Otto Lankia

OHJELMISTOROBOTIIKAN TIETOTURVAN HALLINTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Lankia, Otto
Ohjelmistorobotiikan tietoturvan hallinta
Jyväskylä: Jyväskylän yliopisto, 2021, 66 s.
Tietojärjestelmätiede, pro-gradu tutkielma
Ohjaajat: Järvinen, Janne; Siponen, Mikko

Ohjelmistorobotiikka on teknologia, joka soveltuu rutiininomaisten työtehtävien automatisoimiseen. Tämän tutkielman tarkoituksena oli tutustua ohjelmistorobotiikan ominaispiirteisiin, sekä syventyä tarkastelemaan ohjelmistorobotiikan tietoturvaa ja sen hallintaan. Tavoitteena oli kartoittaa ohjelmistorobotiikkaan kohdistuvia tietoturvahaasteita sekä löytää keinoja näihin haasteisiin vastaamiseksi. Tutkimus koostuu kirjallisuuskatsauksesta sekä empiirisestä osiosta, joka toteutettiin yksittäisenä tapaustutkimuksena. Tutkimusmateriaali kerättiin teemahaastattelujen avulla, jonka analysointiin sovellettiin teorialähtöisen sisällönanalyysin menetelmää. Tutkimus osoitti, että identiteetin- ja pääsynhallinnan kokonaisuus on merkittävin tekijä ohjelmistorobotiikan tietoturvan hallinnan kannalta. Keskeisimmät löydökset liittyivät ohjelmistorobotin digitaalisen identiteetin elinkaareen ja sen hallintaan, salasanakäytäntöihin, tunnistautumismenetelmiin sekä ohjelmistorobotin käyttöoikeuksiin kohdejärjestelmien sisällä. Muita ohjelmistorobotiikan tietoturvanhallintaan keskeisesti liittyviä teemoja olivat datan eheys, informaatioteknologian kuluttajistuminen sekä tietosuoja. Tutkimus osoitti, että keskeisiä keinoja ohjelmistorobotiikan tietoturvan varmistamiseksi ovat organisaation tietoturvapolitiikan ja muiden tietoturvamallien ja -rakenteiden noudattaminen ja soveltaminen, eri sidosryhmien osallistaminen sekä tietoisuuden lisääminen organisaation sisällä.

Asiasanat: ohjelmistorobotiikka, tietoturva, identiteetin- ja pääsynhallinta, datan eheys, informaatioteknologian kuluttajistuminen, tietosuoja

ABSTRACT

Lankia, Otto
Security management of robotic process automation
Jyväskylä: University of Jyväskylä, 2020, 66 pp.
Information Systems Science, Master's Thesis
Supervisors: Järvinen, Janne; Siponen, Mikko

Robotic process automation is a technology that is suitable for automating routine work tasks. The purpose of this study was to explore the characteristics of robotic process automation and focus on its information security and security management. The aim was to detect the security challenges of robotic process automation and to find ways to meet these challenges. This study consists of a literature review and an empirical section, which was conducted as a single case study. The research material was collected through thematic interviews, which were analyzed using the method of theory-based content analysis. The study showed that the area of identity and access management is the most significant factor in the security management of the robotic process automation. The main findings were related to the life cycle and management of software robot's digital identity, password policies, authentication methods, and software robot access rights within the target systems. Other important themes related to information security management in robotic process automation were data integrity, the consumerization of information technology, and data privacy. The study showed that applying the organization's security policy and other information security models is the main way to ensure the security of robotic process automation. Also, involvement of various stakeholders and increasing awareness within the organization are required to ensure proper information security management of robotic process automation.

Keywords: robotic process automation, information security, identity and access management, data integrity, consumerization of information technology, privacy

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Ohjelmistorobotiikasta (engl. *robotic process automation, RPA*) on tulossa olennainen osa organisaatioiden tavasta harjoittaa liiketoimintaa (Madakam, Holmukhe & Jaiswal, 2019). Sen kysyntä on kovassa kasvussa, ja ohjelmistorobotiikkatyökaluja tarjoavien toimijoiden määrä markkinoilla on viime vuosien aikana kasvanut huomattavasti (Van der Aalst, Bichler & Heinzl, 2018). Ohjelmistorobotiikka tarjoaa kustannustehokkaan tavan automatisoida liikeroimintaprosesseja, vaikka järjestelmäympäristöt olisivat ajan saatossa siiloutuneet (Bygstad, 2017). Organisaatioiden kiinnostus ohjelmistorobotiikkaa kohtaan on helposti selitettävissä, sillä se tarjoaa korkean sijoitetun pääoman tuottoasteen (engl. *return on investment, ROI*) (Van der Aalst ym., 2018).

Useissa tutkimuksissa ohjelmistorobotiikan nähdään yleisesti ottaen parantavan prosessien tietoturvaa verrattuna prosessien manuaaliseen toteutukseen (Asatiani & Penttinen, 2016; Syed ym., 2020). Tästä huolimatta noin kolmanneksella ohjelmistorobotiikkaa hyödyntävistä organisaatioista on ollut kyseiseen teknologiaan liittyviä tietoturvahaasteita (Willcocks, Hindle & Lacity, 2018). Vaikka tietoturva on yksi keskeisimmistä tekijöistä uusien teknologioiden menestymisen kannalta (Ramgovind, Eloff & Smith, 2010), niin ohjelmistorobotiikan tietoturva on yhä edelleen riittämättömästi tutkittu aihealue. Näin ollen aihetta tutkimalla on mahdollista lisätä kokonaisvaltaista ymmärrystä ja luoda täysin uutta tietoa aiheesta. Tämä tutkielma suoritetaan toimeksiantona, joten se tarjoaa myös käytännön hyötyä toimeksiantajaorganisaatiolle varmistamalla ohjelmistorobotiikan hyödyntämisen tietoturvallisella tavalla.

Tämän tutkielman toimeksiantajaorganisaatio on hyödyntänyt ohjelmistorobotiikkaa noin kahden vuoden ajan. Organisaatiossa ohjelmistorobotiikan hankintamallina toimii Robotics-as-a-Service (*RaaS*), jossa palveluntarjoaja tarjoaa ohjelmistorobotiikan palveluita pilvipalvelun muodossa. Näin ollen toimeksiantajaorganisaatio ei vastaa IT-infrastruktuurista tai alustasta palvelun takana, vaan nämä kuuluvat palveluntarjoajan vastuualueelle.

Tämän tutkielman tarkoituksena on selvittää, millaisia tieturvaongelmia ohjelmistorobotiikkaan liittyy, ja kuinka nämä ongelmat tulisi ottaa huomioon ohjelmistorobotin elinkaaren eri vaiheissa. Tutkimuksessa tarkastellaan

nimenomaan tietoturvahaasteita, eikä muita ohjelmistorobotiikan ongelmakohtia. Tässä tutkimuksessa ongelman nähdään lukeutuvan tietoturvaongelmiin, mikäli se vaarantaa datan luottamuksellisuuden, eheyden tai saatavuuden suoraan tai välillisesti. Tämän tutkimuksen tutkimuskysymykset ovat seuraavat:

- Mitä tietoturvahaasteita ohjelmistorobotiikkaan liittyy?
- Kuinka ohjelmistorobotiikan tietoturva voidaan varmistaa?

Tutkimuksen kannalta olennaista on tunnistaa ohjelmistorobotiikan tietoturvahaasteet ja löytää mahdolliset syyt tai muut altistavat tekijät niiden taustalla, jotta myös toiseen tutkimuskysymykseen kyetään vastaamaan.

Tämä tutkielma koostuu kahdesta kokonaisuudesta, ohjelmistorobotiikkaa ja sen tietoturvaa käsittelevästä kirjallisuuskatsauksesta sekä toimeksiantajaorganisaation kontekstissa toteutetusta empiirisestä tutkimuksesta. Kirjallisuuskatsauksen tarkoituksena on luoda teoreettinen pohja tutkielman empiiriselle osiolle ja tunnistaa aiemmasta tutkimuksesta mahdollisia puutteita ja tutkimusaukkoja. Tutkielman kirjallisuuskatsauksen pääasiallisina lähteinä toimivat vertaisarvioidut tieteelliset artikkelit, ja Google Scholar toimii keskeisenä työkaluna aineiston etsimisessä. Pääasiallisina hakutermeinä toimivat *robotic process automation*, *RPA*, *security*, *information security* ja *threats*. Lähdeaineistoksi pyritään valitsemaan mahdollisimman laadukkaita julkaisuja, jotka sopivat tutkielman aihepiiriin. Lähteiden laadukkuus pyritään varmistamaan hyödyntämällä julkaisufoorumi-palvelun tarjoamia julkaisukanavien tasoluokituksia, valitsemalla julkaisupäivän perusteella mahdollisimman tuoreita artikkeleita, sekä kiinnittämällä huomiota lähteiden viittausmääriin.

Tutkielman empiirinen osio on toteutettu yksittäisenä tapaustutkimuksena, jonka aineisto kerättiin teemahaastatteluiden avulla. Haastatteluin kerätyn tutkimusmateriaalin analysointi toteutettiin Tuomen ja Sarajärjen (2018) esittelemää teorialähtöisen sisällönanalyysin mallia mukaillen. Empiirisen osion tarkoituksena on tutkia ohjelmistorobotiikan tietoturvaa toimeksiantajaorganisaation kontekstissa, ja myöhemmin verrata näitä tuloksia aiempaan kirjallisuuteen.

Tutkielman rakenne koostuu yhteensä kuudesta sisältöluvusta, joita seuraa yhteenveto. Kirjallisuuskatsaus muodostaa kolme ensimmäistä sisältölukua. Näistä ensimmäinen keskittyy esittelemään ohjelmistorobotiikan käsitettä, sen mahdollisia käyttökohteita sekä kyseisen teknologian tarjoamia hyötyjä. Toisessa sisältöluvussa tarkastellaan tietoturvaa aluksi yleisellä tasolla, jonka jälkeen perehdytään aiempaan tutkimukseen ohjelmistorobotiikan tietoturvasta. Kolmas sisältöluku toimii kirjallisuuskatsauksen yhteenvetona.

Kirjallisuuskatsausta seuraa tutkielman empiirinen osio, jossa on niin ikään kolme sisältölukua. Ensimmäisessä näistä sisältöluvuista kuvataan empiirisen tutkimuksen toteuttamista. Luvussa esitellään valittu tutkimusmenetelmä ja esitellään perusteet sen valinnalle, kuvataan tiedonkeruuprosessin toteutusta sekä analysoidaan teemahaastatteluin kerätty aineisto. Empiirisen osion toisessa sisältöluvussa esitellään yksittäisen tapaustutkimuksen tulokset luokiteltuna kirjallisuuskatsauksessa esiteltyjen kategorioiden mukaisesti. Kolmannessa sisältöluvussa vertaillaan aiempaa kirjallisuutta empiirisen osion tuloksiin. Tämän

vertailun helpottamiseksi aiemmin käytetyt kategoriat ovat osittain jaettu helpommin käsiteltäviin kokonaisuuksiin. Tutkimustulosten vertailun lisäksi sisältöluvussa arvioidaan tutkimuksen luotettavuutta sekä sen tuottamaa hyötyä, sekä esitellään tutkimusprosessin aikana esille nousseita jatkotutkimusaiheita.

Tutkimusraportin viimeisessä luvussa esitellään koko tutkielman yhteenveto, jonka jälkeen esitellään tutkimuksessa käytetyt lähteet lähdeluettelon muodossa. Tutkielma sisältää kaksi liitettä, jotka ovat empiirisessä osiossa käytetty teemahaastattelurunko sekä haastateltaville henkilöille haastattelukutsun yhteydessä lähetetyt keskeisten käsitteiden määritelmät.

2 OHJELMISTOROBOTIIKKA

Tässä luvussa käsitellään ohjelmistorobotiikkaa yleisellä tasolla. Ensimmäisessä alaluvussa määritellään ohjelmistorobotiikan käsite aiempaan tutkimukseen pohjautuen. Toisessa alaluvussa kerrotaan ohjelmistorobotiikan tyypillisistä käyttökohteista, ja kuvataan, millaisten prosessien automatisointiin kyseinen teknologia soveltuu. Kolmannessa alaluvussa tutustutaan tarkemmin ohjelmistorobotiikan tarjoamiin etuihin. Tämän kokonaisuuden tarkoituksena on tarjota lukijalle kokonaisvaltainen ja kattava käsitys ohjelmistorobotiikasta teknologiana sekä sen tyypillisistä käyttökohteista ja eduista.

2.1 Ohjelmistorobotiikan määritelmä

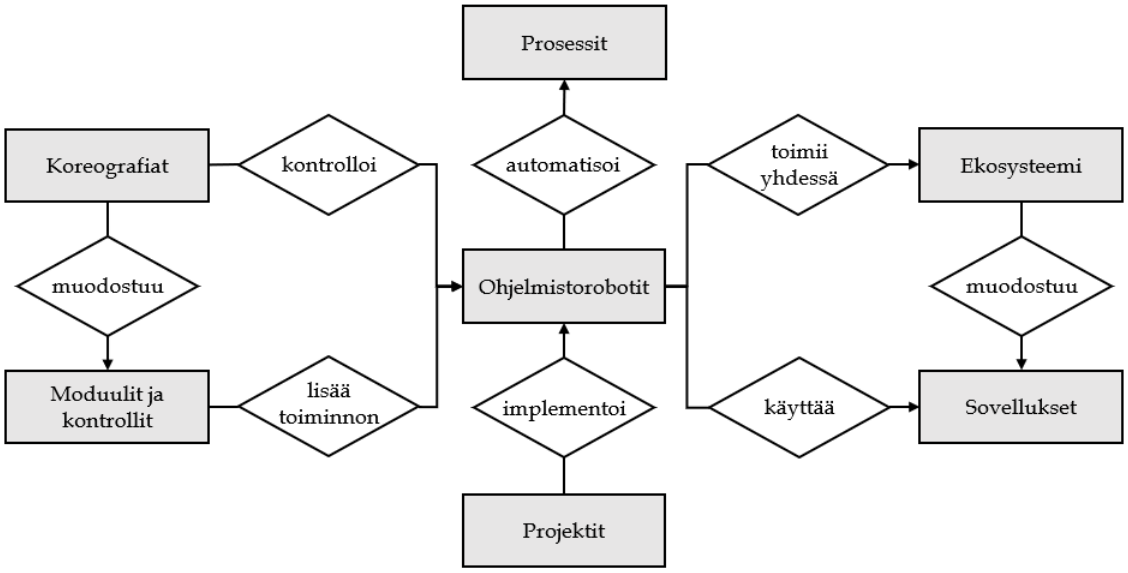
Ohjelmistorobotiikalla tarkoitetaan ohjelmistopohjaisia ratkaisuja, joiden avulla voidaan automatisoida aiemmin ihmisen tekemiä rutiininomaisia työtehtäviä (Asatiani & Penttinen, 2016; Willcocks, Lacity & Craig, 2015). Van der Aalst, Bichler ja Heinzl (2018) kirjoittavat artikkelissaan ohjelmistorobottien operoivan käyttöliittymätasolla, ja käyttävän muita järjestelmiä samalla tavalla kuin ihmiset niitä käyttäisivät. Toisin kuin muut prosessien automatisointiratkaisut, ohjelmistorobotiikka ei edellytä muutoksia muihin järjestelmiin, jotka ovat osana automatisoitavaa prosessissa (Van der Aalst ym., 2018; Willcocks ym., 2015). Eri järjestelmien tekninen yhteensopivuus voi olla heikkoa esimerkiksi, jos järjestelmät ovat huomattavan eri ikäisiä, mikä tekee ohjelmistorobotiikasta houkuttelevan ratkaisun (Hofmann, Samp & Urbach, 2020).

Tornbohm ja Dunie (2017) määrittelevät julkaisussaan ohjelmistorobotiikkatyökalut (engl. *RPA-tools*) sovelluksiksi, jotka suorittavat toimenpiteitä strukturoidulle datalle ennalta määritellyn logiikan mukaisesti. Ohjelmistorobotti kykenee noutamaan, prosessoimaan sekä siirtämään tietoa järjestelmien välillä sille annettujen ohjeiden mukaisesti (Van der Aalst ym., 2018).

Hofmann, Samp ja Urbach (2020) kirjoittavat artikkelissaan, että IEEE Corporate Advisory Group (2017) on määritellyt standardissaan ohjelmistorobotiikan seuraavasti:

> Ennalta konfiguroitu ohjelmistoinstanssi, joka noudattaa liiketoiminnan sääntöjä ja ennalta määriteltyä toimintokoreografiaa prosessien, aktiviteettien, transaktioiden, tehtävien ja niiden yhdistelmien autonomisessa suorittamisessa, joka edellyttää yhden tai useamman järjestelmän käyttöä halutun lopputuloksen saavuttamiseksi. (IEEE Corporate Advisory Group, 2017)

Alla oleva kuvio esittää ohjelmistorobotiikan luonteen visuaalisessa muodossa perustuen IEEE Corporate Advisory Groupin (2017) ohjelmistorobotiikan määritelmään.

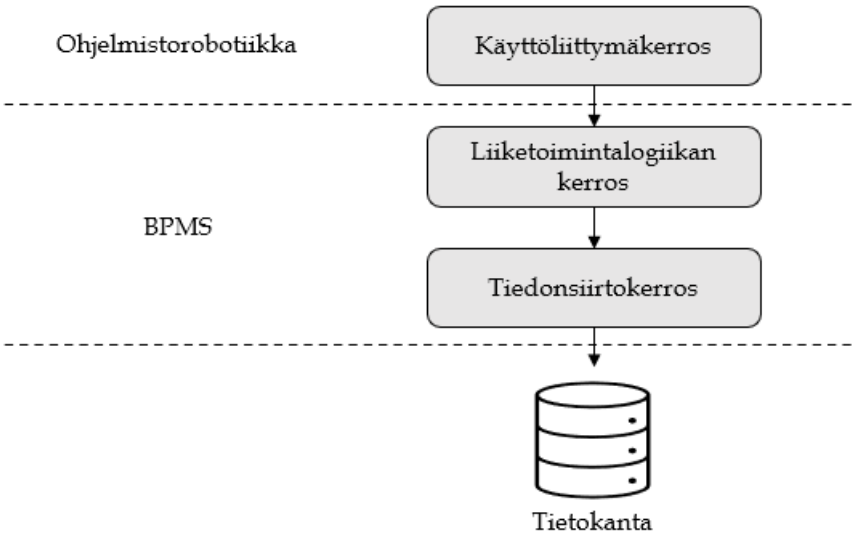


KUVIO 1 Ohjelmistorobotiikan luonne (Hofmann ym., 2020)

Bygstad (2017) kirjoittaa artikkelissaan, että ohjelmistorobotiikkaa pidetään yleisesti ottaen kevyen informaatioteknologian (engl. *lightweight IT*) ratkaisuna. Kevyen IT:n ratkaisulla tarkoitetaan edullisia ja helppokäyttöisiä tietoteknisiä ratkaisuja, joiden käyttöönotto ei edellytä syvällistä tietoteknistä osaamista, mikä on mahdollistanut informaatioteknologian kuluttajistumisen. Raskaan informaatioteknologian (engl. *heavyweight IT*) ratkaisut edellyttävät syvällisempää teknistä osaamista ja perinteisen ohjelmistokehityksen taitoja. Raskaan IT:n ratkaisuihin lukeutuvat muun muassa perinteisemmät integraatioratkaisut, kuten liiketoimintaprosessien hallintajärjestelmät (engl. *business process management system, BPMS*), jotka edellyttävät muutoksia kohdejärjestelmiin (Bygstad, 2017).

Willcocks ym. (2015) kuvaavat artikkelissaan kevyen ja raskaan informaatioteknologian ratkaisujen suhdetta muihin järjestelmiin kuvion 2 avulla. Kuten aiemmin on todettu, prosessien automatisointi raskaan informaatioteknologian ratkaisuilla, kuten liiketoimintaprosessien hallintajärjestelmillä, edellyttää muutoksia prosessissa mukana oleviin järjestelmiin. Tällaiset raskaan

informaatioteknologian ratkaisut ovat vuorovaikutuksessa muiden järjestelmien tiedonsiirtokerroksen sekä liiketoimintalogiikan kerroksen kanssa. Kevyen informaatioteknologian ratkaisut, kuten ohjelmistorobotiikka ovat vuorovaikutuksessa ainoastaan muiden järjestelmien käyttöliittymäkerrokseen, joten nämä ratkaisut eivät edellytä muutoksia muihin järjestelmiin (Willcocks ym., 2015).



KUVIO 2 Ohjelmistorobotiikka kevyen IT:n ratkaisuna (Willcocks ym., 2015)

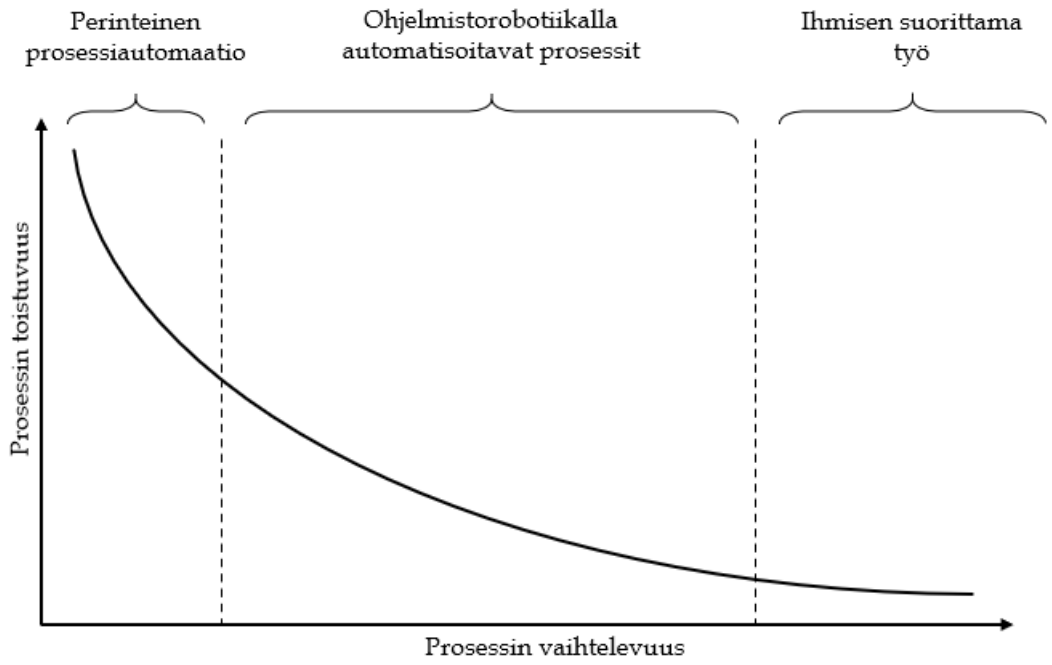
Willcocks ym. (2015) kuitenkin huomauttavat artikkelissaan, että ohjelmistorobotiikka ei ole korvaamassa liiketoimintaprosessien hallintajärjestelmiä tai muita raskaan informaatioteknologian ratkaisuja. Ohjelmistorobotiikka tulee heidän mukaansa nähdä muita ratkaisuja täydentävänä teknologiana, joka tuo lisää mahdollisuuksia erityyppisten prosessien automatisoimiseen (Willcocks ym., 2015).

