisesti suuren virheiden mahdollisuuden ja virheiden epäorganisoidun korjailun myöhemmin.

> Kun on tehty manuaalisesti, se sisältää myös paljon riskejä, esimerkiksi että annetaan vahingossa vääriä oikeuksia ja sitten niitä korjaillaan ja annetaan vain lisää oikeuksia, mutta poistetaanko niitä virheellisiä oikeuksia miten. Toiminta ei ole kauhean selkeää, eikä ainakaan automatisoitua. (Tietohallinto 3)

> Manuaalinen työ on ehkä aavistuksen kyseenalaista, koska siinä on aina inhimillisen erehdyksen mahdollisuus. (Tietohallinto 2)

Muita manuaaliseen työhön liittyviä riskejä haastateltavat tunnistivat prosessien hitauden ja kankeuden, työmäärän sekä jatkokehitysmahdollisuuksien rajallisuuden. Haastattelussa ilmeni, ettei manuaalisesti toteutetussa identiteetin- ja pääsynhallinnassa ollut kovin laajoja kehitysmahdollisuuksia tai erityisominaisuuksia verrattuna muihin organisaatioihin. Identiteetin- ja pääsynhallinnan prosessit on toteutettu kohdeorganisaatiossa lähes kokonaan manuaalisesti, joka teettää organisaatiossa merkittävästi työtä ja on kankea. Viestintää pääsynhallintaan liittyen, kuten käyttöoikeuksien hakemista, tehdään esimerkiksi yksittäisten henkilöiden sähköpostiin, jolloin käyttöoikeudet ovat tämän yhden henkilön varassa.

Identiteetin- ja pääsynhallinnan asiantuntijat
Identiteetin- ja pääsynhallinnan asiantuntijat kiinnittivät haastattelussa myös huomiota manuaalisen työn riskeihin. Asiantuntijoiden mukaan mitä enemmän identiteetin- ja pääsynhallinnan prosesseissa on mukana manuaalista työtä, sitä enemmän on erilaisia virheen mahdollisuuksia ja sattuu vahinkoja. Manuaalinen työ on haastavaa ja altistaa organisaation identiteetin- ja pääsynhallinnan eri tasoisille virheille ja tietoturvariskeille.

> Paljon manuaalista työtä, joka tietysti aina altistaa virheille, joita ilmenee, kun ihminen tekee nämä työt ja prosessit. Ehkä se manuaalisuus on isoin juttu, joka varmasti altistaa virheille. (Asiantuntija 3)

> Jos kyseessä on sellainen järjestelmä, jossa käyttäjät itse tai heidän esimiehensä hakevat oikeuksia, niin silloin on se ongelma, jos oikeudet on jonkin manuaalisen prosessin takana, jossa joku päättää saako henkilö oikeuden vai ei, niin siinä voi aina tapahtua virheitä, esimerkiksi joku antaa henkilölle oikeuden, jota tämän ei pitäisi saada. (Asiantuntija 2)

> Ihan ensimmäisenä tulee mieleen tuo manuaalinen työ, siinä on aina inhimillinen riski. Eli tekee jotain väärin tai antaa jotain väärin ja parhaimmillaan saattaa näkyä virheellistä tietoa järjestelmässä. Manuaalinen työ on aina yksi heikko kohta. Merkittävästi manuaalista työtä ei koskaan ole hyvä, mitä enemmän saadaan automatisoitua, sen parempi. (Asiantuntija 2)

Toisena suurena teemana manuaalisen työn riskeinä oli sen tehottomuus ja työmäärä. Asiantuntijoiden mukaan kohdeorganisaation nykyinen identiteetin- ja pääsynhallinnan toteutus vaikuttaa työläältä ylläpitää, minkä lisäksi se on ainakin osittain vanhentunut ratkaisu. Haastatteluissa nousi esiin automaatio potentiaalisena ratkaisuna prosessien tehostamiselle.

> Nykyinen on niin hajallaan ja manuaalista, niin siihen varmasti kuluu paljon työaikaa, joka voitaisiin käyttää tehokkaammin. (Asiantuntija 1)

> Se (automaatio) edistäisi virheiden vähentymistä ja nopeuttaisi prosessia. (Asiantuntija 3)

> Varsinainen tekeminen on käsityötä, jos saisi hieman automatisoitua niin olisi varmasti huomattavasti tehokkaampaa ja järkevämpää työajan käyttöä sen osalta. (Asiantuntija 1)

Sisäinen tietoturva

Sisäisen tietoturvan henkilöiden haastatteluissa manuaalisen työn riskeinä havaittiin tehoton ajankäyttö ja työläs ylläpito. Haastateltavan mukaan Service Desk voitaisiin siirtää tekemään strategisempia tehtäviä tavanomaisten prosessien toteuttamisen sijaan, koska tällaiset prosessit voidaan teknologian avulla toteuttaa automaattisesti. Lisäksi manuaalisen työn riskeinä nähtiin ihmisen tekemät prosessit, joissa voi tulla virheitä. Myös kohdeorganisaation prosessien hitaus lisäoikeuksien saamisessa nousi esiin haastatteluissa. Taulukkoon 5 on koottu manuaalisen työn riskejä, jotka tunnistettiin kohdeorganisaation haastatteluissa.

Taulukko 5 Manuaalisen työn aiheuttamat riskit identiteetin- ja pääsynhallinnassa

Riski	**Esiintyi haastatteluissa yht.**	**Tietohallinto**	**Identiteetin- ja pääsynhallinnan asiantuntijat**	**Sisäinen tietoturva**
Prosessien hitaus ja kankeus	9	X	X	X
Työläys	9	X	X	X
Tehottomuus	9	X	X	X
Inhimilliset virheet	7	X	X	X
Jatkokehitysmahdollisuuksien rajallisuus	2	X		

5.2 Hajautuneisuus

Tietohallinto
Hajautuneisuus nousi esiin yhtenä merkittävänä kokonaisuutena tutkimuksessa, ja siitä seuraavat riskit. Haastateltavien mukaan identiteetin- ja pääsynhallintaan liittyvä suurempi riskikokonaisuus on sen hajautuneisuus, esimerkiksi useiden eri järjestelmien, joihin on erillisiä käyttäjätunnuksia ja sen seurauksena kokonaisuus on hajallaan ja haastava hallinnoida.

Kohdeorganisaatiossa on tällä hetkellä hajautunut identiteetin- ja pääsynhallinta, jonka seurauksena kokonaisvaltainen näkyvyys käyttäjien identiteetteihin ja oikeuksiin puuttuu. Käyttäjien oikeudet ovat hajallaan eri järjestelmissä, eikä niihin ole tarjolla keskitettyä näkymää. Tämän takia oikeuksien auditoiminen on hyvin haastavaa, ellei jopa mahdotonta.

Auditointikyvykkyyden puutteellisuuden vuoksi käyttäjillä voi olla virheellisiä oikeuksia. Käyttöoikeudet voivat olla vanhentuneet käyttäjän sisäisten tehtävämuutosten vuoksi, koska tehtävämuutosten seurauksena tapahtuvat käyttöoikeusmuutokset ovat manuaalisen työn varassa, eikä siihen ole tarkkaan määriteltyä prosessia.

> Kun katselmointi on oikeastaan aika hankala toteuttaa, niin sitten oikeudet voi olla semmoiset mitkä ei pitäisi olla. (Tietohallinto 1)

> Lisäksi muutostilanteessa missä käyttäjän rooli organisaatiossa muuttuu, ei ole tuettu. (Tietohallinto 1)

Riskinä haastateltavat kokivat myös hajautuneisuudesta johtuvan laajan eri organisaatiojärjestelmien ja -sovellusten määrän. Suuri määrä aiheuttaa sekavuutta ja monia eri toimintatapoja, jotka taas laskevat käyttäjäkokemusta. Ongelmalliseksi koettiin erityisesti AD integroimattomat sovellukset ja niiden oikeuksien oikeellisuus hankalan ja työlään auditoinnin takia.

Identiteetin- ja pääsynhallinnan asiantuntijat
Identiteetin- ja pääsynhallinnan asiantuntijat kokivat hajautuneisuuden myös laajana riskikenttänä. Suurimpana riskinä haastateltavan mukaan on kokonaisvaltainen kokonaisuuden pirstaleisuus. Pirstaleisuuden vuoksi voi olla hankala käsittää prosesseja, ja miten ne ovat muodostuneet. Tämän seurauksena voi joitakin tehtäviä jäädä suorittamatta, koska ei muisteta mitkä tehtävät ovat automaation piirissä ja mitkä vaativat manuaalista työtä.

> Kun meillä on manuaalista työtä, jotain automatisointia, jotain tulee jostain järjestelmästä, niin se aiheuttaa sen riskitekijän, ettei me välttämättä osata huomioida tai tiedetä, mitä tapahtuu automaattisesti, joka taas aiheuttaa, että jotain oikeuksia saattaa jäädä auki, tunnuksia auki. (Asiantuntija 4)

Hankaluus ja työläys nousi esiin myös identiteetin- ja pääsynhallinnan asiantuntijoiden haastatteluissa. Identiteetin- ja pääsynhallinnan toteutuksen ollessa

hajautunut on sen hallittavuus myös haastavampaa ja työllistää organisaatiota huomattavasti enemmän kuin esimerkiksi keskitetty ratkaisu. Asiantuntijoiden mukaan hajautuneisuus vaikuttaa myös loppukäyttäjän kokemaan käyttökokemukseen negatiivisesti.

> Tämä pirstaleisuus on ehkä se suurin riski, ja sitä kautta myös aiheuttaa hallittavuuden hankaluutta tai ainakin työläyttä. (Asiantuntija 4)

> Meillä on monia järjestelmiä, niin puuttuu SSO, joka järjestelmään tulee erikseen pyytää oikeudet, voi olla erilliset tunnuksetkin, mikä hankaloittaa loppukäyttäjänäkökulmasta töitä. (Asiantuntija 4)

Identiteetin- ja pääsynhallinnan ollessa hajautunut, tarkoittaa se myös, etteivät eri organisaatiosovellukset ja -järjestelmät ole integroitu yhteen identiteettikokonaisuuteen, jolloin käyttäjillä on useita eri käyttäjätunnuksia ja salasanoja, joita heidän tulee syöttää useaan kertaan saman istunnon aikana. Asiantuntijoiden mukaan tällaisissa tilanteissa on riskinä samojen salasanojen käyttö useissa eri järjestelmissä tai liian yksinkertaisten salasanojen käyttö. Nämä tekijät laskevat organisaation tietoturvallisuutta merkittävästi ja helpottavat ulkopuolisten henkilöiden pääsyä organisaatioresursseihin.

> Voi olla tuhat eri järjestelmää, mikään niistä ei ole integroitu ja niihin mennään omilla tunnuksilla, jolloin saatetaan käyttää samaa salasanaa monessa järjestelmässä. (Asiantuntija 4)

> Jos vaihtoehtona on jokaiseen paikkaan oma salasana, niin se johtaa vain siihen, että käyttäjät helposti käyttää sitä samaa salasanaa joka paikassa tai ei muuten jaksa keksiä kovin monimutkaista salasanaa. (Asiantuntija 1)

Hajautuneisuuden seurauksena myös auditointiprosessi hankaloituu haastateltavien mukaan. Kohdeorganisaatiossa on AD integroimattomia sovelluksia, joiden auditoiminen on haastavaa ja työlästä, kuten aiemmin on mainittu. Tämän lisäksi AD integroimattomien sovellusten ja järjestelmien auditointiprosessi ylipäätään on asiantuntijoiden mielestä hieman epäselvä.

Hajautuneessa identiteetin- ja pääsynhallinnan ratkaisussa käyttöoikeuspyynnöt eivät ole keskitetty, jonka seurauksena niitä saatetaan pyytää esimerkiksi pääkäyttäjien omien sähköpostien kautta. Pääsynhallintaan liittyvä viestintä henkilöiden omissa sähköposteissa on ongelmallista, koska tällöin niiden pyytämisestä, hyväksymisestä ja antamisesta ei jää tarvittavaa auditointijälkeä myöhempää auditointia varten.

> Kun on monia eri sovelluksia, joihin on oma sisäinen käyttövaltuushallinta joka on luokkaa kysellään pääkäyttäjiltä käytävillä käyttöoikeuksia, niin silloin se keskitetty näkymä, mitä kaikkia oikeuksia kenelläkin täällä talossa on mihinkin järjestelmiin puuttuu kokonaan. Se taas muodostaa mielestäni hyvinkin ison riskin, koska ei tiedetä mitä oikeuksia kenelläkin on ja sitä kautta ei myöskään osata ehkä etsiä asioita oikeista paikoista, jos jotakin tapahtuu. (Asiantuntija 1)

> Lähinnä siis se hajautuneisuus, puuttuu keskitetty automatisoitu näkymä ja kyvykkyys käyttöoikeuksien hallintaan tällä hetkellä. (Asiantuntija 1)

Auditoimattomuuden vuoksi käyttäjillä saattaa olla virheellisiä oikeuksia tai oikeudet jäävät esimerkiksi voimaan käyttäjien lopetettua organisaatiossa. Asiantuntijoiden mukaan tämä on todella suuri riski kohdeorganisaatiolle. Poistamattomat oikeudet jäävät voimaan mahdollisesti sen takia, koska käyttöoikeuksien poiston oletetaan olevan automaation piirissä, mutta se vaatisikin manuaalisen poistamisen. Vastaavat epäselvyydet johtuvat prosessien sekavuudesta ja kokonaisvaltaisesta identiteetin- ja pääsynhallinnan hajautuneisuudesta.

> Näen riskinä vanhat työntekijät, joiden oikeudet jää roikkumaan ihan selvästi. Niitä ei ilmeisesti sitten työntekijän lopettaessa, tai en tiedä millainen prosessi oikeuksien poistamiseen on. (Asiantuntija 3)

> Sitä kautta meiltä jää paljon ehkä oikeuksia poistamatta, koska ei välttämättä huomata, ettei tämä olekaan automaation piirissä. (Asiantuntija 4)

Sisäinen tietoturva

Identiteetin- ja pääsynhallinnan hajautuneisuus nousi yhtenä suurimpana riskiteemana sisäisen tietoturvan haastatteluissa. Haastateltavien mukaan hajautuneisuus aiheuttaa merkittävää järjestelmien monimutkaisuutta, josta seuraa lukuisia erilaisia ongelmia kohdeorganisaation tietoturvalle. Yksittäisten käyttäjien käyttöoikeuksien selvittäminen on hidasta ja monimutkaista tai jopa mahdotonta. Haastateltavien mukaan ongelmia aiheuttavat erityisesti AD integroimattomat sovellukset, prosessien sekavuus ja manuaalityö.

> Jos minä haluaisin vaikka selvittää jonkun meidän työntekijän pääsyjä eri järjestelmien nyt, niin tiedän tyyliin että hänen AD kuuluu johonkin ryhmään, mutta kaikki nämä muut oikeudet hämärän peitossa. Ehkä nyt viimeisinä vuosina on tiketöity ja tavallaan jollain olla saatavissa, mutta se on semmoista tilkkutäkkiä kasaamista. (Tietoturva 3)

Kysymyksiä herätti myös kohdeorganisaation nykyinen identiteetin- ja pääsynhallinnan ratkaisu, joka on hyvin laajalle hajautunut ja monimutkainen. Haastatteluissa on tullut ilmi kohdeorganisaation pyrkivän identiteetin- ja pääsynhallinnan uudistuksella keskitettyyn hallintaan sen tuomien lukuisien etujen vuoksi. Haastateltavat kuitenkin kokivat merkittävänä haasteena nykyisen ratkaisun kyvykkyydet keskittämisen suhteen, jotka ovat rajalliset.

> Varmaan yksi iso haaste meillä on, kun on monia eri järjestelmiä, erilaisia SaaS-ratkaisuja ja vastaavia, että se tuleva ratkaisu, saadaanko näitä kaikkia niputettua sen piiriin. Isoin haaste tällä hetkellä on, että on niin monta eri järjestelmää jotka ei ole meidän keskitetyssä hallinnassa. (Tietoturva 3)

Haastateltavat kokivat hajautuneisuudesta johtuvana ongelmana salasanojen heikkouden. Hajautetussa identiteetin- ja pääsynhallinnan ratkaisussa on haastavaa ylläpitää yhtenäistä salasanapolitiikkaa, koska se tulisi erikseen jokaiseen

erilliseen järjestelmään määritellä ja niiden tulisi olla jollain tavalla yhtenäisessä verkossa, jotta niiden noudattaminen voidaan varmentaa. Haastateltavien mukaan tällä hetkellä kohdeorganisaatiossa ei voida varmistua organisaation salasanapolitiikan noudattamisesta kaikissa laitteissa ja järjestelmissä juuri hajautuneisuuden vuoksi, mikä taas on merkittävä riski.

