Oliver Ahti

TOIMINNANOHJAUSJÄRJESTELMIEN TIETOTURVAUHAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Ahti, Oliver
Toiminnanohjausjärjestelmien tietoturvauhat
Jyväskylä: Jyväskylän yliopisto, 2022, 24 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen, Ville

Tässä kandidaatintutkielmassa tutkitaan toiminnanohjausjärjestelmiin tyypillisesti kohdistuvia tietoturvauhkia sekä näiden uhkien mitigointikeinoja. Tutkielmassa etsitään samalla keinoja parantaa toiminnanohjausjärjestelmien, ja osittain muiden laajojen tietojärjestelmien, yleistä tietoturvallisuutta. Toiminnanohjausjärjestelmät tai ERP-järjestelmät (enterprise resource planning) ovat suuria, monimutkaisia sekä modulaarisia tietojärjestelmiä, joilla pyritään standardoimaan ja integroimaan suurin osa yrityksen liiketoimintaprosesseista yhden tietojärjestelmän alaisuuteen tuottavuuden sekä liiketoimintayksiköiden yhteistyön tehostamista varten. Tutkielmassa perehdytään toiminnanohjausjärjestelmien historiaan, nykytilaan, yleisimpiin moduuleihin sekä käyttömalleihin, kuten pilvimalleihin sekä on-premise-malliin. Tutkielmassa on olennaisessa osassa myös tietoturvallisuuden käsite. Tietoturvallisuus tai *information security* tarkoittaa tiedon luottamuksellisuuden, eheyden sekä saatavuuden ylläpitämistä. Erilaisten tietoturvauhkien mitigointiin eli uhkien toteutumisen todennäköisyyden lieventämiseen on tutkielmassa löydetty monia eri keinoja. Tärkeimpinä keinoina pidetään vahvaa organisaation sisäistä hallintakehystä sekä tietoturvakäytänteitä, jotka esimerkiksi rajoittavat eri käyttäjien käyttöoikeuksia tarpeen mukaan toiminnanohjausjärjestelmässä. Tutkielma on toteutettu kirjallisuuskatsauksena.

Asiasanat: toiminnanohjausjärjestelmä, tietoturva, erp, tietoturvauhka, pilvipalvelu

ABSTRACT

Ahti, Oliver
Information security threats in ERP systems
Jyväskylä: University of Jyväskylä, 2022, 24 pp.
Information Systems, Bachelor's Thesis
Supervisor: Seppänen, Ville

This bachelor's thesis examines some of the most common information security threats facing enterprise resource planning systems or ERP systems, and some ways to mitigate those threats. The thesis also examines some ways to improve the overall level of information security in organizations using enterprise resource planning systems. Enterprise resource planning systems are large, complicated, and modular information systems, that aim to standardize and integrate much of an organizations IT-infrastructure under one single information system. This thesis delves into the history of ERP systems, their current state, some of the most common modules used, and different operating models such as cloud computing/SaaS or the traditional on-premise model. The concept of information security, defined as preserving the confidentiality, integrity and availability of information, is also essential to the thesis. Several methods of mitigating information security threats have been discovered in this thesis. Some of the most important and effective methods are considered to be strong internal control frameworks and information security practices, including role-based access control within the ERP system. This thesis has been conducted as a literature review.

Keywords: enterprise resource planning, information security, information security threat, cloud computing, erp systems

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Toiminnanohjausjärjestelmät tai ERP-järjestelmät ovat iso osa monen yrityksen liiketoimintaa. Toiminnanohjausjärjestelmillä hallitaan suurta osaa yrityksen liiketoiminnasta, aina henkilöstöhallinnasta taloushallintoon ja myyntijärjestelmistä materiaalinhallintaan. Panorama Consulting Groupin suorittamista vuosittaisista raporteista voi huomata trendin, jossa toiminnanohjausjärjestelmät ovat siirtyneet viime vuosina pilvipalvelumallilla toimiviksi (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2017, 2019). Toiminnanohjausjärjestelmien tarjonta on laajempaa kuin koskaan, ja pilvipalvelumalli mahdollistaa myös pienten ja keskisuurten yritysten toiminnanohjausjärjestelmien hankintaa.

Alati digitalisoituvassa maailmassa myös tietoturvauhat nousevat entistä enemmän esiin. Toiminnanohjausjärjestelmien ollessa yhä tärkeämpiä moderneille yrityksille (Shen, Chen & Wang, 2016) onkin aiheellista tutkia sitä, minkälaisia tietoturvauhkia toiminnanohjausjärjestelmiin kohdistuu. Alla on esitetty kaksi tutkimuskysymystä, joihin tässä tutkimuksessa on pyritty löytämään selkeitä vastauksia.

1. Minkälaisia tietoturvauhkia toiminnanohjausjärjestelmiin tyypillisesti kohdistuu?

2. Miten toiminnanohjausjärjestelmien ja niitä käyttävien organisaatioiden yleistä tietoturvallisuutta voidaan parantaa?

Molempiin tutkimuskysymyksiin vastataan tutkielman toisessa pääluvussa.

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena. Lähdekirjallisuutta on haettu pääasiassa Google Scholar- sekä IEEE Xplore-hakukoneilla. Päähakusanat ovat olleet muun muassa ”enterprise resource planning”, ”erp security threat”, ”information security threat”, “infosec risk mitigation” sekä näistä hakusanoista johdetut apuhakusanat. Lähdekirjallisuuden valinnassa on painotettu niin lähteen JUFO-luokitusta kuin myös viittausten määrää. Erityisesti toiminnanohjausjärjestelmiin kohdistuvia tietoturvauh-

kia käsittelevää kirjallisuutta löytyi tutkielmaa varten melko vähän, mutta toiminnanohjausjärjestelmiin kohdistuu siitä huolimatta monia samanlaisia tietoturvauhkia kuin muihinkin suuriin ja monimutkaisiin tietojärjestelmiin.