2.2 Ohjelmistorobotiikan käyttökohteet

Ohjelmistorobotiikka sopii automatisointiratkaisuksi sellaisille prosesseille, jotka ovat luonteeltaan rutiininomaisia eivätkä edellytä subjektiivista päättelyä tai päätöksentekoa (Van der Aalst ym., 2018; Willcocks ym., 2015). Nyrkkisääntönä voidaan pitää sitä, että prosessi voidaan automatisoida ohjelmistorobotiikan avulla, mikäli prosessin kaikki työvaiheet voidaan kirjoittaa täsmällisesti paperille sisältäen kaikki mahdolliset vaihtoehdot ja lopputulemat (Asatiani & Penttinen, 2016). Tyypillisesti tällaiset prosessit ovat erittäin vahvasti sääntöihin pohjautuvia (Syed ym., 2020). Ohjelmistorobotin implementointi on erityisen kannattavaa, kun prosessin tehtävien volyymi on suuri, prosessi on vahvasti standardisoitu ja sen logiikan määrittely on suhteellisen yksinkertaista, tehtävät sisältävät riskin ihmisen tekemille inhimillisille virheille, ja prosessi aiheuttaa merkittäviä kustannuksia manuaalisesti toteutettuna (Asatiani & Penttinen, 2016;

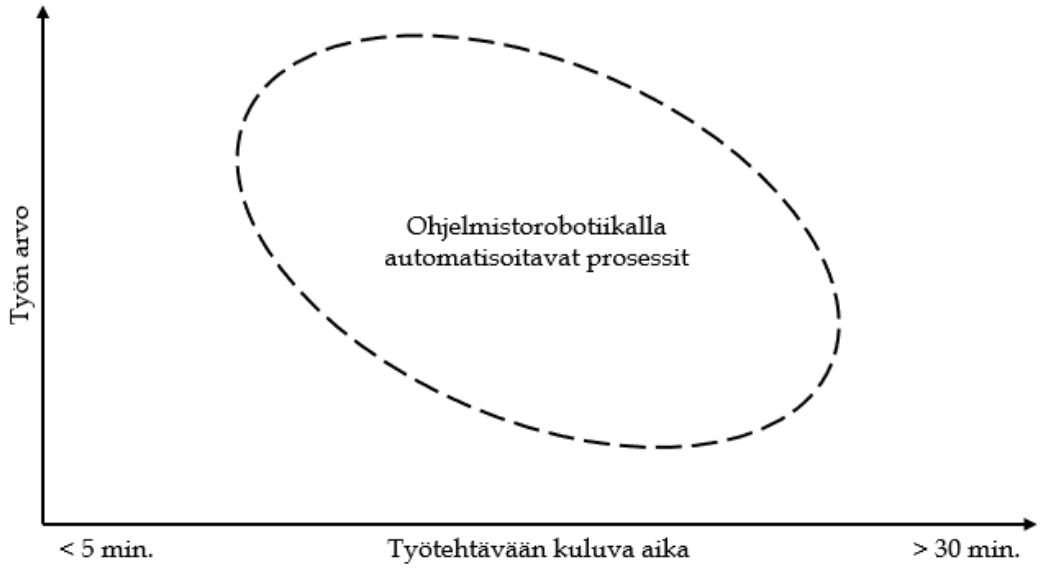
Syed ym., 2020). Mitä vähemmän prosessi sisältää poikkeuksien käsittelyä, sitä helpompaa ohjelmistorobotti on implementoida (Fung, 2014; Jovanović, Đurić & Šibalija, 2018). Ennen ohjelmistorobotin implementointia on tärkeää, että prosessi on hyvin ymmärretty ja siitä on olemassa kattava dokumentaatio (Syed ym., 2020).

Tilanteissa, joissa työn suorittaminen manuaalisesti tai liiketoimintaprosessien hallintajärjestelmien hyödyntäminen on liian kallista tai ei ole muutoin liiketoiminnan näkökulmasta perusteltua, ohjelmistorobotiikka tarjoaa varteenotettavan vaihtoehdon prosessin automatisoimiseksi (Hofmann ym., 2020; Lu, Li, Chen, Kim & Serikawa, 2018). Van der Aalst ym. (2018) esittävätkin artikkelissaan ohjelmistorobotiikan asemoituvan soveltuvuudeltaan perinteisen prosessiautomaation ja ihmisen suorittaman työn väliin kuvion 3 mukaisesti, kun työn suorittamismenetelmää arvioidaan prosessin vaihtelevuuden ja toistuvuuden näkökulmista. Kun prosessin tapaukset noudattavat samaa kaavaa, ja prosessi toistuu erittäin tiheällä frekvenssillä, niin sen automatisoiminen perinteisen prosessiautomaation keinoin on perusteltua. Prosessin monimutkaistuessa sen automatisointi perinteisen prosessiautomaation keinoin ei ole enää kustannustehokasta, jolloin ohjelmistorobotiikka soveltuu paremmin automatisointimenetelmäksi (Van der Aalst ym., 2018). Optimaalinen prosessin tehtävien toistuvuustiheys ohjelmistorobotille on 50–60 kertaa päivässä (Capgemini Consulting, 2016). Harvemmin toistuvat, monimutkaiset ja vaihtelevat prosessit, jotka eivät sisällä itseään toistavaa työtä, ja jotka vaativat subjektiivista päättelyä tai päätöksentekoa eivät kuitenkaan sovellu ohjelmistorobotiikalla automatisoitaviksi, vaan edellyttävät ihmisen tekemää manuaalista työtä (Van der Aalst ym., 2018).



KUVIO 3 Ohjelmistorobotikan soveltuvuus prosessin vaihtelevuuden ja toistuvuuden mukaan (Van der Aalst ym., 2018, s. 270)

Capgemini Consulting (2016) arvioi tutkimuksessaan ohjelmistorobotiikan soveltuvuutta prosessien automatisoimiseksi työn tuottaman arvon ja työtehtävän keston näkökulmasta kuvion 4 mukaisesti. Tutkimus osoittaa, että kun työ tuottaa tarpeeksi arvoa, ja prosessiin kuluu manuaalisesti suoritettuna yli 5 minuuttia, mutta alle 30 minuuttia, ohjelmistorobotiikka on potentiaalinen vaihtoehto prosessin automatisoimiseksi (Capgemini Consulting, 2016).



KUVIO 4 Ohjelmistorobotikan soveltuvuus työhön kuluvan ajan ja työn arvon mukaan (Capgemini Consulting, 2016)

Hofmann ym. (2020) pyrkivät tutkimuksessaan tunnistamaan ohjelmistorobotiikkatyökalujen ydinominaisuuksia, jotka he jakavat kolmeen ylemmän tason funktionaaliseen alueeseen: dataan liittyvään, integroimiseen liittyvään sekä prosessiin liittyvään alueeseen. Funktionaaliset alueet jakautuvat yhä pienemmiksi kokonaisuuksiksi, kahdeksaan funktionaaliseen luokkaan (Hofmann ym., 2020). Alla oleva taulukko esittää funktionaaliset alueet sekä niihin kuuluvat luokat. Taulukko tarjoaa myös jokaisen funktionaalisen luokan selitteen sekä käytännön tason esimerkin.

TAULUKKO 1 Ohjelmistorobotiikan funktionaaliset luokat (Hofmann ym., 2020)

Funktionaalinen alue	Funktionaalinen luokka	Selite	Esimerkki
Dataan liittyvä	Datan siirto	Toiminnot, jotka suorittavat datan siirtämisen	Välimuistin hallinta, datan salaus, tiedostojen siirto ja lataus
	Tiedoston prosessointi	Toiminnot tiedostomuotojen muuttamiseksi ja tiedostojen salaamiseksi	Tiedostojen salaus ja salauksen purkaminen, tiedostomuodon muuttaminen
	Datan analysointi	Toiminnot, jotka mahdollistavat data, kuten tekstin, äänen ja kuvien analysoinnin	Puheen käsittely tekstiksi, optinen merkkien tunnistaminen
Integrointiin liittyvä	Sovellusoperaattori	Toiminnot, jotka mahdollistavat muiden sovellusten käyttämisen	Tunnistetiedoilla järjestelmään kirjautuminen, arvojen muuttaminen laskentataulukossa
	Pilvipalveluoperaattori	Toiminnot, jotka mahdollistavat pilvipalveluiden käyttämisen	Informaation lähettäminen sosiaalisen median alustoille
	Syöttölaiteoperaattori	Toiminnot, jotka matkivat ihmisen toimia käyttöliittymätasolla	Syöttölaitteilla tehtävät toiminnot, kuten klikkaukset, raahaukset sekä ikkunoiden laajentamiset tai sulkemiset
Prosessiin liittyvä	Tapahtuman laukaisu	Toiminnot, jotka odottavat tiettyä tapahtumaa jatkotoimien aloittamiseksi	Muutosten ja tapahtumien havaitseminen, toiminnon käynnistäminen tapahtuman seurauksena
	Kontrollioperaattori	Toiminnot elementtien liittämiseksi koreografiaan	Silmukat, käyttäjän vuorovaikutus

Hofmann ym. (2020) kirjoittavat artikkelissaan, että ohjelmistorobotin on tyypillisesti yhdisteltävä näitä toiminnallisia elementtejä automaatiotehtävän suorittamiseksi. Esimerkiksi ohjelmistorobotin siirtäessä dataa järjestelmästä toiseen, se edellyttäisi sovellusoperaattoria datan noutamiseksi, datan siirtoa, sekä toista sovellusoperaattoria datan tallentamiseksi toiseen järjestelmään (Hofmann ym., 2020).

2.3 Ohjelmistorobotiikan tarjoamat edut

Ohjelmistorobotiikka tarjoaa organisaatioille useita erilaisia etuja. Vitharanage, Bandara, Syed ja Toman (2020) ovat tutkimuksessaan tunnistaneet näitä etuja, ja jakaneet ne neljään eri kategoriaan: operationaalisiin etuihin, johtamisetuihin, strategisiin etuihin sekä organisatorisiin etuihin.

Vitharanage ym. (2020) kirjoittavat artikkelissaan, että operationaalisilla eduilla tarkoitetaan sellaisia etuja, jotka näkyvät päivittäisessä toiminnassa ja liittyvät resurssien hankkimiseen sekä kuluttamiseen. Ohjelmistorobotiikan avulla voidaan vähentää manuaalista työkuormaa (Asatiani & Penttinen, 2016; Ratia, Myllärniemi & Helander, 2018), parantaa prosessien ajallista tehokkuutta (Ratia ym., 2018; Santos, Pereira & Vasconcelos, 2019) sekä parantaa prosessien tarkkuutta ja luotettavuutta (Capgemini Consulting, 2016; Ratia ym., 2018; Vitharanage ym., 2020; Willcocks ym., 2015). Ohjelmistorobotti kykenee suorittamaan manuaaliset toistoa vaativat tehtävät huomattavasti ihmistä nopeammin, eikä robotille satu inhimillisiä virheitä kuten ihmisille (Willcocks ym., 2015). Esimerkiksi tehtävä, joka vaatii tietyn arvon kopioimista useiden rivien ja sarakkeiden joukosta on altis ihmisen tekemille virheille, mutta ohjelmistorobotti ei tee vastaavaa virhettä, sillä se suorittaa tehtävän aina samalla tavalla (Asatiani &

Penttinen, 2016). Lisäksi Vitharanage ym. (2020) ovat tunnistaneet ohjelmistorobotiikan operationaaliseksi hyödyksi asiakaspalvelun ja asiakastyytyväisyyden paranemisen, sillä organisaatiot ovat lyhentäneet asiakaskohtaisten prosessien vasteaikoja automatisoinnin avulla (Lacity & Willcocks, 2016).

Vitharanagen ym. (2020) mukaan johtamisetuihin lukeutuvat edut, jotka ovat sidoksissa liiketoiminnan johtamiseen. Heidän mukaansa ohjelmistorobotiikan keskeinen johtamisetu on henkilöstöresurssien käytön tehostaminen. Ohjelmistorobotin vapauttaessa henkilöstön manuaalisesta ja rutiininomaisesta tehtävistä, henkilöstöresurssit voidaan käyttää haastavampiin ja enemmän arvoa tuottaviin tehtäviin (Asatiani & Penttinen, 2016; Capgemini Consulting, 2016; Ratia ym., 2018; Syed ym., 2020), mikä tehostaa organisaation tavoitteiden saavuttamista (Vitharanage ym., 2020). Ohjelmistorobotiikan avulla on mahdollista myös vähentää oikeudellisia riskejä (Vitharanage ym., 2020), sillä ohjelmistorobotti voi varmistaa liiketoiminnan oikeudellisten vaatimusten sekä muiden säädösten noudattamisen (Lamberton, Brigo & Hoy, 2017; Syed ym., 2020). Säädösten noudattaminen on myös helposti vahvistettavissa robotiikkatyökalujen keräämien lokitiedostojen pohjalta (Syed ym., 2020).

Strategiset edut vaikuttavat ratkaisevasti organisaation menestymiseen tulevaisuudessa, ja ohjelmistorobotiikan osalta tällaiseksi eduksi lukeutuu korkea sijoitetun pääoman tuottoaste (Vitharanage ym., 2020). Kun ohjelmistorobotiikalla automatisoidaan prosesseja ja tehtäviä, niin tämä laskee merkittävästi prosessin aiheuttamia kustannuksia (Lamberton ym., 2017). Capgemini Consulting (2016) arvioi tutkimuksessaan kustannussäästöjen olevan automatisoitavasta prosessista riippuen 20–50 prosenttia. Ohjelmistorobotiikan etu verrattuna muihin automaatioratkaisuihin on nopea ja helppo käyttöönotto. Asaltani ja Penttinen (2016) kirjoittavat artikkelissaan, että ohjelmistorobotin implementointiin kuluu tyypillisesti 2–4 viikkoa, kun perinteisempien automaatioratkaisujen implementointiin voi kulua kuukausia tai jopa vuosi. Näin ollen ohjelmistorobotiikan implementointikustannukset ovat huomattavasti alhaisemmat kuin perinteisen prosessiautomaation (Hofmann ym., 2020). Vitharanage ym. (2020) kirjoittavat artikkelissaan toisen ohjelmistorobotiikan strategisen edun olevan prosessien läpinäkyvyyden ja ymmärryksen parantuminen. Ennen ohjelmistorobotin implementointia prosessi on analysoitava tarkasti, ja eri sidosryhmien vastuualueet on tunnistettava, mikä lisää läpinäkyvyyttä ja yleistä ymmärrystä koko prosessista. Kolmantena ohjelmistorobotiikan strategisena etuna voidaan nähdä teknologian varhaisen omaksumisen mukanaan tuoma kilpailuetu (Vitharanage ym., 2020).

Vitharanage ym. (2020) kirjoittavat, että organisatoriset edut vaikuttavat organisaation sisäiseen kehittymiseen, oppimiseen ja strategian toteuttamiseen. Aiemman tutkimuksen perusteella keskeisin organisatorinen etu on henkilöstön ajankäytön keskittäminen haastavampiin enemmän arvoa tuottaviin tehtäviin, jotka edellyttävät subjektiivista päättelyä ja päätöksentekoa (Asatiani & Penttinen, 2016; Ratia ym., 2018; Vitharanage ym., 2020). Vitharanagen ym. (2020) mukaan tämä heijastuu positiivisesti myös henkilöstön työtyytyväisyyteen, kun työkuorma vähenee ja työtehtävät ovat haastavampia sekä mielekkäämpiä. Lisäksi ohjelmistorobotin implementointi näkyy oppimisena ja kehittymisenä

organisaation sisällä. Prosessien automatisointi ohjelmistorobotiikalla edesauttaa myös organisaation sisäisten politiikkojen noudattamista (Vitharanage ym., 2020).

3 OHJELMISTOROBOTIIKAN TIETOTURVAHAASTEET

Tässä luvussa tutustutaan tietoturvan käsitteeseen sekä aiempaan tutkimukseen ohjelmistorobotiikan tietoturvasta. Ensimmäisessä alaluvussa kuvataan aiempaan tutkimukseen pohjautuen mitä tietoturva tarkoittaa ja mistä osatekijöistä se muodostuu. Toisessa alaluvussa kartoitetaan olemassa oleva tutkimustieto ohjelmistorobotiikan tietoturvasta ja siihen liittyvistä haasteista. Ohjelmistorobotiikan tietoturvahaasteet luokitellaan ryhmiin, joista kuhunkin perehdytään syvemmin omassa alaluvussaan. Tämän osion tarkoituksena on muodostaa kokonaisvaltainen käsitys ohjelmistorobotiikan tietoturvaa käsittelevästä aiemmasta tutkimuksesta. Tämän kokonaisuuden perusteella voidaan tunnistaa puutteet aiemmassa tutkimuksessa ja valmistautua suunnittelemaan pro gradu -tutkielman empiiristä osuutta.

3.1 Tietoturva

Von Solms ja Van Niekerk (2013) kirjoittavat artikkelissaan tietoturvan keskeisen tavoitteen olevan liiketoiminnan jatkuvuuden varmistaminen ja vahinkojen minimoiminen tietoturvauhkien realisoituessa. ISO/EIC 27002 -standardi määrittelee tietoturvan olevan tiedon luottamuksellisuuden (engl. *confidentiality*), eheyden (engl. *integrity*) sekä saatavuuden (engl. *availability*) varmistamista (Von Solms & Van Niekerk, 2013). Yleisesti kuitenkin nähdään, että tietoturva ei koske ainoastaan tiedon suojaamista, vaan tämän lisäksi laitteiden, tietoverkkojen sekä järjestelmien suojaamista (Nweke, 2017).

Samonas ja Coss (2014) kirjoittavat artikkelissaan tiedon luottamuksellisuuden tarkoittavan tiedon suojaamista luvattomalta pääsyltä. Kun tietoon pääsevät käsiksi ainoastaan henkilöt, joilla siihen on perusteltavissa oleva syy, niin luottamuksellisuus toteutuu (Samonas & Coss, 2014).

Tiedon eheydellä tarkoitetaan tiedon luvattoman muokkaamisen tai poistamisen estämistä, ja validiteetin varmistamista (Trivedi, Kim, Roy & Medhi,

2009). Eheyden tarkoituksena on varmistaa tiedon aitous ja paikkansapitävyys (Samonas & Coss, 2014).

Tiedon saatavuudella tarkoitetaan sitä, että tieto on saatavilla ja käytettävissä silloin kun sitä tarvitaan (Trivedi ym., 2009). Saatavuuden tavoitteena on mahdollistaa sujuva työnteko tarjoamalla luotettava tarvittavien resurssien saatavuus (Nweke, 2017).

3.2 Tietoturva ohjelmistorobotiikassa

Ohjelmistorobotiikan aiempi tutkimus koostuu lähinnä systemaattisista kirjallisuuskatsauksista sekä tapaustutkimuksista, joissa arvioidaan ohjelmistorobotiikan etuja sekä soveltuvuutta eri käyttötarkoituksiin. Ohjelmistorobotiikan tietoturvasta on tarjolla melko vähän tieteellistä tutkimusta, ja aihetta on lähinnä käsitelty verkkoartikkeleissa ja blogeissa. Nämä artikkelit ja blogit ovat tyypillisesti teknologia-alan uutissivustojen, ohjelmistorobotiikkapalveluita tarjoavien yritysten tai konsultointiyritysten kirjoittamia. Van der Aalst, Bichler ja Heinzl (2018) nostavatkin artikkelissaan ohjelmistorobotiikan tietoturvan hallinnan keskeiseksi tulevaisuuden tutkimusaiheeksi.

Aiemman tutkimuksen mukaan ohjelmistorobotiikalla toteutetut prosessit olevan yleisesti ottaen tietoturvallisempia, kuin ihmisten suorittamat prosessit (Asatiani & Penttinen, 2016; Syed ym., 2020). Tätä on pääasiassa perusteltu sillä, että ohjelmistorobotti suorittaa työtehtävän aina samalla tavalla, eikä robotti voi tehdä samankaltaisia inhimillisiä virheitä kuin ihminen saattaa tehdä (Asatiani & Penttinen, 2016; Willcocks ym., 2015). Ohjelmistorobotit auttavat siis varmistamaan datan eheyden. Ratia ym. (2018) kuitenkin huomauttavat artikkelissaan, että mikäli ohjelmistorobotin konfiguroinnissa on tehty virheitä tai prosessi ei ole riittävän säännönmukainen ohjelmistorobotiikalla automatisoitavaksi, ohjelmistorobotti tekee tietyssä tilanteessa saman virheen jokaisella toistolla. Ohjelmistorobotin ollessa huomattavasti ihmistä nopeampi työtehtävien suorittamisessa, se tekee myös virheitä huomattavasti nopeammin. Tämä voi johtaa suuriin ongelmiin datan eheyden osalta (Ratia ym., 2018).

Aiempi tutkimus osoittaa myös, että ohjelmistorobotiikka voi parantaa tietoturvaa muihin automaatio- ja integraatioratkaisuihin verrattuna, sillä ohjelmistorobotiikka vähentää järjestelmien välistä monimutkaisuutta (Bygstad, 2017). Willcocks ym. (2015) kirjoittavat artikkelissaan ohjelmistorobottien olevan vuorovaikutuksessa ainoastaan muiden järjestelmien käyttöliittymäkerroksen kanssa, joten muutoksia muihin järjestelmiin ei tarvitse tehdä. Näin ollen myös tietoturva pysyy paremmalla tasolla prosessiin kuuluvien järjestelmien osalta (Suri, Elia & van Hillegersberg, 2017). Lisäksi ohjelmistorobotiikka hyödyntää jo valmiiksi olevassa olevia tietoturva- ja prosessimalleja, joita myös ihmiset käyttävät (Willcocks ym., 2015).

Siitä huolimatta, että ohjelmistorobotiikka nähdään yleisesti ottaen tietoturvallisena teknologiana, noin kolmanneksella ohjelmistorobotiikkaa hyödyntävistä organisaatioista on ollut kyseiseen teknologiaan liittyviä tietoturvahaasteita

(Willcocks ym., 2018). Capgemini Consulting (2016) nostaa esille tutkimuksessaan, että tietoturva on selkeästi suurin ohjelmistorobotiikan huolenaihe sellaisten organisaatioiden keskuudessa, jotka jo tällä hetkellä hyödyntävät ohjelmistorobotiikkaa. Näistä organisaatioista 34 prosenttia pitää tietoturvaa keskeisenä huolenaiheena. Sellaisten organisaatioiden osalta, jotka eivät vielä hyödynnä ohjelmistorobotiikkaa, tietoturvaa pidetään huomattavasti vähäisempänä huolenaiheena. Vain 18 prosenttia näistä organisaatioista luokittelevat tietoturvan huolenaiheeksi. Sen edelle nousevat muun muassa huoli suurista implementointikustannuksista, sekä liian alhaisesta sijoitetun pääoman tuottoasteesta (Capgemini Consulting, 2016). Tämä osoittaa sen, että ohjelmistorobotiikkaan liittyy enemmän tietoturvahaasteita, kuin yleisesti ajatellaan.

Aiemman tutkimuksen perusteella keskeisimmät ohjelmistorobotiikan tietoturvahaasteet liittyvät identiteetin- ja pääsynhallintaan (engl. *identity and access management, IAM*) sekä datan eheyteen poikkeustilanteissa. Lisäksi informaatioteknologian kuluttajistuminen nähdään aiemmassa tutkimuksessa ilmiönä, joka heikentää ohjelmistorobotiikan tietoturvan hallintaa.

3.2.1 Identiteetin- ja pääsynhallinta

Identiteetin- ja pääsynhallinnalla tarkoitetaan prosessien ja työkalujen joukkoa, joiden avulla hallitaan henkilöiden ja muiden kohteiden digitaalista identiteettiä (De Hert, 2008; Kumar & Bhardwaj, 2018), sekä kontrolloidaan pääsyä kriittiseen informaatioon (Kumar & Bhardwaj, 2018). Näiden prosessien ja työkalujen tarkoituksena on mahdollistaa käyttäjien pääsy tarvittaviin resursseihin oikeaan aikaan ja oikeasta syystä (Gartner, 2021). Lindenin (2017) mukaan identiteetin- ja pääsynhallinta nähdään usein yhtenä kokonaisuutena, mutta se voidaan jakaa myös kahteen osa-alueeseen. Identiteetinhallinnan tarkoituksena on esittää kohteet digitaalisina identiteetteinä, kun taas pääsynhallinnan tarkoituksena on tunnistaa digitaalinen identiteetti ja päättää millä laajuudella kohteella on oikeus käyttää eri tietojärjestelmiä (Linden, 2017).

Aiemman tutkimuksen perusteella ohjelmistorobotiikan tietoturvaan liittyy keskeisesti identiteetin- ja pääsynhallinnan haasteet, ja Giesbers (2020) on tunnistanut tutkimuksessaan useita tällaisia haasteita. Ohjelmistorobotiikan identiteetin- ja pääsynhallintaan liittyvät haasteet voidaan luokitella ohjelmistorobotin oikeuksiin ja tehtävien eriyttämiseen (engl. *separation of duties, SOD*) liittyviin haasteisiin, ohjelmistorobotin käyttäjätunnukseen liittyviin haasteisiin, sekä ohjelmistorobotin järjestelmiin tunnistautumiseen liittyviin haasteisiin (Giesbers, 2020).