> Ja miten voimme varmistaa, että kaikissa meidän laitteissa ja järjestelmissä toteutuu meidän salasanapolitiikat? Ei mitenkään, käymättä niitä kaikkia käsin läpi ja se taas on hommana aivan mahdoton. (Tietoturva 2)

> Melko varmasti meillä löytyy sellaisia laitteita ja järjestelmiä, joissa ei ole salasanoja vaihdettu ehkä koskaan. (Tietoturva 2)

Hajautuneisuuden takia haastateltavien mukaan käyttäjien oikeuksien auditointi on melko mahdotonta. Hajautuneisuuden takia oikeuksien ei pystytä katselmoimaan yhdestä järjestelmästä, vaan ne tulisi katselmoida erikseen jokaisesta yksittäisestä järjestelmästä, mikä taas aiheuttaa merkittävästi työtä näiden järjestelmien ja sovellusten pääkäyttäjille. Haastateltavien mukaan kohdeorganisaatiossa ei tällä hetkellä ole varmuutta kaikista käyttäjien oikeuksista eri organisaatiojärjestelmiin ja -sovelluksiin, jotka eivät ole AD-integroituja. AD tarjoaa keskitetyn näkymän sen alaisten sovellusten käyttöoikeuksiin.

> Kyllähän se niin on, ettei meillä ole ihan tarkkaa tietoa siitä nyt ole kuka pääsee mihinkin ja niin edelleen. (Tietoturva 2)

> Puuttuu tavallaan se näkyvyys AD:n ulkopuolella, että mitä siellä tapahtuu. Eli tavallaan jos sanoisin näin, että neljäsosa järjestelmistä ja laitteista on piilossa, koska ei nähdä AD:sta mitä siellä tapahtuu. (Tietoturva 2)

Maineriski nousi esiin sisäisen tietoturvan haastatteluissa. Haastateltavat kokivat riskiksi sen, miten heidän nykyiset ja potentiaaliset asiakkaat näkisivät nykyisen identiteetin- ja pääsynhallinnan toteutuksen. Tämä onkin yksi merkittävä syy, jonka takia identiteetin- ja pääsynhallinnan uudistukseen on päätetty lähteä.

> Ylipäänsä hallittavuus kärsii, mikä on yksi suuri riski mitä näkisin tai se miten me näyttäydytään asiakkaalle se on ehkä yksi iso riski. (Tietoturva 3)

Virheelliset oikeudet ovat myös sisäisen tietoturvan haastateltavien mukaan merkittävä riski ja ongelma hajautuneessa identiteetin- ja pääsynhallinnan ratkaisussa. Monimutkaisuuden ja hajautuneisuuden vuoksi auditointi on hankalaa, ellei mahdotonta, jolloin on haastavaa selvittää, millaiset oikeudet jollakin käyttäjällä on tällä hetkellä. Koska käyttäjien oikeuksia ei pystytä todentamaan, voi heillä mahdollisesti olla virheelliset, kuten vanhentuneet tai liian laajat käyttöoikeudet. Erityisen suurena riskinä haastateltavat näkivät kohdeorganisaation ulkopuoliset tahot, joille on jääneet oikeudet voimaan.

> Se altistaa pienille riskeille tai vähän isommillekin riskeille, että me ei voida sitä verifioida, että onko oikeudet tosiaan ajan tasalla vai ei. (Tietoturva 3)

> Yksi on tosiaan tuo, että oikeudet jää voimaan. Pahin tapaus olisi, jos se on joku ulkopuolinen taho, jolla on vaikka joku ylläpito-oikeus meidän järjestelmiimme, operatiivisiin järjestelmiin ja sitä kautta tietoon. Se on yksi iso riski. (Tietoturva 3)

Haastateltavien mukaan kohdeorganisaatiossa tällä hetkellä ongelmana on tehtävämuutosten seurauksena tapahtuva käyttöoikeuksien päivitys tai sen puute. Tehtävämuutoksissa henkilön vanhat käyttöoikeudet saattavat jäädä voimaan, koska ne tulisi erikseen muuttaa tai poistaa jokaisesta eri järjestelmästä keskitetyn järjestelmän puuttumisen vuoksi. Lisäksi on mahdotonta nähdä mihin ja millaiset oikeudet käyttäjällä on, koska ei ole tarjolla keskitettyä näkymää, josta tämän voisi tarkistaa. Pahimmassa tapauksessa käyttäjä voi saada kaksinkertaiset oikeudet tehtävämuutoksen seurauksena. Taulukkoon 6 on koottu haastatteluissa esiintyneitä hajautuneisuuden aiheuttamia riskejä organisaatioiden identiteetin- ja pääsynhallinnalle.

> Tehtävämuutoksia vastaavat oikeudet jää päivittämättä, jonka seurauksena henkilö pääsee sellaisiin tietoihin mihin hänen ei pitäisi päästä. (Tietoturva 3)

> Jos henkilö vaihtaa tehtävään x, on aika epätodennäköistä että saadaan jokaista paikasta oikeudet päivitettyä. (Tietoturva 3)

> Jos ajatellaan esimerkiksi tämä tilanne, että ihminen vaihtaa osastolta toiselle niin miten me varmistetaan se, että ei saada yhtäkkiä ns. kaksinkertaisia oikeuksia, eli oikeuksia molempien osastojen järjestelmiin ja dataan. (Tietoturva 2)

Taulukko 6 Hajautuneisuuden aiheuttamat riskit identiteetin- ja pääsynhallinnassa

Riski	**Esiintyi haastatteluissa yht.**	**Tietohallinto**	**Identiteetin- ja pääsynhallinnan asiantuntijat**	**Sisäinen tietoturva**
Haastava hallinnoida	9	X	X	X
Virheelliset oikeudet	9	X	X	X
Sekavat ja epäselvät prosessit	9	X	X	X
Kokonaisvaltaisen näkyvyyden puute	8	X	X	X
Auditoinnin hankaluus	7	X	X	X
Suuren sovellus määrän aiheuttama sekavuus	6	X	X	X

5.3 Pilvipalvelut

Tietohallinto

Tietohallinnon haastatteluissa ei pilvipohjaisessa identiteetin- ja pääsynhallinnan ratkaisussa nähty merkittäviä riskejä tässä kohtaa. Kohdeorganisaatiolla on haastateltavan mukaan sopimukselliset asiat kunnossa pilvipalveluntarjoajan kanssa, joten ei ole nähtävissä ongelmia sinne siirtymisessä. Haastateltavien mielestä pilvessä sijaitsevassa identiteetin- ja pääsynhallinnan ratkaisussa ei ole merkittävästi eroa riskien määrässä tai laajuudessa verrattuna on-premiseen, mutta molemmissa on kuitenkin omat riskinsä.

> Olen aika sama mieltä, tai ajattelen samalla tavalla kuin on-premisestä, että pikkaisen se käytäntö muuttuu mutta ei niin oleellisesti. Tietoturva näkökulmasta ajatellen siellä on ehkä suurempi mahdollisuus tehdä vahinkoa, kuin on-premise järjestelmässä. (Tietohallinto 2)

> Totta kai voidaan listata niitä, mutta näin yleisesti ottaen en näe siinä mitään suurempia uhkia kuin mitä meillä on tällä hetkellä. Meillä on sopimukset palveluntarjoajan kanssa kunnossa, joten en näkisi siinä mitään ongelmaa, että olisimme puhtaasti pilvessä. (Tietohallinto 3)

Identiteetin- ja pääsynhallinnan asiantuntijat

Pilvipalveluiden ongelmaksi haastateltavat kokivat datan sijainnin, sen omistajuuden ja erilaisten säännösten noudattamisen. Ylipäätänsä melko perinteiset pilvipalveluihin liittyvät kysymykset puhuttivat haastatteluissa, kuten tietoturvaan, datan omistajuuteen ja tietomurtoihin liittyvät aiheet.

Asiantuntijoiden mielestä ongelmaksi voisi muodostua datan sijaitseminen pilvessä, erityisesti asiakkaiden näkökulmasta. Asiakkaat haluavat tietää missä heidän tietojaan sisältävä data fyysisesti sijaitsee, ja saako heidän tietonsa tarvittaessa kokonaan poistettua sieltä. Joillain asiakkailla saattaa olla niin voimakkaita sääntöjä palveluntarjoajilleen, että täysin pilvipohjaisen identiteetin- ja pääsynhallinnan ratkaisun käyttöönotto saattaisi vaarantaa nykyiset ja potentiaaliset uudet asiakassuhteet. Lisäksi pohdittiin, onko asiakasdatan tallentaminen pilveen kaikkien sääntelyiden mukaista ja voidaanko kolmannen osapuolen tarjoamiin palveluihin ja niiden toimivuuteen luottaa täysin.

> Se miten saadaan data tarvittaessa pois pilvestä, saako sitä mitenkään? Kuka siihen pääsee käsiksi? Missä se data sijaitsee fyysisesti. (Asiantuntija 4)

> Riskinä myös mahdollinen liiketoiminnan rajoittaminen ja regulatory compliance, eli onko se sitten kaikkien säännösten mukaista, jos meillä olisi tämmöinen ratkaisu, sen näen riskinä. Tietysti myös, jos ulkoistetaan kolmannelle osapuolelle ja internetiin, niin niihin liittyvät riskit. (Asiantuntija 3)

> Onhan siinä tietysti se, kun palvelu on ostettu jostain muualta pilvestä, niin silloin ollaan vähän sen pilven varassa, eli kuka sen palvelun tarjoaa ja onko yhteydet hyvät ja

> niin edelleen. Ehkä siinä on suurimpana pelkona se, ettei enää itse pyöritetä, jos palvelu on ostettu jostain. (Asiantuntija 2)

> Mielestäni normaalit pilvipalvelun riskit ja ongelmat on tässäkin mukana, johon tietysti lukeutuu myös se tietoturva, josta en syvällisesti osaa sanoa. (Asiantuntija 4)

> Tulee miettiä halutaanko siirtyä kokonaan pilveen, koska meillä on asiakkaita, jotka eivät halua heidän tietoja käsiteltävän siellä niin jos niin kriittinen osa-alue, kuin IAM olisi pilvessä tai kolmannen osapuolen käsissä, niin onko se ok kaikille asiakkaille. (Asiantuntija 3)

Pilvipalveluissa puhutti riskinä myös sen modifioitavuus kohdeorganisaation omiin tarpeisiin. Organisaation käytössä on runsaasti omia ja ulkopuolisten palveluntarjoajien palveluita, jolloin on olennaista miettiä uuden identiteetin- ja pääsynhallinnan integroitavuutta.

Kohdeorganisaation tavoitetilana koettiin keskitetty identiteetin- ja pääsynhallinnan ratkaisu, joka vaatii valitulta ratkaisulta pitkälle modifioitavuutta, laajasti erilaisia integraatiorajapintoja ja mahdollisuuksia, jotta sellainen voidaan saavuttaa nykyisen hajautuneen ratkaisun tilalle. Asiantuntijoiden kokemuksen mukaan pilvessä sijaitsevan identiteetin- ja pääsynhallinnan ratkaisun kanssa modifioitavuus voi muodostua ongelmaksi.

Sisäinen tietoturva

Pilvipohjaisen identiteetin- ja pääsynhallinnan ratkaisun riskiksi haastatteluissa nousi yrityksen nykyinen osaamistaso. Haastateltavan mukaan kohdeorganisaation nykyinen teknologian tuntemus ei tällä hetkellä ole sillä tasolla, että osattaisiin varautua kaikin mahdollisin keinoin pilvipalveluiden tuomiin riskeihin ja uhkakuviin. Haastateltava kuitenkin koki henkilöstön riittävän koulutuksen ja ohjeistuksen yhdessä asianmukaisten tietoturva-asetusten minimoivan useimpia pilvipohjaiseen identiteetin- ja pääsynhallintaan liittyviä riskejä. Taulukossa 7 on koottuna haastatteluissa esiintyneitä pilvipalveluiden aiheuttamia potentiaalisia riskejä organisaatioiden identiteetin- ja pääsynhallinnalle.

> Se on vähän eri tyyppinen ympäristö. Ainut iso ehkä uhka siinä voi olla se, että sen teknologian tunteminen ei ole ehkä tällä hetkellä meidän talossa niin korkealla, että se osattaisiin siihen ihan täysin kaikin keinoin varautua. Siihen maailman varmasti menee, että se vaan vaatii sitä, että henkilöstöä koulutetaan ja ohjeistetaan ja pyritään varautumaan siihen. Mutta jos se kyseinen palvelu, joka on pilvessä, on oikein konfiguroitu niin en sitä merkittävänä riskinä näkisi. Siinä pitää olla tietyt kontrollit olemassa, jotta sitten tiedetään, jos sitä joku on päässyt käymään sen kimppuun tai käyttämään hyväksi. (Tietoturva 3)

Taulukko 7 Pilvipalveluiden aiheuttamat riskit identiteetin- ja pääsynhallinnalle

Riski	Esiintyi haastatteluissa yht.	Tietohallinto	Identiteetin- ja pääsynhallinnan asiantuntijat	Sisäinen tietoturva
Tietoturva	3	X	X	
Riippuvaisuus palveluntarjoajasta	3		X	
Perinteiset pilvipalveluriskit	3		X	X
Modifioimattomuus	2		X	
Osaamisriski	1		X	
Säännösten noudattamattomuus	1		X	
Asiakkaiden menetys	1		X	

5.4 Keskitetty identiteetin- ja pääsynhallinta

Tietohallinto

Haastattelussa kartoitettiin keskitetyn identiteetin- ja pääsynhallinnan mahdollisia riskejä ja ongelmakohtia. Tietohallinnon haastatteluissa keskitetty ratkaisu nähtiin enimmäkseen positiivisena ratkaisuna, mutta myös mahdollisia ongelmakohtia nousi esiin. Pohdinnan aiheena oli täysin keskitetyn ratkaisun tietoturvallisuus, sekä se, miten mahdollisissa ongelmatilanteissa voitaisiin toimia sen ainoan järjestelmän ollessa poissa käytöstä. Pohdittaessa kohdeorganisaation identiteetin- ja pääsynhallinnan uudistusta oltiin yksimielisiä siitä, että uuden järjestelmän tulisi olla keskitetty, mutta kuitenkin riskinä nähtiin, ettei kaikkia yritysresursseja saataisi integroitua yhden identiteetin- ja pääsynhallinnan järjestelmän alle.

> Keskitetty olisi hyvä, mutta sitten taas tietoturvan kannalta en oikein osaa kommentoida, että pitäisikö mieluummin olla hajautettu. (Tietohallinto 2)

> (Uuden ratkaisun tulisi olla) Yhdestä järjestelmästä hallinnointi (keskitetty identiteetin- ja pääsynhallinnan ratkaisu), mutta varmasti aina jää jotakin (sovellukset, järjestelmät yms.) ulkopuolelle. (Tietohallinto 1)

Havaituista potentiaalisista riskeistä huolimatta keskitetty identiteetin- ja pääsynhallinta koettiin tuovan enemmän mahdollisuuksia kuin uhkakuvia kohdeorganisaatiolle, ja siihen tulisi kohdeorganisaation identiteetin- ja pääsynhallinnan uudistuksessa pyrkiä.

> Tosin jos puhutaan, että halutaan tehdä ketterästi töitä niin silloin keskitetty tietysti olisi aivan loistava. (Tietohallinto 2)

Identiteetin- ja pääsynhallinnan asiantuntijat

Identiteetin- ja pääsynhallinnan asiantuntijat tunnistivat monipuolisesti erilaisia riskejä, jotka liittyvät keskitettyyn identiteetin- ja pääsynhallintaan. Keskitetyn järjestelmän sekä hyvänä että huonona ominaisuutena koettiin sen kokonaisvaltaisuus. Virhetilanteissa ongelmat skaalautuvat laajemmalle, ja vaikuttavat kaikkiin käyttäjiin. Toisaalta taas keskitetty ratkaisu on helpommin hallittava, kuin hajautunut ratkaisu.

Haastatteluissa nousi myös esiin identiteetin- ja pääsynhallinnan ratkaisun integrointimahdollisuudet. Parhaimmillaan identiteetin- ja pääsynhallinnan ratkaisuun voidaan integroida laajasti erilaisia yritysjärjestelmiä ja -resursseja, mutta on tärkeää huomioida myös kaikki sidosryhmät identiteetin- ja pääsynhallinnan ratkaisua valitessa, jotta voidaan tarjota kaikille tyydyttävä ratkaisu.

> Jos jotain menee pahasti pieleen, sen vaikutus skaalautuu myös paljon laajemmalle kuin hajautetussa. Kyllä silti näkisin hyvien ominaisuuksien olevan paljon vahvempia kuin huonojen. Tietysti riippuu paljolti yrityksen koosta, onko keskitetty tarpeellinen vai ei. (Asiantuntija 2)

> Siinä tulee paljon positiivista, koska on keskitetty ja silloin päästään pirstaloituneisuudesta eroon, ja pitäisi silloin lähtökohtaisesti olla helpommin hallittava. Onhan tietysti aina se riski keskitetyssä missä tahansa, niin pystytäänkö sieltä tarjoamaan kaikille sidosryhmille niin tarkasti palveluita, miten he haluavat. Puhutaan sitten oikeuksien antamisesta tai integraatiorajapinnasta, niin riskinä on pystytäänkö vastaamaan kaikkien tarpeisiin tyydyttävällä tasolla. (Asiantuntija 4)

Keskitetyssä identiteetin- ja pääsynhallinnassa nähtiin myös tietoturvariskejä pääkäyttäjätunnuksien kanssa. Keskitetyssä ratkaisussa hallinnoidaan kaikkien käyttäjien identiteetit, käyttöoikeudet ja pääsyvaltuutukset kaikkiin sen alaisiin yritysresursseihin, joten admin-tunnukset omaavalla henkilöllä on silloin merkittävästi vastuuta ja valtaa niissä. Haastattelussa nostettiin tärkeänä huomiona voimakkaimpien oikeuksien valvomisen merkittävyys.