Tutkielma rakentuu johdannosta, kahdesta pääluvusta sekä yhteenvetoluvusta. Ensimmäisessä pääluvussa käydään läpi toiminnanohjausjärjestelmien historiaa, nykytilaa, yleisiä palveluntarjoajia, tärkeimpiä moduuleja sekä vertaillaan eri käyttömalleja. Toisessa pääluvussa perehdytään aluksi tietoturvallisuuden, tietoturvauhan sekä kyberturvallisuuden käsitteisiin, josta jatketaan toiminnanohjausjärjestelmiin kohdistuvien tietoturvauhkien kategoriseen läpikäyntiin. Tietoturvauhkiin pyritään löytämään mitigointikeinoja, joita käydään samoissa kategorioissa läpi. Toisessa pääluvussa etsitään lopuksi ratkaisua myös toiseen tutkimuskysymykseen. Yhteenvetoluvussa kootaan yhteen tutkielman tärkeimmät käsitellyt aiheet, kerrataan yleisimpiä esiinnousseita tietoturvauhkia, ja esitetään ajatuksia jatkotutkimusta varten.

2 TOIMINNANOHJAUSJÄRJESTELMÄT NYKYÄÄN JA ENNEN

Tässä luvussa käydään läpi toiminnanohjausjärjestelmiä kokonaisuutena. Luvussa käsitellään toiminnanohjausjärjestelmien historiaa, moderneja järjestelmiä ja järjestelmäntarjoajia sekä toiminnanohjausjärjestelmien tärkeimpiä toiminnallisuuksia.

Toiminnanohjausjärjestelmät tai ERP-järjestelmät (engl. *enterprise resource planning*) ovat suuria, monimutkaisia sekä modulaarisia tietojärjestelmiä, joilla pyritään standardoimaan ja integroimaan suurin osa yrityksen liiketoimintaprosesseista yhden tietojärjestelmän alaisuuteen tuottavuuden sekä liiketoimintayksiköiden yhteistyön tehostamista varten (Chou & Chang, 2008; Klaus, Rosemann & Gable, 2000). Toiminnanohjausjärjestelmien yleisimmin käytettyjä moduuleja ovat erilaiset taloudenhallintaan, varastointiin, tilaus- ja ostojärjestelmiin sekä henkilöstönhallintaan liittyvät moduulit (Mabert, Soni & Venkataramanan, 2003). Toiminnanohjausjärjestelmien suurimpina hyötyinä nähdään usein kustannustehokkuus, pirstaloituneen IT-infrastruktuurin yhdistäminen yhden järjestelmän alaisuuteen, sekä järjestelmän käyttöönoton yhteydessä tehtävän liiketoimintaprosessien uudelleensuunnittelun (engl. *business process reengineering*) tuomat alan parhaat käytännöt (Luo & Strong, 2004).

Toiminnanohjausjärjestelmät hankitaan hyvin usein kolmannen osapuolen palveluntarjoajalta, kuten SAPilta, Oraclelta tai Microsoftilta. Toiminnanohjausjärjestelmän käyttöönottoon ei ole helppoa keinoa, vaan se vaatii yksityiskohtaiset käyttöönottosuunnitelmat ja kommunikaatiostrategiat, paljon resursseja sekä melko usein liiketoimintaprosessien uudelleensuunnittelua (Panorama Consulting Solutions, 2019). Käyttöönoton hankaluudesta kielii myös se, että edelleen noin puolet toiminnanohjausjärjestelmiä käyttöönottavista organisaatioista ylittää suunnitellun käyttöönottobudjettinsa ja/tai käyttöönottoon suunnitellun aikataulun (Panorama Consulting Group, 2021).

2.1 Toiminnanohjausjärjestelmien historia

Ymmärtääkseen modernien toiminnanohjausjärjestelmien toimintatapoja sekä palveluntarjoajien valikoimaa, on syytä palata hetkellisesti toiminnanohjausjärjestelmien historiaan.

Toiminnanohjausjärjestelmien edeltäjinä pidetään MRP-järjestelmiä, eli tuotannonohjausjärjestelmiä (engl. *material requirements planning*). IBM sekä traktorivalmistaja J.I. Case kehittivät yhteistyössä ensimmäisen MRP-järjestelmän 1960-luvun loppuvaiheilla (Jacobs & Weston, 2007). MRP-järjestelmät kykenivät muun muassa inventaarionhallintaan ja materiaaliluetteloiden sekä päätuotantoaikataulun hallitsemiseen. MRP-järjestelmät olivat isoja, kalliita sekä hankalia ylläpidettäviä, sillä niitä ajettiin suurtietokoneilla kuten IBM:n 7094:llä (Jacobs & Weston, 2007). 1970-luvulla perustettiin useita tunnettuja toiminnanohjausjärjestelmiä edelleen kehittäviä teknologiayrityksiä, kuten saksalainen SAP sekä yhdysvaltalainen Oracle.

Kun uudet tuotannonohjausjärjestelmät kattoivat entistä enemmän liiketoiminta-alueita, tarvittiin niille uusi nimi. MRP II-termiä ruvettiin käyttämään 1980-luvun alkuvaiheilla, ja samalla MRP-lyhenteen merkitys vaihtui *manufacturing resource planning*iksi (Jacobs & Weston, 2007). MRP II-järjestelmät korjasivat MRP-järjestelmien heikkoina pidettyjä alueita (Ptak, 1991) ja ne kykenivät MRP-järjestelmän toimintojen lisäksi myös taloudenhallintatoimintoihin, inventaarion kysynnän ennustamiseen, laadunvarmistukseen sekä tuotantolaitteiden kapasiteetinhallintaan (Boehm, 2020).