Tehtävien eriyttäminen tarkoittaa sitä, että kriittisten tehtävien osalta koko tehtäväketjua ei voida suorittaa vain yhden käyttäjän toimesta, vaan tehtävän loppuunsaattamiseksi tarvitaan vähintään kaksi henkilöä (Knorr & Stormer, 2001). Sen lisäksi, ettei yksittäisen ohjelmistorobotin käyttäjäoikeudet riko tehtävien eriyttämisen periaatetta, on myös huomioitava ohjelmistorobottien omistajuus. Yksi henkilö ei saa omistaa useita ohjelmistorobotteja siten, että henkilö voisi halutessaan suorittaa kriittisen tehtäväketjun alusta loppuun näiden ohjelmistorobottien käyttäjätunnuksilla (Deloitte, 2019). Santos ym. (2019) kirjoittavat

artikkelissaan, että ohjelmistorobotin käyttäjäoikeuksien kannalta on myös olennaista rajata oikeudet prosessin kannalta vain välttämättömien toimenpiteiden mukaisesti. Ohjelmistorobotin liian laajat oikeudet eri tietojärjestelmien sisällä ovat uhka datan luottamuksellisuudelle, eheydelle ja saatavuudelle, mikäli ohjelmistorobotin käyttäjätunnus ja salasana päätyvät väärän henkilön haltuun (Santos ym., 2019). Lisäksi ohjelmistorobotin liian laajoihin oikeuksiin voi kohdistua sisäinen riski, sillä ohjelmistorobotin omistaja tai kehittäjä voi käyttää ohjelmistorobotin tunnuksia vääriin tarkoituksiin (Giesbers, 2020). On kuitenkin hyvä huomata, että liian tiukat rajaukset voivat estää ohjelmistorobottia toimimasta halutulla tavalla (Syed ym., 2020).

Ohjelmistorobotin käyttäjätunnukseen liittyvät haasteet ovat sidoksissa ohjelmistorobotin identiteettiin ja sen hallintaan. Aivan kuten organisaation työntekijöillä, myös ohjelmistorobotilla täytyy olla uniikki digitaalinen identiteetti, jotta ohjelmistorobotti voi olla yksilöitävissä ja tunnistautua eri järjestelmiin (Lacity & Willcocks, 2017). Uniikki identiteetti mahdollistaa myös lokitietojen keräämisen ohjelmistorobotin tekemistä toimenpiteistä, mikä edesauttaa virhetilanteiden selvittämistä (Deloitte, 2019). Lisäksi ohjelmistorobotin käyttäjätunnuksen haasteisiin liittyen nousee esille kysymyksiä, kuten kuka määrittelee ohjelmistorobottien salasanat, milloin salasanat tulisi vaihtaa, ja kuinka salasanojen vaihto toteutetaan tietoturvallisesti (Giesbers, 2020; Lacity & Willcocks, 2017).

Ohjelmistorobotin järjestelmiin tunnistautumiseen liittyvien haasteiden osalta on otettava huomioon turvallinen sisäänkirjautumismenetelmä (Giesbers, 2020; Syed ym., 2020), tunnistautumistietojen säilytystapa (CyberArk, 2021) sekä organisaation salasanapolitiikka (Deloitte, 2019). Deloitten (2019) julkaiseman raportin mukaan kertakirjautuminen (Single Sign-On, SSO) ei ole tarpeeksi turvallinen menetelmä ohjelmistorobotin tunnistautumisessa eri järjestelmiin. Raportin mukaan ohjelmistorobotiikassa tulisi soveltaa monivaiheista tunnistautumista (engl. *multifactor authentication, MFA*) esimerkiksi ohjelmointirajapintoihin (engl. *application programming interface, API*) pohjautuvien ratkaisujen kautta (Deloitte, 2019). Tunnistautumiseen käytettävän salasanan ei tulisi koskaan olla kovakoodattuna skripteihin, sillä skriptissä salasana on nähtävissä selkokielisessä muodossa (CyberArk, 2021; Rahman, Parnin & Williams, 2019). Ohjelmistorobotin salasanoja tulisi säilyttää keskitetyssä ja salatussa sijainnissa (CyberArk, 2021). Lisäksi ohjelmistorobotiikan yhteydessä käytettävien salasanojen ei koskaan tulisi olla geneerisiä, vaan salasanojen tulisi täyttää samat kriteerit mitä vaaditaan myös organisaation henkilöstön käyttäjätunnusten salasanoilta (Deloitte, 2019).

3.2.2 Datan eheys poikkeustilanteissa

Ohjelmistorobotin implementoinnin kannalta on tärkeää, että automatisoitavan prosessin kaikki vaiheet, poikkeukset ja lopputulemat on mahdollista kuvata yksiselitteisesti (Asatiani & Penttinen, 2016). Ratia ym. (2018) kirjoittavat artikkelissaan, että jos automatisoitu prosessi sisältää virheitä tai sellaisia poikkeustilanteita, joita ei ole määritelty, niin riski ohjelmistorobotin tekemille virheille on olemassa. Ohjelmistorobotin ollessa huomattavasti ihmistä tehokkaampi, myös

virheitä voi syntyä huomattavasti nopeammin ja enemmän kuin ihmisen toimesta (Santos ym., 2019).

Ratian ym. (2018) mukaan on tärkeää, että ohjelmistorobotin implementoinnissa on mukana henkilöitä, jotka tuntevat automatisoitavan prosessin hyvin. Tämä edesauttaa prosessin mahdollisten poikkeustilanteiden tunnistamista ja näin ollen vähentää datan eheyteen liittyviä riskejä (Ratia ym., 2018). Lisäksi Zaharia-Rădulescu, Pricop, Shuleski ja Ioan (2017) huomauttavat julkaisussaan, että ohjelmistorobotiikalla automatisoitavaan prosessiin voidaan myös sisällyttää välivaiheita, jotka edellyttävät ihmisen manuaalisia toimenpiteitä. Ihminen voi esimerkiksi valitoida ohjelmistorobotin luomat tilauslomakkeet, ennen kuin ohjelmistorobotti siirtää ne järjestelmässä eteenpäin (Zaharia-Rădulescu ym., 2017). Tämän kaltaisilla lisäkontrolleilla voidaan laskea datan eheyteen liittyviä riskejä, mutta samalla ne laskevat automaation astetta.

3.2.3 Informaatioteknologian kuluttajistumisen vaikutus tietoturvaan

Informaatioteknologian kuluttajistuminen (engl. *consumerization*) on ilmiö, jolla tarkoitetaan IT-resurssien hallinnan siirtymistä keskitetyltä IT-yksiköltä teknologian loppukäyttäjälle itselleen (Bygstad, 2017; Niehaves, Köffer & Ortbach, 2012). Bygstad ym. (2017) kirjoittavat artikkelissaan, että ilmiö on tyypillisesti havaittavissa kevyen informaatioteknologian ratkaisujen kohdalla, sillä ne eivät vaadi syvällistä tietoteknistä osaamista. Myös ohjelmistorobotiikka lukeutuu kevyen informaatioteknologian ratkaisuihin (Bygstad, 2017). Muita yleisesti tieteellisessä tutkimuksessa käytettyjä termejä samalle ilmiölle ovat varjo-IT (engl. *shadow IT*) ja käyttäjäjohtoinen IT (engl. *user-led IT*) (Willcocks ym., 2015).

Aiemman tieteellisen tutkimuksen perusteella informaatioteknologian kuluttajistumisella on negatiivinen vaikutus tietoturvaan (Bygstad, 2017; Hofmann ym., 2020; Niehaves ym., 2012; Suri ym., 2017; Willcocks ym., 2015). Raskaan informaatioteknologian ratkaisut kehitetään tyypillisesti ohjelmistokehitykseen erikoistuneiden asiantuntijoiden toimesta, jolloin tietoturva osataan ottaa huomioon (Willcocks, Lacity & Craig, 2016). Asia ei kuitenkaan aina ole näin kevyen informaatioteknologian ratkaisuiden kohdalla. Suri ym. (2017) kirjoittavat artikkelissaan, että ohjelmistorobottien loppukäyttäjien toimesta tapahtuva itsenäinen kehittäminen ja implementointi nähdään usein teknologian mahdollistamana etuna, mutta sillä on myös varjopuoli. Vaikka toimintatapa saattaa olla suoraviivainen ja kustannustehokas (Suri ym., 2017), niin ilman IT-asiantuntijoiden työpanosta organisaatiot ottavat suuren tietoturvariskin (Bygstad, 2017; Suri ym., 2017; Willcocks ym., 2015).

Willcocksin ym. (2015) mukaan keskeinen informaatioteknologian kuluttajistumisen haaste ohjelmistorobotiikan kohdalla on tasapainon löytäminen liiketoiminnan tarpeiden ja IT-lähtöisen turvallisuuden hallinnan ja kontrollin välille. Liiketoimintayksiköillä on tyypillisesti tarpeena saada uusia ratkaisuja käyttöön mahdollisimman edullisesti ja nopealla aikataululla, jotta suorituskyky jatkuvasti muuttuvassa toimintaympäristössä pysyy vaaditulla tasolla (Willcocks ym., 2015). Ohjelmistorobotiikkaa ei voi kuitenkaan tarkastella yksinomaan liiketoiminnan näkökulmasta (Hofmann ym., 2020).

Kirjallisuudessa nostetaan esille kaksi keinoa, joilla pyritään estämään ohjelmistorobotiikan kuluttajistumisesta aiheutuvia tietoturvaongelmia. Ensinäkin kaikkien sidosryhmien tulisi olla mukana ohjelmistorobotin kehitysprojektissa varhaisesta vaiheesta alkaen (Hofmann ym., 2020; Suri ym., 2017; Willcocks ym., 2015). IT-henkilöstön mukanaolo ohjelmistorobottien kehittämiseen liittyvässä päätöksentekoprosessissa on välttämätöntä tietoturvallisen toteutuksen varmistamiseksi (Hofmann ym., 2020). Sidosryhmien osallistamisen lisäksi Willcocks ym. (2015) ehdottavat, että ohjelmistorobotiikkaan tulisi soveltaa samoja hallintoperiaatteita, kuin raskaan informaatioteknologian ratkaisuihin. Tämän tarkoituksena on hillitä informaatioteknologian kuluttajistumista ja näin ollen hallita siihen liittyviä tietoturvariskejä (Willcocks ym., 2015).

4 YHTEENVETO AIEMMASTA KIRJALLISUUDESTA

Aiempaan kirjallisuuteen tutustumisen tavoitteena oli luoda teoreettinen pohja pro gradu -tutkielmalle, johon empiirisen osion tuloksia voidaan peilata. Kirjallisuuskatsauksella saavutettiin kattava kokonaiskuva ohjelmistorobotiikasta teknologiana, sekä perehdyttiin aiemmassa kirjallisuudessa tunnistettuihin tietoturvahaasteisiin, sekä keinoihin, joiden avulla voidaan varmistaa ohjelmistorobotiikan tietoturvallinen hallinta. Kirjallisuuskatsauksessa käytettiin lähdeaineistona pääasiassa tieteellisiä vertaisarvioituja artikkeleita, ja lähteiden valinnassa käytettiin apuna julkaisufoorumi-palvelun tarjoamia julkaisukanavien tasoluokituksia.

Tutkielman ensimmäisessä sisältöluvussa tutustuttiin ohjelmistorobotiikkaan yleisellä tasolla. Luvussa esiteltiin ohjelmistorobotiikan määritelmä, kuvattiin sen soveltuvuutta erilaisiin käyttötarkoituksiin, sekä kuvattiin ja luokiteltiin ohjelmistorobotiikan tarjoamia etuja. Kirjallisuuden pohjalta ohjelmistorobotiikan voidaan todeta olevan prosessien automatisoimiseen käytettävä teknologia (Asatiani & Penttinen, 2016; Willcocks ym., 2015), joka operoi eri järjestelmien käyttöliittymätasolla ihmisen kaltaisesti (Van der Aalst ym., 2018) ja sille etukäteen määritellyn toimintalogiikan mukaisesti (IEEE Corporate Advisory Group, 2017; Tornbohm & Dunie, 2017). Ohjelmistorobotiikka osoittautui sopivan erityisesti sellaisten tehtävien automatisoimiseen, jotka ovat luonteeltaan rutiininomaisia ja vahvasti standardisoituja (Asatiani & Penttinen, 2016; Syed ym., 2020), sisältävät paljon manuaalista työtä, eivät edellytä subjektiivista päättelyä tai päätöksentekoa (Van der Aalst ym., 2018; Willcocks ym., 2015), ja toistuvat useita kertoja päivittäin (Capgemini Consulting, 2016). Soveltuvuudeltaan prosessien automatisoinnissa ohjelmistorobotiikka osoittautui sijoittuvan liiketoimintaprosessien hallintajärjestelmien ja ihmisen suorittaman manuaalisen työn välimaastoon (Hofmann ym., 2020; Lu ym., 2018). Ohjelmistorobotiikan keskeisimpinä etuina nähdään olevan prosessien tehokkuuden, tarkkuuden ja luotettavuuden parantaminen (Capgemini Consulting, 2016; Ratia ym., 2018; Willcocks ym., 2015), kustannussäästöjen ja ketteryyden lisääminen (Capgemini Consulting, 2016; Lamberton ym., 2017), manuaalisen työkuorman vähentäminen (Asatiani & Penttinen, 2016; Ratia ym., 2018), henkilöstöresurssien kohdistaminen

haastavampiin ja enemmän arvoa tuottaviin työtehtäviin (Asatiani & Penttinen, 2016; Capgemini Consulting, 2016; Ratia ym., 2018; Syed ym., 2020; Vitharanage ym., 2020), prosessien läpinäkyvyyden parantaminen sekä työtyytyväisuuden kohentuminen (Vitharanage ym., 2020).

Tutkielman toisessa sisältöluvussa tutustuttiin aiempaan tutkimukseen ohjelmistorobotiikan tietoturvahaasteita, mikä on tämän tutkielman tutkimuskysymyksiin vastaamisen kannalta keskeisessä asemassa. Aiemman kirjallisuuden perusteella ohjelmistorobotiikan keskeisimpien tietoturvahaasteiden voidaan todeta liittyvän identiteetin- ja pääsynhallintaan sekä datan eheyteen poikkeustilanteissa.

Aiemman tutkimuksen perusteella ohjelmistorobotiikalla automatisoidut prosessit ovat pääsääntöisesti tietoturvallisempia kuin ihmisten manuaalisesti suorittamat prosessit (Asatiani & Penttinen, 2016; Syed ym., 2020). Ohjelmistorobotiikan tietoturvallisen toteuttamiseen liittyy kuitenkin haasteita. Identiteetin- ja pääsynhallinta on erittäin keskeinen osa-alue ohjelmistorobotiikan tietoturvan hallinnan kannalta (Giesbers, 2020). Santosin ym. (2019) mukaan keskeistä on robotiikkatunnusten käyttöoikeuksien tarkoituksenmukainen rajaaminen. Rajaamalla ohjelmistorobotin käyttöoikeudet vain välttämättömien toimenpiteiden suorittamiseen eri järjestelmien sisällä voidaan minimoida mahdollisten väärinkäytösten seuraamukset (Giesbers, 2020; Santos ym., 2019). Kirjallisuuden perusteella myös tehtävien eriyttämisen periaatetta on noudatettava ohjelmistorobotiikkaa hyödyntäessä aivan kuten ihmisten käyttäjätunnustenkin kohdalla (Giesbers, 2020). Tässä on huomioitava myös ohjelmistorobottien omistajuus, ettei tehtävien eriyttämisen periaatetta rikota organisaation sisällä välillisesti (Deloitte, 2019). Kirjallisuuskatsaus osoitti myös ohjelmistorobotiikan käyttäjätunnusten hallinnan olevan keskeinen seikka tietoturvan näkökulmasta. Turvallisen hallinnan takaamiseksi ohjelmistorobotilla tulee olla uniikki digitaalinen identiteetti (Deloitte, 2019; Lacity & Willcocks, 2017), ja ohjelmistorobotin salasanan määrittämiselle, säilyttämiselle sekä vaihtamiselle tulee olla turvalliset prosessit (CyberArk, 2021; Giesbers, 2020; Lacity & Willcocks, 2017). Lisäksi kirjallisuuskatsaus osoitti ohjelmistorobottien järjestelmiin tunnistautumisen muodostavan haasteita tietoturvalle. Tietoturvan takaamiseksi käytettävien salasanojen tulee noudattaa organisaation salasanapolitiikkoja, salasanoja tulee säilyttää keskitetyssä salatussa sijainnissa, ja tunnistautumiseen tulisi aina käyttää monivaiheisen tunnistautumisen menetelmiä (Deloitte, 2019). Ohjelmistorobotin skripteihin kovakoodatut salasanat luovat merkittäviä tietoturvauhkia (CyberArk, 2021; Rahman ym., 2019).

Aiemman kirjallisuuden perusteella datan eheys poikkeustilanteissa osoittautui toiseksi keskeiseksi ohjelmistorobotiikan tietoturvahaasteeksi. Virheet tai puutteet ohjelmistorobotin konfiguraatiossa voivat johtaa ohjelmistorobotin tekemiin virheisiin, mikä vaarantaa datan eheyden (Ratia ym., 2018). Ohjelmistorobotin ollessa ihmistä tehokkaampi, myös virheitä voi syntyä merkittäviä määriä (Santos ym., 2019). Kirjallisuuskatsauksen perusteella tämä riski voidaan minimoida osallistamalla ohjelmistorobotin kehitys- ja implementointiprosessiin sellaisia henkilöitä, jotka tuntevat prosessin mahdollisimman hyvin, mikä

edesauttaa prosessissa esiintyvien poikkeusten tunnistamista (Ratia ym., 2018). Lisäksi automatisoitaviin prosesseihin voidaan lisätä ihmisen manuaalisia toimenpiteitä edellyttäviä välivaiheita, jolloin voidaan varmistua ohjelmistorobotin halutunlaisesta toiminnasta (Zaharia-Rădulescu ym., 2017).

Aiemmassa kirjallisuudessa informaatioteknologian kuluttajistuminen tunnistettiin ilmiöksi, mikä heikentää ohjelmistorobotiikan tietoturvan hallintaa. Vaikka ohjelmistorobotiikka onkin kevyen informaatioteknologian ratkaisu (Bygstad, 2017), niin tietoturvan hallinnan näkökulmasta sitä ei voi jättää täysin loppukäyttäjän vastuulle (Hofmann ym., 2020). Keskeinen haaste on löytää tasapaino liiketoiminnan tarpeiden ja IT-lähtöisen turvallisuuden hallinnan ja kontrollin välille (Willcocks ym., 2015). Aiempi kirjallisuus tarjoaa tähän keinoiksi kaikkien sidosryhmien osallistamisen ohjelmistorobotin suunnitteluvaiheen alusta asti (Hofmann ym., 2020; Suri ym., 2017; Willcocks ym., 2015), sekä raskaan informaatioteknologian hallintoperiaatteiden soveltamisen myös ohjelmistorobotiikkaan (Willcocks ym., 2015).

Kokonaisuudessaan ohjelmistorobotiikkaa on tutkittu kohtuullisen paljon, mutta ohjelmistorobotiikan tietoturva on jäänyt aikaisemmassa tutkimuksessa huomattavan vähäiselle huomiolle. Ohjelmistorobotiikan tietoturvaa käsitellään vain harvoissa aiemmassa tutkimuksessa, ja näissäkin tutkimuksissa tietoturva jää sivurooliin. Yksinomaan ohjelmistorobotiikan tietoturvaa käsittelevää tutkimusta ei kirjallisuuskatsaus laatiessa ollut saatavilla. Kirjallisuuskatsauksen rajoitteiden vuoksi tutkimuksen empiirisessä osiossa on tarve saada kerättyä mahdollisimman laaja ja rikas tutkimusaineisto.

5 TUTKIMUKSEN TOTEUTTAMINEN

Tämän luvun tarkoituksena on tutustua tutkimuksen empiirisessä osiossa käytettyihin tutkimusmenetelmiin. Luvussa esitellä tutkimuksessa käytetyt tutkimus-, tiedonkeruu- ja analysointimenetelmät, sekä kuvataan näiden prosessien kulkua tarkemmalla tasolla.

5.1 Tutkimusmenetelmä

Tämän tutkielman tarkoituksena oli tunnistaa ohjelmistorobotiikkaan liittyviä tietoturvahaasteita ja mahdollisia syitä niiden taustalla, sekä tarjota keinoja ohjelmistorobotiikan tietoturvan varmistamiseksi. Tutkielman empiirisen osion tutkimusmenetelmäksi valikoitui yksittäinen tapaustutkimus, jossa sovelletaan laadullisia aineistonkeruun ja analysoinnin menetelmiä.

Darke, Shanks ja Broadbent (1998) kirjoittavat artikkelissaan tapaustutkimuksen olevan tyypillinen menetelmä, kun tutkitaan informaatioteknologian tai -järjestelmän kehittämistä, implementointia tai käyttöönottoa sen eri näkökulmista. Tapaustutkimuksille ominaisia tutkimuskysymysten asetteluja ovat kysymykset, kuten *mitä, miten* ja *miksi (*Yin, 1994*)*. Kyseinen tutkimusmenetelmä soveltuu tilanteisiin, joissa tutkitaan ajankohtaista ilmiötä sen luonnollisessa ympäristössä (Benbasat, Goldstein & Mead, 1987; Yin, 1994), ja kun ilmiö ei ole vielä tarpeeksi hyvin ymmärretty tai tunnettu (Darke ym., 1998). Tapaustutkimus tutkii ennalta määritettyä ilmiötä, ja keskittyy ilmiön ja sen kontekstin syvälliseen ymmärtämiseen (Cavaye, 1996). Ohjelmistorobotiikka on suhteellisen tuore ja nopeasti suosiotaan kasvattava teknologia, joten tutkielman aihe on hyvin ajankohtainen. Tutkielmalle on valittu myös rajattu näkökulma, joka ei ole vielä tarpeeksi hyvin tunnettu. Tutkimus toteutetaan toimeksiantajaorganisaation kontekstissa, mitä voidaan pitää ilmiölle luonnollisena ympäristönä.

Darke, Shanks ja Broadbent (1998) kirjoittavat artikkelissaan, että tapaustutkimus voi käsitellä joko yksittäistä tapausta tai useaa tapausta. Yksittäinen tapaustutkimus soveltuu tilanteeseen, jossa tutkimustapaus täyttää kaikki

tapaustutkimuksen edellytykset, tai jos tutkitaan uniikkia tapausta (Darke ym., 1998). Lisäksi yksittäinen tapaustutkimus on perusteltavissa oleva menetelmä, kun tarkastellaan tapausta, jota ei ole aiemmin tutkittu tieteellisesti (Yin, 1994). Monitapaustutkimus tarkastelee useita tapauksia, ja näin ollen mahdollistaa tutkittavan ilmiön analysoinnin ja vertailun eri olosuhteissa (Darke ym., 1998). Tässä tutkielmassa päädyttiin yksittäiseen tapaustutkimukseen, sillä ohjelmistorobotiikasta ei ole saatavilla sellaista aiempaa tutkimusta, joka käsittelee yksinomaan tietoturvan näkökulmaa. Lisäksi tutkielmassa tarkastellaan ilmiötä toimeksiantajaorganisaation kontekstissa, joten tutkimustapausta voidaan pitää uniikkina.