> Ne liittyy mielestäni siihen että kuka valvoo sitä valvojaa eli ketkä ovat isoimmilla oikeuksilla ja on suurimmat käyttöoikeudet itse varsinaista IAM-ratkaisua hallinnoida ja siellä toimii pääkäyttäjänä. (Asiantuntija 1)

Haastattelussa huomioitiin keskitetyn ratkaisun ja pilvipalveluiden kombinaation ongelmallisuus. Kohdeorganisaatiossa käsitellään merkittävää määrää asiakkaiden sensitiivistä dataa, jolloin myös asiakkailla on voimakkaita vaatimuksia asiantuntijaorganisaatiolleen. Kohdeorganisaation asiakkaat eivät välttämättä halua heihin liittyvää dokumentaatiota ja muita resursseja käsiteltävän pilvessä, jolloin täysin keskitetty pilvipohjainen identiteetin- ja pääsynhallinta ratkaisu nousisi ongelmaksi sopimusneuvotteluissa. Riskinä tällaisessa tilanteessa voisi olla sopimusneuvotteluiden pysähtyminen ja asiakassuhteen menetys nykyisten sekä uusien potentiaalisten asiakkaiden kanssa.

> Lähinnä liittyy enemmän siihen, jos ratkaisu on pilvessä, niin siinä näen ongelmia. Näen riskin pilviratkaisussa, mutta jos ei ole pilvessä ja on keskitetty, niin en näe sii-

> nä ongelmia. Tietysti sekin voi sisältää joitain ongelmia, esimerkiksi jos joku asiakas ei halua tehdä yhteistyötä, koska meidän identiteetin- ja pääsynhallinta on hallittu keskitetysti, ja sitä kautta voitaisiin päästä heidän tietoihin. Kuitenkin isoimmat riskin näen pilviratkaisussa. (Asiantuntija 3)

> Jos kyseessä on keskitetty ratkaisu, joka sijaitsee pilvessä, niin riskinä on nykyisten tai potentiaalisten asiakkaiden, jotka ei halua tietojaan käsiteltävän pilvessä mahdollinen menettäminen. (Asiantuntija 3)

Sisäinen tietoturva

Sisäisessä tietoturvassa keskitetty identiteetin- ja pääsynhallinta nähtiin positiivisena asiana kohdeorganisaatiolle, eikä potentiaalisiin riskeihin osattu tässä vaiheessa ottaa kantaa. Yhtenä potentiaalisena riskinä nousi esiin puutteellinen suojaus järjestelmässä, mikä voisi aiheuttaa tietoturvariskejä ja -vuotoja kohdeorganisaatiolle. Ratkaisuna tähän riskiin kuitenkin koettiin keskitetyn ratkaisun välttämisen sijaan huolellinen valmistautuminen järjestelmän suunnittelussa ja käyttöönotossa.

> Ainut on tuo, että jos jostain paikasta se olisi vaikka puutteellisesti suojattu. Sitä voisi käyttää myös väärin tarkoituksen tai sitä kautta voisi koittaa elevoida oikeuksia jollain tavalla, mutta enemmän näkisin, että siihen liittyy, että se pohjatyö pitää tehdä kunnolla ja hallinnoida tuota riskiä. Näkisin enemmän positiivisia asioita kuin mahdollista riskiä. (Tietoturva 3)

> On siinä varmasti riskejä, mutten lähde tällä hetkellä pohtimaan, koska ne taas riippuvat siitä, mitä ratkaisu valitaan ja riskien arviointi on siinä kohtaa ajankohtaista. Jokaisessa uudessa järjestelmässä on riskit, ja niitä tulee käytännössä minimoida. Jos riski eskaloituu, tulee jäljet korjata mahdollisimman hyvin, ja otetaan opiksi tehdyistä virheistä. (Tietoturva 1)

Identiteetin- ja pääsynhallinnan asiantuntijan haastattelussa jo esiinnoussut keskitetyn identiteetin- ja pääsynhallinnan ja pilvipalveluiden kombinaatio sai huomiota myös sisäisen tietoturvan asiantuntijan haastattelussa. Haastateltava pohti aiheuttaisiko uniikki, yksittäinen pilvessä sijaitseva identiteetti ongelmia kohdeorganisaatiolle, muttei vielä osannut ottaa siihen näillä tiedoilla kantaa. Taulukossa 8 on koottuna kaikki haastattelututkimuksessa esiintyneet keskitettyyn identiteetin- ja pääsynhallintaan potentiaalisesti liittyvät riskit organisaatiokontekstissa.

> Mutta onko se meille merkittävä riski, jos meillä olisi yksi ainoa identiteetti, jota säilytettäisiin jossain pilvessä, niin se varmaan täytyy jättää myöhempään pohdintaan, siihen en osaa nyt heti ottaa lopullista kantaa. (Tietoturva 2)

Taulukko 8 Keskitetyn identiteetin- ja pääsynhallinnan aiheuttamat riskit

Riski	Esiintyi haastatteluissa yht.	Tietohallinto	Identiteetin- ja pääsynhallinnan asiantuntijat	Sisäinen tietoturva
Riippuvaisuus yhdestä sovelluksesta tai järjestelmästä	5	X	X	X
Sisäpiirin hyökkäykset	3		X	X
Kustannukset	3		X	X
Tietoturva	2	X		X
Laajalle skaalautuvat ongelmat	2	X	X	
Haastava implementointi	2	X	X	

5.5 Automaatio

Tietohallinto

Haastatteluissa kartoitettiin automaatioon liittyviä riskejä, joita kohdeorganisaation haastateltavat tunnistivat. Automaatio nousi kirjallisuudessa vahvasti identiteetin- ja pääsynhallintaan liittyväksi osa-alueeksi ja onnistuneen ratkaisun tavoitetilaksi. Tietohallinnon haastateltavat tunnistivat riskiksi automaation, jolle ei anneta enää huomiota sen rakentamisen jälkeen. Vuosien kuluessa automaatiota tulee kehittää ja varmistaa sen toimivuus.

> Totta kai, se ei ole prosessi, että tehtiin automaatio ja annetaan pyöriä viisi vuotta, vaan se vaatii jatkuvasti työtä, selvitystä ja varmistusta, että asiat menee oikein. (Tietohallinto 3)

Toinen haastatteluissa tunnistettu riski oli virheellisesti rakennettu automaatio, jonka seurauksena käyttäjille myönnettäisiin liian suuria oikeuksia. Haastatteluissa nousi myös riskiksi automaation tuntemuksen puutteellisuus sekä se, voisiko prosessin väliin tarvittaessa mennä tai voisiko edes tietää missä vaiheessa automaatioprosessi missäkin vaiheessa menee. Verrattuna manuaaliseen ihmisen tekemään prosessiin saattaisi olla hankalampaa seurata prosessin etenemistä.

> Ainut mikä tulee mieleeni voisi olla joku semmoinen, jos sen asian statusta on hankalaa esimerkiksi tietää, että missä vaiheessa se menee. Tavallaan siis ihminen ihmiselle kontaktissa pitäisi voida selvittää, missä vaiheessa esimerkiksi oikeuspyyntö on. Olisi hyvä olla ominaisuutena tällainen, tai ainakin vähintään tiedossa kuinka kauan jokin prosessi kestää, jotta pystytään loppukäyttäjää informoimaan, eikä tarvitse sanoa ”en tiedä”. (Tietohallinto 1)

> Silloin se automaatiopuoli pitäisi tuntea ainakin niiltä osin, että mitä se tekee. Ja sitten kun tulee jokin muutostilanne, niin se pitää sitten muistaa ja osata hoitaa se muutos tai sitten tehdä tiketti automaatioryhmälle. (Tietohallinto 2)

Suurilta osin haastateltavat kuitenkin näkivät automaation positiivisena asiana, ja enemmänkin tavoitetilana kuin riskikenttänä. Haastateltavat kuitenkin tunnistivat automatisoituun identiteetin- ja pääsynhallintaan liittyviä riskejä. Automaation hyvinä ominaisuuksina mainittiin prosessien nopeutuminen ja inhimillisen virheen poistaminen.

> En nyt ehkä haittaa näkisi, koska se tekee juuri sen mitä siltä pyydetään kun puhutaan automaatista. (Tietohallinto 2)

> On helppo saada oikeuksia, vaikka niin helppoa että ne voidaan antaa viiden minuutin tai minuutin sisään kun tarvitsee, mutta pitää olla keino auditoida ja varmistaa, ettei anneta liikaa ja että hyväksynnät ovat oikein jne. Se on jatkuvaa prosessien kehittämistä ja mietintää. (Tietohallinto 3)

> Ehkä simppeleimmät asiat voisi automatisoida ja joissa on ehkä eniten mahdollisuuksia tämmöiseen inhimilliseen virheeseen, kuten typojuttuja tai muuta vastaavaa. (Tietohallinto 2)

Identiteetin- ja pääsynhallinnan asiantuntijat

Haastateltavat tunnistivat automaatioon liittyviä riskejä laajasti liittyen sen takana olevaan prosessiin. Identiteetin- ja pääsynhallinnan asiantuntijoiden mukaan automaation taustalla oleva prosessi on tunnettava todella hyvin ja määrittely tehtävä tarkasti, koska automaatio vaatii taustalleen prosessin, joka on tarkoin määritelty ja tunnetaan, jotta voidaan taata haluttu lopputulema.

Prosessien joustamattomuus nousi myös automaation kohdalla haastatteluissa tunnistettuihin identiteetin- ja pääsynhallinnan riskeihin. Asiantuntijoita mietitytti järjestelmän automaatioprosessien muokkaaminen tarvittaessa, ja se olisiko modifioimien välttämättä edes mahdollista. Pohdiskelua aiheutti myös kaikki mahdolliset poikkeustapaukset, että voidaanko koskaan edes saada täysin automatisoitua ratkaisua.

> Ongelma tai haaste siinä on ehkä se, että meidän pitää pystyä määrittelemään se prosessi siten, että se pystytään automatisoimaan. Meidän täytyy ymmärtää mitä tarvitaan missäkin vaiheessa, mitkä niiden vaikutukset on kokonaisuuden kannalta ja niistä päästään ehkä mahdolliseen haittaan. (Asiantuntija 4)

> Tuli mieleen mahdollinen joustamattomuus, tai jos on jotakin poikkeustapauksia, niin miten nopeasti ja ketterästi ne pystytään ratkaisemaan, jos on todella pitkälle automatisoitu ratkaisu. Ja onko meillä tarpeita, jotka vaatisivat enemmän tilannekohtaista pohdintaa. (Asiantuntija 3)

Yhtenä riskinä nousi myös automatisoidun ratkaisun yhteiskustannukset. Haastateltavan mukaan mitä pidemmälle identiteetin- ja pääsynhallinnan ratkaisu on automatisoitu, sitä kalliimmaksi se tulee ylläpidon ja huollon osalta ja vaatii kohdeorganisaatiolta enemmän ajallisia ja rahallisia resursseja.

Automaatioon liittyväksi riskiksi identiteetin- ja pääsynhallinnassa nousi haastatteluissa virheiden mahdollisuus. Automatisoidussa prosessissa virheitä voi tapahtuma huomaamatta, koska siinä ei olla ihmisen kanssa kontaktissa. Virheet myös helpommin moninkertaistuvat, mikäli niitä ei huomata nopeasti. Virheiden minimointi vaatii jatkuvaa monitorointia ja prosessien seuraamista. Automaatio poistaa inhimilliset virheet, mutta voi aiheuttaa erilaisia järjestelmävirheitä. Tämän lisäksi automaation aiheuttamia virheitä pidemmältä aikaväliltä voi olla hyvin hidasta ja työlästä korjata myöhemmin.

> Tietysti automaatiossa voi tapahtua myös sellaisia huomaamattomia virheitä helposti. Jos joku automaatiossa menee rikki, voi vahingossa olla, ettei viikon tai kuukauden aikana kukaan saa uusia oikeuksia, ja jos siinä ei ole mitään manuaalista backuppia, se voi aiheuttaa ongelmia. (Asiantuntija 2)

> Automaatio muuttaa inhimilliset virheet järjestelmävirheiksi. (Asiantuntija 2)

> Ehkä riskit liittyy siihen, jos järjestelmä tekee mitä sen on kerrottu, niin jos siinä on tapahtunut jotakin virheitä, miten se on määritelty toimivan. Silloin tietysti ne vahingot kertautuu, koska jokaista käyttöoikeuden provisiointia tai myöntämistä ei ole ihminen aina erikseen katsomassa, vaan järjestelmä tekee mitä sen on prosessiin kuvattu tekevän. Jos prosessi itsessään on viallinen, niin silloin nopeasti tapahtuu useampi virhe kerrallaan. (Asiantuntija 1)

Sisäinen tietoturva

Sisäisen tietoturvan haastatteluissa haastateltavat tunnistivat automaation riskeiksi automaation virheellisen määrittelyn. Virheellisesti määritellyt automaatioprosessit aiheuttavat ylimääräistä manuaalityötä ja selvitystä ja lisäävät riskien määrää organisaatiossa. Lisäksi nostettiin esiin jälleen poikkeustapaukset, ja se pystyykö automaatio kattamaan aivan kaikki mahdolliset identiteetin- ja pääsynhallinnan skenaariot.

> Jos automaatio pettää, niin siinä tapauksessa olemme aikamoisessa suossa. Jos automaatio on väärin määritelty, se saattaa olla riski. Kaikki mitä tehdään väärin on riski. Siinä vaiheessa kun automatiikka pettää, meidän käsihommat räjähtää käsiin. Onhan se mahdollinen haitta ja riski. (Tietoturva 1)

> Minulla ei ole hirveästi tuosta omakohtaista kokemusta, mutta kyllä varmasti on vaikea tehdä semmoista automatisointia, joka pätee ihan kaikkeen. (Tietoturva 3)

Tietoturvan asiantuntijat kokivat riskiksi automaatiot, jotka rapauttavat kohdeorganisaation tietoturvaa. Kun mietittiin mahdollisuutta myöntää käyttäjille hetkellisesti voimakkaammat oikeudet erilaisten tilannetekijöiden perusteella, voi olla uhkana niiden myöntäminen liian kevyin perustein. Jos esimerkiksi admin-oikeuksien saamiselle hetkellisesti riittää tietoturvapäivitysten asentaminen ja organisaation omassa verkossa työskentely, on uhkana erilaiset tahalliset ja tahattomat sisäpiirin riskit, kuten haittaohjelmien asentaminen.

Haastateltavien mukaan automaatio vaatii erilaisia kontrolleja ja monitorointeja, joilla varmistetaan automaatioiden säännösten mukaisuus. Haastatel-

tavan mukaan kohdeorganisaation identiteetin- ja pääsynhallinnasta tulisi olla vastuussa useampi ihminen, esimerkiksi jokin ennalta määritelty tiimi, jotta voidaan varmistua automaatioiden tekevän niille määritellyt tehtävät tietoturvallisesti. Lisäksi tietojen kahdentaminen useampaan tietokohteeseen oli toivottavaa, jotta mahdollisiin virheisiin voidaan reagoida nopeammin ja helpommin. Taulukkoon yhdeksän on koottu kaikki haastatteluissa esiintyneet automaatioon liittyvät potentiaaliset riskit organisaatioiden identiteetin- ja pääsynhallinnassa.

Taulukko 9 Automaation aiheuttamat riskit identiteetin- ja pääsynhallinnalle

Riski	**Esiintyi haastatteluissa yht.**	**Tietohallinto**	**Identiteetin- ja pääsynhallinnan asiantuntijat**	**Sisäinen tietoturva**
Prosessien joustamattomuus ja poikkeustapaukset	7	X	X	X
Virheellinen toteutus	6	X	X	X
Huoleton ylläpito	6	X	X	X
Osaamisriski	4	X	X	X
Järjestelmävirheet	4		X	X
Kustannukset	1		X	

5.6 Organisaation sisäiset riskit

Tietohallinto

Haastatteluissa nousi esiin erilaisia organisaation sisäisiä riskejä identiteetin- ja pääsynhallinnalle. Perinteisiä teknologiaan liittyviä riskejä koettiin myös identiteetin- ja pääsynhallintaan liittyen, kuten muutosvastaisuus ja osaamisriski. Haastateltavan mukaan aina kun ollaan tekemisissä uusien teknologioiden kanssa käyttäjien tunteet tulevat mukaan, ja niihin tulisi osata varautua ennakkoon mahdollisimman perusteellisesti.

Osaamisriskin kohdalla haluttiin poistaa nykyisin kohdeorganisaatiossa vallitseva tilanne, jossa erityisesti pääsynhallintaan liittyvät työtehtävät ja prosessit henkilöityvät vahvasti tiettyihin henkilöihin. Tulevaisuudessa ei haluta sellaisia prosesseja tai toimintoja, jotka ovat hyvin vahvasti yhden henkilön osaamisen varassa.

Organisaation sisäisinä riskeinä haastateltavat tunnistavat myös erilaiset tahalliset ja tahattomat sisäpiirin hyökkäykset. Kohdeorganisaatiossa käyttäjä kykenee tällä hetkellä asentamaan joitakin organisaation hyväksymättömiä sovelluksia, mutta niiden asennuksia monitoroidaan säännöllisesti.