Gartner Group käytti ensimmäisenä ERP-termiä 1990-luvun alussa. 90-luvulla IBM:n johtoasema markkinoilla oli pienentynyt merkittävästi, ja isoja ERP-järjestelmätarjoajia olivat SAP, Oracle, J.D. Edwards, PeopleSoft sekä Baan (Jacobs & Weston, 2007). 2000-luvun alussa tapahtui jonkin verran yritysfuusioita, jotka konsolidoivat koko toiminnanohjausjärjestelmäkenttää. Yritysfuusioita toteuttivat muun muassa vielä tänä päivänäkin merkittävät Oracle sekä Microsoft. Oracle osti J.D. Edwardsin sekä PeopleSoftin ja sulautti niiden järjestelmätarjonnat omaan portfolioonsa, kun taas Microsoft lanseerasi yrityshankintojen tukemana Dynamics-toiminnanohjausjärjestelmäportfolionsa.

2.2 Modernit toiminnanohjausjärjestelmät

Tässä alaluvussa käsitellään modernien toiminnanohjausjärjestelmien kyvykkyyksiä, tasojaottelua sekä muutamaa eri käyttömallia, kuten pilvipalvelumalleja sekä on-premise-mallia.

2.2.1 Toiminnanohjausjärjestelmän valintaan vaikuttavat tekijät

Toiminnanohjausjärjestelmän valintaan vaikuttaa moni tekijä. Yksi merkittävä tekijä on käyttöönottavan organisaation koko, sillä eri toiminnanohjausjärjes-

telmät vastaavat parhaiten tietyn kokoluokan organisaation tarpeita. Toiminnanohjausjärjestelmät luokitellaan kohdeorganisaation koon mukaan yleensä kolmeen tasoon (engl. *tier*) (Panorama Consulting Group, 2021). Eri tasoja on esitelty taulukossa 1. Tason I toiminnanohjausjärjestelmät ovat suunniteltu valtaville käyttäjäorganisaatioille, joilla on yli 750 miljoonaa dollaria vuosittaista liikevaihtoa. Tason I toiminnanohjausjärjestelmät kattavat useita eri toimialoja, ja nämä järjestelmät ovat isoimpia, kalliimpia sekä monimutkaisimpia markkinoilla olevia toiminnanohjausjärjestelmiä. Esimerkkejä tason I toiminnanohjausjärjestelmistä ovat muun muassa SAP S/4HANA sekä Oracle ERP Cloud (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2019).

Panorama (2021, 2019) jakaa tason II vielä kahteen alatasoon – ylempään ja alempaan. Ylemmän tason II toiminnanohjausjärjestelmät ovat suunnattu yrityksille, joilla on noin 250–750 miljoonan dollarin vuosittainen liikevaihto. Ylemmän tason II toiminnanohjausjärjestelmät eivät ole yhtä laaja-alaisia järjestelmiä kuin tason I toiminnanohjausjärjestelmät, mutta ne voivat silti kattaa useita eri toimialoja ja liiketoimintayksiköitä. Tyypillisiä ylemmän tason II toiminnanohjausjärjestelmiä ovat muun muassa Microsoft Dynamics 365 Finance sekä Sage X3 (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2019). Alemman tason II toiminnanohjausjärjestelmät palvelevat Panoraman (2021, 2019) mukaan PK-yrityksiä, joilla on noin 10–250 miljoonan euron vuosittainen liikevaihto. Alemman tason II toiminnanohjausjärjestelmiä käyttävillä yrityksillä ovat usein keskittyneet yksittäiseen toimialaan, eikä käytettävän toiminnanohjausjärjestelmänkään täten tarvitse tukea useampaa toimialaa. Tyypillisiä alemman tason II toiminnanohjausjärjestelmiä on Microsoft Dynamics 365 Business Central, Oracle Netsuite sekä SYSPRO (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2019).

Pienimmät eli tason III toiminnanohjausjärjestelmät ovat usein kehitetty jotain tiettyä käyttötapausta varten, eivätkä ne tarjoa juurikaan muuta toiminnallisuutta käyttötapauksen lisäksi. Esimerkiksi yhdysvaltalainen Aptean tarjoaa erillisiä toiminnanohjausjärjestelmiä niin elintarvikeyritysten kuin varustevuokraamoiden käyttöön (Aptean, 2021). Tason III toiminnanohjausjärjestelmät voivat myös tukea ja täydentää isompia toiminnanohjausjärjestelmiä, jolloin nämä pienet toiminnanohjausjärjestelmät sopivat myös isommille käyttäjäorganisaatioille.

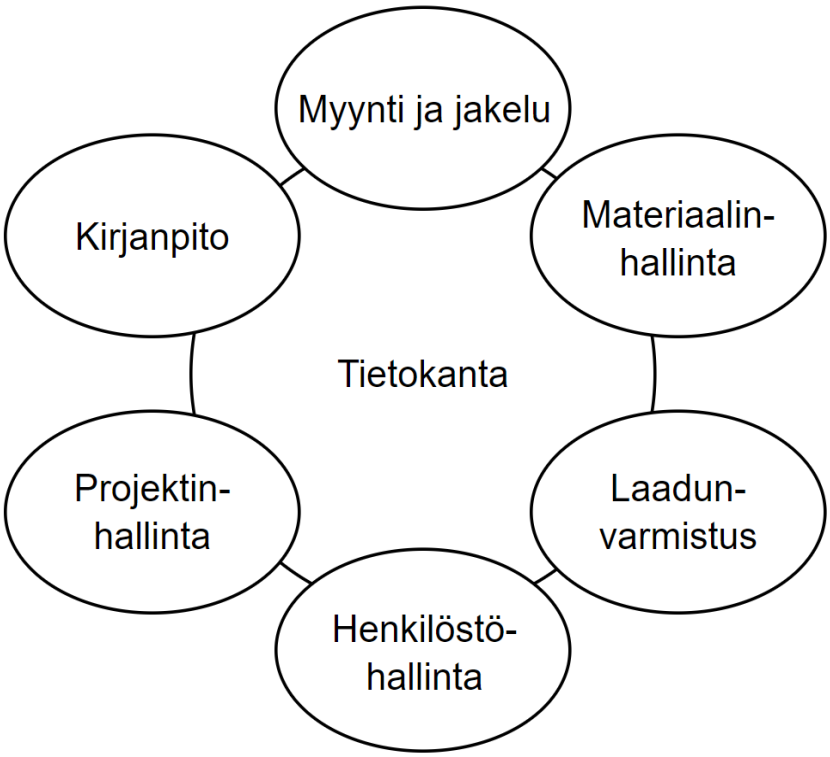
TAULUKKO 1 Toiminnanohjausjärjestelmien kokoluokat