Tapaustutkimuksissa voidaan soveltaa sekä laadullisia että määrällisiä tutkimusmenetelmiä (Yin, 1994), mutta tyypillisesti niissä käytetään laadullisen tutkimuksen menetelmiä, ja tapaustutkimus onkin eniten käytetty laadullinen tutkimusmenetelmä tietojärjestelmätieteen tutkimusalueella (Orlikowski & Baroudi, 1991). Campbell (2014) kirjoittaa artikkelissaan, että toisin kuin kvantitatiivisessa tutkimuksessa, laadullisessa tutkimuksessa ei keskitytä tarkkoihin ja objektiivisiin mittauksiin numeraalisen datan pohjalta, vaan tulkitaan ja analysoidaan avointa, sanallisessa muodossa olevaa dataa. Laadullinen tutkimus tavoittelee tutkittavan ilmiön ymmärtämistä usein sen luonnollisessa ympäristössä. Tutkimusmateriaali laadullisissa tutkimuksissa kerätään usein interaktiivisin keinoin, kuten esimerkiksi haastattelujen avulla (Campbell, 2014).

5.2 Tiedonkeruumenetelmän valinta ja toteutus

Tapaustutkimus voi hyödyntää yhtä tai useampaa aineistonkeruumenetelmää, kuten haastatteluja, observointia, kyselyitä tai dokumenttianalyysia (Darke ym., 1998). Tässä tutkimuksessa aineistonkeruutavaksi valikoitui teemahaastattelut. Hirsijärven ja Hurmeen (2001) mukaan teemahaastattelu on puolistrukturoitu haastattelumenetelmä, jossa haastattelun runko muodostuu yksityiskohtaisesti määriteltyjen kysymysten sijaan ennalta määritellyistä teemoista. Teemat ovat kaikille haastateltaville samoja, mutta kysymyksillä ei ole tarkkaa järjestystä tai muotoa, vaan haastattelu etenee keskustelunomaisesti (Hirsijärvi & Hurme, 2001). Teemahaastattelussa haastateltavalle voidaan esittää tarkentavia kysymyksiä hänen vastaustensa perusteella (Tuomi & Sarajärvi, 2018). Näin ollen teemahaastattelu on lähempänä strukturoimatonta haastattelua kuin puolistrukturoitua haastattelua (Hirsijärvi & Hurme, 2001).

Teemahaastattelu valikoitui käytettäväksi haastattelumenetelmäksi, sillä haastateltaviksi valikoitui henkilöitä keskenään erilaisista työtehtävistä, jolloin haastateltavat katsoivat ohjelmistorobotiikkaa hyvin erilaisista näkökulmista. Näin ollen kaikille haastateltaville soveltuvan kysymyspatteriston laatiminen olisi ollut mahdotonta. Teemahaastattelu toi haastatteluihin paljon joustavuutta, ja haastatteluiden välillä oli suuria eroja mihin teemaan keskustelu painottui. Teemahaastattelu osoittautui toimivaksi menetelmäksi, sillä sen avulla jokaisen haastateltavan oli mahdollista keskittyä heidän omaan osaamisalueeseensa sekä

heille tärkeisiin teemoihin, eikä aikaa kulunut turhaan sellaisten asioiden käsittelyyn, joista haastateltavalla ei ollut juurikaan näkemystä. Haastatteluрungon teema-alueet pohjautuivat ohjelmistorobotiikan tietoturvan aiempaan tieteelliseen tutkimukseen, ja ne olivat ohjelmistorobotiikan tietoturva yleisesti, identiteetin- ja pääsynhallinta, datan eheys poikkeustilanteissa sekä informaatioteknologian kuluttajistumisen vaikutus tietoturvan hallintaan. Haastatteluрungon teemojen alle lisättiin apukysymyksiä, joiden kautta keskustelu lähti liikkeelle. Haastatteluissa käytetty runko on tämän tutkielman liitteenä.

Tutkimuksen haastateltaviksi henkilöiksi valittiin tarkoituksenmukaisia henkilöitä toimeksiantajaorganisaation sisältä, minkä lisäksi haastateltiin toimeksiantajaorganisaation yhteistyökumppanin palveluksessa työskenteleviä asiantuntijoita. Haastateltavien keräämisessä käytettiin lisäksi lumipallo-otantaa (engl. *snowball sampling*), eli haastatteluiden yhteydessä haastateltavilta tiedusteltiin muita henkilöitä, joita kannattaisi haastatella (Sharma, 2017), ja tätä jatkettiin, kunnes uusia haastateltavia ei enää löytynyt. Haastattelukutsuja lähetettiin yhteensä 16, joista 12 toteutui. Kaikki haastattelut toteutettiin Microsoft Teams -työkalun välityksellä. Haastattelut kestivät keskimäärin 48 minuuttia, ja haastattelumateriaalia kertyi yhteensä yli yhdeksän tunnin edestä.

5.3 Aineiston analysointi

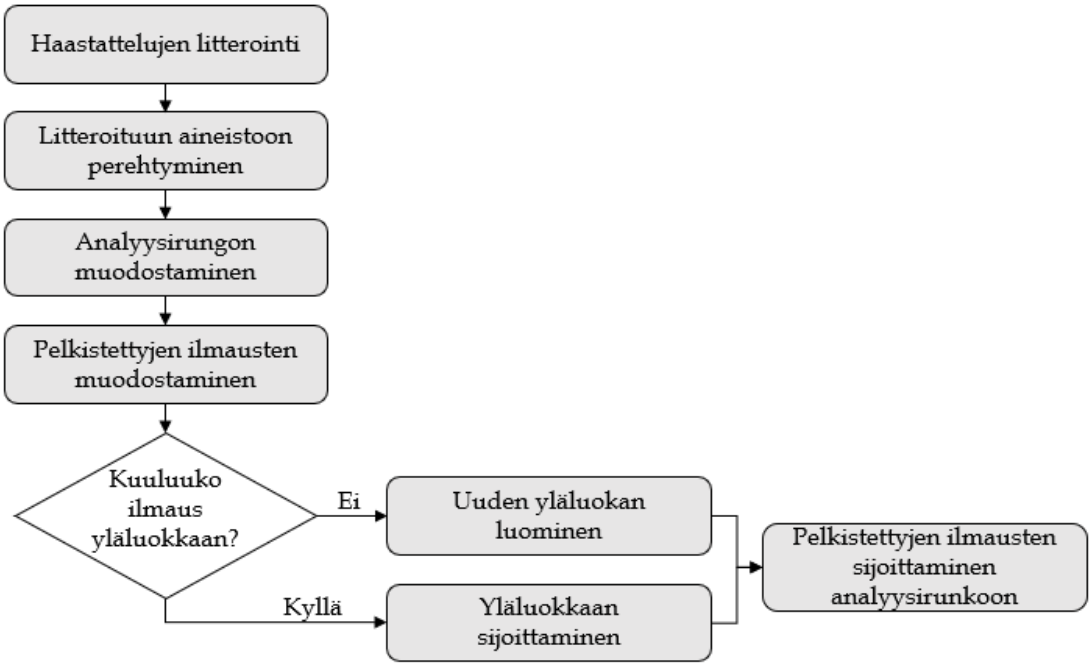
Aineiston analysointi toteutettiin soveltamalla sisällönanalyysin menetelmiä. Tuomen ja Sarajärven (2018) mukaan sisällönanalyysi on perusanalyysimenetelmä, joka soveltuu käytettäväksi laadullisessa tutkimuksessa. Sen avulla voidaan analysoida kirjallisessa muodossa olevia dokumentteja systemaattisesti ja objektiivisesti. Sisällönanalyysin tarkoituksena on mahdollistaa tutkimuksen johtopäätösten teon tiivistämällä aineisto järjestettyyn muotoon.

Tuomi ja Sarajärvi (2018) jaottelevat laadullisen sisällönanalyysin päättelyprosessin kolmeen eri malliin, jotka ovat aineistolähtöinen, teoriasidonnainen sekä teorialähtöinen analyysin malli. Näistä malleista tähän tutkimukseen soveltui parhaiten teorialähtöinen analyysi. Tuomen ja Sarajärven (2018) mukaan teorialähtöisessä analyysissä nojataan aikaisemmin tutkittuun tietoon, teoriaan, kehykseen tai malliin. Aineiston analysoinnissa hyödynnetään aiemmasta tutkimuksesta johdettuja käsitteitä ja kategorioita, eikä niitä luoda puhtaasti aineiston pohjalta, kuten aineistolähtöisessä analyysissa. Hsieh ja Shannon (2005) kutsuvat teoriasidonnaista sisällönanalyysiä artikkelissaan suunnatuksi sisällönanalyysi (engl. *derected content analysis*). Heidän mukaansa teorialähtöisen sisällönanalyysin avulla pyritään tyypillisesti vahvistamaan tai laajentamaan aiempien tutkimusten tuloksia, ja teorialähtöinen sisällönanalyysi soveltuukin tilanteisiin, joissa tutkittava ilmiö ei ole vielä kovinkaan tarkasti tunnettu. Mikäli tutkimusmateriaalista kuitenkin nousee esille asioita, jotka eivät sovi ennalta muodostettuihin kategorioihin, niin tässä tapauksessa näille asioille luodaan uusi kategoria aineistolähtöisen sisällönanalyysin tapaisesti. Teorialähtöinen sisällönanalyysi soveltuu hyvin aineiston analysointimenetelmäksi, kun data on kerätty

haastatteluiden avulla, joissa on hyödynnetty sekä avoimia että kohdennettuja kysymyksiä (Hsieh & Shannon, 2005).

Teorialähtöisen sisällönanalyysin nähtiin olevan tämän tutkimuksen kohdalla sopivin menetelmä, sillä tutkittava ilmiö ei ole vielä tarpeeksi hyvin tunnettu, ja tutkimuksen tarkoituksena on laajentaa ja täydentää olemassa olevaa tutkittua tietoa. Lisäksi haastattelurungon teemat ovat johdettu ohjelmistorobotiikan tietoturvan aiemman tutkimuksen tuloksista, jolloin samat teemat ovat sujuvasti hyödynnettävissä myös sisällönanalyysin vaiheessa.

Tuomen ja Sarajärven (2018) mukaan haastatteluiden litteroinnin ja litteroituun aineistoon perehtymisen jälkeen teorialähtöisen sisällönanalyysin seuraava vaihe on analyysirungon muodostaminen, jossa yläluokat johdetaan aiemmasta tieteellisestä tutkimuksesta. Tämän jälkeen litteroidusta aineistosta muodostetaan pelkistettyjä ilmauksia, jotka sijoitetaan analyysirunkoon yläluokan alle. Mikäli sopivaa yläluokkaa ei ole olemassa, niin pelkistetylle ilmaukselle luodaan uusi pääluokka samaan tapaan kuin aineistolähtöisessä sisällönanalyysissa (Tuomi & Sarajärvi, 2018). Alla olevassa kuviossa (Kuvio 5) kuvataan tässä tutkimuksessa käytetyt Tuomen ja Sarajärven (2018) esittelemät teorialähtöisen sisällönanalyysin vaiheet.



Kuvio 5 Teorialähtöinen sisällönanalyysi (Tuomi & Sarajärvi, 2018)

6 EMPIIRISEN OSION TULOKSET

Tässä luvussa esitellään teemahaastatteluin toteutetun tutkimuksen tulokset haastattelurungon teemajaottelua mukaillen. Kokonaisuudessaan kerätty haastattelumateriaali on melko yhdenmukaista, mutta myös keskenään ristiriidassa olevia näkemyksiä nousi esille. Haastatteluissa käsiteltiin kirjallisuuskatsauksesta tuttuja teemoja, minkä lisäksi myös tietosuojan merkitys ohjelmistorobotiikan kontekstissa nousi esille.

6.1 Identiteetin- ja pääsynhallinta

Identiteetin- ja pääsynhallinnan kokonaisuus osoittautui haastattelujen perusteella ohjelmistorobotiikan tietoturvan hallinnan keskeisimmäksi osa-alueeksi, ja haastattelumateriaalista saatiinkin poimittua yhteensä 75 tätä osa-aluetta käsittelevää vastausta. Identiteetin- ja pääsynhallinnan keskeisimpiä teemoja haastattelujen perusteella ovat ohjelmistorobottien käyttäjätunnukset, niiden elinkaaren ja salasanojen hallinta, tunnistautumismenetelmät, ohjelmistorobottien käyttäjäoikeudet eri järjestelmien sisällä sekä tehtävien eriyttämisen periaate. Haastattelujen perusteella identiteetin- ja pääsynhallinta on yksi tietoturvan kivijaloista, eikä tämä näkemys jakanut mielipiteitä.

> [...] mutta totta kai identiteettihän on tuossakin tietoturvariskeistä yksi isoimpia, elikkä kuinka se ohjelmistorobotin käyttämä identiteetti suojataan, koska jos se kompromisoituu, niin sehän taas mahdollistaa sen identiteetin väärinkäytön vahvasti. (H3)

Tietoturvan kannalta järjestelmällinen robotiikkatunnusten elinkaarenhallinta on avainasemassa. Elinkaarenhallinnassa tärkeitä huomioon otettavia asioita ovat nimeämisstandardit, tunnusten omistajien ja käyttötarkoitusten dokumentointi sekä prosessien noudattaminen tunnusten hallinnassa. Ilman toimivaa tunnusten elinkaarenhallintaa voidaan päätyä tilanteeseen, jossa kriittistä prosessia ajetaan tunnuksella, josta kenelläkään ei lopulta ole tarkempaa tietoa.

Optimaalisessa tilanteessa kaikki tarvittava tieto mukaan lukien ohjelmistorobotin käyttöoikeudet ovat ylläpidettynä ja saatavilla keskitetyssä identiteetinhallintajärjestelmässä.

> Tapojahan on varmasti monia, mutta jos sen [robotiikkatunnusten hallinnan] toteuttaa elinkaarihallinnan ja järjestelmällisen raportoinnin kannalta alusta loppuun, niin silloin se on varmastikin tietoturvallista. Näillä tunnuksilla tulee olla jonkinnäköinen omistaja ja validointi, ja sitten meillä itsellä tulee olla kyvykkyys raportoida esimerkiksi, että jotakin RPA tunnusta käytetään tällaiseen tarkoitukseen ja sillä on tällaiset oikeudet. Silloin se on varmasti aika lähellä sellaista optimia tietoturvankin kannalta. Mutta toki sitten se voi olla myös toinen ääripää, että luodaan tunnuksia, joista kukaan ei tiedä mitään, ja sitten vielä oikeuksia annetaan niille tunnuksille prosessin ohi. (H8)

Ohjelmistorobotiikkatunnusten elinkaarenhallintaa ohjaavat hyvin pitkälti organisaation oma tietoturvapolitiikka (engl. *Information Security Policy*) sekä identiteetin- ja pääsynhallinnan käytännöt. Parhaan mahdollisen tietoturvan varmistamiseksi näihin on kuitenkin hyvä yhteensovittaa myös ohjelmistorobotiikan parhaat käytännöt. Mikäli organisaatio ostaa ohjelmistorobotiikkaa palveluna ulkoiselta kumppanilta, niin on tärkeää, että sekä asiakas että robotiikkapalvelun tuottaja hyväksyvät yhteisen toimintatavan.

> [...] asiakkailla on kaikilla vähän erilaiset Information Security Policyt, esimerkiksi miten IAM:a suoritetaan, joillain se on tarkempaa ja joillain ei ole ihan yhtä tarkkaa. Tää kertoo hyvin siitä, että se nyrkkisääntö on, että mennään aina sen asiakkaan information security -käytäntöjen mukaan ja pyritään toteuttamaan niitä, plus sitten näitä RPA:n best practiceja tunnushallinnan suhteen. Ne sitten vaan nidotaan yhteen sellaiseksi paketiksi minkä asiakas hyväksyy, ja minkä sitten myös RPA tuottaja hyväksyy sillä tavalla, että me ei itse nähdä siinä mitään riskiä meidän näkökulmasta. (H10)

Ohjelmistorobotiikassa tunnuksenhallinnan parhaisiin käytäntöihin kuuluu, että robotiikkatunnusten luomiseen käytetään organisaation käytössä olevaa käyttäjätietokantaa, kuten Microsoftin tarjoamaa Active Directory -palvelua, jossa robotiikkatunnusten identiteettejä ylläpidetään. Parhaiden käytäntöjen mukaan ohjelmistorobottien pääsyä eri järjestelmiin tulee kontrolloida samalla tavalla kuin ihmiskäyttäjienkin oikeuksia, keskitetyn käyttäjäoikeuksien hallintajärjestelmän kautta.

> [...] se robotti saa identiteetin asiakkaan Active Directorysta, eli käytetään ihan sitä asiakaan omaa identiteettihallintaa. Eli sinne luodaan robotille identiteetti ja asiakas itse määrittelee mihin sillä robotilla on pääsy, millä tasolla sillä on pääsy minnekin ja samalla asiakkaalla on keskitetty identiteetin hallinta samalla tavalla kuin hallitsevat ihan ihmiskäyttäjiä, niin ne robotit menevät siellä samalla tavalla mukana. Ja ihan samalla tavalla myös robotille järjestetään se pääsy sitten, kun sillä on se identiteetti, niin sille järjestetään sitten pääsy tiettyyn kohdejärjestelmään. (H10)

Kaikilla haastateltavilla oli keskenään hyvin samankaltainen näkemys ohjelmistorobotiikassa käytettävistä salasanakäytännöistä, mikä myötäilee myös ohjelmistorobotiikan parhaita käytäntöjä. Parhaiden käytäntöjen mukaan ohjelmistorobotiikkaan sovelletaan organisaation olemassa olevia salasanapolitiikkoja, mitkä määrittelevät salasanoille vähimmäisvaatimukset, vaaditun vaihtovälin, sekä säännöt salasanojen hallinta- ja säilytystapaan.

Ohjelmistorobotit simuloivat loppukäyttäjiä, joten nyrkkisääntönä voidaan pitää, että salasanojen vähimmäisvaatimukset ovat samoja kuin loppukäyttäjilläkin. Huomioon on kuitenkin otettava ympäristökohtaiset erot ja vaatimukset, sillä esimerkiksi tiettyjen verkkosegmenttien sisällä operoivilta tunnuksilta voidaan vaatia pidempiä ja monimutkaisempia salasanoja, mitä pääsääntöisesti organisaation politiikat edellyttävät. Huomionarvoista on myös noudattaa organisaation politiikkoja myös sellaisten, paikallisten järjestelmien osalta, johon tietoturvakontrollit eivät teknisesti ylety.

> [...] jos se on domainissa tai Azuressa se tunnus, niin siihen pätee tietysti keskitetty sääntö, kuten meidän käyttäjiinkin, se on mun mielestä aika helppo juttu. Sitten kun mennään näihin paikallisiin järjestelmiin, niin meillähän ei lonkerot yllä sinne millään, koska ne [käyttäjätunnukset] on täysin paikallisia siellä järjestelmän sisällä. Politiikka sanoo, että niiden täytyy noudattaa samaa politiikkaa mitä AD-tunnusten, esimerkiksi salasanapolitiikka. Ne ei ole IAM:n, tietoturvan tai AD-palvelun kontrollissa nää paikalliset tunnukset, mutta se ei tarkoita sitä, että niissä ei salasanaa vaihdettaisi tai että niissä ei pätisi samat politiikat. (H8)

Salasanojen vaihtoväli on ohjelmistorobotiikan kohdalla haastava kysymys, sillä tyypillisesti ohjelmistorobottien identiteettejä käsitellään organisaatioiden käyttäjätietokannoissa samalla tavalla kuin palvelutunnuksia, joilla saattaa olla oletusarvoisesti ikuinen salasana. Robotiikan osalta muuttumattomat ja heikot salasanat nähdään kuitenkin tietoturvan kannalta riskinä, sillä käyttäjätunnukset ovat kuitenkin suhteellisen helposti löydettävissä.

> [...] ja niissä ei oo vaihtuvaa salasanaa niinkuin normaaleilla käyttäjillä on. Eli periaatteessa jos joku saa sen käyttäjätunnuksen, ja ne käyttäjätunnukset on aika helposti löydettävissä, mutta sitten vielä sen salasanankin, niin periaatteessa pystyt käyttämään sitä robotiikan käyttötunnusta tavallaan nimettömänä. (H4)

Yleiseksi huoleksi ohjelmistorobotin salasanan vaihdossa osoittautui prosessin jatkuvuuden varmistaminen. Manuaalisesti toteutettuna salasanan vaihtoprosessi nähdään työläänä, sillä manuaalisesti vaihdettu salasana pitää toimittaa myös ohjelmistorobotin kehityksestä vastaavalle henkilölle, jonka täytyy syöttää uusi salasana robotiikkaprosessin käyttöön. Lisäksi hallinnollisesta näkökulmasta tällainen manuaalinen työnkulku nähdään huonona toimintatapana ja myös alttiiksi inhimillisille virheille. Manuaalinen työ voidaan kuitenkin välttää ja prosessin jatkuvuus voidaan turvata automatisoimalla myös salasananvaihtoprosessi, jolloin ohjelmistorobotti suorittaa koko toimenpiteen itsenäisesti.

> Tää on semmoinen varmaan, mikä pitää siinä tietoturvassa ottaa huomioon, että miten niitä säilytetään ja vaihdetaanko niitä. Itse katsoisin, että se voisi jopa toimia automaattisesti, että robotti hoitaisi sen. Että tää henkilö ei tietäisi että se käynnistettäisiin tää prosessi, robotti vaihtaisi itselleen salasanan ja sitä salasanaa ei kukaan tiedä. (H4)

> [...] ainakin yhdelle asiakkaalla puolen vuoden välein vaihtuu se salasana, mutta sitä varten me ollaan itseasiassa kehitetty sellainen vaihda salasana objekti, joka tunnistaa sisäänkirjautumisen yhteydessä, että nyt se järjestelmä ilmoittaa, että tälle käyttäjätunnukselle täytyy vaihtaa uusi salasana. Silloin meidän oma RPA prosessi generoi uuden tietoturvallisen salasanan sen prosessin sisällä, ja tallentaa sen vielä encryptattuna sinne robotiikkasovelluksen tietokantaan sille kyseiselle accountille. Eli tässä tapauksessa ihminen ei missään vaiheessa sekaannu siihen puolen vuoden välein tehtävään salasanan vaihtoon. (H5)

> Yleensä kun puhutaan AD-tunnuksista, niin se on tiedossa silloin kun se AD-tunnus luodaan, se ensimmäinen salasana, mutta sen jälkeen yleensä tehdään siihen prosessiin tällainen salasanan vaihto steppi, eli robotti itse vaihtaa salasanansa ja sen jälkeen kukaan ihminen ei enää tiedä mikä se salasana on. Se on sellainen best practice, mitä mun mielestä kannattaa käyttää, koska silloin se riski siinä, että se salasana esimerkiksi vuotaisi jonnekin, niin on hyvin minimaalinen, koska se on vaan sillä robotilla tiedossa eikä kukaan ihminen tiedä sitä. (H10)

Käyttäjätunnusten ja salasanojen säilyttäminen käytetyssä ohjelmistorobotiikkasovelluksessa itsessään on tietoturvallista, sillä robotiikkasovellukset tyypillisesti mahdollistavat salasanojen säilyttämisen salatussa muodossa riippumatta siitä onko kyseessä käyttäjätietokannassa hallinnoitu käyttäjätunnus, vai jonkin lokaalin järjestelmän käyttäjätunnus, joka on erillään keskitetystä tunnushallinnasta. On kuitenkin mahdollista, että käyttäjätunnusten salasanoja on tarve säilyttää myös muualla. Esimerkiksi virhetilanteissa voi olla tarpeellista kirjautua sisään ohjelmistorobotin käyttäjätunnuksilla, jotta prosessi saadaan uudelleen käyntiin. Tällaisissa tapauksille tulee kuitenkin olla omat prosessit, jotta jälkikäteen voidaan varmistua siitä, millaisia toimenpiteitä ohjelmistorobotin käyttäjätunnuksella on tehty ja kenen toimesta.

> Jos se vaatii tosiaan sen, että sun täytyy kirjautua robotin tunnuksilla sisään, niin sitten se vaatii sen. Sille pitää vaan olla hyvät syyt ja prosessit ja mieluiten sitten myös, että siitä jää joku jälki johonkin change managementtiin tai johonkin, eli että se sitten lokitetaan, että nyt ollaan vaihdettu salasana ja tehty tällainen asia vianetsintä tarkoituksessa. Sitten se tehdään sillä tavalla. (H10)

> [...] sinne [kohdejärjestelmään] pitää kuitenkin olla pääsy [ohjelmistorobotin tunnuksilla], niin mun mielestä on tärkeämpää, että on ohjeistettua, että miten sitä käytetään ja kuka sitä käyttää. (H6)

Tällaisia tapauksia varten ohjelmistorobottien salasanat tulee säilyttää tietoturvan varmistamiseksi salatussa muodossa siten, että pääsy niihin on tarkasti rajattu. Salasanojen säilytystapaa ohjaa tyypillisesti organisaatioiden tietoturvaa koskevat politiikat.