Toisena sisäpiirin hyökkäyksiin liittyväksi ongelmaksi tunnistettiin SSO eli kertakirjautuminen, joka tarkoittaa hyvin pitkälle integroituna, ettei käyttäjän tarvitse syöttää käyttäjätunnustaan tai salasanaan enää tietokoneelleen si-

säänkirjautumisen jälkeen mihinkään organisaatiojärjestelmään tai -resurssiin, mihin hänen käyttöoikeudet riittävät.

> Se on vähän sekä että, eli mitä pidemmälle yhdellä salasanalla pääsee järjestelmiin sisälle, niin sen helpompi on ikään kuin päästä väärinkäyttämään tiettyjä oikeuksia. (Tietohallinto 2)

> Esimerkiksi jos läppäri varastetaan ja se saadaan hakkeroitua auki, niin sitten on ns. valtatie auki kaikkeen. Eli kyllä se hieman ongelmallinen on. (Tietohallinto 2)

Pitkälle integroitu kertakirjautuminen koettiin haastatteluissa ongelmalliseksi mahdollisissa laitteiden varkaustilanteissa. Jos kohdeorganisaation omistama laite pääsee sellaisiin käsiin, johon ei kuuluisi päästä ja salasana joko onnistutaan murtamaan tai laite on jäänyt sisäänkirjautuneeksi, pääsee sen avulla käsiksi hyvin laajasti erilaisiin organisaatioresursseihin ja -järjestelmiin. Tällaisessa tilanteessa pitkälle integroitu kertakirjautuminen koettiin hyvin ongelmalliseksi.

Identiteetin- ja pääsynhallinnan asiantuntijat

Muutosvastaisuus nousi esiin riskinä myös identiteetin- ja pääsynhallinnan asiantuntijoiden haastatteluissa. Muutosjohtamisen ja -viestinnän tärkeys nousee haastateltavan mukaan hyvin tärkeään asemaan organisaatioiden identiteetin- ja pääsynhallinnan uudistuksissa.

Uudistusten tärkeys tulee saada selvitettyä organisaation johtohenkilöstölle, jotta varmistetaan identiteetin- ja pääsynhallinnan uudistusten onnistuminen. Identiteetin- ja pääsynhallinnan ratkaisuiden uudistukset ovat yleensä arvokkaita investointeja organisaatioissa, ja riskinä koetaan niiden laajojen mahdollisuuksien hyödyntämättä jättäminen, ellei saada käyttöönottoa onnistumaan ja järjestelmää integroitua organisaatiokulttuuriin.

> Eli teknologiaa ei hyödynnetä niin laajasti mihin olisi mahdollisuus vaan mennään siihen tilanteeseen, jossa osa käyttää ja osa ei ja osaa ei kiinnosta käyttää. Se että saadaan koko talo sitoutettua uuden ratkaisun hyödyntämiseen ja käyttämiseen on mielestäni keskeinen asia ja siihen liittyy keskeisimmät riskitkin. Ei tehdä sellaista investointia, jossa on hienot ominaisuudet ja mahtavat teknologiset ratkaisut, mutta sitten kukaan ei käytä niitä. Se on mielestäni iso mörkö taustalla. (Asiantuntija 1)

Toisena muutosvastaisuuteen liittyvänä riskinä haastateltavat tunnistivat muiden organisaatioryhmien osallistumisen puutteen. Haastateltavien mukaan onnistunut identiteetin- ja pääsynhallinnan uudistusprojekti vaatii tukea ja osallistumista laajasti erilaisilta organisaatioryhmiltä. Identiteetin- ja pääsynhallinnan ratkaisuiden uudistukset ovat koko organisaatiota koskettavia toimintoja, jolloin jokaisen osallisen tulee ymmärtää oma vastuunsa ja osallistua vaadituissa määrin.

> Suurin riski näissä projektissa on, että ylemmiltä kerroksilta jossain kohtaa loppuu tuki tai sitä ei ole ollenkaan. Eli nähdään tämä IAM:in kehittäminen vain IT:n harjoituksena, jos asenne on tämä niin projekti ei tule onnistumaan vaan vaatii eri liiketoiminta-alueilta myös vahvaa ja aktiivista osallistumista. (Asiantuntija 1)

Identiteetin- ja pääsynhallinnan asiantuntijoiden haastatteluissa yhdeksi riskiksi havaittiin osaamisriski. Osaamisriski koettiin riskiksi useammalla tavalla. Ensinnäkin kuten tietohallinnonkin haastatteluissa ilmeni, osaamisriskiksi koettiin yhteen tai muutamaan henkilöön henkilöityvä osaaminen. Mikäli osaaminen keskittyy vain muutamaan henkilöön, tulee tästä ongelma esimerkiksi näiden henkilöiden poistuessa organisaatiosta.

Toinen osaamisriski haastateltavien mukaan on liian monimutkaisen identiteetin- ja pääsynhallinnan järjestelmän tavoittelu. Monimutkaisen järjestelmän tavoittelu hankaloittaa projektinhallintaa, koska jos halutaan toteuttaa ratkaisu jonka tulisi sisältää hyvin paljon kaikkea, aikataulu tulee venymään ja projektista tulee huomattavasti vaativampi myös hallinnoimisen kannalta. Haastateltavien mukaan identiteetin- ja pääsynhallinnan uudistusprojektit pitkittyvät, koska ei ymmärretä kokonaisuutta.

> Toinen on tietysti se, että halutaan tehdä liian hieno systeemi. Kyllä meillä on aiemmissa asiakkuuksissa suurimmat ongelmat ovat olleet, kun on haluttu todella monimutkainen prosessi. (Asiantuntija 4)

> Näen isona riskinä liian monimutkaisen järjestelmän tavoittelun. Kokemukseni mukaan mitä yksinkertaisempi järjestelmä, sen parempi. (Asiantuntija 4)

Identiteetin- ja pääsynhallinnan kokonaiskustannukset puhuttivat asiantuntijoiden haastatteluissa. Keskitetty identiteetin- ja pääsynhallinnan ratkaisu on kustannuksiltaan huomattavasti esimerkiksi kohdeorganisaatiossa tällä hetkellä olevaa hajautettua identiteetin- ja pääsynhallintaa arvokkaampi. Lisäksi mitä pidemmälle automatisoitu ratkaisu on, sitä korkeammat ovat sen kokonaiskustannukset.

Sisäpiirin hyökkäykset tunnistettiin mahdolliseksi riskiksi myös identiteetin- ja pääsynhallinnan asiantuntijoiden haastatteluissa. Riskeinä haastatteluissa nousi admin-oikeudet. Admin-oikeudet omaavalla henkilöllä on merkittävästi enemmän oikeuksia verrattuna tavalliseen käyttäjään. Tällaisten oikeuksien kanssa varustettu henkilö voi saada tahallaan tai tahattomasti paljonkin tuhoa aikaan organisaatioresursseissa. Tunnusten valvomiseen tulisi haastatteluiden mukaan olla erilaisia työkaluja ja menetelmiä, jotta väärinkäytökset minimoidaan.

> Tunnuksien ja oikeuksien valvomiseen tulee olla olemassa menetelmät ja mahdolliset työkalut, jotta siellä ei pääse tapahtumaan väärinkäytöksiä tai vahinkoja, jotka altistaisi suuremmille ongelmille. (Asiantuntija 1)

Kertakirjautuminen eli SSO koettiin liian pitkälle vietynä myös riskimahdollisuutena. Pitkälle integroitu SSO luottaa voimakkaasti siihen, että käyttäjä itse

toimii luottamuksellisesti ja vastuullisesti, eli kirjautuu aina ulos laitteeltaan, kun ei ole siinä eikä hänen tunnuksillaan pääse kirjautumaan kukaan muu kuin käyttäjä itse. Kertakirjautumisen koettiin helpottavan järjestelmien käyttöä merkittävästi, mutta sisältää omat riskinsä, joiden vuoksi vaaditaan erilaisia kyvykkyyksiä huolehtimaan organisaatioresurssien tietoturvasta.

> Siinä on se klassinen riski jos joku saa käyttäjän tunnukset tai istunnon haltuunsa, niin sitten hän pääsee joka paikkaan. Tämän takia rinnalle mielestäni olisi hyvä olla kyvykkyyksiä, mitkä pystyy myöskin valvomaan miten tunnuksia käytetään. (Asiantuntija 1)

> Tosiaan SSO on käyttöä merkittävästi helpottava asia, mutta tunnuksen joutuessa vääriin käsiin siihen liittyy omat riskinsä. (Asiantuntija 1)

Haastateltavien mukaan kuitenkaan aivan kaikkia yritysjärjestelmiä ja -resursseja ei välttämättä voida sisällyttää kertakirjautumisen piiriin, vaikka se tarjoaisi paremman käyttäjäkokemuksen. Identiteetin- ja pääsynhallintaa suunnitellessa tulee miettiä millaiset organisaatioresurssit ovat niin kriittisiä, että ne halutaan edelleen jättää erillisen kirjautumisen piiriin turvallisuuden takia.

> Varmasti ehkä tulee sellaisia asioita, joita tulee miettiä onko joku järjestelmä oikeasti niin kriittinen, ettei sinne haluta tarjota SSO. (Asiantuntija 4)

> Silloin kun puhutaan jostain hyvin kriittisistä järjestelmistä, niissä ainakin tulisi olla erilliset kirjautumiset ja lyhyet uloskirjaamisajat. Ei ihan voi mennä niin, että kerran kirjautuu sisään ja voi siellä pysyä tunteja. (Asiantuntija 2)

Haastatteluissa koettiin identiteetin- ja pääsynhallinnan yhdeksi riskiksi prosesseihin liittyvät ongelmat. Haastateltavien mukaan prosessit tulee määritellä huolellisesti, jotta vältetään niihin liittyvät ongelmat. Identiteetin- ja pääsynhallinta on osa suurempaa kokonaisuutta, joten sen prosessit tulee ymmärtää ja osata määritellä.

> Yleensä teknologia ei ole kompastuskivi vaan organisaation sisäiset toimintatavat, johon ne riskit yleensä sijoittuu. (Asiantuntija 1)

> Se on iso riski, jollei niitä (prosessien määrityksiä) tehdä kunnolla ollaan ongelmissa. (Asiantuntija 4)

> Riskinä on myös kokonaisprosessin ymmärtämättömyys. Kun puhutaan IDM:stä tai IAM:sta niin se on vain yksi osa kokonaisprosessia ja -flowta. (Asiantuntija 4)

Sisäinen tietoturva

Haastatteluissa nousi esiin osaamisriski jälleen. Haastateltavien mukaan kohdeorganisaatiossa ei ole tällä hetkellä tarvittavaa osaamista, jotta voidaan tehdä toivotunlainen identiteetin- ja pääsynhallinnan uudistus. Kohdeorganisaation osaamistasoa tekniseltä puolelta tulisi nostaa, ennen kuin uudistukseen voidaan ryhtyä sen onnistumisen maksimoimiseksi.

Haastattelussa koettiin riskinä myös identiteetin- ja pääsynhallinnan uudistuksen kokonaiskustannukset. Pelkona nousi halutun tasoisen uudistuksen kariutuminen kustannusten takia, jolloin nykyiseen ratkaisuun tehdään vain pieniä muutoksia kokonaisvaltaisen uudistuksen sijaan.

Sisäpiirin hyökkäyksen riskit koettiin uhkana sisäisen tietoturvankin haastatteluissa. Kohdeorganisaatiossa ei tällä hetkellä ole tavallisilla käyttäjillä asennusoikeuksia laitteille, joka rajaa tahallisten ja tahattomien sisäpiirin hyökkäysten mahdollisuuksia. Ilman asennusoikeuksia käyttäjä ei pysty asentamaan laitteelle organisaation ulkopuolisia ohjelmia. Haastateltavien mukaan haittaohjelmien lataaminen organisaation laitteille on estetty, ja siihen tulisi muutenkin ottaa kantaa jonkin muun kontrollin kuin identiteetin- ja pääsynhallinnan ratkaisun. Voimakkaammat oikeudet omaavat käyttäjät voivat kuitenkin aiheuttaa vahinkoa itse tahallisesti tai heidän oikeuksien ajautuessa väärille käyttäjille.

> En näe tätä riskinä, jos on rakennettu oikein. Meillä on muita ratkaisuja, IAM-ratkaisu ei tule olemaan ainut, joka ottaa kantaa tähän asiaa. Meillä on virustorjunta, palomuurit ja niiden tulee ottaa kantaa, jos joku onnistuu lataamaan haittaohjelman. Jonkun muun kuin IAM tulee huutaa tällaisessa tilanteessa. (Tietoturva 1)

> Meillä nyt tällä hetkellä jos työntekijä haluaa tehdä pahaa ja hänellä on vähänkin jotakin parempia paukkuja ikään kuin meidän järjestelmiin kyllähän hän pystyy tekemään pahaa. (Tietoturva 2)

Kertakirjautumisen koettiin olevan enemmän tavoitetila kuin suuri riskitekijä. Haastateltavat kuitenkin tunnistivat riskinä, jos kirjautuneeksi jäänyt laite pääsee väärien henkilöiden haltuun, voi se silloin aiheuttaa eri tasoisia riskejä. Tämä kuitenkin tulisi olla estettynä erilaisten sääntelyiden avulla, jotka reagoivat poikkeavaan käytökseen. Kertakirjautumisen etuna oli, ettei käyttäjän tarvitse kirjoittaa tunnuksiaan useasti, mikä puolestaan nostaa tietoturvallisuutta tutkitusti.

> Toki jos kone jää auki, ja joku toinen siihen kirjautuu ja lähtee tekemään, siinä tapauksessa se on riski. Ne pitäisi käytännössä silloin olla politiikoilla estetty, ja se on jokaisen oma virhe, jos ei huolehdi että kone on kirjautunut, ja joku ulkopuolinen pääsee siihen. (Tietoturva 1)

> Jos toteutetaan integraatiot ihan ajantasaisten ja oikeuden standardien mukaan, enemmän näkisin että siihen pitäisi pyrkiä. Mitä vähemmän sitä tunnusta tarvitsee käyttäjän kirjata, sitä turvallisempaa se on. Tämä näkyy ihan näissä phishing caseissa ja muissakin, että joka ikinen kerta, kun tunnus ja salasana pitää laittaa, niin kyllä se minun mielestä se on se iso riski tällä hetkellä. (Tietoturva 3)

Haastateltavat kokivat kertakirjautuminen positiivisena asiana, johon tulisi pyrkiä mahdollisuuksien mukaan. Yksi haastateltavista kuitenkin epäili, ettei puhtaaseen kertakirjautumiseen koskaan tulla pääsemään, vaan kohdeorganisaatiolla tulisi edelleenkin olla joihinkin kriittisimpiin organisaatiojärjestelmiin monivaiheinen todennus eli MFA.

Prosesseihin tunnistettiin liittyvän erilaisia riskejä tällä hetkellä kohdeorganisaatiossa. Käyttöoikeuksia pyydetään ja annetaan tällä hetkellä ohi prosessien ja niiden pyytäminen voi tapahtua kasvotusten, jolloin niistä ei jää auditointijälkeä eivätkä oikeuksien hyväksymiset välttämättä mene protokollan mukaisesti. Tällaisten ongelmien ratkaisemiseksi vaaditaan tiukasti määritellyt käytännöt ja prosessit, jottei prosessien ohittaminen aiheuta ongelmien identiteetin- ja pääsynhallinnalle sen uudistuksen jälkeen. Taulukkoon kymmenen on koottu kaikki haastatteluissa esiintyneet potentiaaliset organisaation sisäiset riskit identiteetin- ja pääsynhallinnassa.

Taulukko 10 Organisaation sisäiset riskit identiteetin- ja pääsynhallinnalle

Riski	**Esiintyi haastatteluissa yht.**	**Tietohallinto**	**Identiteetin- ja pääsynhallinnan asiantuntijat**	**Sisäinen tietoturva**
Prosesseihin liittyvät ongelmat	6	X	X	X
Osaamisriski	6	X	X	X
Sisäpiirin hyökkäykset	5	X	X	X
Kustannukset	4	X	X	X
Sidosryhmien sitouttaminen	3	X	X	
Muutosvastaisuus	2	X	X	

6 JOHTOPÄÄTÖKSET JA JATKOTUTKIMUSAIHEET

Tässä luvussa pohditaan empiirisen tutkimuksen tuloksia, ja vertaillaan niitä suhteessa kirjallisuuskatsauksen tuloksiin. Luvussa edetään teemoittain, jotka ovat esitelty tutkimustulokset luvussa. Tutkimustulosten pohdinnan lisäksi luvussa arvioidaan tutkimuksen luotettavuutta ja esitellään relevantteja jatkotutkimusaiheita.

6.1 Tulosten pohdinta

Teemahaastattelututkimuksessa haastateltavat tunnistivat runsaasti erilaisia identiteetin- ja pääsynhallintaan liittyviä riskejä organisaatiokontekstissa. Tutkimuksen tulokset esitettiin luvussa viisi kuuteen teemaan jaettuna:

- Manuaalityö
- Hajautuneisuus
- Pilvipalvelut
- Keskitetty identiteetin- ja pääsynhallinta
- Automaatio
- Organisaation sisäiset riskit

Haastattelututkimuksessa yhtenä merkittävimpänä riskinä nähtiin identiteetin- ja pääsynhallinnan hajautuneisuus. Hajautuneisuus nähtiin todennäköisesti haastatteluissa merkittävänä riskinä, koska kohdeorganisaation oma identiteetin- ja pääsynhallinta on tällä hetkellä hajautunut. Omakohtainen kokemus helpottaa riskien arviointia, koska ne voidaan konkretisoida omaan kokemuskontekstiin. Tämän lisäksi hajautuneisuus havaittiin haastatteluissa aiheuttavan runsaasti muita riskejä, kuten ylläpidon hankaluudesta ja monimutkaisuudesta aiheutuvat vanhentuneet ja virheelliset oikeudet käyttäjillä. Virheellisillä oikeuksilla varustettu henkilö on selkeä tietoturvariski, koska tämä voi tahallaan tai vahingossa aiheuttaa sisäpiirin hyökkäyksen.