Taso	**Liikevaihto**	**Esimerkkejä järjestelmistä**
Taso I	> 750 milj. €	SAP S/4 HANA, Oracle ERP Cloud
Ylempi taso II	250–750 milj. €	Microsoft Dynamics 365 Finance, Sage X3
Alempi taso II	10–250 milj. €	Business Central, Oracle Netsuite, SYSPRO
Taso III	< 10 milj. €	Aptean Bakery ERP, Aptean Dairy ERP

2.2.2 Modulaarisuus

Modulaarisuus on yksi toiminnanohjausjärjestelmien tärkeimmistä ominaisuuksista. Etenkin isoimmat markkinoilla olevat toiminnanohjausjärjestelmät kykenevät suorittamaan usean eri liiketoimintayksikön tai jopa toimialan liiketoimintaprosesseja, ja onkin harvinaista, että yksittäinen käyttäjäorganisaatio tarvitsisi joka ikistä toiminnanohjausjärjestelmän toimintoa. Toiminnanohjausjärjestelmien modulaarisuuden ansiosta käyttäjäorganisaatioiden ei tarvitse maksaa ylimääräistä hintaa niistä toiminnoista, joita organisaatio ei tarvitse.

Kuten aiemmin mainittiin, toiminnanohjausjärjestelmistä löytyy moduuleja moniin eri tarkoituksiin. Esimerkkejä yleisistä moduuleista ovat kirjanpitomoduulit, tilausjärjestelmämoduulit, henkilöstöhallintomoduulit, materiaalinhallintamoduulit sekä laadunvarmistusmoduulit (Luo & Strong, 2004; Shehab, Sharp, Supramaniam & Spedding, 2004). Yleisiä moduuleja ja niiden linkittymistä toiminnanohjausjärjestelmän keskeiseen tietokantaan on nähtävillä kuviossa 1. Käytettävien moduulien valinta suoritetaan yleensä käyttöönoton yhteydessä (Luo & Strong, 2004). Moduulivalintoja voidaan tarpeen vaatiessa muuttaa myöhemmin toiminnanohjausjärjestelmän elinkaaren aikana, joko ottamalla uusia moduuleja käyttöön tai poistamalla tarpeettomia moduuleja käytöstä. Toiminnanohjausjärjestelmien modulaarinen toimintatapa helpottaa myös siirtymää toiminnanohjausjärjestelmästä toiseen, koska siirtymässä voidaan modulaarisuuden ansiosta hyödyntää ”moduuli kerrallaan”-lähestymistapaa (Panorama Consulting Group, 2021).



Kuvio 1. Toiminnanohjausjärjestelmien yleisiä moduuleita. Mukaillen Shebab ym. (2004)

2.2.3 Käyttömallit

Toiminnanohjausjärjestelmät voivat pyöriä joko asiakkaan omilla palvelimilla (engl. *on-premise)*, hybridipilvimallina (engl. *hybrid cloud*) tai pilvipalvelumallilla (Panorama Consulting Solutions, 2019). Pilvipalveluina toimivat toiminnanohjausjärjestelmät ovat kasvattaneet suosiotaan viime vuosien aikana (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2017, 2019), mutta edelleen Panoraman vuoden 2021 raportissa noin puolet vastaajista ilmoittivat valinneensa hiljattaisessa käyttöönotossa on-premise-mallilla toimivan toiminnanohjausjärjestelmän pilvipalvelumallin sijaan (Panorama Consulting Group, 2021).

Pilvipalvelumallilla pyörivien toiminnanohjausjärjestelmien käyttömalliksi valittiin Panoraman (2021) mukaan 76.5 % ajasta SaaS-malli. SaaS (engl. *software as a service)* tarkoittaa palveluntarjoajalta tilattavaa ja pilvipalveluna pyörivää ohjelmistoa (Puthal, Sahoo, Mishra & Swain, 2015; Wang ym., 2010). SaaS-mallilla toimivilla toiminnanohjausjärjestelmillä on monia hyötyjä, kuten matalammat aloituskustannukset IT-infrastruktuurin ulkoistamisen ansiosta, tehokkaampi skaalautuvuus, automaattiset päivitykset, ennustettavat käyttökustannukset sekä järjestelmän hyvä saatavuus (Abd Elmonem, Nasr & Geith, 2016). SaaS-mallissa on myös heikkouksia verrattuna on-premise-malliin, kuten riippuvuuden muodostuminen pilvipalveluntarjoajaan, toiminnanohjausjärjestelmän omistajuuden ja hallinnoinnin siirtäminen pilvipalveluntarjoajalle ja se, että suuri osa tietoturvallisuudesta huolehtimisesta siirtyy pilvipalveluntarjoajalle (Abd Elmonem ym., 2016). Etenkin PK-yritykset suosivat pilvipalveluina toimivia toiminnanohjausjärjestelmiä, sillä PK-yrityksillä on harvoin varaa investoida on-premise-mallilla toimiviin toiminnanohjausjärjestelmiin (Gupta & Misra, 2016).