> Meillä on itseasiassa tällainen IAM-politiikka [...], että salasanaa ei saa tallentaa selkokielisenä tekstinä yhtään mihinkään, kuten esimerkiksi serverin levynkulmalle, vaan se täytyy olla jossain holvissa, johon ei ole kuin tietyillä ihmisillä pääsy, tai sitten tällaisessa password manager ohjelmistossa. (H8)

Haastattelujen perusteella tietoturvariskit kasvavat sen myötä mitä useammalla henkilöllä ohjelmistorobotin salasana on tiedossa. Tämän vuoksi ohjelmistorobotin tunnistautumistietoihin pääsy pitäisi rajata tarkasti siten, että ainoastaan välttämättömät henkilöt pääsevät niihin käsiksi. Haastateltujen henkilöiden vastausten perusteella sellaisten käyttäjien pääsyä ohjelmistorobotin käyttäjätunnuksiin voidaan pitää perusteltuna ja tietoturvan näkökulmasta hyväksyttävänä, joilla on itsellään kohdejärjestelmässä laajemmat käyttöoikeudet, kuin ohjelmistorobotilla.

> [...] [ohjelmistorobottien] tunnuksia käytännössä luovutettiin käyttöön vaan sitten näille siihen prosessiin liittyville avainhenkilöille, eli se tarkoittaa sitä, että meiltä se oli tiedossa sillä meidän IT-vastaavalla, ja sen lisäksi niillä key-usereilla, ketkä sitä prosessia testasi. Minä itse en esimerkiksi koskaan saanut näitä robottien käyttäjätunnuksia, ja jos tunnukset sain niin salasanaa en saanut. Eli se rajattiin vaan niille tarpeellisille henkilöille. (H7)

Haastatteluissa keskeiseksi tietoturvariskiksi nostettiin ohjelmistorobottien liian laajat oikeudet toimia kohdejärjestelmien sisällä. Mikäli ohjelmistorobotin käyttäjätunnukselle annetaan liian laajat käyttöoikeudet, väärinkäytösten riski ja vaikutukset kasvavat huomattavasti, mikäli tunnus päätyy vääriin käsiin tai tunnusta käytetään vääriin tarkoituksiin. Haastateltujen henkilöiden näkemyksen mukaan on olemassa riski, että ohjelmistorobotille annetaan liian laajat käyttöoikeudet, mikäli ei ole riittävää ymmärrystä millaisia oikeuksia ohjelmistorobotti todellisuudessa tarvitsee tehtävän suorittamiseksi.

> Sitten toinen asia mikä varmasti on iso juttu, kun puhutaan identiteetin käytöstä applikaation sisällä, niin kuinka tällainen role based authorization tai authentication tyyppinen ratkaisu siellä on mahdollista tehdä. Elikkä mitä kaikkea sille robotiikkatunnukselle annetaan oikeuksia tehdä siellä sovelluksessa. Että ehkä sudenkuoppana on se, että helposti annetaan liian suuret oikeudet sille accountille, että se ei jää se automatisointi siitä kiinni, ettei sillä ole oikeutta tehdä jotain toimintoa. Mutta toisaalta siinä kohdin me avataan myös sille hyökkääjälle tai väärinkäyttäjälle mahdollisuus tehdä sillä tunnuksella myös muita asioita, mitä sen ei pitäisi. (H3)

> [...] niin kyllä se [ohjelmistorobotin liian laajat oikeudet kohdejärjestelmässä] kohtuullinen riski olisi siinä mielessä, vaikkakin sitä robottia olisi opetettu tekemään tietyt jutut, mutta mistäs sen sitten voi todentaa, ettei joku väärinkäytä niitä samoja tunnuksia. (H7)

> [...] meidän ERP-ratkaisu, jossa tehtiin tähän maksuliikenneprosessiin toinen robotti, niin siellä tuli ilmi myös tällainen käyttöoikeuksiin liittyvä haaste. Siinä vaiheessa, kun se robotti oli menossa tuotantoon, niin tuli ilmi, että sille on annettu liian laajat käyttöoikeudet, minkä seurauksena sitä prosessia sitten jouduttiin muokkaamaan. (H1)

Tietoturvan varmistamiseksi tämän osa-alueen kohdalla haastateltujen henkilöiden yleisesti vallitseva näkemys oli vähäisimpien oikeuksien periaatteen (engl. *Principle of Least Privilege, PoLP*) noudattaminen. Tämä tarkoittaa sitä, että ohjelmistorobotille tulisi antaa aina pienimmät mahdolliset oikeudet, joilla se pystyy suorittamaan sille määritellyt tehtävät kohdejärjestelmissä.

> Mun mielestä, on se sitten mikä tunnus tahansa, niin pitää noudattaa tällaista Least Privilege -periaatetta. Enkä mä usko, että eihän se [ohjelmistorobotti] mallinna sitä loppukäyttäjää, jos sillä suoritetaan vaan jotain tiettyä tehtävää ja sitten sille lätkäistään joku järjestelmän pääkäyttäjän oikeus, niin ei missään nimessä. (H8)

> Eli sille [ohjelmistorobotille] ei ikinä anneta minkään näköisiä liiallisia oikeuksia, eli aina selvitetään se, että minkälaiset oikeudet se robotti sinne kohdejärjestelmään tarvitsee. (H10)

> Ja tuota no se miten me sitten käytännössä pyrittiin kuitenkin niinkun mitigoimaan sitä riskiä mitä siihen liittyy, niin oli ihan se, että annettiin mahdollisimman rajatut käyttöoikeudet sille robotille sinne järjestelmään että se pystyy tekemään ja näkemään vaan sen datan mitä se robotti tarvitsee ja tekemään vain ja ainoastaan ne rajatut toimenpiteet sillä järjestelmällä mitä tarvitsee. (H1)

> Meillä oli käytännössä kaksi vaihtoehtoa, miten me robotin prosessi järjestetään ja siinä oli sillä tavalla vaihtoehtona, että A) me tehdään monimutkaisempi prosessi, ja robotille tulee silloin sellaiset kapeat käyttöoikeudet, samanlaiset mitä ihmiskäyttäjällä olisi. Vaihtoehto B) oli, että me saadaan todella helppo ja suoraviivainen prosessi, mutta me annetaan silloin robotille sellaiset järjestelmänhaltija oikeudet. Lopputuloksena oli se, että me annettiin ne kapeat oikeudet, koska me ei haluttu sitten kuitenkaan ottaa sitä riskiä siinä, että robotille annettaisiin käytännössä järjestelmänhaltijan oikeudet. Se oli niinkuin riskienhallintavinkkelistä tämä päätös. Se oli loppupelissä hyvin selkeä, koska se oli koko yhtiötä koskeva politiikka mikä sen sitten saneli. (H7)

Haastatteluissa todettiin myös, että vähäisimpien oikeuksien periaatteen noudattaminen ei ole aina täysin mahdollista johtuen eri kohdejärjestelmien arkkitehtuureista. Joissakin järjestelmissä käyttöoikeuksia voidaan määritellä hyvinkin spesifillä tasolla, kun taas osa järjestelmistä mahdollistaa ainoastaan tiettyjen oletusarvoisten roolien valinnan.

> Sitten meillä on saattanut olla jossain vaikka nyt tässä viimeisessä virityksessä, niin meillä on ollut sitten toissijaisena tietolähteenä vaikkapa meidän

> legacy [toiminnanohjausjärjestelmä], jossa taas tällaista ihan näin tarkkaa käyttöoikeuksien rajausta ei oikein pystyt tekemään. (H2)

> Jos sovellus antaa periksi, niin tällaisella robotiikka accountilla pitäisi olla hyvin custom oikeudet tehdä tasan tarkkaan ne toimenpiteet mihin se on suunniteltu, eikä yhtään mitään muuta. Mutta sitten jos mennään legacy sovelluksiin, niin niissähän ei taas ole mahdollista tehdä tällaisia käyttöoikeuksia. (H3)

Yksittäisten ohjelmistorobottien käyttöoikeuksia pystytään minimoimaan luomalla jokaista automatisoitavaa prosessia varten oma ohjelmistorobotti. Mikäli samaa ohjelmistorobottia käytetään useiden prosessien automatisoimiseen, niin tämä väistämättä laajentaa robotin käyttöoikeuksia kohdejärjestelmien sisällä.

> Mun näkemyksen mukaan ja omien kokemusten mukaan niissä asiakkuuksissa missä mä oon ollut, niin turvallisin tapa on ollut se, että jokaiselle automatisoidulle liiketoimintaprosessille on oma robottitunnus. Eli yleensä prosessit määritellään esimerkiksi "process 10", jolloin sille on olemassa sitten ikään kuin "rpa10" tunnus näin kärjistetysti. [...] Sitten kun määritetään aina uutta prosessia varten sille spesifi robottitunnus, niin samalla se voidaan tsekata tarkkaan, että tätä prosessia varten täytyy olla pääsyt paikkaan X ja Y, eikä muualle, jolloin sillä kyseisellä tunnuksella on pääsy vaan niihin tiettyihin paikkoihin. (H5)

> Yleensä se menee niin, että yhdellä robotilla on pääsy yhteen kohdejärjestelmään ja siellä kohdejärjestelmässä tällä tunnuksella on tietyt oikeudet tehdä asioita mitä sen täytyykin sen prosessin määreissä pystyä tekemään. (H10)

Tehtävien eriyttämisen periaatteen noudattaminen jakoi haastateltujen henkilöiden kesken paljon mielipiteitä, sillä se sai vastauksia sekä puolesta että vastaan. Osa haastatelluista henkilöistä oli sitä mieltä, että tehtävien eriyttämisen periaatetta pitää soveltaa ohjelmistorobottien kohdalla samalla tavalla kuin ihmistenkin osalta. Keskeisimpänä perusteluna tälle näkemykselle esitettiin sitä, että ohjelmistorobotti simuloi loppukäyttäjää, joten sitä on myös koskettava samat lainalaisuudet tietoturvan varmistamiseksi.

> Mä ajattelen, että se robotti on yksi käyttäjä ja sen pitää noudattaa ihan niitä samoja periaatteita kuin muuallakin. Jos ajatellaan maksuliikenneprosessia, niin sama henkilö ei saa hyväksyä laskua ja maksaa sitä, tai sama henkilö ei voi syöttää maksua ja lähettää sitä pankkiin, vaan tietty pätkä prosessia pitää olla yhden roolin vastuulla. Jos samalla tunnuksella pystyy tekemään liikaa asioita, niin siinä on riski, että käyttäjä pystyisi tekemään jonkun väärinkäytöksen. (H1)

> Me ollaan päädytty siihen, että me eriytetään myös robotilla. Jos se robottiprosessi on samanlainen kuin mitä se olisi manuaalisesti tehtynä, niin sitten

> me ollaan eriytetty se vaikka kahdelle eri robottitunnukselle. Siitä asiasta ollaan pidetty kiinni myös robottimaailmassa. (H7)

> Mun näkökulmasta robotti on kuin ihmiskäyttäjä, joten kyllä se [tehtävien eriyttäminen] samalla tavalla menee kuin ihmiskäyttäjälläkin robotin suhteen. (H10)

Osa haastatelluista henkilöistä oli sitä mieltä, että tehtävien eriyttämisen periaatetta ei ole tarve noudattaa robottien kohdalla yhtä tarkasti, mikäli ohjelmistorobotiikan tietoturva on muuten huomioitu riittävällä tasolla. Nämä henkilöt kuitenkin korostivat, että tehtävien eriyttämisen periaatteesta poikkeamista on aina harkittava tapauskohtaisesti.

> Mun mielestä se paine siirtyy osittain sinne ikään kuin prosessin alkupäähän, elikkä sen prosessin määrittelyyn, koska siellähän voidaan tehdä jo sellaisia hyvin vääriä olettamia. Näkisin että sitten kun prosessin päätöksentekopisteet saadaan määriteltyä ja speksattua riittävällä tasolla, niin silloin mun mielestä se on ihan turvallista toimia sillä yhdellä robotilla siinä, vaikka se muuten olisikin tällainen kaksi ihmistä vaativa. Mutta se vaatii totta kai sen ymmärryksen siitä prosessista, että se on hyvin case by case mietittävä. (H2)

> En näe sellaista isoa riskiä näissä roboteissa väärinkäytösten osalta, jos katsotaan että se on muuten sen robotin tietoturva hoidettu. Mutta sitten kun mennään prosessissa pidemmälle, niin siellä on varmaan se datan tarkistuksen vaihe. Kyllä meillä varmaan jossain kohtaa pitää tsekata se, ettei robotti hakkaa väärää tietoa järjestelmään. (H4)

> Kuitenkin siihen liittyy aina selkeät säännönmukaisuudet mitä milloinkin voi tehdä, ja mikäli joku maksu lähtee eteenpäin, niin sille on varmasti selkeät säännöt, jonka perusteella se päätös tehdään. En usko, että siinä on sinänsä mitään tietoturvariskiä. Robotti ei ole korruptoitunut niin sanotusti. (H5)

> Kaikessa maksamisessa mä pitäisin aina sen neljän silmän periaatteen myös robottien osalta. [...] Mutta sitten jos puhutaan taas jostain kirjanpidon puolen asioista, tiliotekäsittelystä tai jostain tämän tyyppisestä, niin siellä mä nään, että se riski on paljon pienempi ja kaikki on korjattavissa, niin miksi ei. (H6)

Tätä näkemystä perusteltiin myös hieman psykologisemmasta näkökulmasta, sillä tyypillisesti hyväksymisketjuissa ensimmäinen hyväksyntä menee melko automaattisesti läpi. Näin ollen uhkaskenaario on lopulta sama tilanteissa, joissa hyväksyjäketjun toisen henkilön tunnukset vuotavat vääriin käsiin, tai sellaisen ohjelmistorobotin tunnukset, jonka osalta ei noudateta tehtävien eriyttämisen periaatetta, päätyvät vääriin käsiin.

> Entäs jos meillä on kaksi päätöksentekijää joista toisen tunnukset vuotavat, ja sitten psykologisesti se menee useimmiten sillä tavalla, että sen toisen suositus menee varsin automaattisesti läpi. Se on vaan inhimillistä

> toimintaa ja se on se, miten meidän toimintatavat järjestyy inhimilliseltä näkökannalta ja tässä suhteessa se robotti ja se henkilö hengittävä loppukäyttäjä ei oo lainkaan erilaisia. Se uhkaskenaario ei ole eri, se on täysin sama. (H11)

Haastatteluissa myös nostettiin esille myös se, että kaikkia hyväksymisketjuja sisältäviä prosesseja ei välttämättä kannata automatisoida, ja tätä tulisi aina harkita tilannekohtaisesti. Olennaista on osata tehdä selkeä rajanveto siihen, mitä ohjelmistorobotiikalla on viisasta tehdä.

> Tällaisen hyväksymisketjun, missä pitää olla useampia silmäpareja, niin sellaisen automatisointi ei ehkä ole hirveän hyvä. Mutta sitten taas, jos ajatellaan siitä pisteestä, että herra X:n esimies on hyväksynyt sen laskun finapuolelle, niin siitä eteenpäin sen laskun loppuun meneminen voi olla hyvinkin robotiikalla. (H3)

Ohjelmistorobottien tunnistautumismenetelmä kohdejärjestelmiin oli teema, mistä kaikki haastatellut henkilöt olivat yhdenmielisiä. Haastattelujen perusteella tietoturvallinen käytäntö ohjelmistorobottien kohdejärjestelmiin tunnistautumiselle on noudattaa samaa tunnustautumismenetelmää, mitä myös järjestelmien muut loppukäyttäjät käyttävät. Robotille ei ole syytä kehittää erillisiä tunnistautumismekanismeja, sillä robotit tekevät järjestelmissä joka tapauksessa samaa, mitä myös ihmiskäyttäjät tekevät. Tyypillisesti ohjelmistorobotit tunnistautuvat järjestelmiin kertakirjautumisen menetelmällä, mutta lokaaleihin järjestelmiin, joihin tarvitaan erillinen käyttäjätunnus ja salasana, robotti kirjautuu syöttämällä nämä erilliset tunnistetiedot aivan kuten ihminenkin.

> Joo, se on juurikin näin, eli robotille ei tehdä mitään erilaisia tunnistautumismekanismeja, koska robotti periaatteessa tekee täysin saman asian mitä ihmiskäyttäjäkin tekee. Eli jos on SSO käytössä ja varsinkin kun käytetään Active Direcotry -tunnuksia, niin monen asiakkaan järjestelmissä käytetään single sign-onia, joten se robotti sitten pääsee ihan omilla tunnuksilla suoraan kirjautumaan. [...] Jos se ei pysty sitä AD-tunnusta käyttämään, niin sitten sillä tosiaan on oma tunnus ja salasana sinne, mutta sama periaate pätee. (H10)

Tämä on yleisesti vallitseva paras käytäntö ohjelmistorobotiikan osa-alueella, vaikka osa alan toimijoista antaakin omia suosituksiaan, muun muassa koskien monivaiheista tunnistautumista. Monivaiheinen tunnistautuminen on kuitenkin erityisen haastavaa toteuttaa ohjelmistorobotille, eikä tämä ole yleisesti sovellettu toimintatapa.

> Nyt esimerkiksi Microsoft suosittelee, että käytetään yhtä salasanaa koko ajan, mutta siihen pitää sitten leipoa se multifactor autentikaatio päälle. Sen robotin kannalta se multifactor autentikaatio on hyvin hankala, koska multifactor autentikaatio tarvitsee yleensä jonkun kolmannen osapuolen laitteen, puhelimen tai jonkun, mistä sitten otetaan se koodi tai minkälainen MFA nyt sattuu olemaankaan, niin se on hyvin hankala robotille toteuttaa. Se best practice sitten siinä on, että MFA:ta ei käytetä roboteilla. Varsinkin

> tällaiset captcha jutut, niin nehän on suunniteltu nimenomaan sitä varten, että botti ei pysty siitä menemään eteenpäin, koska se on periaatteessa mahdotonta opettaa sille robotille, jos ei aleta käyttämään jotain hyvin monimutkaisia kuvantunnistamisalgoritmeja sun muuta, mutta sillä ei ole sitten enää mitään tekemistä RPA:n kanssa. (H10)

> SSO on kyllä ollut meillä käytössä yllättävänkin paljon ja mä uskon, että se on ihan riittävän tietoturvallinen. Sit taas tuollainen multifactor autentikoituminen tai vastaava, niin mä en ainakaan henkilökohtaisesti tiedä miten se olisi toteutettavissa robottitunnuksilla. Jos tällä hetkellä se tehdään esimerkiksi lähettämällä tekstiviesti, niin kyllä siihen jonkinlaisen prosessin varmaan voisi kikkailla, mutta se menee tosi haastavaksi. (H5)

> Se aina vähän riippuu siitä, että mitkä sen kohdejärjestelmän kyvykkyydet on. Useimmat kohdejärjestelmät, niillä ei ole edes mahdollisuutta tarjota jotain muita vaihtoehtoja tai muita tapoja autentikoitua. Siinä mielessä voi olla kohtuuton vaatimuskin lähteä edellyttämään, että robotilta vaadittaisiin jotain eri autentikoitumismenetelmää kuin muilta käyttäjiltä. (H11)

6.2 Datan eheyden poikkeamat

Haastatellut henkilöt tunnistivat datan eheyden poikkeamat tietoturvariskeiksi, joilla voi olla merkittäviäkin seurauksia. Tyypillisimmillään datan eheyden poikkeamat johtuvat automatisoitavan prosessin puutteellisesta määrittelystä tai virheistä ohjelmistorobotin konfiguraatiossa, mutta myös sellaisia tilanteita on esiintynyt, joissa lähdedata on ollut virheellistä. Datan eheyden poikkeamien korjaus prosessissa edellyttää manuaalista työtä, joka taas on altista inhimillisille virheille. Tällaisissa tilanteissa on esimerkiksi riskinä, että järjestelmistä jää puuttumaan dataa, tai järjestelmiin voi syntyä duplikaatteja, joilla voi olla myös taloudellisia seuraamuksia.

> Meidän prosesseista se toimittajille maksettava laskuaineiston valmisteluun liittyvä on sellainen riskienhallintamielessä mielenkiintoisin, että siinä se ongelma voi johtua siitä, että jostain kumman syystä se robotti ei ole saanut kohdejärjestelmässä suoritettua kaikkia automaattiajoja, jotka sen olisi pitänyt suorittaa, josta on aiheutunut virheellistä dataa. Sitten henkilön on pitänyt kirjautua robotin tunnuksilla järjestelmään, käydä poistamassa sieltä tietyt virheellisen datan aineistot ja sitten joko suorittaa itse manuaalisesti se prosessi loppuun tai käynnistää robotti uudestaan. Tällä riskinä voisi olla esimerkiksi se, että järjestelmään jäisi jo robotin valmistelemia maksunippuja, joiden perusteella maksettaisiin toimittajille, ja sitten kun ajetaan manuaalisesti prosessi uudestaan, niin samat laskut menisi uudestaan maksettavaksi ja maksettaisiin tuplana. (H7)

Lisäksi haastatteluissa korostettiin, että ohjelmistorobotiikkaa hyödyntäessä datan eheyden poikkeamat kumuloituvat huomattavasti nopeammin kuin

manuaalisesti suoritettavissa prosesseissa, sillä ohjelmistorobotiikan myötä prosessien suorittaminen nopeutuu huomattavasti. Lisäksi tällaisten virheiden havaitseminen voi olla hitaampaa automatisoiduissa prosesseissa kuin manuaalisesti suoritetuissa. Tämä myös lisää huomattavasti manuaalisen työn määrää virheiden korjaamisessa.

Datan eheyden poikkeamat, jotka syntyvät suoritettavan ohjelmistorobotiikalla automatisoidun prosessin aikana voidaan jakaa liiketoiminnan poikkeuksiin (engl. *business exceptions*) ja järjestelmäpoikkeuksiin (engl. *system exceptions*). Liiketoiminnan poikkeuksia voi syntyä, mikäli kaikkia automatisoitavassa prosessissa esiintyviä poikkeuksia ja erilaisia tehtävänkulkuja ei olla osattu tunnistaa ja määritellä robotin kehitysvaiheessa, ja näin ollen robotti ei osaa toimia oikealla tavalla tällaisen tilanteen tullessa vastaan. Liiketoimintapoikkeuksien ennaltaehkäisyn näkökulmasta keskeistä on määritellä prosessi mahdollisimman tarkalla tasolla ennen sen automatisointia. Prosessidokumentaatio ja järjestelmällinen testaus ovat keinoja, joilla voidaan edesauttaa prosessin riskikohtien tunnistamista, ja nämä kuuluvat myös ohjelmistorobotin kehittämisen parhaisiin käytäntöihin.

> Tää riski pyritään minimoimaan sillä tarkalla prosessidokumentaatiolla ja sitten myös sillä quality assurance ja user acceptance testauksella. Eli kun sitä [prosessiautomaatiota] ajetaan ennen kuin se viedään tuotantoon, niin pyritään saamaan jo kiinni tällaiset tapaukset, mutta niitä voi olla satoja tai tuhansia, niin se voi välillä olla haastavaa löytää ne kaikki. (H10)

Järjestelmäpoikkeukset ovat tilanteita, joissa jokin järjestelmässä esiintyvä poikkeustilanne estää ohjelmistorobottia toimimasta oikealla tavalla, tai keskeyttää koko prosessinkulun. Esimerkiksi kohdejärjestelmän käyttöliittymän eteen ilmestyvä ponnahdusikkuna voi aiheuttaa järjestelmäpoikkeuksen. Järjestelmäpoikkeuksia esiintyy erityisesti järjestelmissä tai ympäristöissä, jotka ovat vielä aktiivisesti kehityksen alla. Tämän vuoksi järjestelmän kypsyyttä tulisi aina arvioida kriittisesti ennen prosessin automatisointiprojektin aloittamista, sillä säännönmukaisesti päivittyvä järjestelmä on kriittinen riski automaation toimivuuden sekä datan eheyden näkökulmasta.