Sisäpiirin hyökkäykset ovat haastatteluiden perusteella haastava riskikokonaisuus, koska käyttäjillä tulee olla työtehtäviin vaaditut käyttöoikeudet, mutta kuitenkin oikeudet tulee olla rajalliset sisäpiirin hyökkäysten estämiseksi. Sisäpiirin hyökkäykset ovat myös siitä ongelmallisia, että niiden estäminen on haastavaa, ellei mahdotonta.

Manuaalisuus nähtiin haastatteluissa merkittävänä riskinä identiteetin- ja pääsynhallinnassa. Manuaalisuus aiheuttaa tutkimuksen perusteella inhimillisiä virheitä, kuten vääriä oikeuksia ja prosessien sekavuutta. Kun prosessit ovat epäselvät ja työt tehdään manuaalisesti voi esimerkiksi lopettavien henkilöiden käyttöoikeudet jäädä voimaan, jolloin jo yrityksestä poistunut henkilö pääsee edelleen organisaation järjestelmiin ja resursseihin, joka on todella merkittävä riski.

Seuraavaksi tutkimuksen tulokset analysoidaan teemoittain, samoin kuten tulokset ovat esitelty luvussa viisi. Teemahaastattelututkimuksen tuloksia verrataan kirjallisuuskatsauksen tuloksiin ja tehdään päätelmiä niiden perusteella.

Manuaalityö

Manuaalinen identiteetin- ja pääsynhallinta altistaa yrityksen erilaisille riskeille (Bradford ym., 2014; Bulgurcu ym., 2010; Hummer ym., 2016; Kumar & Bhardwaj, 2018). Kaikki haastateltavat tunnistivat manuaaliseen työhön liittyvän erilaisia riskejä. Manuaalinen työ nousi myös haastattelun teemoista toiseksi keskeisimmistä riskiteemoista yhdessä hajautuneisuuden kanssa. Identiteetin- ja pääsynhallinnan kontekstissa manuaalinen työ haastateltavien mukaan aiheuttaa viiteen eri kategoriaan jaettavia riskejä, joita ovat:

- Inhimilliset virheet
- Prosessien hitaus ja kankeus
- Jatkokehitysmahdollisuuksien rajallisuus
- Tehottomuus
- Työläys

Haastatteluissa eniten esiintyviä riskejä olivat prosessien hitaus ja kankeus, tehottomuus ja työläys. Kaikki nämä kolme voidaan sanoa liittyvän organisaation tekemisen tehokkuuteen ja tekemisen tehostamiseen. Manuaalisessa työssä nähtiin yhdeksän kymmenestä haastateltavan mukaan riskinä prosessien hitaus ja kankeus. Haastateltavien mukaan automatisoimalla manuaalisia tehtäviä ja prosesseja päästäisiin eroon monesta ongelmasta prosesseissa.

Kirjallisuudessa Kumar ja Bhardwaj (2018) nostivat esiin manuaalisin työn aiheuttavan monimutkaisuutta ja sitä vähentämällä työntekijät on mahdollista siirtää muihin strategisesti tärkeämpiin tehtäviin. Manuaalisuus aiheuttaa merkittävästi työtä organisaatioissa, mikä voitaisiin poistaa erilaisten teknologisten ratkaisuiden, kuten juuri automaation avulla. Bradfordin ym. (2014) ja Hummerin ym. (2016) mukaan manuaalinen työ aiheuttaa tehottomuutta organisaatioissa. Tehottomuus nousi haastatteluissakin esiin yhdeksän henkilön haastattelussa, joka on merkittävä määrä ottaen huomioon haastateltavien yhteislu-

kumäärän (10). Identiteetin- ja pääsynhallinnan mukaan manuaalinen tekeminen identiteetin- ja pääsynhallinnassa on usein tehotonta, ja aiheuttaa merkittävästi rutiininomaista tekemistä organisaatioissa.

Manuaalisen työn aiheuttama työläys oli kolmas haastatteluissa eniten esiintynyt manuaalisuuteen liittyvä riski. Sisäisen tietoturvan haastateltavan mukaan kohdeorganisaatiossa tehdään tällä hetkellä sellaisia tehtäviä manuaalisesti, jotka ovat hyvin työläitä ja jotka monet muut organisaatiot toteuttavat jo täysin automatisoidusti. Haastatteluissa nousikin useasti esiin vastakkainasettelu manuaalisuuden ja automaation välillä, mikä oli tunnistettavissa myös kirjallisuuskatsauksen perusteella. Tähän varmasti merkittävä syy on, että monesti organisaatioiden tavoitteena on toteuttaa organisaation identiteetin- ja pääsynhallinta automaation avulla, koska se on jatkuvasti yleistymässä ja mahdollista toteuttaa niin.

Inhimilliset virheet nousivat esiin seitsemässä haastattelussa. Haastateltavien mukaan manuaalisessa työssä on aina riskejä, koska ihminen on inhimillinen tekijä, jolloin virheet ovat mahdollisia. Bradfordin ym. (2014) ja Hummerin ym. (2016) mukaan manuaalisen työn aiheuttama inhimillisen virheen mahdollisuus on merkittävä manuaaliseen työhön liittyvä riski organisaatioissa. Lisäksi Kumar ja Bhardwaj (2018) totesivat manuaalisen työn lisäävän virheiden mahdollisuutta, hankaloittavan ylläpitoa ja auditointitoimintoja, jolloin suurena riskinä on käyttäjien liialliset tai vanhentuneet oikeudet. (Kumar & Bhardwaj, 2018). Inhimillisyys voi aiheuttaa tahallisia tai tahattomia virheitä, joiden korjaaminen voi pahimmillaan aiheuttaa esimerkiksi kaksinkertaisia käyttöoikeuksia käyttäjille virheitä korjatessa. Kaksinkertaisilla tai muuten virheellisillä oikeuksilla varustettu käyttäjä on todella merkittävä riski organisaatiolle sisäpiirin hyökkäysten ja tietomurtojen takia. Ihminen on usein tietoturvan kannalta epävarmin tekijä (Bulgurcu ym., 2010).

Tietohallinnon haastatteluissa nousi kahdessa kolmesta esiin riskinä myös manuaalisesti toteutetun identiteetin- ja pääsynhallinnan ratkaisun jatkokehitysmahdollisuuksien rajallisuus. Jatkokehitysmahdollisuuksien rajallisuus nousi riskinä vain tietohallinnon henkilöiden haastatteluissa. Kirjallisuuskatsauksessa tämä ei noussut esiin identiteetin- ja pääsynhallinnan riskinä. Muuten samat manuaalisuuteen liittyvät riskit nousivat esiin sekä kirjallisuuskatsauksessa että empiirisen tutkimuksen haastatteluissa.

Manuaaliseen työhön liittyy useita eri riskejä, jotka tunnistettiin kirjallisuuskatsauksessa sekä kohdeorganisaation haastatteluissa, joten manuaalisen työn voidaan todeta olevan yksi merkittävä riskiteema organisaatioiden identiteetin- ja pääsynhallinnassa. Manuaalisuuteen liittyy paljon inhimillisiä virheitä, kuten unohduksia ja vahinkoja, joista seuraa nopeasti tai pidemmän aikavälin kuluttua erilaisia riskejä organisaatiolle. Kuten kirjallisuudessakin todettiin, henkilö jolla on omaan työhönsä nähden virheelliset tai vanhentuneet oikeudet on riski organisaatiolle, koska hänellä on pääsy sellaisiin organisaatioresursseihin, joita työtehtävät eivät vaadi.

Lisäksi manuaalisuudessa on riski, ettei virheitä muisteta korjata, tai niitä ei osata korjata vaaditulla laajuudella. Tällöin virheellisesti myönnetty oikeus

voi jäädä voimaan, tai henkilöltä virheellisesti poistetaan joitain tarpeellisia käyttövaltuuksia. Työntekijöillä tulisi aina olla työtehtäviensä tekemiseen vaaditut käyttöoikeudet, jotta heidän työnsä ei seisahdu käyttöoikeuksien takia.

Manuaalisuus identiteetin- ja pääsynhallinnassa voidaan todeta olevan merkittävä riski, josta voi seurata organisaatiolle eri laajuisia seurauksia. Vaikka manuaalisesti toteutetut tehtävät ja prosessit aiheuttavat merkittäviä riskejä asiantuntijaorganisaatioille, mitkä olisivat automaation avulla mahdollista poistaa, ei automaatio itsessään kuitenkaan ole täysin riskitön ratkaisu. Automaatioon liittyviä riskejä käsitellään myöhemmin tässä alaluvussa.

Hajautuneisuus

Hajautettu pääsynhallintamalli nostaa riskien mahdollisuuksia, koska se on usein hankalasti hallittavissa (Bradford ym., 2014). Identiteetin- ja pääsynhallinnan hajautuneisuus nousi merkittävänä identiteetin- ja pääsynhallintaan liittyvänä riskinä haastatteluissa. Haastateltavat tunnistivat kuusi hajautuneisuuteen liittyvää riskiä.

- Haastava hallinnoida
- Kokonaisvaltaisen näkyvyyden puute
- Virheelliset oikeudet
- Auditoinnin hankaluus
- Sekavat ja epäselvät prosessit
- Suuren sovellus määrän aiheuttama sekavuus

Haastatteluissa eniten esiintyviä hajautuneisuuteen liittyviä riskejä olivat haastavuus hallinnoimisessa, virheelliset oikeudet sekä sekavat ja epäselvät prosessit. Bradfordin ym. (2014) mukaan hajautuneesti toteutetun identiteetin- ja pääsynhallinnan riskien aiheuttajana on juuri haastavuus hallinnoimisessa. Tämä aiheuttaa virheellisiä oikeuksia sekä sekavia ja epäselviä prosesseja, koska kokonaisuus on niin epäselvä ja hajallaan. Hajautunut identiteetin- ja pääsynhallinta myös monimutkaistaa ja hankaloittaa käytäntöjä huomattavasti (Bradford ym., 2014; Hummer ym., 2016; Tuecke ym., 2016).

Virheelliset oikeudet ovat hajautuneen identiteetin- ja pääsynhallinnan suuri riski. Kun väärillä oikeuksilla varustettu käyttäjä pääsee yrityksen tietojärjestelmiin, voivat seuraukset olla todella tuhoisia (Feng ym., 2008). Kumarin ja Bhardwajin (2018) mukaan suurimpina riskeinä identiteetin- ja pääsynhallinnan osa-alueella on käyttäjien liialliset oikeudet. Liiallisilla oikeuksilla varustetut käyttäjät voivat aiheuttaa vahingossa tai tahallisella toiminnallaan organisaatiolle menetyksiä, jotka voivat olla muun muassa taloudellisia tai maineeseen liittyviä (Bulgurcu ym., 2010; Gauthier & Merlo, 2012; Kumar & Bhardwaj, 2018).

Asiantuntijaorganisaatioille maine on todella merkittävä, koska asiakkaiden luottamus rakentaa kestävän kilpailuedun ja aseman markkinoilla. Maineriskit ovat monesti taloudellisia riskejä vaarallisempia, koska maineriskit aiheuttavat myös taloudellisia ongelmia muun muassa asiakkaiden menetyksen

takia ja maineen korjaaminen voi kestää monia vuosia. Joskus maine voi olla niin pahasti tuhoutunut, ettei sitä enää ole mahdollista saada korjattua.

Käyttäjien oikeuksia voi haastateltavien mukaan jäädä päivittämättä tämän lopettaessa tai tehtävänkuvan muuttuessa hajautuneisuuden takia, koska ei esimerkiksi huomata jonkin toimen olevan manuaalisen työn varassa automaation sijaan. Lisäksi hajautuneisuus pahimmillaan aiheuttaa jokaiselle sovellukselle ja järjestelmälle oman identiteetin- ja pääsynhallinnan, jolloin käyttäjillä voi olla yhtä aikaa monia eri käyttäjätunnuksia ja salasanoja työtehtäviensä hoitamiseksi. Kun käyttäjillä on useita eri käyttäjätunnuksia, heidän salasanansa ovat monesti yksinkertaisempia tai niitä ei vaihdeta tarpeeksi usein. Haastateltavien mukaan tällainen on todella suuri riski kohdeorganisaatiolle, koska ei voida varmistaa organisaation yhteisen salasanapolitiikan noudattamista kaikissa laitteissa ja järjestelmissä.

Haastateltavien mukaan hajautunut identiteetin- ja pääsynhallinta aiheuttaa kokonaisvaltaisen näkemyksen puutteen, jonka seurauksena organisaatiossa ei ole selkeää kuvaa eri käyttäjien oikeuksista, niiden myöntämisprosessista tai käyttöasteesta. Hajautuneeseen identiteetin- ja pääsynhallintaan liittyviä riskejä ovat esimerkiksi sisäpiirinhyökkäykset, liialliset ja vanhentuneet käyttöoikeudet, käyttäjien toimien jäljitettävyys sekä monimutkaisuus (Baracaldo & Joshi, 2013; Bradford ym., 2014; Chen & Crampton, 2011; Hummer ym., 2016).

Haastateltavista seitsemän nosti hajautuneisuuden ongelmaksi auditoinnin hankaluuden. Haastateltavien mukaan käyttäjien oikeuksia on hyvin haastavaa, ellei jopa mahdotonta auditoida, koska heidän oikeutensa eivät ole yhdessä keskitetyssä järjestelmässä. Hajautuneessa identiteetin- ja pääsynhallinnassa käyttäjien oikeuksia hallinnoidaan eri sijainneista, jolloin auditoidessa tulisi käydä jokaisen sovelluksen ja resurssin käyttöoikeudet yksittäin läpi. Bradfordin ym. (2014) mukaan hajautuneessa identiteetin- ja pääsynhallinnan ratkaisussa on mahdotonta tai vähintään hyvin hankalaa todistaa, hallita ja seurata kenellä käyttäjistä pääsy mihinkin informaatioon, sekä ovatko nämä käyttöoikeudet linjassa organisaation sisäisten ja ulkoisten määräysten sekä käytäntöjen kanssa.

Jokainen haastateltava ryhmistä, tietohallinto, identiteetin- ja pääsynhallinnan asiantuntijat sekä sisäinen tietoturva nostivat hajautuneisuudesta johtuvaksi riskiksi myös suuren sovellus määrän aiheuttaman sekavuuden. Tämä ei suoranaisesti ole vain hajautuneen identiteetin- ja pääsynhallinnan ongelma, mutta suuri määrä sovelluksia yhdistettynä hajautettuun identiteetin- ja pääsynhallintaan on todella työläs ja hankalasti hallittava kokonaisuus, josta seuraa lukuisia tietoturvariskejä, kuten juuri aiemmin mainittuja virheellisiä oikeuksia ja auditoinnin mahdottomuus.

Kaikki kuusi hajautuneisuuteen liittyvää riskiä identiteetin- ja pääsynhallinnan organisaatiokontekstissa tunnistettiin niin kirjallisuuskatsauksessa kuin myös haastattelututkimuksessa. Hajautuneisuus aiheuttaa tutkimuksen mukaan monimutkaisuutta ja hallinnan hankaluutta. Kun järjestelmä on hankalasti hallittavissa, on sen auditointi ja ylläpito myös hankalaa, jonka seurauksena esimerkiksi käyttäjien käyttöoikeuksien tarkistaminen voi olla haastavaa, hidas-

ta ja pahimmillaan organisaatiossa ei edes ole kokonaisvaltaista työkalua työntekijöiden oikeuksien tarkasteluun. Hajautuneisuuden voidaan täten todeta aiheuttavan monia riskejä organisaatioiden identiteetin- ja pääsynhallinnalle.

Pilvipalvelut

Tutkimuksessa kartoitettiin pilvipalveluihin liittyviä riskejä identiteetin ja pääsynhallinnassa, vaikkei niistä juurikaan ollut mainittu kirjallisuuskatsauksessa. Pilvipalvelut koettiin kuitenkin merkittäväksi osaksi nykypäivän identiteetin- ja pääsynhallintaa, koska moni nykypäivän asiantuntijaorganisaatio käyttää pilvipalveluita ja monet pilvipalveluntarjoajat tarjoavat myös identiteetin- ja pääsynhallinnan ratkaisuita organisaatioille. Tutkimushaastatteluissa haastateltavat tunnistivat seitsemän pilvipalveluihin liittyvää riskiä organisaatioiden identiteetin- ja pääsynhallinnassa.

- Tietoturva
- Osaamisriski
- Perinteiset pilvipalveluriskit
- Säännösten noudattaminen
- Modifioimattomuus
- Asiakkaiden menetys
- Riippuvaisuus palveluntarjoajasta

Pilvipalveluihin liittyvien riskien monipuolisuudesta huolimatta haastateltavat tunnistivat identiteetin- ja pääsynhallintaan liittyviä pilvipalveluriskejä melko niukasti. Tähän saattoi mahdollisesti vaikuttaa, ettei organisaatiossa tällä hetkellä ole käytössä täysin pilvipohjaista identiteetin- ja pääsynhallintaa. Kokemus helpottaa riskien tunnistamista, koska niistä saattaa olla aiempaa kokemusta tai riskien konkretisoiminen on muuten helpompaa.