3 TOIMINNANOHJAUSJÄRJESTELMIEN TIETOTURVAUHKIA JA NIIDEN MITIGOINTIA

Tässä luvussa käsitellään aluksi tietoturvaa sekä tietoturvauhkia konseptina. Tämän jälkeen siirrytään käsittelemään toiminnanohjausjärjestelmiin kohdistuvia tietoturvauhkia, joiden ohessa esitellään mitigointikeinoja kutakin uhkakategoriaa kohden. Luvun viimeisessä alaluvussa käsitellään toiminnanohjausjärjestelmien ja niitä käyttävien yritysten yleistä tietoturvallisuutta nostavia menetelmiä. Tässä luvussa vastataan molempiin tutkimuskysymyksiin, ensimmäiseen alaluvussa 3.2 ja toiseen alaluvussa 3.3.

3.1 Tietoturvallisuus

Tietoturvallisuuden määritelmä ei ole aivan yksiselitteinen, mutta yksinkertaisimmillaan ISO-standardin 27002 mukaan tietoturvallisuus (engl. *information security*) tarkoittaa tiedon luottamuksellisuuden, eheyden sekä saatavuuden ylläpitämistä (von Solms & van Niekerk, 2013). Whitman ja Mattord (2011) lisäävät edelliseen määritelmään vielä sen, että tietoturvallisuus saavutetaan käytänteiden, koulutuksen, tietoisuuden sekä teknologian avulla (Whitman & Mattord, 2011). Tietoturvallisuuden tavoitteena yritysten näkökulmasta on varmistaa yrityksen toiminnan jatkuvuus sekä minimoida liiketoimintaan kohdistuvaa haittaa estämällä tietoturvauhkia ja minimoimalla tietoturvauhkien aiheuttamaa vahinkoa (von Solms, 1998).

Tietoturvallisuuteen kytkeytyy vahvasti kyberturvallisuuden käsite. Kyberturvallisuus (engl. *cyber security*) ja tietoturva kulkevat keskustelussa usein käsi kädessä, mutta kyberturvallisuus on käsitteenä paljon laajempi, ja se kattaa paljon laajemman alueen. Tietoturvallisuuden tarkoituksena on ylläpitää informaation luottamuksellisuutta, eheyttä sekä saatavuutta, kun taas kyberturvallisuus kattaa tietoturvallisuuden lisäksi myös varsinaisen tietoteknisen laitteiston turvallisuuden, tietoverkon käyttäjien turvallisuuden sekä kaikkien

verkkohyökkäyksille potentiaalisten kohteiden turvallisuuden (von Solms & van Niekerk, 2013).

Tietoturvauhka (engl. *information security threat*) tarkoittaa ei-toivottua tapahtumaa tai tilannetta, joka uhkaa järjestelmän tietoturvallisuutta. Tietoturvauhat voidaan jakaa karkeasti sisäisiin sekä ulkoisiin tietoturvauhkiin. Sisäinen tietoturvauhka tarkoittaa uhkaa joka on lähtöisin yrityksen sisältä, hyödyntäen joko valtuutettua käyttäjätiliä yrityksen sisäiseen verkkoon tai fyysistä pääsyä yrityksen sisäiseen verkkoon (Jouini, Rabai & Aissa, 2014). Sisäiset tietoturvauhat johtuvat usein joko yrityksen työntekijän toiminnasta tai virheestä jossain liiketoimintaprosessissa (Jouini ym., 2014). Ulkoiset tietoturvauhat taas ovat lähtöisin yrityksen ulkopuolelta, ja ne saattavat hyödyntää luvatonta pääsyä yrityksen tietoverkkoon. Ulkoiset tietoturvauhat voivat myös olla muita ulkoisia tapahtumia, jotka jollain tavalla uhkaavat tietoturvallisuutta, kuten erilaiset luonnonkatastrofit tai muut informaation saatavuutta, eheyttä tai luottamuksellisuutta häiritsevät onnettomuudet.

3.2 Toiminnanohjausjärjestelmiin kohdistuvat tietoturvauhat ja niiden mitigointi

Tässä luvussa tullaan luokittelemaan erilaisia toiminnanohjausjärjestelmiin kohdistuvia tietoturvauhkia eri kategorioihin, kuten sisäisiin ja ulkoisiin tietoturvauhkiin tai käyttömalliin liittyviin uhkiin. Uhkien mitigointikeinoja eli tapoja vähentää tietoturvauhkien tapahtumisen todennäköisyyttä tai hallita niiden tuottamaa vahinkoa käsitellään samoissa uhkakategorioissa.

Suurin osa tässä luvussa käsiteltävistä tietoturvauhista ei koske pelkästään toiminnanohjausjärjestelmiä, vaan ne voivat uhata myös muita suuria, monen käyttäjän tietojärjestelmiä. Pelkästään toiminnanohjausjärjestelmiä koskevista tietoturvauhista on hyvin vähän kirjallisuutta olemassa, luultavasti edellä mainitusta syystä. Lähdekirjallisuutta tähän alalukuun on haettu enimmäkseen Google Scholar- sekä IEEE Xplore-hakukoneita hyödyntäen, muun muassa hakusanoilla ”erp security threat”, ”information security threat” sekä ”enterprise resource planning security”.