> Nyrkkisääntönä ei kannata rakentaa ensinnäkään, jos ei järjestelmä oo vielä valmis, ja vakiintunut, että joku sanoo että tää on valmis, niin odota vielä puoli vuotta ja aloita sitten se rakentaminen, että se varmasti vakiintuu se tilanne. (H5)

Järjestelmäpoikkeuksien esiintymistä voidaan ehkäistä lisäämällä logiikkaa ohjelmistorobotin konfiguraatioon. Ohjelmistorobotti voidaan esimerkiksi konfiguroida tarkistamaan ennen datan kenttään syöttämistä, että kenttä on varmasti olemassa, sekä tarkistamaan toimenpiteen jälkeen, että syötetty data on varmasti tallentunut.

Poikkeamat lähdedatassa ovat haastattelujen perusteella harvinaisempia kuin prosessissa esiintyvien virhetilanteiden seurauksena syntyvät poikkeamat. Lähdedatan poikkeamat ovat haastattelujen perusteella liittyneet

kohdeorganisaatiossa poikkeuksetta ongelmiin datan saatavuudessa tai tilanteisiin, joissa dataa on ollut tarve hakea pitkältä aikaväliltä, sillä näissä tilanteissa datan laatu ja eheys ei ole aina ollut samalla tasolla kuin nyt. Virheellisen lähdedatan aiheuttamat tilanteet voidaan kuitenkin välttää datan validoinnin keinoin. Ohjelmistorobotti voidaan esimerkiksi konfiguroida vertailemaan dataa eri datalähteiden välillä tietyissä validointipisteissä.

> Virheellinen data yleensä, se toki pitää aina pystyä speksaamaan alkuvaiheessa, että missä kohtaa voi piillä riskejä, että se data ei ole validia ja sitä varten yleensä tehdään aina datan validointi ennen kuin sitä aletaan prosessoimaan. Sitä varten tietysti pitää olla säännönmukaisuudet, millä se varmistetaan. (H5)

> Tehtiin käytännössä tiettyjä vertailuja datan eri lähteiden välillä ja mikäli siellä tuli poikkeavuuksia, niin pystyttiin nostamaan ne sitten manuaalisesti hanskattavaksi tai poikkeuslistalle. Lähinnä haluttiin saada aikaan tilanne, että se robotti ei tee väärää oletusta. Elikkä haluttiin eliminoida tilanteet, joissa se vois tehdä oletuksen, mikä olisi väärä. (H2)

Toinen datan validoinnin keino on tunnistaa ja validoida ohjelmistorobotin käsittelemän datan sekä kohdejärjestelmän välisiä riippuvuuksia. Tämä voidaan toteuttaa esimerkiksi lisäämällä ohjelmistorobotin konfiguraatioon välivaihe, joka tarkistaa, että tekstikenttään syötetty data on tekstiä. Haastatteluissa nousi esille myös esimerkki, jossa tämän kaltainen kontrolli lisäsi huomattavasti datan eheyttä verrattuna prosessin automatisointia edeltävään aikaan.

> Meillä on rakennettu sinne robottiin sellainen validointi, että kohtaako maksutapa ja vaikka tilinumerotyyppi ja valuutta. Tämän tyyppisiä validointimääritelmiä on tehty sinne [toiminnanohjausjärjestelmään implementoituun] robottiin, ennen kuin se ajaa sen maksuajon läpi. Käytännössä aina kun se ajaa sen maksuajon läpi, niin se on aina 100 % oikeaa dataa, mikä kuuluukin siihen maksutapaan. Kun taas ihminen tekee sen, niin sähän katsot sen vaan silmämääräisesti, ja siellä on käytännössä aina virheitä. Meillä on tosi paljon laskunkäsittelyssä virheitä, niin tää robotti hoitaa ne kyllä tosi hyvin. (H6)

Datan eheydestä voidaan varmistua myös sisällyttämällä ohjelmistorobotiikalla automatisoitavaan prosessiin human-in-the-loop-käsittelyitä. Käytännössä tämä tarkoittaa sitä, että prosessiin lisätään vaihe, jonka ihminen suorittaa manuaalisesti. Human-in-the-loop-käsittely voi aloittaa tai lopettaa prosessin, tai se voi esiintyä keskellä suoritettavaa prosessia.

> Toisaalta taas varmaan tulevaisuudessa tulee olemaan entistä enemmän näitä ratkaisuja, joissa on niin sanottu human-in-the-loop, että tehdään jotain ja ihminen käy tekemässä välissä jonkun manuaalisen taskin mihin robotti ei pysty, ja sitten robotti jatkaa loppuun. (H5)

> Joo, se on tällainen human-in-the-loop, eli robotti tekee asian X, sitten se lähettää vaikka sähköpostin ihmiselle, joka tekee asian Y, lähettää sen taas

> takaisin robotille ja sitten robotti jatkaa siitä sitä hommaansa. Mä en tiedä kuinka usein tällaisia tehdään, mutta tää on ihan täysin mahdollista ja on varmasti meillä prosesseissa myös käytössä. (H10)

Sen lisäksi, että datan eheyden poikkeamien syntymisen mahdollisuutta ennaltaehkäistään proaktiivisilla toimilla, niin myös reaktiivinen toiminta on avainasemassa tietoturvan varmistamiseksi, mikäli datan eheydessä esiintyy poikkeamia ennakoivista toimista huolimatta. Ongelmatilanteita varten tulisi olla hyvin suunniteltu ja dokumentoitu prosessi, jossa olisi sovittu roolit ja vastuut, kuinka tilanteissa toimitaan. Myös riittävän resursoinnin varmistaminen poikkeustilanteiden varalle on riskinhallintanäkökulmasta tärkeää.

> Ihan samalla tavalla, kun johonkin muuhunkin tekniseen toteutukseen tällaiset asiat tulisi määritellä ja sopia liiketoiminnan ja IT:n ja sen palveluntarjoajan kanssa, että miten niissä häiriötilanteissa sitten toimintaan, kun se tulee, niin se auttaa kun se olis etukäteen sovittu. (H1)

> Pitää olla riittävä resursointi myös katsomaan sen robotin perään ja huolehtimaan siitä robotista sillä tavalla, että jos me tiedetään, että kohdejärjestelmissä tulee olemaan vaikka huoltokatkoja tiettyinä aikoina tai jos meidän tarvii tehdä jotakin ylimääräisiä prosessointeja siihen samaan prosessiin liittyen mitä robotti tekee, niin me pystytään ennakoimaan sitten tällaisia poikkeustilanteita. (H7)

Virhetilanteiden ilmentyessä vianselvityksen tärkein työkalu ovat ohjelmistorobotiikkajärjestelmän audit lokit. Audit lokeihin tallentuu ohjelmistorobotin suorittamat työvaiheet, jolloin lokien perusteella voidaan todeta missä kohtaa robotti on toiminut väärin tai mihin kohtaan prosessi on pysähtynyt. Tämän tiedon valossa automatisoituun prosessiin voidaan tehdä myös korjauksia, jotta vastaavat tilanteet voidaan välttää jatkossa.

6.3 Informaatioteknologian kuluttajistuminen

Informaatioteknologian kuluttajistumisen ilmiö oli valtaosalle haastatelluista henkilöistä työelämästä tuttu, ja osa oli havainnut ilmiön esiintyneen myös ohjelmistorobotiikan osa-alueella. Haastateltavat tunnistivat informaatioteknologian kuluttajistumisella olevan sekä positiivisia että negatiivisia vaikutuksia ohjelmistorobotiikan kontekstissa. Negatiiviset vaikutukset liittyvät nimenomaan ohjelmistorobotiikan tietoturvan hallintaan. Haastateltavat olivat huolissaan siitä, että tietoturva voi jäädä osittain huomioimatta ohjelmistorobotiikan kehitysprojekteissa, mikäli vastuu painottuu liikaa teknologian loppukäyttäjälle, kuten esimerkiksi liiketoimintayksikölle itselleen.

> Siinä on just se, että ei pystytä varmistamaan sitä, että kehityksessä otetaan huomioon tietoturvavaatimukset. Tää on yleisesti ottaen syy, minkä takia IT huolehtii sovelluksista ja siitä ympäristöstä, koska sinne on valikoitunut

> ne ihmiset, jotka ovat kiinnostuneita myöskin tällaisista jatkuvuusasioista, ja tietoturva on nyt yksi laatuasia. Siellä IT puolella on nyt dedikoitunut ihmisiä, joilla se näkemys on ehkä tietyllä tapaa laajempi. [...] Ne [loppukäyttäjät] katsoo sitä [ohjelmistorobotiikkaa] niin eri kantilta ja kyllä mä nään siinä sen riskin. (H3)

> Kyllähän sellaisessa tapauksessa tietysti on tietoturvariskejä, jos siellä tehdään erilaisia muutoksia tai tieto liikkuu tavalla, josta IT-porukka ei tiedä, tai avataan oikeuksia jonnekin minne ei pitäisi. (H5)

> Ilman muuta muodostuu riskejä. Tietoturvakin on oma osaamisen ala. Jos sieltä jätetään tietoturvaihmiset pois, niin eihän heiltä [loppukäyttäjiltä] voida odottaa, että he tietävät mitä pitää tehdä. (H12)

Haastattelujen perusteella informaatioteknologian kuluttajistumisella voidaan nähdä olevan myös positiivisia vaikutuksia, ja se nähdään osittain myös positiivisena kehityssuuntana. Informaatioteknologian kuluttajistuminen suoraviivaistaa toimintaa ja tekee siitä ketterämpää. Haasteena on kuitenkin tasapainon löytäminen organisaation IT-yksikön tietoturvavaatimusten ja kontrollin sekä liiketoimintayksiköiden tarpeiden välille. IT-yksikön tulisikin kyetä varmistamaan, että informaatioteknologian kuluttajistuminen tapahtuu hallitulla ja tietoturvallisella tavalla.

> Sillä [informaatioteknologian kuluttajistumisella] on varmaan negatiivinen vaikutus tietoturvaan ja sen hallintaan, mutta sitten taas IT:n pitää huolehtia, että se tapahtuu hallitusti. IT on siinä vaan se enabler, eli me tarjotaan työkalut siihen, että se on secure enough, ja loppu hoituu sitten siellä busineksessa. (H8)

> Meidän [IT:n] täytyy vaan huolehtia siitä, että ihmisillä on mahdillisuus tehdä oikein asioita. (H11)

Haastatteluissa nousi esille kolme keskeistä keinoa, joiden avulla voidaan hillitä informaatioteknologian kuluttajistumisen negatiivisia vaikutuksia tietoturvalle, ja osittain myös mahdollistaa informaatioteknologian kuluttajistuminen kontrolloidulla ja tietoturvallisella tavalla. Nämä kolme keinoa ovat tietoisuuden lisääminen, sidosryhmien osallistaminen sekä toimintamallien luominen ja noudattaminen.

Tietoisuuden lisäämisellä tarkoitetaan ennen kaikkea ohjelmistorobotiikkaan ja sen tietoturvaan liittyvän kokonaisvaltaisen ymmärryksen lisäämistä teknologian loppukäyttäjien parissa. Tiedon ja ymmärryksen leviäminen edesauttaa myös luottamussuhteen rakentamisessa organisaation IT-osaston sekä liiketoimintayksiköiden välillä, ja tekee toiminnasta läpinäkyvämpää. Ohjelmistorobotiikka ja tietoturvatietämyksen lisäksi liiketoimintayksiköissä olisi hyvä olla entistä kattavampi ymmärrys kohdejärjestelmistä myös teknisellä tasolla. Tämä edesauttaisi tietoturvahaasteiden tunnistamista entistä laajemmalla rintamalla. Esimerkiksi hyvä tuntemus kohdejärjestelmän kyvykkyyksistä käyttäjätunnusten käyttöoikeuksien kustomoinnissa auttaa minimoimaan

tietoturvapoikkeamien mahdollisuuden. Haastattelujen perusteella liiketoimintayksiköiltä odotetaan laajempaa tietoteknistä osaamista kuin ennen, ja kehityksen suunta näyttäisi jatkuvan samana.

> Kyllä sielläkin [liiketoimintayksiköissä] täytyy mennä sillein aallonharjalla, kun kaikki liittyy jollain tavalla informaatioteknologiaan. Mä en oikein osaa enää hyväksyä sellaista selitystä, että käyttäjä ei osaa käyttää IT-järjestelmiä tai ei jaksa opetella. Ei raksallekaan pääse hommiin, jos ei saha pysy kädessä tai ei osaa käyttää jotain mittalaitetta. (H8)

> Niiden [loppukäyttäjien] pitää yhä enemmän ymmärtää niistä järjestelmistä, niistä arkkitehtuureista, ja millä tavalla ne vaikuttaa siihen lopputulokseen, kun prosesseja automatisoidaan robotiikalla. Se on ollut ylipäätään trendi tässä viime vuosina, että ollaan alettu ymmärtämään, että businekselta voidaan vaatia, että siellä on tällaista osaamista. [...] Yksi kaikkien keskeisimmistä asioista tilanteen parantamiseksi on miettiä se, että miten me mahdollistetaan ihmisten oppiminen, että heillä on se kaikki tieto mitä he tarvitsevat, että he pystyvät menestyksekkäästi sen tavoitteensa tekemään ja saavuttamaan. (H11)

Haastatteluissa esille nousseita keinoja tietoisuuden lisäämiseksi ovat loppukäyttäjien kouluttaminen, avoin kommunikointi ja tiedon jakaminen, työkierto IT-yksikön ja liiketoimintayksiköiden välillä sekä keskeisen tiedon dokumentointi.

Sidosryhmien osallistamisella tarkoitetaan sitä, että kaikki tarvittavat henkilöt pidetään tietoisina sellaisista ohjelmistorobotiikan kehitysprojekteista, jotka jollain tavalla liittyvät heihin. Tämä ei tarkoita sitä, että kaikkien näiden henkilöiden pitäisi osallistua jokaiseen työvaiheeseen, mutta on tärkeää, että näillä henkilöillä on näkyvyys kehitysprojektien tilanteeseen, jotta heidän osaamisensa ja tietämyksensä on oikealla hetkellä käytettävissä. Keskeisiä sidosryhmiä ovat esimerkiksi prosessien omistajat, järjestelmäomistajat sekä tietoturva-asiantuntijat. Kun ohjelmistorobottia ja sen kehitystä tarkastellaan useista eri näkökulmista samanaikaisesti, niin myös tietoturvanäkökulma kyetään huomioimaan tarkemmalla tasolla. Sidosryhmien osallistaminen mahdollistaa myös haasteiden ja puutteiden tunnistamisen mahdollisimman aikaisessa vaiheessa, jolloin niihin voidaan reagoida mahdollisimman ketterästi, ja näin ollen säästää aikaa ja kustannuksia.

> Sitten kun tehdään jotain päätöksiä, tän mä oon nähnyt niin monta kertaa, että ei enää sormet ja varpaat riitä niiden laskemiseen, että ollaan tehty jotain päätöksiä ja aletaan toteuttamaan jotain, niin sitten siellä tulee joku yleensä tietoturvaan tai domain hallinnan kaveri ja sanoo, että mitä te ootte tekemässä, että tää ei mee ollenkaan meidän tietoturvapolitiikkojen mukaan. [...] Sitten se projekti pitenee sen takia, että asiakas itse ei ole ymmärtänyt, että meidän pitää konsultoida näistä asioista vielä sisäisesti vähän laajemmin kuin sen liiketoimintayksikön kesken. (H10)

> Voisi ottaa jo vähän aikaisemmin mukaan asiantuntijoita katsomaan robotiikkakehityksiä niin, että se ei sitten tuu yllätyksenä jossain deployment vaiheessa, että ollaankin nyt tekemässä jotain tietoturvapolitiikkojen vastaista. (H10)

Haastattelujen perusteella erittäin keskeinen osa sidosryhmien osallistamista on tarkoituksenmukainen ja tehokas kommunikointi. Osa haastatelluista henkilöistä pitivät kommunikaation puutetta syynä organisaatiossa esiintyneisiin ohjelmistorobotiikan ja sen tietoturvan haasteisiin.

Haastattelut osoittivat, että pidemmällä aikavälillä sidosryhmien osallistamisella on positiivinen vaikutus myös tietoisuuden lisäämiselle. Kun eri sidosryhmät tekevät keskenään yhteistyötä, niin tietämys leviää laajemmalle organisaation sisällä.

Toimintamallien luomisen ja noudattamisen tarkoituksena on varmistaa, että ohjelmistorobottien koko elinkaaren ajan noudatetaan yhteisiä toimintamalleja ja käytäntöjä koko organisaation laajuisesti. Lähtökohtana näille toimintamalleille tulee toimia organisaation tietoturvapolitiikka ja muut tietoturvaa koskevat käytännöt, kuten esimerkiksi identiteetin- ja pääsynhallinnan politiikat. Organisaation jo olemassa olevien politiikkojen soveltaminen ohjelmistorobotiikan osa-alueella on tyypillinen ja parhaiden käytäntöjen mukainen tapa toimia. Tämänkaltaisten toimintamallien tarkoituksena on siis asettaa organisaatiossa tietyt raamit, joiden sisällä ohjelmistorobotiikkaa toteutetaan.

> Just näin, että siinä [toimintamallien noudattamisessa] jää mahdollisimman vähän liikkumavaraa ja tulkinnanvaraa niihin [tietoturva] asioihin, niin se vie mun mielestä asioita oikeaan suuntaan ja ainakin pienentää sitä [tietoturvaongelmien] riskiä. (H2)

> Omasta mielestä pitäisi aina enforcettaa niin paljon kun vaan pystytään, mutta aina se ei ole mahdollista tai kovin käyttäjäystävällistä. (H10)

Haastatteluissa korostui se, että yhteiset toimintamallit ja tietoisuuden lisääminen tukevat toisiaan tietoturvan edistämisessä. Yhteiset toimintamallit vaikuttaisivat olevan erityisen tärkeitä etenkin siinä vaiheessa, kun tietoisuus ei ole vielä levinnyt organisaatiossa riittävän kattavasti.

> Mun mielestä tässä oli ongelmana se, että nää [robotiikkakehitykset] on uusia asioita. [Liiketoimintayksikössä] ei ehkä tunnistettu, että millä tavalla näitä pitää tehdä, niin tarkemmat ohjeet sieltä [IT-yksiköstä], kun niitä robottitunnuksia on lähdetty tekemään ja miettimään, niin mun mielestä se olisi siinä vaiheessa pitänyt käydä läpi. Eikä sillein, että me voidaan testata puoli vuotta ja sitten ollaan sillein, että no eipäs tää nyt ollutkaan hyvä tapa. Että tarkemmat ohjeet, mutta nyt mä uskon kun [liiketoimintayksikössä] ollaan puolitoista vuotta pyöritelty näitä, niin nyt alkaa varmaan olemaan parempi ymmärrys täälläkin, että mikä on homma. (H6)

Lisäksi on hyvä huomata, että yhteisten toimintamallien luominen ja noudattaminen ei yksinään riitä, vaan myös tietoisuuden lisääminen on välttämätöntä.

Suuri osa ohjelmistorobotiikkakehitysten vaiheista noudattavat samoja periaatteita, mutta kaikki kehitysprosesseissa esille nousevat tietoturvaan liittyvät asiat eivät ole vakioitavissa. Tästä syystä toimintamallit eivät voi täysin kattaa ja varmistaa ohjelmistorobottien tietoturvallista toteutusta.

Yhteisten toimintamallien luomisen ja noudattamisen avulla organisaation IT-yksikön jatkuvan läsnäolon tarve pienenee robotiikkakehitysprojekteissa, mikä osaltaan mahdollistaa informaatioteknologian kuluttajistumista turvallisella ja kontrolloidulla tavalla. Yhteisten toimintamallien noudattamista tulisi kuitenkin kyetä seuraamaan, jotta tietoturvallisesta menettelytavasta voitaisiin varmistua. Tätä varten tulisi olla käytössä työkalu, jonka avulla voidaan dokumentoida tietoturvasidonnaisia asioita robotiikkakehitysprojekteissa.

Haastattelujen tulosten perusteella voidaan sanoa, että organisaation IT-yksikköä ei voida sivuuttaa ohjelmistorobotiikan hallinnassa, sillä se on liian suuri riski tietoturvan toteutumiselle. Edellä esiteltyjen keinojen avulla hallinnan painopistettä voidaan kuitenkin siirtää turvallisesti teknologian loppukäyttäjän suuntaan, mikä mahdollistaa toiminnan tehostamisen ja ketteryyden parantamisen.

6.4 Tietosuoja

Haastatteluissa nousi esille myös tietosuojan merkitys ohjelmistorobotiikan tietoturvan hallinnassa, etenkin jos organisaatio ostaa ohjelmistorobotiikan palveluita ulkoiselta toimittajalta. Tietosuojan huomioimisen merkitys on korostunut erityisesti Euroopan unionin yleisen tietosuoja-asetuksen (engl. *General Data Protection Regulation, GDPR*) voimaan astumisen myötä. Tietosuoja ja tietoturva eivät tarkoita samaa asiaa, mutta liittyvät vahvasti toisiinsa. Tietosuojan ja tietoturvan liittymäkohtina haastatteluissa nousi esille erityisesti EU:n yleisen tietosuoja-asetuksen artikla 28.

EU:n yleisen tietosuoja-asetuksen artikla 28 käsittelee henkilötietojen käsittelijän roolia sekä rekisterinpitäjän ja henkilötietojen käsittelijän välistä henkilötietojen käsittelysopimusta. Artiklan määrittelemien velvoitteiden tarkoituksena on varmistaa henkilötietojen asianmukainen suojaaminen.

> Jos se robotti esimerkiksi tekee cut and pasten jollekin kentälle, jossa on nyt vaikka henkilön nimi, niin se on jo henkilötietojen käsittelyä, tai henkilön sähköpostiosoite, se on henkilötietojen käsittelyä. Ja silloin se robotiikkapalvelun toimittaja toimii yleisen tietoasetuksen mukaisena henkilötietojen käsittelijänä tässä yhteydessä, vaikka he ei sitä tietoa itselleen kopioi eikä sille mitään varsinaisesti tee. Ja silloin ainakin astuu voimaan yleisen tietosuoja-asetuksen 28 artiklan mukainen vaatimus siitä, että meidän ja sen robotiikkatoimittajan välillä täytyy olla henkilötietojen käsittelyä koskeva käsittelysopimus. (H9)

Mikäli rekisterinpitäjän ja henkilötietojen käsittelijän väliset sopimukset, kuten esimerkiksi henkilötietojen käsittelyä koskeva sopimus eivät täytä Euroopan

unionin yleisen tietosuoja-asetuksen vaatimuksia, niin viranomaisilla on mahdollisuus antaa rangaistuksia eri osapuolille. Huomionarvoista on se, että rekisterinpitäjällä on huomattavasti suurempi vastuu, ja näin ollen rekisterinpitäjää rangaistaan huomattavasti helpommin. Tyypillisesti rangaistuksena toimii sakko, mutta viranomaisilla on myös muita mahdollisia toimenpiteitä. He voivat määrätä esimerkiksi henkilötietojen käsittelykiellon, joka voi olla organisaatiolle usein sakkoa merkittävämpi rangaistus.