Identiteetin- ja pääsynhallinnan asiantuntijat tunnistivat eniten pilvipalveluihin liittyviä riskejä. Tähän mahdollisena syynä on heidän kokemuksensa erilaisista asiakasprojekteista, joissa on ollut käytössä pilvipohjainen identiteetin- ja pääsynhallinnan ratkaisu. Tietohallinnon haastatteluissa tunnistettiin vain yksi pilvipalveluihin liittyvä riski identiteetin- ja pääsynhallinnan kontekstissa, joka oli tietoturvaan liittyvät riskit. Haastateltavan mukaan pilvipohjaiseen identiteetin- ja pääsynhallinnan ratkaisuun liittyy enemmän ja laajemmin erilaisia riskejä, kuin verrattaessa paikalliseen ratkaisuun. Haastateltavat näkivät pilvipalvelut enemmän positiivisena asiana, jota kohti tulisi pyrkiä.

Kirjallisuudessa ei suoranaisesti käsitelty pilvipohjaisen identiteetin- ja pääsynhallinnan riskejä, mutta Godha ym. (2014) nostivat riskinä verkkoon kytketyn ratkaisun, koska se tuo lukuisia uusia riskejä, kuten että järjestelmään voidaan murtautua, jolloin rikollinen pääsee käsiksi organisaation resursseihin (Godha ym., 2014).

Pilvipalveluihin liittyvät riskit, jotka nousivat haastatteluissa useimmiten esiin, olivat tietoturvariskit, perinteiset pilvipalveluriskit sekä riippuvaisuus palveluntarjoajista. Haastateltavien mukaan kohdeorganisaatiossa voitaisiin

nähdä riskiksi riippuvaisuus palveluntarjoajasta, koska tähän asti identiteetin- ja pääsynhallinta on toteutettu paikallisesti ja sen hallinnointi on ollut organisaation vastuulla. Esiin tulivat myös perinteiset pilvipalveluihin liittyvät riskit, kuten missä data tulisi fyysisesti sijaitsemaan ja voisiko siihen vaikuttaa. Haastateltavat kokivat ongelmaksi, mikäli sijaintia ei itse voisi määrittää tai siitä ei olisi varmuutta, koska joillakin asiakkailla voi olla tiukat vaatimukset heidän tietojensa säilyttämiseen liittyen. Haastatteluissa myös pohdittiin saisiko dataa pilvipalveluista tarvittaessa enää pois.

Yksittäisissä haastatteluissa nostettiin riskeiksi aiemmin mainittujen lisäksi organisaation osaaminen, modifioimattomuus ja asiakkaiden menetys. Identiteetin- ja pääsynhallinnan asiantuntijoiden mukaan riskiksi kohdeorganisaatiossa pilvipalveluiden kanssa saattaa tulla osaamattomuus. Modifioimattomuus nostettiin myös ongelmaksi, koska hankittaessa ulkopuolisen palveluntarjoajan tarjoama pilvipalvelu, ovat modifiointimahdollisuudet todennäköisesti jollain tasolla rajalliset, ja silloin voi tulla tilanteita, joissa ratkaisu ei palvele kaikkien sidosryhmien tarpeita. Yksi identiteetin- ja pääsynhallinnan asiantuntija myös koki merkittäväksi riskiksi asiakkaiden menettämisen, koska kuten aiemmin mainittua, joillain asiakkailla saattaa olla hyvin tiukat määräykset ja vaatimukset heidän tietojen käsittelystä pilvitietokannoissa.

Pilvipalveluriskit nousivat haastatteluissa esiin identiteetin- ja pääsynhallintaan liittyvänä riskinä, mutta kirjallisuuskatsauksen lähdekirjallisuudessa niistä ei erikseen ollut mainintaa identiteetin- ja pääsynhallinnan kontekstissa. Kirjallisuuskatsauksessa kuitenkin nostettiin esiin yleisesti verkkoon kytkettyjen järjestelmien riskejä, joihin myös pilvipalveluratkaisut voidaan katsoa kuuluvan. Haastateltavat kuitenkin tunnistivat useita eri riskejä, ja osa niistä sai useamman henkilön kannatuksen. Tutkimuksessa havaitut riskit olivat suurimmalta osin sellaisia riskejä, jotka liittyvät yleisesti pilvipalveluihin, eivätkä ole ainoastaan identiteetin- ja pääsynhallintaan kytköksissä olevia riskejä. Täten voidaan todeta pilvipalvelun aiheuttavan potentiaalisia riskejä, mutta ei kuitenkaan merkittävästi niitä.

Keskitetty identiteetin- ja pääsynhallinta

Keskitetty identiteetin- ja pääsynhallinnan malli vähentää tietoturvariskejä, koska sen hallinnoiminen on helpompaa ja mahdollistaa kokonaisvaltaisen näkemyksen oikeuksiin ja niiden monitorointiin (Bradford ym., 2014). Keskitetty identiteetin- ja pääsynhallinta siis poistaa monia hajautuneisuuden ongelmia, mutta myös keskitetty ratkaisu sisältää riskejä. Haastateltavat tunnistivat seitsemän keskitettyyn identiteetin- ja pääsynhallintaan liittyvää potentiaalista riskiä.

- Tietoturva
- Riippuvaisuus yhdestä sovelluksesta tai järjestelmästä
- Laajalle skaalautuvat ongelmat
- Sisäpiirin hyökkäykset
- Toiminta ongelmatilanteissa

- Haastava implementointi
- Kustannukset

Haastatteluissa eniten esiintynyt keskitetyn identiteetin- ja pääsynhallinnan riski oli riippuvaisuus yhdestä sovelluksesta tai järjestelmästä. Haastatteluissa nousi esiin epävarmuus siitä, miten voitaisiin toimia, mikäli se ainoa identiteetin- ja pääsynhallinnan järjestelmä olisi poissa toiminnasta jostain syystä. Haastateltavat kokivat riskiksi vain yhteen järjestelmään luottamisen näinkin kriittisellä organisaation toiminta-alueella. Lisäksi haastateltavat kokivat ongelmalliseksi modifioitavuuden ja pystyykö yksi valittu järjestelmä vastaamaan kaikkiin organisaation omiin ja sen sidosryhmien toiveisiin ja tarpeisiin.

Keskitetyn identiteetinhallinnan saavuttaminen ei ole helppoa tai yksinkertaista. Keskitetyn identiteetin- ja pääsynhallinnan implementointi on kallista ja aikaa vievää (Bradford ym., 2014; Kunz ym., 2019). Haastateltavat tunnistivat riskiksi implementoinnin haastavuuden ja keskitetyn järjestelmän aloitus- sekä ylläpitokustannukset. Nämä samat teemat nousivat myös kirjallisuudessa keskeisenä keskitettyyn identiteetin- ja pääsynhallintaan liittyvänä riskinä. Bradfordin ym. (2014) ja Kunzin ym. (2019) mukaan keskitetyn identiteetin- ja pääsynhallinnan käyttöönotto on hyvin hidasta ja todella monimutkaista, minkä lisäksi sen implementointiin liittyy runsaasti epäonnistumisen mahdollisuuksia (Bradford ym., 2014; Hummer ym., 2016; Kunz ym., 2019).

Haastatteluissa koettiin myös yhtenä riskinä sisäpiirin hyökkäykset ja pääkäyttäjäoikeudet. Haastateltavien mukaan esimerkiksi pääkäyttäjäoikeuksilla varustettu henkilö voisi saada keskitetyssä identiteetin- ja pääsynhallinnan järjestelmässä halutessaan merkittävästi pahaa aikaan, koska hänellä on pääsy kaikkiin organisaation identiteetteihin ja niiden käyttöoikeuksiin kaikissa organisaatioresursseissa. Haastateltavien mukaan keskitetyssä identiteetin- ja pääsynhallinnassa tulisikin kiinnittää erityistä huomiota laajemmilla oikeuksilla varustettuihin henkilöihin ja heidän käyttäytymiseensä.

Muutamassa haastattelussa koettiin keskitetyn identiteetin- ja pääsynhallinnan riskiksi laajemmalle skaalautuvat ongelmat. Toimiessa vain yhden järjestelmän varassa myös ongelmat skaalautuvat laajemmalle, koska ne vaikuttavat kaikkeen. Kun jokainen organisaation sovellus, järjestelmä ja resurssi on kytketty yhteen keskitettyyn ratkaisuun, myös siinä tapahtuvat ongelmat voivat pahimmillaan koskea kaikkia organisaationresursseja.

Kirjallisuuskatsauksessa keskitetyn identiteetin- ja pääsynhallinnan riskeiksi nousivat lähinnä kustannuksiin sekä implementointiin liittyvät riskit. Haastatteluissa tunnistettiin laajemmin erilaisia riskejä, kuten riippuvaisuus yhdestä keskitetystä järjestelmästä. Tämä huomio oli mielenkiintoinen ja merkittävä tutkimuksen kannalta. Tutkimuksessa esiin tulleista riskeistä huolimatta useimmat haastateltavista nostivat kuitenkin keskitetyn identiteetin- ja pääsynhallinnan edut suuremmaksi, mitä siihen liittyvät riskit ovat. Täten voidaankin todeta keskitettyyn identiteetin- ja pääsynhallintaan liittyvän erilaisia riskejä, mutta tutkimus ei ota kantaa niiden merkittävyyteen organisaatioissa.

Automaatio

Haastateltavista kaikki kokivat automaation tuovan enemmän positiivisia asioita kuin riskejä kohdeorganisaation identiteetin- ja pääsynhallinnalle, mutta pystyivät kuitenkin tunnistamaan monipuolisesti siihen liittyviä erilaisia riskejä. Haastatteluissa yhtä lukuun ottamatta kaikki haastateltavat tunnistivat automaatioon liittyviä riskejä organisaatioiden identiteetin- ja pääsynhallinnassa. Yhteensä haastatteluissa tunnistettiin kuusi automaatioon liittyvää riskiä, jotka liittyvät identiteetin- ja pääsynhallintaan organisaatiokontekstissa.

- Virheellinen toteutus
- Huoleton ylläpito
- Prosessien joustamattomuus ja poikkeustapaukset
- Kustannukset
- Järjestelmävirheet
- Osaamisriski

Kirjallisuuskatsauksessa automaation riskeiksi nostettiin teknologiaan luottaminen, joka on melko perinteinen uusiin teknologioihin liittyvä pelko ihmisillä. Hoffmanin ym. (2013) mukaan käyttäjien luottamus teknologiajärjestelmiin edustaa jossain määrin heidän luottamustaan tällaisten järjestelmien kehittäjiin. Tämän lisäksi teknologian ja sen mahdollisuuksien rajallinen ymmärrys aiheuttaa luottamuspulaa teknologiaa kohtaan (Hoffman ym., 2013).

Haastatteluissa useimmiten esiintyneet automaatioon liittyvät riskit olivat virheellinen toteutus, huoleton ylläpito sekä prosessien joustamattomuus ja poikkeustapaukset. Kaikki kolme eniten esiin noussutta riskiä ovat hyvin käytännön läheisiä, joka voi kertoa epävarmuudesta teknologiaan luottamisen suhteen. Haastateltavien mukaan on suuri riski, mikäli automaatio on jotenkin virheellisesti toteutettu, ja sen vuoksi esimerkiksi myöntää käyttäjille automaattisesti käyttöoikeuksia sellaisiin toimintoihin tai organisaatioresursseihin, joihin ei pitäisi sallia pääsyä. Lisäksi koettiin ongelmalliseksi, mikäli automaatio hajoaa ja pitäisi selvittää mitä käyttäjien pyyntöjä tulisi selvittää käsin virheellisten prosessien seurauksena.

Useissa haastatteluissa nousi esiin pelko automaatioon liialliseen nojautumiseen sen käyttöönoton jälkeen. Haastateltavien mukaan automaatioita tulee jatkuvasti päivittää ja seurata, jotta ne ovat ajantasaisia ja toimivat halutusti. Modifioitavuus nousi esiin tässäkin teemassa, ja haastateltavat kokivat yhtenä riskinä automatisoidun järjestelmän ja prosessin toimivuuden erilaisissa poikkeustapauksissa. Hyvin pitkälle automatisoitu ratkaisu saattaisi olla melko joustamaton, jolloin erilaiset poikkeustapaukset voisivat edelleen olla manuaalisen työn varassa. Nostettiin myös esiin se, onko edes mahdollista toteuttaa sellaista automaatiota, joka pystyisi vastaamaan jokaiseen organisaation identiteetin- ja pääsynhallinnan skenaarioon.

Osaamisriski nostettiin haastatteluissa esiin yhdeksi kohdeorganisaation riskiksi identiteetin- ja pääsynhallinnan automaatiossa. Kaikissa haastattelukategorioissa, tietohallinnon, identiteetin- ja pääsynhallinnan asiantuntijoiden se-

kä sisäisen tietoturvan haastatteluissa nostettiin esiin osaamisriski, ja että kohdeorganisaation kohdalla osaamisen puute saattaisi muodostua ongelmaksi automaation kanssa kohdeorganisaatiossa. Eräs haastateltava kuitenkin nosti esiin, että henkilöstöä kouluttamalla tultaisiin pääsemään haluttuun osaamistilaan kohdeorganisaatiossa. Toinen organisaation sisäinen riski automaatiossa oli kustannukset, ja kuinka uudistettu pitkälle automatisoitu identiteetin- ja pääsynhallinnan ratkaisu todennäköisesti tulisi merkittävästi arvokkaammaksi mitä nykyinen toteutus. Erään haastateltavan mukaa korkeat kokonaiskustannukset saattaisivat jopa olla uudistuksen esteenä.

Kaikkien identiteetin- ja pääsynhallinnan asiantuntijoiden haastatteluissa he nostivat esiin yhtenä automaatioon liittyvänä riskinä järjestelmävirheet. Heidän mukaansa automatisoitu ratkaisu poistaisi manuaalisen työn aiheuttamat virheet, kuten inhimilliset virheet, mutta sisältää kuitenkin uusia virheitä, kuten järjestelmävirheitä.

Kirjallisuudessa automaatioon liittyvät riskit identiteetin- ja pääsynhallinnassa liittyivät teknologiaan luottamiseen ja sen rajalliseen ymmärrykseen. Kirjallisuuskatsauksessa ei tunnistettu erityisesti identiteetin- ja pääsynhallinnan automaatioon liittyviä riskejä, vaan riskit olivat enemmän yleisen tason riskejä liittyen teknologiaan ja automaatioon. Osaamisriskin lisäksi automaatioon kuitenkin liittyy monia muita riskejä, jotka nousivat esiin kohdeorganisaation haastatteluissa. Riskeistä huolimatta jokainen haastateltava oli kuitenkin vahvasti automaation kannalla, ja kokivat sen mahdollistavan asiantuntijaorganisaatioille runsaasti erilaisia etuja.

Organisaation sisäiset riskit

Asiantuntijaorganisaatioiden identiteetin- ja pääsynhallintaan liittyy monia erilaisia organisaation sisäisiä riskejä ulkoisten lisäksi. Identiteetin- ja pääsynhallinnan onnistumiseen vaikuttavat myös tietyt sisäiset rajoitteet, kuten tekniset, organisaatiolliset ja ympäristölliset, jotka haittaavat sen käyttöönottoa, mikäli niitä ei osata ottaa huomioon ja johtaa oikein (Bradford ym., 2014). Organisaation sisäisiä riskejä nousi esiin niin kirjallisuuskatsauksessa kuin haastattelututkimuksessa. Haastateltavat tunnistavat kuusi organisaation sisäistä riskiä identiteetin- ja pääsynhallinnassa.

- Prosesseihin liittyvät ongelmat
- Sisäpiirin hyökkäykset
- Kustannukset
- Osaamisriski
- Sidosryhmien sitouttaminen
- Muutosvastaisuus

Useimmiten haastatteluissa organisaation sisäisistä riskeistä nostettiin esiin ongelmat prosessissa sekä osaamisriski. Osaamisriski esitettiin riskinä myös automaation kohdalla, mutta se käsitti vain automaatioon liittyvän osaamisriskin.

Tässä teemassa osaamisriski käsittää kokonaisvaltaisen osaamattomuuteen liittyvän riskin organisaation identiteetin- ja pääsynhallinnassa.

Osaamisriski koettiin haastatteluissa kahdella eri tavalla, liian kapealle ulottuva osaaminen organisaatiossa sekä liian vähäinen osaaminen. Liian kapealla osaamisella tarkoitetaan, että osaaminen keskittyy yhteen tai korkeintaan muutamaan henkilöön, joka aiheuttaa merkittävän riskin näiden henkilöiden poistuessa organisaation palveluksesta. Nämä henkilöt vievät mukanaan suuren määrän osaamista, jota muilla ei tällä hetkellä organisaatiossa ole. Liian vähäinen osaaminen taas tarkoittaa, ettei organisaatiossa ole vaadittua osaamista identiteetin- ja pääsynhallintaan. Liian vähäinen osaaminen kuitenkin koettiin väliaikaiseksi riskiksi kohdeorganisaatiossa, joka voidaan poistaa lisäämällä henkilöstön koulutusta aihealueesta.