3.2.1 Sisäiset tietoturvauhat

Kuten edellä mainittiin, sisäiset tietoturvauhat ovat yrityksen tai organisaation sisältä lähtöisin olevia uhkia, jotka hyödyntävät yrityksen sisäisiä hyökkäyskulmia, kuten valtuutettuja käyttäjätilejä sekä liiketoimintaprosesseja. Sisäiset uhat voidaan vielä Jouinin ym. (2014) esittämän mallin mukaan jakaa kolmeen alaluokkaan; ihmislähtöisiin tietoturvauhkiin, ympäristölähtöisiin tietoturvauhkiin sekä teknologialähtöisiin tietoturvauhkiin (Jouini ym., 2014).

Ihmislähtöiset uhat voidaan edellä mainitun mallin mukaan jakaa niin tahattomiin kuin tahallisiin tietoturvauhkiin (Jouini ym., 2014). Esimerkkejä tahallisestä ihmislähtöisestä sisäisestä tietoturvauhasta voisivat olla muun muassa

työntekijän tietoisesti suorittama datan tuhoaminen tai väärän datan syöttäminen (Sumner, 2009). Tahattomia ihmislähtöisiä sisäisiä tietoturvauhkia taas voisivat olla esimerkiksi lukitsemattomat tietokoneet, helposti arvattavat salasanat, vahingossa tapahtuneet datan tuhoamistilanteet tai väärän datan syöttämistilanteet (Sumner, 2009).

Ihmislähtöisiä sisäisiä tietoturvauhkia voidaan mitigoida eri tavoin, joista vahvat sisäiset hallintakehykset sekä tietoturvakäytännöt nousevat esiin tärkeimpinä. Eräässä tutkimuksessa kehitettiin empiirisen tutkimuksen pohjalta eräänlainen sisäisen hallinnan viitekehys (engl. *internal control framework*), jota voidaan hyödyntää toiminnanohjausjärjestelmien kontekstissa (Chang, Yen, Chang & Jan, 2014). Tutkimuksen pohjalta kehitetyssä viitekehyksessä oli 12 näkökulmaa ja 37 ohjauskohdetta. Jokaisen ohjauskohteen tärkeys sisäisten tietoturvauhkien estämisen kannalta on myös arvosteltu kolmiportaisella asteikolla. Tärkeimpinä ohjauskohteina pidettiin muun muassa seuraavia:

- Suljetaanko työntekijöiden tilit heidän poistuessaan yrityksestä?
- Onko järjestelmässä salasanasuojauksia?
- Onko järjestelmässä eri käyttöoikeustasoja eri käyttötarpeisiin?
- Varmuuskopioidaanko järjestelmädata säännöllisesti?
- Onko järjestelmään syötettävä data todennettu etukäteen relevanteilla ohjelmilla?

Edellä mainittuja sekä monia muita Changin ym. (2014) mallissa esitettyjä ohjauskohteita voidaan hyödyntää ihmislähtöisten sisäisten tietoturvauhkien mitigoinnissa. Roolipohjainen käyttöoikeustason säätäminen nousee esille myös muissa toiminnanohjausjärjestelmien turvallisuuteen keskittyvissä artikkeleissa (She & Thuraisingham, 2007).

Ihmislähtöiset tietoturvauhat eivät kuitenkaan ole ainoita sisäisiin tietoturvauhkiin luettavia uhkia. Jouinin ym. mallin mukaan tietoturvauhat voidaan jakaa ihmislähtöisten uhkien lisäksi vielä teknologia- sekä ympäristölähtöisiin tietoturvauhkiin (Jouini ym., 2014). Tässä tutkielmassa tullaan tarkastelemaan ympäristölähtöisiä uhkia kuitenkin vasta ulkoisten tietoturvauhkien yhteydessä.

Teknologialähtöiset sisäiset tietoturvauhat voivat johtua esimerkiksi toiminnanohjausjärjestelmän ohjelmistokoodin virheistä, haavoittuvuuksista tai IT-infrastruktuurin vikatilanteista (Sumner, 2009). Changin ym. (2014) mallissa on myös useita ohjauskohteita, joilla voidaan mitigoida teknologialähtöisiä sisäisiä tietoturvauhkia:

- Onko organisaatiossa nimettyjä henkilöitä, jotka ovat vastuussa järjestelmän tietokannasta?
- Onko organisaation teknisen huollon henkilökunnan vastuualueet määritelty selkeästi?
- Onko kehittämistyölle sekä testaustyölle olemassa omat, itsenäiset [virtuaali]ympäristöt?

- Arvioivatko järjestelmän käyttäjät uudet tai muokatut sovelluskomponentit?

3.2.2 Ulkoiset tietoturvauhat

Ulkoiset tietoturvauhat ovat sellaisia tietoturvauhkia, jotka ovat lähtöisin organisaation ulkopuolelta. Ulkoiset tietoturvauhat voivat hyödyntää luvatonta pääsyä yrityksen tietoverkkoon tai järjestelmiin kuten toiminnanohjausjärjestelmään, mutta ulkoiset tietoturvauhat voivat olla myös mitä tahansa muita organisaation ulkopuolisia tapahtumia tai tilanteita, jotka uhkaavat tietoturvallisuuden kolmea edellytystä. Aiemmin esitellyn Jouinin ym. mallin mukaan myös ulkoiset tietoturvauhat voidaan sisäisten tietoturvauhkien tapaan jakaa niin ihmislähtöisiin, teknologialähtöisiin kuin ympäristölähtöisiin tietoturvauhkiin (Jouini ym., 2014).