> GDPR tuli voimaan noin kolme vuotta sitten, sen jälkeen viranomaiset on julkistaneet Euroopassa yli 700 sakkomääräystä, mutta kaikkia ei julkisteta. Mulla ei oo sitä todellista määrää tiedossa. Ne ei ole euromääräisesti olleet kauhean suuria, mutta joidenkin pienien yritysten tapauksessa prosentuaalisesti ne on kyllä ollut ihan merkittäviä. Saksassa on sellaisia 2 % vuotuisesta liikevaihdosta tyyppisiä sakkoja ollut, mutta se mahdollisuushan on siis 4 % yrityksen globaalista vuosittaisesta liikevaihdosta tai 20 miljoonaa euroa, kumpi tahansa on suurempi, että kyllä se mahdollistaa suuret sakot, ja kyllä ne on ollut kohtuu merkittäviä. (H9)

Vaikka käytännön tasolla henkilötietojen käsittely tapahtuisi palveluntarjoajan toimesta, niin tästä huolimatta rekisterinpitäjä nähdään lainsäädännöllisesti päävastuullisena. Tästä syystä tietoturvan hallinnan näkökulmasta on hyvin tärkeää huolehtia, että asiakasorganisaation ja palveluntarjoajan väliset sopimukset ovat ajan tasalla ja täyttävät lainsäädännön vaatimukset. Haastattelut osoittivat, että Euroopan unionin yleisen tietosuoja-asetuksen soveltamisen alkuaikoina etenkin pienempien palveluntarjoajien keskuudessa oli epätietoisuutta uuden tietosuoja-asetuksen velvoitteista ja sopimusten vaatimuksista, mistä seuraa merkittävä riski sopimuksellisten puutteiden syntymiselle. Haastatteluiden mukaan tilanne on muuttunut parempaan suuntaan, mutta siitä huolimatta sopimushallinnassa tulisi aina hyödyntää organisaation sisältä löytyvää asiantuntemusta, kuten hankinta- tietoturva- ja tietosuoja-asiantuntijoita.

> Se on toki [organisaation] intresseissä ja silloin myös tietosuoja ja tietoturvaihmisten intresseissä pitää ne sopimukset ajan tasalla, että meidän tehtävä on siinä auttaa. [...] Me kyllä tiedostetaan, että heillä [palveluiden omistajilla] on niin paljon vastuita, että me halutaan olla avuksi tässä ja varmistaa, että he tietää velvoitteensa, ja ollaan myös avuksi niissä sopimusneuvotteluissa. (H9)

Tämän lisäksi uusia sopimuksia tehdessä hyvänä käytäntönä on hyödyntää valmiita standardisopimuksia, jotka täyttävät jo valmiiksi yleisen tietotosuoja-asetuksen mukaiset ehdot. Lisäksi sopimuksiin voidaan sisällyttää vaatimuksia palveluntarjoajalle tietoturvasertifikaateista, mikä osaltaan auttaa varmistamaan ostettavan palvelun tietoturvan tason.

7 TUTKIMUKSEN TULOKSET JA POHDINTA

Tämän luvun tarkoituksena on verrata tutkielman empiirisien osion tuloksia aiempaan kirjallisuuteen aiheesta ja esittää tämän pohjalta tutkijan muodostamat johtopäätökset tutkimuksen tuloksista. Lisäksi tässä luvussa arvioidaan tutkimuksen tuottamaa hyötyä ja sen luotettavuutta, sekä pohditaan mahdollisia jatkotutkimusaiheita.

7.1 Tutkimuksen tulokset

Tämän tutkimuksen keskeisenä tavoitteena oli tunnistaa ohjelmistorobotiikkaan liittyviä tietoturvahaasteita ja löytää keinoja mitä organisaatioilla on käytettävissään näihin haasteisiin vastaamiseksi. Tutkimuskysymyksiä asetettiin kaksi, jotka olivat:

- Mitä tietoturvahaasteita ohjelmistorobotiikkaan liittyy?
- Kuinka ohjelmistorobotiikan tietoturva voidaan varmistaa?

Tutkimuskysymyksiin pyrittiin vastaamaan kirjallisuuskatsauksen sekä laadullisia tutkimusmenetelmiä soveltavan yksittäinen tapaustutkimuksen avulla, jonka aineistonkeruutapana toimivat teemahaastattelut. Aineiston analysoinnissa hyödynnettiin Tuomen ja Sarajärven (2018) esittelemää teorialähtöistä sisällönanalyysiä, jossa hyödynnetään aiemmassa tutkimuksessa esille nousseita käsitteitä sekä kategorioita. Seuraavaksi kirjallisuuskatsauksen ja tutkielman empiirisen osion tuloksia vertaillaan toisiinsa, ja vertailun pohjalta esitetään tutkimuksen johtopäätökset.

Kirjallisuuskatsauksen ja tutkimuksen empiirisen osion tuloksista on löydettävissä paljon yhtäläisyyksiä, mutta niiden välillä vallitsee myös ristiriitoja. Sekä aiemman tutkimuksen että tämän tutkielman empiirisen osuuden perusteella voidaan todeta, että identiteetin- ja pääsynhallinnan kokonaisuus on kaikista oleellisin tekijä ohjelmistorobotiikan tietoturvan hallinnan kannalta.

Sekä aiemmassa kirjallisuudessa että teemahaastatteluissa tunnistettiin samoja identiteetin- ja pääsynhallinnan osa-alueita, jotka ovat vahvasti sidoksissa ohjelmistorobotiikan tietoturvaan. Tällaisia osa-alueita ovat ohjelmistorobotin käyttäjätunnukset ja niiden elinkaarenhallinta, salasanat ja kohdejärjestelmiin tunnistautuminen, sekä käyttöoikeudet kohdejärjestelmien sisällä ja tehtävien eriyttäminen. Sekä aiempien tutkimusten että tämän tutkielman empiirisen osion mukaan näiden kaikkien osa-alueiden osalla tulisi lähtökohtaisesti soveltaa olemassa olevia identiteetin- ja pääsynhallinnan kokonaisuuden tietoturva- ja prosessimalleja, joita käytetään myös muiden käyttäjätunnusten kohdalla.

Datan eheyden osalta aiemmassa tutkimuksessa sekä tämän tutkielman empiirisessä osiossa tunnistettiin samoja riskejä, mutta syitä niiden taustalla käsiteltiin empiirisessä osiossa aiempaa tutkimusta kattavammin. Tämän tutkielman molempien osioiden mukaan datan eheyden varmistamisen suurimmat haasteet liittyvät automatisoitavissa prosesseissa esiintyvien poikkeustilanteiden tunnistamiseen. Aiemman tutkimuksen ja haastattelujen väliltä ei löytynyt ristiriitaista tietoa.

Informaatioteknologian kuluttajistuminen nähtiin sekä aiemmassa tutkimuksessa että haastatteluissa uhkana tietoturvan hallinnalle, vaikka ilmiöllä on myös positiivisia vaikutuksia. Myös ehdotetut keinot tietoturvan hallinnan parantamiseksi olivat tutkielman molemmissa osissa pääosin samankaltaisia. Aiempi tutkimus kuitenkin tuki toimenpiteitä, jotka estävät ohjelmistorobotiikan kuluttajistumista, kun taas haastattelujen mukaan ohjelmistorobotiin kuluttajistuminen halutaan mahdollistaa kontrolloidulla tavalla.

Seuraavissa alaluvuissa esitellään ja vertaillaan keskenään aiemman kirjallisuuden sekä tämän tutkielman empiirisen osion tuloksia edellä esiteltyjen teemojen osalta. Vertailun helpottamiseksi käsiteltävät teemat ovat osin jaettu pienempiin kokonaisuuksiin. Tietosuojaa käsiteltiin ainoastaan tämän tutkielman empiirisessä osiossa, joten sen osalta tuloksia ei voida verrata aiempaan tutkimukseen.

7.1.1 Digitaalinen identiteetti ja sen elinkaaren hallinta

Tutkimuksen empiirisen osuuden mukaan ohjelmistorobotin digitaalisen identiteetin kompromisoituminen nähdään ohjelmistorobotiikan kriittisenä tietoturvariskinä, ja myös aiempi kirjallisuus tukee tätä väitettä. Kuten Lacity ja Willcocks (2017) artikkelissaan kirjoittavat, jokaisella ohjelmistorobotilla tulisi olla oma digitaalinen identiteetti, jotta niiden yksilöiminen on mahdollista. Jotta ohjelmistorobottien digitaaliset identiteetit voidaan suojata tietoturvan varmistamiseksi, niin niiden elinkaarenhallinta on toteutettava järjestelmällisellä tavalla. Tutkimuksen tulosten sekä ohjelmistorobotiikan parhaimpien käytäntöjen mukaan elinkaarenhallintaa ohjaa hyvin pitkälti organisaation vallitsevat tietoturva- ja identiteetinhallinnan käytännöt. Ohjelmistorobottien digitaalisten identiteettien ylläpitoon ja hallintaan tulisi sekä aiemman kirjallisuuden että tutkimuksen empiirisen osuuden mukaan hyödyntää olemassa olevia tietoturva- ja prosessimalleja, kuten esimerkiksi olemassa olevaa käyttäjätietokantaa.

7.1.2 Salasanat ja kohdejärjestelmiin tunnistautuminen

Empiirisen osion haastatteluissa nousi esille samoja asioita kuin aiemmassa kirjallisuudessakin ohjelmistorobottien salasanoihin liittyen. Tutkimuksen tulokset tukevat väitettä, että ohjelmistorobottien salasanakäytäntöjä koskevat samat vaatimukset kuin organisaation henkilöstön käyttäjätunnuksia. Tietoturvan varmistamiseksi salasanojen täytyy täyttää niille asetetut minimivaatimukset ja niitä täytyy vaihtaa tietyin väliajoin. Salasanojen vaihtaminen on huomionarvoista, sillä ohjelmistorobottien tunnukset rinnastetaan usein muihin palvelutunnuksiin, joiden salasanoja ei tyypillisesti vaihdeta tietyin aikavälein.

Aiemman kirjallisuuden mukaan ohjelmistorobottien salasanoja tulisi säilyttää ainoastaan salatussa sijainnissa. Tutkimuksen empiirinen osio on tämän osalta linjassa aiempien tutkimusten kanssa. Tämän lisäksi haastatteluissa nousi esille, että joillakin käyttäjillä voi olla perusteltavissa oleva tarve päästä käsiksi ohjelmistorobotin salasanoihin, esimerkiksi vianselvitystarkoituksia varten. Käyttäjäryhmä, jolla on pääsy salasanoihin, tulee kuitenkin valita hyvin tarkasti. Tutkimuksen empiirisen osion mukaan sellaisella käyttäjällä ei saa olla pääsyä ohjelmistorobotin tunnuksiin, joka ei pääsyä välttämättömästi tarvitse.

Aiempi kirjallisuus ja empiirisessä osiossa kerätty materiaali eivät tukeneet toisiaan ohjelmistorobottien kohdejärjestelmiin autentikoitumismenetelmän osalta. Aiemman kirjallisuuden mukaan ohjelmistorobottien tulisi hyödyntää monivaiheista tunnistautumista kohdejärjestelmiin autentikoitumisessa. Haastattelumateriaalin perusteella ohjelmistorobottien kohdejärjestelmiin tunnistautuminen on tietoturvallista, kun hyödynnetään samaa autentikoitumismenetelmää kuin mitä loppukäyttäjät hyödyntävät, ja tätä näkemystä tukevat kattavat perustelut. Ohjelmistorobotit simuloivat loppukäyttäjää, ja niillä on tyypillisesti saman laajuiset tai rajatummat käyttöoikeudet kohdejärjestelmissä kuin muilla käyttäjillä, joten sen osalta ei ole perusteltavissa, että ohjelmistoroboteilta vaadittaisiin vahvempaa tunnistautumismenetelmää. Lisäksi monivaiheisen tunnistautumisen tekninen toteuttaminen ohjelmistorobotille olisi todella haastavaa ja epäkäytännöllistä. Tutkimuksen empiirisessä osiossa nousi esille myös kohdejärjestelmien kyvykkyyksien vaikutus tunnistautumistapaan. Joissain kohdejärjestelmissä ainut mahdollinen autentikoitumismenetelmä voi olla esimerkiksi lokaalin käyttäjätunnuksen ja salasanan käyttäminen, jolloin vahvemmat tunnistautumismenetelmät eivät ole teknisesti mahdollisia.

7.1.3 Käyttöoikeudet kohdejärjestelmissä ja tehtävien eriyttäminen

Sekä tutkimuksen empiirisen osion että aiemman kirjallisuuden mukaan ohjelmistoroboteille tulisi myöntää kohdejärjestelmiin vähäisimmät mahdolliset käyttöoikeudet, mitkä mahdollistavat työtehtävän suorittamisen, sillä liian laajat käyttöoikeudet mahdollistavat tunnusten laajemman väärinkäytön, mikäli ohjelmistorobotin digitaalinen identiteetti kompromisoituu. Tälläkin osa-alueella tulee siis hyödyntää olemassa olevia tietoturvamalleja, mitä sovelletaan myös muiden käyttäjätunnustyyppien osalta. Tämä kattaa myös käyttöoikeuksien

ylläpidon keskitetyssä käyttöoikeuksien hallintajärjestelmässä, kuten empiirisen osion tulokset osoittivat.

Aiempien tutkimusten mukaan tehtävien eriyttämisen käytäntö tulee huomioida myös, kun automatisoidaan prosesseja ohjelmistorobotiikalla. Myös haastatteluiden perusteella tämä on asia mikä tulee ottaa huomioon, mutta haastattelujen tulokset eivät ole kuitenkaan täysin linjassa aiemman kirjallisuuden kanssa, sillä myös haastatteluiden välillä oli runsaasti näkemyseroja. Kun huomioidaan sekä aiempien tutkimusten tulokset sekä haastatteluiden avulla kerätty materiaali, niin johtopäätöksenä voidaan todeta, että tehtävien eriyttämistä edellyttävien prosessien automatisointia ohjelmistorobotiikan avulla tulee aina harkita tapauskohtaisesti. Mikäli prosessia ei ole mahdollista toteuttaa yhden käyttäjän toimesta, niin siinä tapauksessa myös automatisoinnin yhteydessä tehtävien eriyttämisen periaatetta on noudatettava. Prosessin automatisoinnin suunnittelun yhteydessä tulisi kuitenkin pohtia voisiko prosessia kehittää sellaiseksi, että sen voisi suorittaa yhden ohjelmistorobotin toimesta, tai onko prosessi mahdollisesti sellainen, ettei sen automatisointi ohjelmistorobotiikan keinoin ole ylipäätään järkevää.

7.1.4 Datan eheyden haasteet

Datan eheyden haasteiden osalta teemahaastatteluin kerätty tutkimusmateriaali tuki täysin aiempien tutkimusten tuloksia, mutta toi mukanaan myös paljon sellaista tietoa, mitä aiemmissa tutkimuksissa ei ollut käsitelty. Ristiriitoja aiempien tutkimusten ja teemahaastatteluin kerätyn materiaalin väliltä ei löytynyt ollenkaan.

Tutkimuksen empiirisen osion mukaan tyypillisin syy datan eheyden ongelmiin ohjelmistorobotiikan kontekstissa ovat liiketoimintapoikkeukset, jotka johtuvat puutteista tai virheistä ohjelmistorobotin konfiguraatiossa, mutta ne voivat johtua myös jo lähtökohtaisesti virheellisestä datasta. Nämä poikkeukset voivat johtaa siihen, että ohjelmistorobotti prosessoi järjestelmässä eteenpäin puutteellista tai virheellistä dataa. Kuten myös Santos ym. (2019) artikkelissan kirjoittivat, ohjelmistorobotin ollessa huomattavasti ihmistä tehokkaampi, se tekee myös virheitä huomattavasti nopeammin.

Sekä aiempi tutkimus että tutkimuksen empiirinen osio osoittavat, että liiketoimintapoikkeukset voidaan välttää, mikäli automatisoitavan prosessin kaikki vaiheet, poikkeukset ja lopputulemat kyetään määrittelemään yksiselitteisesti. Tutkimuksen empiirisen osion mukaan kaikkien prosessissa esiintyvien poikkeustilanteiden tunnistaminen voi olla joskus hyvin haastavaa niiden suuren lukumäärän vuoksi. Aiemman kirjallisuuden mukaan tärkein keino näiden poikkeustilanteiden tunnistamiseksi on osallistaa ohjelmistorobotin määrittelyvaiheeseen henkilöitä, jotka tuntevat prosessin tarkalla tasolla. Tämän lisäksi empiirisen osion tulokset tarjoavat keinoksi järjestelmällistä testausta ja prosessidokumentaation luomista. Jo lähtökohtaisesti virheellisestä datasta johtuvat poikkeukset voidaan pyrkiä välttämään datan validoinnin keinoin, esimerkiksi tarkistamalla datan tyyppi tai vertailemalla eri lähteiden datoja keskenään.

Aiemmasta kirjallisuudesta poiketen tutkimuksen empiirinen osio nosti esille myös järjestelmäpoikkeukset, mitkä voivat johtaa datan eheyden ongelmiin. Järjestelmäpoikkeuksia voidaan pyrkiä välttämään ylimääräisen logiikan lisäämisällä ohjelmistorobotin konfiguraatioon. Ohjelmistorobotti voi esimerkiksi itse tarkistaa onko jokin kenttä olemassa, tai että data on varmasti syötetty kenttään.

Toinen datan eheyden varmistamisen keino, joka nousi esille aiemmissa tutkimuksissa, on human-in-the-loop-käsittelyt, joissa ihminen suorittaa osan ohjelmistorobotiikalla automatisoidusta prosessista. Tutkimuksen empiirisen osion mukaan human-in-the-loop-käsittelyiden hyödyntäminen on yleistymässä.

Aiemman tutkimuksen keskittyessä ainoastaan datan eheyden ongelmien ennaltaehkäisyyn, empiirisessä osiossa korostettiin myös reaktiivisen toiminnan tärkeyttä mahdollisten ongelmatilanteiden syntyessä. Empiirisen osion mukaan virhetilanteiden varalle tulisi olla ennalta suunniteltu ja dokumentoitu prosessi, joka sisältäisi vastuut ja sovitut toimintamallit. Tämän avulla voidaan varmistaa myös riittävä resursointi ongelmien korjaamisen varalle.

7.1.5 Informaatioteknologian kuluttajistumisen vaikutus tietoturvaan ja sen hallintaan

Sekä aiempi kirjallisuus että tämän tutkielman empiirinen osio tunnistavat informaatioteknologian kuluttajistumisen ilmiön ja sen negatiiviset vaikutukset tietoturvan hallinnalle ohjelmistorobotiikan kontekstissa. Aiempi tutkimus sekä tutkielman empiirinen osio tunnistavat myös informaatioteknologian kuluttajistumisen positiivisia vaikutuksia, mutta empiirisen osion tulokset näkevät ilmiön selvästi positiivisemmassa valossa, kuin aiempi tutkimus sen esittää. Empiirisen osion mukaan informaatioteknologian kuluttajistuminen on jossain määrin jopa tavoiteltavaa, kun se tapahtuu hallitulla tavalla. Aiempi tutkimus taas näkee ilmiön estämisen olevan tarkoituksenmukainen keino tietoturvan varmistamisen kannalta.

Aiemmissa tutkimuksissa ohjelmistorobotiikan kuluttajistumisen negatiivisia vaikutuksia tietoturvan hallinnalle perusteltiin pääasiassa sillä, ettei teknologian loppukäyttäjät tarkastelevat ohjelmistorobotiikkaa hyvin erilaisesta näkökulmasta kuin organisaation IT-yksikössä työskentelevät henkilöt. Hofmann ym. (2020) kirjoittavatkin artikkelissaan, ettei ohjelmistorobotiikkaa voi tarkastella ainoastaan liiketoiminnan näkökulmasta. Ilman teknisempää näkökulmaa tietoturvan hallinta voi jäädä heikolle tasolle. Tämän tutkimuksen haastateltavat olivat tästä yhtä mieltä riippumatta heidän omasta roolistaan ohjelmistorobotiikan parissa. Tutkimuksen empiirisen osion mukaan teknologian loppukäyttäjiltä ei voida odottaa vastaavaa tietoturvaosaamista kuin tietoturvan asiantuntojoilta, vaikka loppukäyttäjiltä vaaditaankin jatkuvasti teknistä tietämystä kasvavissa määrin. Näin ollen ohjelmistorobotiikan tietoturvan hallintaa ei voi jättää vain loppukäyttäjien vastuulle.

Aiemmissa tutkimuksissa keskeisimpänä keinona ohjelmistorobotiikan kuluttajistumisen negatiivisten vaikutusten hillitsemiseksi nähtiin eri sidosryhmien osallistaminen. Tällä tarkoitetaan sitä, että organisaation sisältä löytyvää osaamista hyödynnetään mahdollisimman korkealla tasolla, jotta

ohjelmistorobotiikan tietoturvanäkökulma kyetään huomiomaan kattavasti. Tämän tutkimuksen empiirinen osio tukee aiempaa tutkimusta, ja korostaa sidosryhmien osallistamisessa kommunikaation tärkeyttä, sillä haastattelujen perusteella monet tietoturvan hallinnan haasteet olisi voitu välttää paremmalla kommunikaatiolla. Lisäksi tietoisuuden lisääminen loppukäyttäjien keskuudessa nähtiin empiirisen osion mukaan keskeisenä keinona tietoturvan hallinnan parantamiseksi. Haastattelujen mukaan sidosryhmien osallistaminen sekä tietoisuuden lisääminen tukevat toisiaan. Tämän lisäksi tietoisuutta loppukäyttäjien keskuudessa voidaan lisätä esimerkiksi kouluttamisella, tehokkaalla tiedon jakamisella sekä työkierrolla IT-yksikön ja liiketoimintayksiköiden välillä.

Toinen aiemman tutkimuksen ehdottama ratkaisu ohjelmistorobotiikan kuluttajistumisen negatiivisten vaikutusten estämiseksi on raskaan informaatioteknologian hallintoperiaatteiden soveltaminen ohjelmistorobotiikan kontekstissa. Käytännössä tämä tarkoittaa ohjelmistorobotiikan kuluttajistumisen estämistä. Haastattelujen perusteella organisaation IT-yksikön täytyy asettaa ohjelmistorobotiikan soveltamiselle tietyt toimintamallit, joita koko organisaation tulee noudattaa, mutta tällä ei kuitenkaan haluta estää informaatioteknologian kuluttajistumisen ilmiötä. Empiirisen osion mukaan yhteisten toimintamallien tarkoituksena on mahdollistaa tietoturvallinen toiminta myös teknologian loppukäyttäjien keskuudessa, jotta kuluttajistuminen voi tapahtua hallitulla ja kontrolloidulla tavalla. Tutkimuksen empiirisessä osiossa kuitenkin korostui, ettei yhteiset toimintamallit ja niiden noudattaminen ole kuitenkaan riittävä keino ohjelmistorobotiikan hyvän tietoturvan hallinnan varmistamiseksi, vaan tietoturvatietoisuuden lisääminen kattavasti organisaation sisällä on välttämätöntä.

7.2 Tutkimuksen luotettavuus ja sen tuottama hyöty

Noble ja Smith (2015) kirjoittavat artikkelissaan, että laadullisen tutkimuksen luotettavuutta voidaan arvioida validiteetin (engl. *validity*), reliabiliteetin (engl. *reliability*) sekä yleistettävyyden (engl. *generalisability*) näkökulmista. Validiteetilla tarkoitetaan tutkimuksen tulosten tarkkuutta ja paikkansapitävyyttä, kun taas reliabiliteetilla tarkoitetaan tutkimuksen läpinäkyvyyttä ja toistettavuutta sekä käytettyjen tutkimusmenetelmien johdonmukaisuutta. Tutkimuksen yleistettävyydellä tarkoitetaan tutkimustulosten soveltumista myös tutkimuskontekstin ulkopuolisiin yhteyksiin (Noble & Smith, 2015).

Tämän tutkielman validiteetti on pyritty varmistamaan kirjallisuuskatsauksen osalta valitsemalla kattavasti mahdollisimman laadukkaita lähdemateriaaleja ja raportoimalla niiden sisältö mahdollisimman todenmukaisesti. Empiirisen osion validiteetti on pyritty varmistamaan riittävän suurella otannalla sekä soveltamalla tarkoituksenmukaisia menetelmiä aineiston keräämiseen sekä analysointiin. Tutkielman validiteetin haasteena oli aihealueen aiemman tutkimuksen vähäisyys, jonka vuoksi kirjallisuuskatsaus jäi haluttua suppeammaksi. Empiirisen osion kohdalla tutkimusmateriaalia saatiin kerättyä riittävän kattavasti, jotta

empiirisen osion tuloksia voidaan pitää validina toimeksiantajaorganisaation kontekstissa.