Osaamisriskin teemaan liittyy myös halu toteuttaa identiteetin- ja pääsynhallinnalla jotakin, mikä on liian monimutkaista ja aiheuttaa ongelmia prosesseille. Osaamattomuuden takia halutaan saada liian monimutkainen identiteetin- ja pääsynhallinnan ratkaisu, joka ei ole taloudellisesti tai teknisesti järkevää. Asiantuntijoiden mukaan yksinkertaisempi ratkaisu on usein parempi vaihtoehto. Monimutkaisen ratkaisun tavoittelu aiheuttaa runsaasti implementoinnin epäonnistumisen mahdollisuuksia (Bradford ym., 2014; Hummer ym., 2016; Kunz ym., 2019).

Ongelmat prosesseissa olivat identiteetin- ja pääsynhallinnan asiantuntijoiden mielestä yksi vakava riski organisaatioiden identiteetin- ja pääsynhallinnassa. Prosesseihin liittyviä ongelmia ovat niiden monimutkaisuus, epäselvyys ja ymmärryksen puute, joka johtaa kasvavaan roolien määrään, kokonaisvaltaiseen roolien laadun laskuun sekä paljastaa tietoturva haavoittuvuuksille virheellisesti myönnettyjen tai vanhentuneiden oikeuksien seurauksena (Kunz ym., 2015b). Lisäksi asiantuntijoiden mukaan prosessit itsessään tulisi olla kunnossa ennen kuin minkäänlaiseen uudistukseen voidaan ryhtyä, koska uuteen ratkaisuun ei haluta siirtää vanhan toteutuksen ongelmia ja riskejä. Haastateltavien mukaan prosesseihin liittyvien ongelmien takia kohdeorganisaatio altistuu erilaisille riskeille esimerkiksi virheellisten tai voimaan jääneiden oikeuksien takia.

Sisäpiirin hyökkäykset esiintyivät kirjallisuuskatsauksessa sekä haastattelututkimuksessa identiteetin- ja pääsynhallintaan liittyvänä riskinä organisaatioille. Bulgurcun ym. (2010) mukaan ihminen on usein tietoturvan kannalta epävarmin tekijä ja Baracaldo ja Joshi (2013) nostivat sisäpiirin hyökkäykset suurena nykypäivän organisaatioihin liittyvänä riskinä.

Sisäpiirin hyökkäykset ovat hankala riski organisaatioille, koska ne voivat olla joko tahallisia tai vahinkoja, jolloin käyttäjän toiminnan seuraaminen ja poikkeamiin reagoiminen ovat ainoita keinoja niiden välttämiselle. Identiteetin- ja pääsynhallinnan ratkaisun tulisi sisältää ominaisuuksia, jotka mahdollistavat esimerkiksi käyttäjän oikeuksien jäädyttämisen tämän toimiessa merkittävästi poikkeavalla tavalla, joka voisi olla haitaksi organisaatiolle. Haastateltavien mukaan identiteetin- ja pääsynhallinnan ei tulisi olla ainoa toimija, joka reagoi poikkeamiin vaan myös tietoturvajärjestelmien tulisi hälyttää poikkeamissa.

Kustannukset nostettiin esiin sekä haastatteluissa että kirjallisuuskatsauksessa identiteetin- ja pääsynhallinnan riskiksi. Bradfordin ym. (2014) mukaan kustannukset nousevat, mikäli järjestelmien käyttäjien elinkaaressa olevat rutiinitehtävät tehdään käsin, kuten käyttöoikeuksien myöntäminen tai peruuttaminen ja salasanan palautus. Manuaalisen työn kustannusten lisäksi kirjallisuudessa nostettiin keskitetyn identiteetin- ja pääsynhallinnan suuret aloituskustannukset (Anilkumar & Sumathy, 2018; Coyne & Weil, 2013; Kunz ym., 2015b) sekä identiteetin- ja pääsynhallinan uudistusten yleisesti suuret kustannukset (Bradford ym., 2014; Kunz ym., 2019).

Haastateltavien mukaan nykyinen ratkaisu on todennäköisesti kustannustehokkaampi ratkaisu, mutta sisältää suuremman määrän riskejä. Lisäksi vaikka suorat kustannukset voivat nousta niin välilliset laskevat, koska henkilöstö vapautuu tekemään muita strategisesti merkittävämpiä tehtäviä. Riskinä koettiin myös uudistuksen suuret kokonaiskustannukset, jotka pelättiin olevan mahdollinen riski koko identiteetin- ja pääsynhallinnan uudistukselle kohdeorganisaatiossa.

Sidosryhmien sitouttaminen esiintyi riskinä muutamissa haastatteluissa. Etenkin identiteetin- ja pääsynhallinnan asiantuntijoiden mielestä organisaatioiden identiteetin- ja pääsynhallinnan uudistuksissa useimmiten epäonnistumisen aiheuttaa sidosryhmien sitoutumattomuus siihen. Identiteetin- ja pääsynhallinta on merkittävä osa organisaatioita ja koskettaa kaikkia sidosryhmiä, joten heidän tulisi olla mukana myös sen suunnittelussa ja käyttöönotossa. Muutosvastaisuus on perinteinen teknologiaan liittyvä riski, joka nousi esiin myös tässä tutkimuksessa.

Erilaiset organisaation sisäiset riskit esiintyivät niin kirjallisuuskatsauksessa, kuin empiirisessä tutkimuksessakin. Haastattelututkimuksessa esiin nousseet riskit olivat huomattavasti käytännön läheisimpiä kuin kirjallisuuskatsauksen löydät, mutta molemmissa tunnistettiin samoja riskejä. Kirjallisuudessa sisäpiirin hyökkäykset nostettiin identiteetin- ja pääsynhallinnan merkittävänä riskinä, ja tämä tunnistetiin myös haastatteluissa. Haastatteluiden mukaan sisäpiirin hyökkäykset ovat organisaatioille hyvin haastava riski, mutta niiden välttämiseen on paljon eri keinoja, jotka ulottuvat myös identiteetin- ja pääsynhallinnan rajojen ulkopuolelle. Organisaation sisäiset riskit ovatkin riskiteemana sellainen kokonaisuus, johon ratkaisukeinoja tulee löytää paljon laajemmalta organisaatiosta, kuten viestinnästä, työntekijöiden koulutuksesta ja erilaisista tietoturvakäytännöistä. Pelkästään identiteetin- ja pääsynhallinnan keinot eivät riitä kaikkien näiden riskien ratkaisuun tai välttämiseen.

6.2 Tutkimuksen luotettavuus

Aineiston ja tutkimuksen luotettavuutta tarkastellaan validiteetilla ja reliabiliteetilla. Tutkimuksen luotettavuus tarkoittaa pätevyyttä ja ilmaisee kuinka hyvin tutkimuksessa käytetty tutkimusmenetelmä mittaa tutkittavaa ilmiötä (Hirsijärvi ym., 2009). Tutkimuksen luotettavuutta pyrittiin varmistamaan tutki-

musmenetelmän valinnalla ja empiirisen tutkimuksen sekä kirjallisuuskatsauksen tulosten kriittisellä vertailulla.

Teemahaastattelu antaa rikkaammat tulokset tällaisessa tutkimuksessa, jonka tarkoituksena oli kartoittaa riskejä haastateltaville ennestään tutusta aihepiiristä. Teemahaastattelu antoi mahdollisuuden esittää kysymyksiä teemoittain, joka auttoi haastateltavia hahmottamaan riskejä, mutta antoi myös heille hyvin laajasti mahdollisuuksia pohtia haastattelun teemoja laajasti. Teemahaastattelu antoi myös tutkijalle mahdollisuuden esittää tarkempia kysymyksiä halutessaan kattavampien vastausten saamiseksi, koska tutkimuksen rakenne ei ollut absoluuttinen.

Tutkimuksen luotettavuutta tukee kahden eri tutkimusmenetelmän käyttö, joka mahdollisti tutkimustulosten vertailun. Tutkimuksessa käytettiin tutkimusongelman ratkaisemiseen kirjallisuuskatsausta ja tapaustutkimusta. Kahden tutkimustavan käyttäminen antoi tuloksille vertailukohdetta ja tässä tutkimuksessa suurin osa näiden kahden tuloksista tuki toisiaan. Molempien tutkimusten tulokset olivat linjassa, mutta sisälsivät myös tiettyjä eroavaisuuksia.

Tutkimuksen luotettavuutta pyrittiin saavuttamaan tarkkaan kuvatulla ja avoimella tutkimusprosessilla. Lisäksi tutkimuksessa haastateltiin tutkimuksen aiheen asiantuntijoita, joilla on kokemusta lukuisista identiteetin- ja pääsynhallinnan ratkaisuista, toteutuksista ja projekteista. Kuitenkin kyseessä on yhden asiantuntijaorganisaation tapaustutkimus, johon haastateltiin kymmentä henkilöä, joten tulokset eivät ole yleistettävissä, mikä toisaalta ei ole tapaustutkimuksen tavoite. Empiirisessä tutkimuksessa haastateltiin henkilöitä useista eri organisaatioryhmistä, koska haluttiin saada mahdollisimman monipuoliset tulokset aihepiirin osaajilta.

6.3 Jatkotutkimusaiheet

Tämän tutkielman tavoitteena oli kartoittaa identiteetin- ja pääsynhallintaan liittyviä riskejä asiantuntijaorganisaatioissa. Tutkimuksessa on joitakin rajoitteita ja tutkimuksessa huomattiin tarve myös jatkotutkimukselle.

Tässä tutkielmassa käsiteltiin ainoastaan identiteetin- ja pääsynhallinnan riskejä, eikä otettu kantaa esimerkiksi riskien minimoimiseen tai välttämiseen mitenkään. Jatkotutkimusaiheena voisi pohtia, miten näitä havaittuja riskejä voidaan minimoida organisaatioissa tai mahdollisesti välttää kokonaan. Kuten tutkielmassa todettiin, identiteetin- ja pääsynhallintaan liittyvät riskit voivat olla organisaatioille todella merkittäviä, joten aiheen jatkotutkiminen olisi tärkeää.

Lisäksi tutkimuksen aikana nousi esiin useita kertoja niin kirjallisuuskatsauksessa, kuin empiirisessä tutkimuksessakin jonkin riskin olevan sen hyötyjä pienempi. Tämän vuoksi olisi mielenkiintoista pohtia, kuinka merkittäviä nämä tutkimuksessa havaitut riskit todellisuudessa ovat organisaatioille. Toisaalta olisi myös mielenkiintoista saada laajempaa empiiristä tutkimusmateriaalia esimerkiksi tekemällä laajemman tapaustutkimuksen useassa organisaatiossa.

Vaikka tutkimuksen laaja-alaisuutta pyrittiin saavuttamaan valikoimalla sopiva haastatteluotanta ja haastateltavia useista eri asiantuntijaryhmistä, on tutkimus kuitenkin toteutettu vain yhden organisaation sisällä.

On myös hyvä huomioida, että tässä tutkimuksessa keskityttiin vain asiantuntijaorganisaatioihin, joten riskit voivat olla aivan erilaisia tai eri merkityksessä eri toimialoilla. Näistä jatkotutkimusaiheista saatavien tietojen perusteella voitaisiin merkittävästi tehostaa organisaatioiden identiteetin- ja pääsynhallinnan riskikartoitusta sekä riskien torjuntaa.

7 YHTEENVETO

Nykypäivän organisaatioissa käsitellään suurta määrää omaa sekä asiakkaidensa sensitiivistä dataa. Erilaiset tietovuodot ja tietoturvariskit ovat merkittäviä uhkia organisaatioiden maineelle sekä taloudelle. Identiteetin- ja pääsynhallinta ovat suuressa roolissa yrityksen resurssien turvaamiseksi, koska niiden avulla voidaan varmistaa organisaatioresursseihin pääsy vain oikeille auktorisoiduille tahoille.

Tämän pro gradu -tutkielman tavoitteena oli selvittää, millaisia riskejä identiteetin- ja pääsynhallintaan liittyy asiantuntijaorganisaatioissa. Tutkimus oli tapaustutkimus, joka toteutettiin toimeksiantoja kohdeorganisaatiolle. Kohdeorganisaatio sopi tapaustutkimuksen kohteeksi, koska kohdeorganisaatiossa työskentelee tutkielman aihepiirin asiantuntijoita, jonka lisäksi organisaatiossa suunnitellaan merkittäviä muutoksia identiteetin- ja pääsynhallintaan.

Tämän tutkielman tutkimusongelma oli ”Millaisia potentiaalisia riskejä identiteetin- ja pääsynhallintaan liittyy asiantuntijaorganisaatioiden näkökulmasta?”

Tutkimuskysymyksiksi laadittiin seuraavat:

1. Mitä identiteetin- ja pääsynhallinta tarkoittaa organisaatiokontekstissa?
2. Millaisia riskejä identiteetin- ja pääsynhallintaan liittyy asiantuntijaorganisaatioiden näkökulmasta?

Ensimmäiseen tutkimuskysymykseen vastattiin kokonaisuudessaan kirjallisuuskatsauksen avulla, luvuissa kaksi ja kolme, joissa esiteltiin identiteetin- ja pääsynhallintaa yleisesti organisaatiokontekstissa sekä identiteetin- ja pääsynhallinnan malleja. Identiteetin- ja pääsynhallinnan mallit ovat merkittävä osa tätä kokonaisuutta, jonka vuoksi niistä yleisimmät esiteltiin kirjallisuuskatsauksessa.

Identiteetin- ja pääsynhallinta tarkoittaa organisaatioissa kaikkea, mikä liittyy käyttäjien käyttöoikeuksiin tai käyttäjän identiteettiinsä organisaatiossa. Kyse voi olla organisaation työntekijöiden identiteettienhallinnasta tai työnteki-

jöiden ja asiakkaiden. Tässä tutkielmassa käsiteltiin organisaation sisäistä identiteetin- ja pääsynhallintaa, eikä otettu kantaa asiakkaiden identiteetin- ja pääsynhallintaan.

Identiteetin- ja pääsynhallinta koostuu kahdesta kokonaisuudesta, identiteetinhallinnasta ja pääsynhallinnasta. Identiteetinhallinta kattaa käyttäjän identiteettiin liittyvät toiminnot ja prosessit, kuten identiteetin varastoinnin ja sen käsittelyn. Pääsynhallinta puolestaan sisältää käyttäjän valtuuttamiseen, tunnistamiseen ja todentamiseen liittyvät toiminnot ja prosessit. Pääsynhallinnan toimintoja ovat muun muassa käyttöoikeuden myöntäminen käyttäjälle tiettyyn organisaatioresurssiin.

Identiteetin- ja pääsynhallinta siis kattaa organisaatioissa kaikki käyttäjän identiteettiin ja käyttöoikeuksiin liittyvät toiminnot tämän työsuhteen alusta loppuun. Identiteetin- ja pääsynhallinta on tärkeä osa organisaation toimintaa, koska sen avulla voidaan ylläpitää tietoturvaa ja varmistaa järjestelmiin ja resursseihin pääsy vain sellaisilta henkilöitä, joilla on siihen oikeus. Tämän lisäksi työntekijöillä tulee olla tarvittavat oikeudet silloin kun niitä tarvitaan, jotta työntekoon ei tule seisauksia.

Identiteetin- ja pääsynhallinta voi olla hallittu keskitetysti tai hajautetusti, riippuen onko organisaatiolla käytössä hajautettu- vai keskitetty identiteetinhallintamalli. Keskitetyssä identiteetinhallintamallissa kaikki toiminnot toteutetaan yhdestä keskitetystä järjestelmästä, ja kaikki identiteetit ja käyttäjien oikeudet hallitaan sen kautta. Keskitetty identiteetin- ja pääsynhallinta on yleisesti organisaatioissa tavoitetila, koska se mahdollistaa huomattavasti selkeämmät toimintatavat ja helpottaa identiteetin- ja pääsynhallintaa. Selkeät toimintatavat ja prosessit lisäävät hallittavuutta, jonka seurauksena tietoturvallisuus kasvaa ja ylläpito on yksinkertaisempaa. Selkeät ja yksinkertaiset toimintatavat helpottavat esimerkiksi käyttöoikeuksien katselmointia, ja minimoivat virheellisten käyttöoikeuksien mahdollisuutta.

Automaatio on merkittävässä roolissa identiteetin- ja pääsynhallinnassa. Nykyisin hyvin moni identiteetin- ja pääsynhallinnan toiminto on mahdollista automatisoida, ja siten vapautta organisaatioissa työaikaa strategisempiin tehtäviin rutiinitehtävistä. Automaatio myös nopeuttaa prosesseja ja poistaa inhimillisten virheiden mahdollisuuden, jota manuaalisuus aiheuttaa. Toisaalta taas automaatiokin voi tehdä virheitä, ja vaatii ylläpitoa ja jatkuvaa seurantaa. On myös hyvä huomioida, ettei kaikkia toimintoja välttämättä pystytä saamaan automaation piiriin esimerkiksi monimutkaisuuden takia.

Toiseen tutkimuskysymykseen haettiin vastausta sekä lähdekirjallisuudesta että empiriasta. Luvussa 2.5. esiteltiin identiteetin- ja pääsynhallintaan yleisesti liittyviä riskejä ja luvussa kolme tiettyihin malleihin liitonnaisia riskejä. Näiden kirjallisuuskatsauksesta löydettyjen riskien perusteella muodostettiin teemahaastattelurunko empiiriseen tutkimukseen, jolla pyrittiin selvittämään identiteetin- ja pääsynhallintaan liittyviä riskejä organisaatiokontekstissa.