Ulkoiset ihmislähtöiset tietoturvauhat ovat ehkä ensimmäinen kategoria, joka tietoturvauhkia ajatellessa nousee mieleen. Tähän kategoriaan voidaan katsoa Jouinin ym. (2014) mukaan ainakin sabotaasi, datan varastaminen, datan tuhoaminen sekä erilaiset spoofing-hyökkäykset (Jouini ym., 2014). Spoofing-hyökkäyksessä hyökkääjä muuttaa lähetettävien IP-pakettien lähettäjäosoitteita esittääkseen olevansa jokin muu valtuutettu henkilö tai ohjelma, jolla olisi normaalisti pääsy tietojärjestelmään (Duan, Yuan & Chandrashekar, 2008). Edellä mainitut ulkoiset ihmislähtöiset tietoturvauhat ovat kaikki tahallisia, ja niiden voidaan katsoa olevan kyberhyökkäyksiä. Jouini ym. (2014) sisältää vielä mallissaan terrorismin sekä poliittisen sodankäynnin ulkoisiksi ihmislähtöisiksi tietoturvauhiksi, jotka voisivat johtaa tietoturvallisuuden kriteerien vaarantamisen (Jouini ym., 2014). Ulkoisia ihmislähtöisiä tietoturvauhkia voidaan osittain mitigoida muun muassa samanlaisella sisäisen hallinnan viitekehyksellä kuin sisäisiä ihmislähtöisiä tietoturvauhkia. Changin ym. (2014) mallissa on useita ohjauskohteita, jotka sopivat myös luvattomasti järjestelmään päässeiden hyökkääjien aiheuttamien vahinkojen estämiseen tai lieventämiseen:

- Onko IT-infrastruktuurilaitteisto suojattu turvatoimilla?
- Onko yrityksen tiloissa pääsynhallintaa?
- Onko yrityksen tiloissa muita turvatoimia?
- Onko IT-infrastruktuurin etäkäyttöön olemassa hallintatyökaluja?
- Onko järjestelmän varmuuskopioita olemassa myös muualla kuin yrityksen tiloissa?

Edellä mainitut ohjauskohteet ovat toiminnanohjausjärjestelmän käyttömallista riippuen joko pilvipalveluntarjoajan tai asiakasyrityksen itse hallittavissa sekä vastuulla.

Ulkoisista ei-ihmislähtöisistä tietoturvauhista, jotka koskevat erityisesti toiminnanohjausjärjestelmiä, ei löytynyt tätä tutkielmaa varten merkittävää määrää relevanttia kirjallisuutta. On kuitenkin vaikeaa nähdä, miksei toiminnanohjausjärjestelmiä koskisi yhtä lailla samat ulkoiset ei-ihmislähtöiset tieto-

turvauhat kuin muitakin suuria tietojärjestelmiä, kuten maanjäristykset, tulvat tai häiriöt sähköverkossa (Jouini ym., 2014).

3.2.3 Käyttömalliin liittyvät tietoturvauhat

Toiminnanohjausjärjestelmien tietoturvauhat voivat vaihdella eri käyttömalleilla toimivien järjestelmien välillä. Tässä alaluvussa keskitytään enemmän pilvipalvelumallilla toimivien kuin on-premise-mallilla toimivien toiminnanohjausjärjestelmien tietoturvauhkiin.

Pilvipalvelumallilla toimivat toiminnanohjausjärjestelmät ovat yleistyneet huomattavasti viime vuosina (Panorama Consulting Group, 2021; Panorama Consulting Solutions, 2019). Pilvipalvelumallilla toimivat toiminnanohjausjärjestelmät eroavat on-premise-mallilla toimivista toiminnanohjausjärjestelmistä tietoturvallisuuden osalta merkittävästi, sillä toiminnanohjausjärjestelmän pyörittäminen on ulkoistettu pilvipalveluntarjoajalle. Samalla ulkoistetaan organisaation omaa hallintaa toiminnanohjausjärjestelmästä ja sen datasta pilvipalveluntarjoajalle. Tämän tietoturvallisuuden vastuun ulkoistaminen pilvipalveluntarjoajalle tuo mukanaan niin hyötyjä kuin haittoja, joiden suhde vaihtelee usein organisaation koon mukaan (Johansson, Alajbegovic, Alexopoulo & Desalermos, 2015).

Pilvipalvelumallilla toimivissa toiminnanohjausjärjestelmissä sekä pilvipalvelumallissa yleisesti on useita tietoturvallisuuteen liittyviä kysymyksiä ja uhkia asiakasorganisaation kannalta. Järjestelmän sekä datan hallinnan ulkoistaminen pilvipalvelutarjoajalle vaikuttaa luonnollisesti tiedon luottamuksellisuuteen, sillä data säilötään pilvipalveluntarjoajan konesalissa. Herkän datan hallinnan antaminen pilvipalveluntarjoajalle on aiheuttanut suurta huolta monessa yrityksessä (Johansson ym., 2015). Suuret yritykset haluavat PK-yrityksiin verrattuna pitää kriittisen datansa useammin täysin omassa hallinnassaan. Toisaalta PK-yrityksillä ei yleensä ole käytettävissään sellaisia resursseja, joilla kriittinen data olisi paremmassa turvassa yrityksen omassa on-premise-järjestelmässä kuin pilvipalveluntarjoajan konesaleissa (Johansson ym., 2015).

Toinen tiedon luottamuksellisuutta uhkaava SaaS-pilvipalvelumallin ominaisuus on se, että asiakasorganisaatiolla ei juurikaan ole hallintaa varsinaisesta IT-infrastruktuurista, jolla toiminnanohjausjärjestelmä pyörii (Saa, Costales, Moscoso-Zea & Lujan-Mora, 2017). Samalla fyysisellä palvelimella pyörii usein myös muiden asiakkaiden virtuaalisia palvelimia, mikä nostaa riskiä datan vuotamiseen tai sekoittumiseen muiden asiakkaiden datan kanssa (Puthal ym., 2015). Tätä voitaisiin luonnehtia teknologialähtöiseksi tietoturvauhaksi. Kolmantena tiedon luottamuksellisuutta uhkaavana tekijänä pilvipalvelumallilla pyörivissä toiminnanohjausjärjestelmissä voidaan nostaa esille se, ettei asiakasorganisaatiolla ole hallintaa pilvipalveluntarjoajan tietoturvastandardeista tai tietoturvaprotokollista (Hashizume, Rosado, Fernández-Medina & Fernandez, 2013). Osa pilvipalveluntarjoajista voi ostaa esimerkiksi varmuuskopiointipalveluita kolmannelta osapuolelta. Pilvipalveluntarjoajan konesalit voivat myös sijaita eri valtiossa, jolla voi olla erilaista regulaatiota tietoturvallisuuden suhteen kuin asiakasorganisaation valtiolla (Hashizume ym., 2013). Pilvipalve-