Tutkielman reliabiliteetti on pyritty varmistamaan raportoimalla tutkimuksen työvaiheita ja perustelemalla siinä sovellettujen tutkimusmenetelmien valintaa mahdollisimman tarkalla tasolla. Reliabiliteetin varmistamisen tueksi tämän tutkielman yhteyteen on liitetty myös kaksi liitettä, jotka ovat teemahaastattelurunko sekä haastateltaville haastattelukutsujen yhteydessä lähetetyt keskeisten käsitteiden määritelmät.

Tutkielmaa ei voida pitää täysin yleistettävänä, sillä empiirinen osio on toteutettu tutkielman toimeksiantajan kontekstissa. Vaikka tutkimuksen otanta oli toimeksiantajaorganisaation näkökulmasta riittävä aihealueen laajaan tarkasteluun, niin tulosten laajemman yleistämisen kannalta otanta oli suhteellisen pieni. Tämän tutkielman empiirinen osio kuitenkin tukee aiempaa tutkimusta suurilta osin, joten pääpiirteittäin tutkimuksen tuloksia voidaan soveltaa myös sen kontekstin ulkopuolella.

Ohjelmistorobotiikan tietoturva ja sen hallinta ovat aihealueita, joita ei ole aiemmassa kirjallisuudessa juurikaan tutkittu, ja tämän tutkielman kirjallisuuskatsaus muodostaa kattavan käsityksen aiemman tutkimuksen laajuudesta. Tämä tutkielma kykenee syventämään tietoa sekä nostamaan esille uusia näkökulmia ohjelmistorobotiikan tietoturvahaasteista ja niihin vastaamisesta.

Suurimman hyödyn tutkielma tarjoaa toimeksiantajaorganisaatiolle, sillä tutkielman empiirisen osion tutkimusmateriaali on kerätty haastattelemalla toimeksiantajaorganisaation henkilöstöä sekä ulkoisen yhteistyökumppanin asiantuntijoita. Tutkielma tarjoaa nostaa esille organisaation sisällä havaittuja haasteita ja arvioi erilaisia keinoja vastata näihin haasteisiin sekä niiden toimivuutta organisaation kontekstissa. Tutkielma huomioi kattavasti erilaiset näkökulmat organisaation sisällä, sillä haastateltavia henkilöitä valittiin mahdollisimman monesta eri sidosryhmästä. Tämän lisäksi tutkielma tarjoaa hyötyä myös kohdeorganisaation ulkopuolelle, sillä tutkielma tarjoaa laajan läpileikkauksen aiheen aiemmasta tutkimuksesta rikastaen tätä tietoa sellaisen organisaation näkökulmasta, jossa ohjelmistorobotiikkaa on ehditty hyödyntämään noin kahden vuoden ajan.

7.3 Jatkotutkimusaiheet

Ohjelmistorobotiikan tietoturva ja hallinta on kokonaisuudessaan hyvin vähän tutkittu aihealue, joka tarvitsee tulevaisuudessa jatkotutkimusta. Tämän tutkimuksen tarkoituksena oli kartoittaa ohjelmistorobotiikkaan liittyviä tietoturvahaasteita sekä keinoja näihin haasteisiin vastaamiseksi. Tutkielman empiirinen osio tarkasteli ilmiötä ainoastaan yhden organisaation näkökulmasta, joten tulosten pohjalta ei voida tehdä suoria yleistyksiä laajemmassa kontekstissa, vaikkakin empiirisen osion tulokset tukivat suurilta osin aiempien tutkimusten tuloksia.

Tässä tutkielmassa käsiteltiin sellaisia ohjelmistorobotiikan tietoturvaan liittyviä haasteita, jotka olivat luokiteltavissa identiteetin- ja pääsynhallinnan,

datan eheyden, informaatioteknologian kuluttajistumisen sekä tietosuojan kokonaisuuksiin. Näistä kokonaisuuksista tietosuojaa ei käsitelty ollenkaan ohjelmistorobotiikkaa käsittelevässä aiemmassa tutkimuksessa, joten erityisesti tämä on aihealue, mikä kaipaa erityistä huomiota tulevaisuudessa.

Toisena jatkotutkimusaiheena olisi hyödyllistä tarkastella vaikuttaako ohjelmistorobotiikan eri hankintamallit merkittävästi tietoturvahaasteisiin ja tietoturvan hallintaan. Tämän tutkielman empiirinen osio keskittyi aiheen tarkasteluun ainoastaan toimeksiantajaorganisaation näkökulmasta, jossa ohjelmistorobotiikkaa hankitaan pilvipalvelun muodossa, niin kutsutulla Robotics-as-a-Service (*RaaS*) -mallilla.

Tämä tutkimus osoitti, että ohjelmistorobotiikalla automatisoitavissa prosesseissa käytetyt kohdejärjestelmät ovat keskenään hyvin erilaisia, ja niiden tarjoamilla kyvykkyyksillä on suuri vaikutus myös ohjelmistorobotiikan tietoturvan hallintaan. Näin ollen jatkotutkimusta olisi hyvä tehdä siitä, kuinka järjestelmäkehityksessä tulisi ottaa huomioon järjestelmien soveltuvuus ohjelmistorobotiikan hyödyntämiselle. Tämä on aihe, jota olisi mahdollisesti hyvä tutkia laajemmin ohjelmistorobotiikan lisäksi myös muiden uusien teknologioiden näkökulmasta.

8 YHTEENVETO

Ohjelmistorobotiikka on suhteellisen uusi teknologia, josta on jo kirjoitettu kohtalaisen paljon tieteellistä tutkimusta. Ohjelmistorobotiikan tietoturva on kuitenkin jäänyt aiemmassa tutkimuksessa varsin vähälle huomiolle. Tämän tutkielman tarkoituksena oli tunnistaa ohjelmistorobotiikkaan liittyviä tietoturvahaasteita sekä löytää keinoja, joiden avulla ohjelmistorobotiikan tietoturvaa voidaan hallita parhaalla mahdollisella tavalla. Tutkielman tutkimuskysymykset olivat *"Mitä tietoturvahaasteita ohjelmistorobotiikkaan liittyy?"* sekä *"Kuinka ohjelmistorobotiikan tietoturva voidaan varmistaa?"*.

Tutkielma koostui kirjallisuuskatsauksesta sekä empiirisestä osiosta. Kirjallisuuskatsauksen tarkoituksena oli luoda kattava kokonaiskuva ohjelmistorobotiikasta teknologiana sekä syventyä ohjelmistorobotiikan tietoturvaa käsittelevään aiempaan tutkimukseen. Kirjallisuuskatsaus toimi myös teoreettisena perustana tutkielman empiiriselle osiolle.

Tutkielman empiirinen osio toteutettiin yksittäisenä tapaustutkimuksena tutkielman toimeksiantajaorganisaation kontekstissa. Tapaustutkimuksen tutkimusmateriaali kerättiin teemahaastattelujen avulla, joiden haastattelurunko muodostettiin kirjallisuuskatsauksen tulosten pohjalta. Litteroitu haastattelumateriaali analysoitiin teorialähtöisen sisällönanalyysin mallia mukaillen, joka niin ikään pohjautui kirjallisuuskatsausosiossa muodostettuun teoreettiseen pohjaan.

Sekä aiempi tutkimus että tutkielman empiirinen osio osoittivat, että identiteetin- ja pääsynhallinnan kokonaisuus on merkittävin osa-alue ohjelmistorobotiikan tietoturvan hallinnassa. Tutkielma osoitti, että ohjelmistorobotin digitaalisen identiteetin kompromisoituminen on merkittävä uhka tietoturvalle. Toinen ohjelmistorobotiikan tietoturvaa uhkaava kokonaisuus on datan eheyden haasteet, jotka voivat johtua joko liiketoimintapoikkeuksista tai järjestelmäpoikkeuksista. Ohjelmistorobotit suorittavat työtehtäviä huomattavasti ihmistä nopeammin, joten poikkeustilanteissa puutteet datan eheydessä voivat lisääntyä erittäin nopeasti. Lisäksi tutkielma osoitti, että informaatioteknologian kuluttajistumisen ilmiö on uhka tietoturvan hallinnalle, mikäli kuluttajistuminen ei tapahdu hallitulla ja kontrolloidulla tavalla. Tutkielman empiirisessä osiossa havaittiin

myös tietosuojan olevan merkityksellinen tekijä ohjelmistorobotiikan tietoturvan hallinnassa erityisesti henkilötietojen käsittelyn osalta.

Tutkielman tulosten mukaan identiteetin- ja pääsynhallinnan osa-alueen tietoturvallinen toteutus voidaan varmistaa järjestelmällisellä robotiikkatunnusten elinkaarenhallinnalla ja hyödyntämällä jo olemassa olevia toimintamalleja, joita käytetään myös muun tyyppisten tunnusten hallinnassa. Ohjelmistorobotiikan kohdalla tulee myös noudattaa organisaation tietoturvaan liittyviä politiikkoja, kuten esimerkiksi salasanapolitiikkaa. Tämän lisäksi ohjelmistorobotiikkaa sovellettaessa on tärkeää noudattaa vähäisimpien oikeuksien periaatetta, jotta mahdollisten väärinkäytösten vaikutukset voidaan minimoida. Tutkielman tulosten mukaan myös tehtävien eriyttämisen periaatteen noudattaminen parantaa ohjelmistorobotiikan tietoturvaa. Empiirisen osion tulokset kuitenkin osoittivat, että tehtävien eriyttämistä edellyttävien prosessien automatisointia ohjelmistorobotiikalla tulee aina harkita tapauskohtaisesti. Aiempi tutkimus ja tutkielman empiirinen osio olivat kuitenkin ristiriidassa ohjelmistorobottien tietoturvallisen järjestelmiin tunnistautumismenetelmän osalta. Aiemman tutkimuksen mukaan ohjelmistorobottien tulisi aina hyödyntää monivaiheista tunnistautumista, kun taas empiirisen osion mukaan ohjelmistorobottien tunnistautumiselle ei ole syytä asettaa tiukempia vaatimuksia kuin muun tyyppisille käyttäjätunnuksille organisaation sisällä

Tutkielma osoitti, että tyypillisin syy liiketoimintapoikkeuksista aiheutuvien datan eheyden haasteiden takana on puutteellinen prosessien määrittely. Jotta liiketoimintapoikkeuksilta voidaan välttyä, prosessin kaikki mahdolliset poikkeustilanteet ja lopputulemat on kyettävä tunnistamaan. Prosessin määrittelyvaiheeseen tulisi tämän vuoksi osallistaa aina sellaisia henkilöitä, jotka tuntevat prosessin parhaiten. Lisäksi järjestelmällinen testaus, datan validointi ja prosessien tarkka dokumentointi ovat keinoja liiketoimintapoikkeuksien välttämiseksi. Tutkielman tulosten mukaan järjestelmäpoikkeuksien syntymistä voidaan ehkäistä ylimääräisellä logiikalla ohjelmistorobotin konfiguraatiossa, jolloin robotti voi esimerkiksi itse tarkistaa, onko data tallentunut oikeaan kenttään. Lisäksi human-in-the-loop-käsittelyjen avulla voidaan varmistua datan eheydestä.

Tutkielman tulosten mukaan informaatioteknologian kuluttajistumisen negatiivisia vaikutuksia tietoturvan hallinnalle voidaan hillitä sidosryhmien osallistamisella, tietoisuuden lisäämisellä sekä yhteisten toimintamallien noudattamisella. Mikäli ohjelmistorobottien kehitysprojekteissa kyetään hyödyntämään organisaation sisältä löytyvää osaamista ja tietotaitoa mahdollisimman laajasti, niin myös tietoturvariskit havaitaan todennäköisemmin jo varhaisessa vaiheessa. Aiempi tutkimus ja tutkielman empiirinen osio olivat kuitenkin osittain ristiriidassa yhteisten toimintamallien luomisen ja noudattamisen osalta. Aiemmassa tutkimuksessa ehdotettiin raskaan informaatioteknologian hallintomallien soveltamista myös ohjelmistorobotiikan kohdalla, jolla pyritään estämään ohjelmistorobotiikan kuluttajistuminen. Tutkielman empiirisen osion tulosten mukaan informaatioteknologian kuluttajistumista ei ole kuitenkaan syytä estää, mutta yhteisiä toimintamalleja tarvitaan, jotta kuluttajistuminen voi tapahtua kontrolloidulla tavalla.

Tutkielman empiirinen osio osoitti, että mikäli ohjelmistorobotiikalla automatisoitavassa prosessissa käsitellään henkilötietoja, niin myös tietosuojan huomioiminen on välttämätöntä. Vaikka henkilötietojen käsittely tapahtuisi kolmannen osapuolen toimesta, niin rekisterinpitäjä nähdään Euroopan unionin yleisen tietosuoja-asetuksen valossa päävastuullisena. Mikäli robotiikkapalveluita ostetaan ulkoiselta palveluntarjoajalta, niin on erityisen tärkeää huolehtia, että palveluntarjoajan ja asiakasorganisaation väliset sopimukset täyttävät lainsäädännön asettamat vaatimukset. Hyvä käytäntö uusia sopimuksia solmittaessa on hyödyntää valmiita standardisopimuksia sekä hankinta- ja tietosuoja-asiantuntijoiden osaamista.

Tämä tutkielma saavutti sille asetetut tavoitteet, sillä se kykeni luomaan käsityksen ohjelmistorobotiikkaa koskevista tietoturvahaasteista ja keinoista vastata näihin haasteisiin toimeksiantajaorganisaation kontekstissa. Sen lisäksi, että tutkielma tarjosi arvokasta tietoa toimeksiantajaorganisaatiolle, se kokosi myös yhteen aiempien aihealuetta käsittelevien tutkimusten tulokset ja vahvisti ne suurilta osin tapaustutkimuksen avulla. On kuitenkin tärkeää huomioida, että tämän tutkielman empiirinen osio toteutettiin yhden organisaation kontekstissa, joten tuloksia ei voida pitää täysin yleistettävinä.

LÄHTEET

Asatiani, A. & Penttinen, E. (2016). Turning robotic process automation into commercial success – case OpusCapita. *Journal of Information Technology Teaching Cases, 6*(2), 67-74.

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

Bygstad, B. (2017). Generative innovation: A comparison of lightweight and heavyweight IT. *Journal of Information Technology, 32*(2), 180-193.

Campbell, S. (2014). What is qualitative research? *Clinical Laboratory Science, 27*(1), 3.

Capgemini Consulting. (2016). Robotic process automation - robots conquer business processes in back offices. *A 2016 Study Conducted by Capgemini Consulting and Capgemini Business Services,* Haettu osoitteesta https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/robotic-process-automation-study.pdf

Cavaye, A. L. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal, 6*(3), 227-242.

CyberArk. (2021). Robotic process automation (RPA). Haettu osoitteesta https://www.cyberark.com/what-is/robotic-process-automation/

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

De Hert, P. (2008). Identity management of e-ID, privacy and security in europe. A human rights view. *Information Security Technical Report, 13*(2), 71-75.

Deloitte. (2019). BOT identity management. *Secured BOT Series,* Haettu osoitteesta https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-bot-identity-management-presentation-noexp.pdf

Fung, H. P. (2014). Criteria, use cases and effects of information technology process automation (ITPA). *Advances in Robotics & Automation,* (3)

Gartner. (2021, Haettu 6.4.). Identity and access management (IAM). Haettu osoitteesta https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Giesbers, S. (2020). Robotic process automation and internal control: A guideline. *Research in IT-Auditing A Multidisciplinary View,* (Edition 2020)

Hirsijärvi, S. & Hurme, H. (2001). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Helsinki: Yliopistopaino.

Hofmann, P., Samp, C. & Urbach, N. (2020). Robotic process automation. *Electronic Markets, 30*(1), 99-106.

Hsieh, H. & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288.

IEEE Corporate Advisory Group. (2017). IEEE guide for terms and concepts in intelligent process automation., 1-16.

Jovanović, S. Z., Đurić, J. S. & Šibalija, T. V. (2018). Robotic process automation: Overview and opportunities. *Int.J.Adv.Qual, 46*(3-4), 34-39.

Knorr, K. & Stormer, H. (2001). Modeling and analyzing separation of duties in workflow environments. (s. 199-212). IFIP International Information Security Conference: Springer, Boston, MA.

Kumar, V. & Bhardwaj, A. (2018). Identity management systems: A comparative analysis. *International Journal of Strategic Decision Sciences (IJSDS), 9*(1), 63-78.

Lacity, M. C. & Willcocks, L. P. (2016). A new approach to automating services. *MIT Sloan Management Review, 58*(1), 41-49.

Lacity, M. & Willcocks, L. P. (2017). *Robotic process automation and risk mitigation: The definitive guide.* Haettu osoitteesta: http://eprints.lse.ac.uk/87820/.

Lamberton, C., Brigo, D. & Hoy, D. (2017). Impact of robotics, RPA and AI on the insurance industry: Challenges and opportunities. *Journal of Financial Perspectives, 4*(1)

Linden, M. (2017). Identiteetin-ja pääsynhallinta. *Tietotekniikan Laboratorio. Raportti; Vuosikerta 7,* (Tampereen teknillinen yliopisto)

Lu, H., Li, Y., Chen, M., Kim, H. & Serikawa, S. (2018). Brain intelligence: Go beyond artificial intelligence. *Mobile Networks and Applications, 23*(2), 368-375.

Madakam, S., Holmukhe, R. M. & Jaiswal, D. K. (2019). The future digital work force: Robotic process automation (RPA). *JISTEM-Journal of Information Systems and Technology Management, 16*

Niehaves, B., Köffer, S. & Ortbach, K. (2012). IT consumerization–a theory and practice review. *Amcis 2012 Isbn,* (Seattle)

Noble, H. & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35.

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal, 6*

Orlikowski, W. J. & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Rahman, A., Parnin, C. & Williams, L. (2019). The seven sins: Security smells in infrastructure as code scripts. (s. 164-175) IEEE.

Ramgovind, S., Eloff, M. M. & Smith, E. (2010). The management of security in cloud computing. (s. 1-7). Information Security for South Africa: IEEE.

Ratia, M., Myllärniemi, J. & Helander, N. (2018). Robotic process automation-creating value by digitalizing work in the private healthcare? (s. 222-227)

Samonas, S. & Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3)

Santos, F., Pereira, R. & Vasconcelos, J. B. (2019). Toward robotic process automation implementation: An end-to-end perspective. *Business Process Management Journal*

Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research, 3*(7), 749-752.

Suri, V. K., Elia, M. & van Hillegersberg, J. (2017). Software bots-the next frontier for shared services and functional excellence. (s. 81-94) Springer.

Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J., Ouyang, C., . . . Reijers, H. A. (2020). Robotic process automation: Contemporary themes and challenges. *Computers in Industry, 115*, 103162.

Tornbohm, C. & Dunie, R. (2017). Gartner market guide for robotic process automation software. *Report G00319864.Gartner*

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Kustannusosakeyhtiö Tammi.

Van der Aalst, W., Bichler, M. & Heinzl, A. (2018). Robotic process automation. *Business & Information Systems Engineering, 60*(4), 269-272.

Vitharanage, I., Bandara, W., Syed, R. & Toman, D. (2020). An empirically supported conceptualisation of robotic process automation (RPA) benefits. Association for Information Systems.

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

Willcocks, L., Lacity, M. & Craig, A. (2016). Robotic process automation at telefonica O2. *MIS Q Exec, 15*(1), 21-35.

Willcocks, L., Hindle, J. & Lacity, M. (2018). Keys to RPA success. . Executive Research Report.: Knowledge Capital Partners.

Willcocks, L., Lacity, M. & Craig, A. (2015). The IT function and robotic process automation. *The London School of Economics and Political Science,* (Haettu osoitteesta http://eprints.lse.ac.uk/64519/)

Yin, R. K. (1994). *Case study research: Design and methods (2nd ed.). Newbury park, CA: SAGE publications*

Zaharia-Rădulescu, A., Pricop, C. L., Shuleski, D. & Ioan, A. C. (2017). RPA and the future of workforce.

LIITE 1 HAASTATTELURUNKO

TAUSTATIEDOT

- Haastateltavan tehtävänimike
- Ohjelmistorobotiikkaan liittyvät työtehtävät ja työkokemus näissä tehtävissä

OHJELMISTOROBOTIIKAN TIETOTURVA

1. **Ohjelmistorobotiikan tietoturva yleisesti**
    - Pidätkö ohjelmistorobotiikkaa yleisesti ottaen tietoturvallisena tapana automatisoida prosesseja?
    - Millaisiin asioihin ohjelmistorobotiikan tietoturvan hallinnassa pitäisi mielestäsi kiinnittää erityisesti huomiota?
2. **Identiteetin- ja pääsynhallinta**
    - Oletko kohdannut ohjelmistorobotiikan kohdalla identiteetin- ja pääsynhallintaan liittyviä tietoturvahaasteita?
        - Millaisia?
        - Miten haasteet on ratkaistu?
        - Onko jotakin jäänyt ratkaisematta?
    - Millaisilla käytännöillä ja keinoilla näihin haasteisiin pyritään kokemustesi perusteella vastaamaan?
        - Onko keinot toimivia? Miksi?
        - Mitä pitäisi tehdä toisin?
3. **Datan eheys poikkeustilanteissa**
    - Oletko kohdannut ohjelmistorobotiikan kohdalla datan eheyteen liittyviä tietoturvahaasteita?
        - Millaisia?
        - Miten haasteet on ratkaistu?
        - Onko jotakin jäänyt ratkaisematta?
    - Millaisilla käytännöillä ja keinoilla näihin haasteisiin pyritään kokemustesi perusteella vastaamaan?
        - Onko keinot toimivia? Miksi?
    - Mitä pitäisi tehdä toisin
4. **Informaatioteknologian kuluttajistumisen vaikutus tietoturvaan**
    - Oletko havainnut informaatioteknologian kuluttajistumisen ilmiötä ohjelmistorobotiikan kohdalla
    - Koetko informaatioteknologian kuluttajistumisen vaikuttavan ohjelmistorobotiikan tietoturvaan / sen hallintaan?
        - Miksi? Miten?
    - Miten negatiivisia vaikutuksia voisi ehkäistä?

LISÄKYSYMYKSET

- Jäikö jokin ohjelmistorobotiikan tietoturvaan liittyvä aihealue mielestäsi käsittelemättä?
- Tuleeko sinulla mieleen muita henkilöitä, joita olisi hyvä haastatella?
- Vapaita kommentteja aiheesta

LIITE 2 HAASTATELTAVILLE ANNETUT KÄSITTEIDEN MÄÄRITELMÄT

IDENTITEETIN- JA PÄÄSYNHALLINTA

Identiteetin- ja pääsynhallinnalla tarkoitetaan prosesseja, työkaluja ja käytänteitä, joiden avulla hallitaan eri kohteiden (tässä tapauksessa ohjelmistorobottien) digitaalista identiteettiä sekä kontrolloidaan pääsyä järjestelmiin ja kriittiseen informaatioon.

DATAN EHEYS POIKKEUS

Datan eheydellä tarkoitetaan tiedon paikkansapitävyyttä ja validiteettia.

Poikkeustilanteella tarkoitetaan automatisoitavassa prosessissa esiintyvää, työnkulkuun vaikuttavaa poikkeustapausta, joka ohjelmistorobotin tulee osata käsitellä oikealla tavalla. Poikkeustapaukseksi voidaan luokitella myös se, jos ohjelmistorobotti saa käsiteltäväkseen jo lähtökohtaisesti virheellistä dataa.

INFORMAATIETEKNOLOGIAN KULUTTAJISTUMINEN

Informaatioteknologian kuluttajistumisella tarkoitetaan ilmiötä, jonka myötä helposti käyttöönotettavien IT-resurssien, kuten ohjelmistorobotiikan hallinta siirtyy keskitetyltä IT-yksiköltä teknologian loppukäyttäjälle, kuten liiketoimintayksikölle itselleen. Ilmiölle on tyypillistä, että entistä suurempi osa yhteistyöstä ja kommunikaatiosta tapahtuu suoraan teknologian loppukäyttäjän ja toimittajan välillä, jolloin organisaation IT-yksikön rooli jää vähäisemmäksi.