Empiirinen tutkimus toteutettiin laadullisella tutkimusotteella, tapaustutkimuksena teemahaastatteluiden avulla. Teemahaastatteluun osallistui kymmenen kohdeorganisaation työntekijää, kolmesta eri asiantuntijaryhmästä. Tut-

kimukseen osallistuneita asiantuntijaryhmiä olivat tietohallinnon asiantuntijat, identiteetin- ja pääsynhallinnan asiantuntijat sekä sisäisen tietoturvan asiantuntijat.

Kirjallisuuskasauksessa havaittuja riskiteemoja olivat automaatioon liittyvät riskit, organisaation sisäiset riskit, keskitettyyn identiteetin- ja pääsynhallintaan liittyvät riskit, hajautuneisuuteen liittyvät riskit sekä manuaalityön riskit. Pilvipalveluihin liittyviä riskejä ei erikseen käsitelty kirjallisuudessa identiteetin- ja pääsynhallinnan yhteydessä, mutta pilvipalveluiden riskeihin liittyvä kysymys otettiin haastattelurunkoon mukaan, koska pilvipohjaiset identiteetin- ja pääsynhallinnan järjestelmät ovat hyvin yleisiä nykypäivänä. Empiirisen tutkimuksen perusteella nostettiin nämä samat riskit selkeinä teemoina esiin, koska kaikki teemat toistuivat myös empiirisessä tutkimuksessa lukuisia kertoja. Näin ollen voidaan todeta identiteetin- ja pääsynhallintaan liittyvän seuraavia riskiteemoja organisaatiokontekstissa:

- manuaalityön riskit
- hajautuneisuudesta johtuvat riskit
- pilvipalveluihin liittyvät riskit
- keskitetyn identiteetin- ja pääsynhallinnan riskit
- automaation riskit
- organisaation sisäiset riskit

Kirjallisuuskatsauksen perusteella muodostetut identiteetin- ja pääsynhallinnan riskiteemat tunnistettiin riskeiksi myös empiirisessä tutkimuksessa. Haastateltavat tunnistivat runsaasti näihin teemoihin liittyviä riskejä. Manuaalisen työn riskit vaihtelivat todella merkittävistä pienempiin, lähinnä tehokkuutta laskeviin riskeihin. Toisaalta taas manuaalinen työ vaatii tekijältään paljon resursseja, koska manuaaliset prosessit voivat olla todella hitaita ja monimutkaisia. Monimutkaisuus nostaa inhimillisen virheen mahdollisuutta, ja kiireessä riskien määrä moninkertaistuu. Tämän lisäksi puhuttaessa manuaalisista prosesseista on niiden toteutus aina ihmisen varassa, jolloin jokin pieni unohdus tai vahinko voi aiheuttaa mittavia seurauksia organisaatioille.

Nykypäivänä identiteetin- ja pääsynhallinnassa pyritään eroon manuaalisuudesta ja tilalle on tullut automaatio. Automaatio tehostaa ja selkeyttää prosesseja, jonka lisäksi se vapauttaa työntekijät rutiinitehtävistä strategisempiin työtehtäviin. Automaatio itsessään sisältää kuitenkin myös ongelmia, joita tutkimuksessa nousi esiin runsaasti. Onkin olennaista miettiä, kuinka merkittäviä nämä automaation riskit ovat verrattuna manuaalisen työn riskeihin, ja kumpi toteutustapa on organisaatiolle parempi valinta. Haastatteluissa nousi esiin automatisoitujen prosessien määrän kannattavuuden riittävän kohdeorganisaation koosta. Pienempien organisaatioiden voi olla kannattavampaa toteuttaa prosessit manuaalisesti, kun taas suuremmille se on todella työläs toteutustapa.

Tutkimuksessa esiintyneistä riskeistä osa on sellaisia, joiden ratkaisuun eivät pelkästään identiteetin- ja pääsynhallinnan työkalut ja keinot riitä. Esimerkiksi organisaation sisäisten riskien minimoimiseen vaaditaan useamman

eri organisaatioryhmän ja osa-alueen apua. Lisäksi tutkimuksessa esiintyneet riskit liittyen pilvipalveluihin ja automaatioon olivat enemmän yleisesti pilvipalveluihin liittyviä riskejä, eivätkä ole vain liitoksissa identiteetin- ja pääsynhallintaan.

Tutkimuksen tulosten perusteella voidaan todeta identiteetin- ja pääsynhallintaan liittyvän runsaasti erilaisia riskejä asiantuntijaorganisaatioissa. Näillä riskeillä voi olla organisaatioille tuhoisia seurauksia, kuten taloudellisia tai maineeseen liittyvä riskejä. Organisaatioiden tulisikin ottaa nämä tutkielmassa esiin nousseet identiteetin- ja pääsynhallinnan riskit huomioon, etenkin suunnitellessaan identiteetin- ja pääsynhallinnan uudistuksia.

LÄHTEET

Anilkumar, C., & Sumathy, S. (2018). Security strategies for cloud identity management—A study. *International Journal of Engineering & Technology*, 7(2), 732-741.

Anttila, P. (2000). Tutkimuksen taito ja tiedon hankinta. 3. painos. Jyväskylä, Gummerus.

Azure. (15.6.2020a). Azure Active Directory. Haettu osoitteesta: https://azure.microsoft.com/en-gb/services/active-directory/

Azure. (17.6.2020b). Azure Active Directory security and governance. Haettu osoitteesta: https://azure.microsoft.com/en-gb/services/active-directory/security/

Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for federated identity management. Journal of Computer Security, 18(4), 541-572.

Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. Computers & Security, 39, 237-254.

Benbasat, I., Goldstein, D. K. & Mead, M. (1987). The case research strategy in studies of information systems. MIS Quarterly, 369-386.

Bodkin, R. (2004, March). Enterprise security aspects. In AOSD'04 International Conference on Aspect-Oriented Software Development (pp. 1-12).

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. International Journal of Accounting Information Systems, 15(2), 149-165.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Camp, J. L. (2004). Digital identity. IEEE Technology and society Magazine, 23(3), 34-41.

Chadwick, D. W. (2009). Federated identity management. In Foundations of security analysis and design V (pp. 96-120). Springer, Berlin, Heidelberg.

Chen, L., & Crampton, J. (2011, June). Risk-aware role-based access control. In International Workshop on Security and Trust Management (pp. 140-156). Springer, Berlin, Heidelberg.

Coyne, E., & Weil, T. R. (2013). ABAC and RBAC: scalable, flexible, and auditable access management. IT Professional, (3), 14-16.

Darke, P., Shanks, G. & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. Information systems journal, 8(4), 273-289.

Deng, H. F., Deng, W., Li, H., & Yang, H. J. (2010). Authentication and access control in RFID based logistics-customs clearance service platform. International Journal of Automation and Computing, 7(2), 180-189.

Dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2014, May). A dynamic risk-based access control architecture for cloud computing. In 2014 IEEE Network Operations and Management Symposium (NOMS) (pp. 1-9). IEEE.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), 20-29.

Eriksson, P., & Koistinen, K. (2005). Monenlainen tapaustutkimus. Kuluttajantutkimuskeskus. Haettu 9.5.2020 osoitteesta: https://helda.helsinki.fi/bitstream/handle/10138/152279/Monenlainen_tapaustutkimus.pdf

Eskola, J., & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Feng, F., Lin, C., Peng, D., & Li, J. (2008, September). A trust and context based access control model for distributed systems. In 2008 10th IEEE International Conference on High Performance Computing and Communications (pp. 629-634). IEEE.

Gauthier, F., & Merlo, E. (2012, October). Fast detection of access control vulnerabilities in php applications. In 2012 19th Working Conference on Reverse Engineering (pp. 247-256). IEEE.

Godha, R., Prateek, S., & Kataria, N. (2014). Home automation: Access control for IoT devices. International journal of scientific and research publications, 4(10), 1.

Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. IEEE security & privacy, 9(5), 48.

Hirsjärvi, S. & Huttunen, J. (1995). Johdatus Kasvatustieteeseen. ISBN 951-0-20512-5.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. Helsinki: Tammi.

Hirsjärvi, S., & Hurme, H. (2015). Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö Sirkka Hirsjärvi & Helena Hurme. Gaudeamus Helsinki University Press.

Hoffman, R. R., Johnson, M., Bradshaw, J. M., & Underbrink, A. (2013). Trust in automation. *IEEE Intelligent Systems*, *28*(1), 84-88.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human factors*, *57*(3), 407-434.

Hummer, M., Kunz, M., Netter, M., Fuchs, L., & Pernul, G. (2016). Adaptive identity and access management—contextual data based policies. EURASIP Journal on Information Security, 2016(1), 19.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). NIST special publication, 800(162).

Khan, A. R. (2012). Access control in cloud computing environment. ARPN Journal of Engineering and Applied Sciences, 7(5), 613-615.

Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48(2), 458-472.

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308-319.

Kumar, V., & Bhardwaj, A. (2018). Identity Management Systems: A Comparative Analysis. International Journal of Strategic Decision Sciences (IJSDS), 9(1), 63-78.

Kunz, M., Fuchs, L., Hummer, M., & Pernul, G. (2015a, December). Introducing dynamic identity and access management in organizations. In International Conference on Information Systems Security (pp. 139-158). Springer, Cham.

Kunz, M., Fuchs, L., Netter, M., & Pernul, G. (2015b, February). Analyzing quality criteria in role-based identity and access management. In 2015 International Conference on Information Systems Security and Privacy (ICISSP) (pp. 1-9). IEEE.

Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. Journal of information security and applications, 44, 64-79.

Maesa, D. D. F., Mori, P., & Ricci, L. (2017, June). Blockchain based access control. In IFIP International Conference on Distributed Applications and Interoperable Systems (pp. 206-220). Springer, Cham.

Metsämuuronen, J. (2008). Laadullisen tutkimuksen perusteet (3. uud. p.). Helsinki: International Methelp.

Microsoft. (15.6.2020a). What is Azure Active Directory? Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (15.6.2020b). Classic subscription administrator roles, Azure roles, and Azure AD roles. Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/role-based-access-control/rbac-and-directory-admin-roles

Microsoft. (17.6.2020c). What is Azure role-based access control (Azure RBAC). Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/role-based-access-control/overview

Microsoft. (17.6.2020d). What is Conditional Access? Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/overview

Microsoft. (17.6.2020e). What is Azure AD Identity Governance? Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/active-directory/governance/identity-governance-overview

Microsoft. (17.6.2020f). What is Azure AD entitlement management? Haettu osoitteesta: https://docs.microsoft.com/en-gb/azure/active-directory/governance/entitlement-management-overview

Myers, M. D. (1997). Qualitative Research in Information Systems. MIS Quarterly 21 (2), 241-242.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and organization, 17(1), 2-26.

Näpärä. (2017). Haastattelun lajityypit. Spoken". Haettu 14.5.2020 osoitteesta: https://spoken.fi/2180/

Petrovska, J., Memeti, A., & Imeri, F. (2019, June). SOA Approach-Identity and Access Management for the Risk Management Platform. In 2019 8th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-4). IEEE.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Popescu, I. P., Barbu, C. A., & Popescu, M. (2015). Identity and access management-a risk-based approach. In Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE (Vol. 9, No. 1, pp. 572-580). Faculty of Management, Academy of Economic Studies, Bucharest, Romania.

Sarajärvi, A., & Tuomi, J. (2017). Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos. Tammi.

Sirisha, A., & Kumari, G. G. (2010, December). API access control in cloud using the role based access control model. In Trendz in Information Sciences & Computing (TISC2010) (pp. 135-137). IEEE.

Sun, F., Xu, L., & Su, Z. (2011, August). Static Detection of Access Control Vulnerabilities in Web Applications. In USENIX Security Symposium (Vol. 64).

Tuecke, S., Ananthakrishnan, R., Chard, K., Lidman, M., McCollam, B., Rosen, S., & Foster, I. (2016, October). Globus Auth: A research identity and access management platform. In 2016 IEEE 12th International Conference on e-Science (e-Science) (pp. 203-212). IEEE.

Van Swol, L. M., & Sniezek, J. A. (2005). Factors affecting the acceptance of expert advice. British journal of social psychology, 44(3), 443-461.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Yin, R. K. (2003). Case study research: Design and methods. Sage publications.

LIITE 1 HAASTATTELURUNKO

Haastattelukysymykset

Perustiedot

1. Mikä on roolisi organisaatiossa?
2. Mikä on kokemuksesi identiteetin ja pääsynhallinnasta?
3. Millainen rooli sinulla on yrityksen identiteetin- ja pääsynhallinnan ratkaisuihin liittyvissä päätöksissä?

Nykyinen ratkaisu

4. Miten identiteetin- ja pääsynhallinta on nyt toteutettu?
5. Miten käyttäjien oikeudet määräytyvät? (esim. roolit, ominaisuudet)
6. Miten lisäoikeuksien pyytäminen ja myöntäminen on toteutettu?
7. Katselmoidaanko oikeuksia mitenkään? Miten ja kuinka usein?
8. Onko nykyisessä ratkaisussa ollut ongelmia? Millaisia?
9. Millaisia riskejä nykyisessä ratkaisussa on?
10. Miksi nykyinen ratkaisu päädyttiin vaihtamaan?

Uusi ratkaisu

11. Millaisia asioita uudelta IAM-ratkaisulta toivotaan?
12. Olisiko uusi ratkaisu keskitetty vai hajautettu järjestelmä?
13. Miten käyttäjien oikeudet määräytyvät?
14. Minkä verran automaatiota olisi tarpeen olla uudessa ratkaisussa?
15. Mitä vahvuuksia uudella ratkaisulla tulee olla verrattuna vanhaan toteutukseen?
16. Miten IAM-ratkaisun valinta tehdään?

Riskit

17. Millaisia riskejä näet uudessa ratkaisussa? (haastateltavan kuvaama)
18. Miten IAM-ratkaisun riskejä arvioidaan?
19. Millaisia mahdollisia riskejä keskitetyssä hallintamallissa on?
20. Pidätkö riskialttiina ratkaisua, jossa on pitkälle integroitu SSO, eli käyttäjän kirjauduttua sisään laitteelle, pääsee hän kaikkialle kirjautumatta, johon käyttöoikeudet riittävät? Onko riski mielestäsi kuinka todennäköinen?
21. Miten mahdollisiin sisäpiirin hyökkäyksiin on varauduttu? Eli työntekijä tahallaan tai vahingossa vahingoittaa yrityksen resursseja, esim. haittaohjelmilla, tietovuodoilla tai muutoin.
22. Millaisia riskejä tai uhkia pilvipohjaisessa IAM-järjestelmässä on?
23. Mitä mahdollisia haittoja pitkälle automatisoiduissa ratkaisuissa on?

Lisättävää?

LIITE 2 HAASTATTELUTUTKIMUSTULOSTEN KOONTITAULUKKO

Riskiteema	Riski	Esiintyi haastatteluissa yht.	Tietohallinto	Identiteetin- ja pääsynhallinnan asiantuntijat	Sisäinen tietoturva
Manuaalisuuteen liittyvät riskit	Tehottomuus	9	X	X	X
	Työläys	9	X	X	X
	Prosessien hitaus ja kankeus	9	X	X	X
	Inhimilliset virheet	7	X	X	X
	Jatkokehitysmahdollisuuksien rajallisuus	2	X		
Hajautuneisuuteen liittyvät riskit	Haastava hallinnoida	9	X	X	X
	Virheelliset oikeudet	9	X	X	X
	Sekavat ja epäselvät prosessit	9	X	X	X
	Kokonaisvaltaisen näkyvyyden puute	8	X	X	X
	Auditoinnin hankaluus	7	X	X	X
	Suuren sovellus määrän aiheuttama sekavuus	6	X	X	X
Pilvipalveluihin liittyvät riskit identiteetin- ja pääsynhallinnalle	Tietoturva	3	X	X	
	Riippuvaisuus palveluntarjoajasta	3		X	
	Perinteiset pilvipalveluriskit	3		X	X
	Modifioimattomuus	2		X	
	Osaamisriski	1		X	
	Asiakkaiden menetys	1		X	
	Säännösten noudattamattomuus	1		X	
	Riippuvaisuus yhdestä sovelluksesta tai järjestelmästä	5	X	X	X
	Kustannukset	3		X	X

Keskitettyyn identiteetin- ja pääsynhallintaan liittyvät riskit	Sisäpiirin hyökkäykset	3		X	X
	Tietoturva	2	X		X
	Haastava implementointi	2	X	X	
	Laajalle skaalautuvat ongelmat	2	X	X	
Automaation aiheuttamat riskit	Prosessien joustamattomuus ja poikkeustapaukset	7	X	X	X
	Virheellinen toteutus	6	X	X	X
	Huoleton ylläpito	6	X	X	X
	Osaamisriski	4	X	X	X
	Järjestelmävirheet	4		X	X
	Kustannukset	1		X	
Organisaation sisäiset riskit	Prosesseihin liittyvät ongelmat	6	X	X	X
	Osaamisriski	6	X	X	X
	Sisäpiirin hyökkäykset	5	X	X	X
	Kustannukset	4	X	X	X
	Sidosryhmien sitouttaminen	3	X	X	
	Muutosvastaisuus	2	X	X	