lumallissa toiminnanohjausjärjestelmän käyttäjän pitää myös olla aina kytköksissä internetiin, sillä palvelimet, joilla toiminnanohjausjärjestelmät pyörivät, eivät sijaitse samassa sijainnissa kuin toiminnanohjausjärjestelmän käyttäjä. Käyttäjän internet-yhteyden katkeaminen katkaisee samalla yhteyden toiminnanohjausjärjestelmään, estäen tiedon saatavuuden ja uhaten siten tietoturvallisuutta.

Edellä mainittuja pilvipalvelumallien tietoturvauhkia niin tiedon luottamuksellisuuden kuin tiedon saatavuuden kannalta voidaan mitigoida tai ehkäistä esimerkiksi seuraavilla tavoilla:

- Asiakasorganisaatioiden pitäisi ennen pilvipalvelumallilla toimivien toiminnanohjausjärjestelmien käyttöönottoa tarkistaa ja sopia riittävän kattava palvelutasosopimus (engl. *service-level agreement*) vaatimuksen mukaisen palvelun varmistamiseksi (Weng & Hung, 2014).
- Asiakasorganisaatioiden omien IT-asiantuntijoiden pitäisi olla mukana pilvipalveluna toimivan toiminnanohjausjärjestelmän valinnassa (Hashizume ym., 2013)
- Asiakasorganisaatioiden pitäisi kouluttaa työntekijöitään pilvipalvelupohjaisten toiminnanohjausjärjestelmien tietoturvariskeistä ja toimenpiteistä niiden estämiseksi (Hashizume ym., 2013)

Vaikka pilvipalvelumallilla toimivissa toiminnanohjausjärjestelmissä on useita tietoturvauhkia, on niillä myös useita tietoturvallisuusetuja on-premise-mallilla toimiviin toiminnanohjausjärjestelmiin nähden. Toiminnanohjausjärjestelmän ja sen myötä tietoturvallisuuden ulkoistaminen isolle pilvipalveluntarjoajalle voi kustannustehokkuuden lisäksi olla jopa tietoturvallisempaa kuin oman on-premise-toiminnanohjausjärjestelmän hankkiminen. Etenkin pienet tai keskisuuret yritykset suosivat pilvipalveluina toimivia toiminnanohjausjärjestelmiä, sillä oman IT-infrastruktuurin hankkiminen on-premise-mallilla toimivaa toiminnanohjausjärjestelmää varten on usein liian suuri menoerä pienemmälle yritykselle (Gupta & Misra, 2016). Pilvipalvelumallilla toimiva toiminnanohjausjärjestelmä voi myös olla kestävämpi ympäristölähtöisissä häiriötilanteissa, kuten sähkökatkoksissa tai maanjäristyksissä kuin on-premise-järjestelmä, sillä suuret pilvipalvelumallilla toimivat tietojärjestelmät voidaan yleensä replikoida nopeasti toisessa pilvipalveluntarjoajan eri sijainnissa sijaitsevassa konesalissa (Boru, Kliazovich, Granelli, Bouvry & Zomaya, 2015; Li, Yang & Yuan, 2011).

3.3 Toiminnanohjausjärjestelmien yleisen tietoturvallisuuden parantaminen

Toiminnanohjausjärjestelmien ja niitä käyttävien yritysten yleistä tietoturvallisuutta toiminnanohjausjärjestelmiin liittyen voidaan kohottaa monella eri taval-

la. Useasta paperista nousee esille seuraavat yleistä tietoturvallisuutta parantavat tekijät:

- Tietoisuuden nostaminen tietoturvallisuuden periaatteista ja tietoturvakulttuurin iskostaminen organisaatioon (Da Veiga & Eloff, 2010; Martins & Elofe, 2002)
- Toiminnanohjausjärjestelmän tai muun tietojärjestelmän vahva sisäisen hallinnan viitekehys (Chang ym., 2014)
- Roolipohjaiset käyttöoikeudet (Chang ym., 2014; She & Thuraisingham, 2007)
- Käyttömallin valinta (Abd Elmonem ym., 2016; Puthal ym., 2015)

3.3.1 Tietoturvakulttuuri

Ihminen on usein heikoin lenkki tietoturvallisuuden ketjussa (Martins & Elofe, 2002), mutta ihmislähtöisiä tietoturvauhkia voidaan mitigoida tietoturvakulttuurin avulla. Tietoturvakulttuurin iskostamisella organisaatioon voidaan minimoida tietoturvauhkia, mikä osaltaan edistää organisaation tavoitteita (Da Veiga & Eloff, 2010). Tietoturvakulttuurin iskostaminen organisaatioon vaatii käytännössä organisaation sisäistä tietoturvakoulutusta, sillä tehokas tietoturvakulttuuri vaatii jokaisen prosessin tietoturvallista suorittamista, joka taas vaatii tietämystä hyvistä tietoturvakäytännöistä (Van Niekerk & Von Solms, 2010).

3.3.2 Toiminnanohjausjärjestelmien sisäiset mekanismit

Sisäisen hallinnan viitekehykset ja roolipohjaiset käyttöoikeudet ovat esimerkkejä tietojärjestelmän kuten toiminnanohjausjärjestelmän sisäisistä mekanismeista, joilla voidaan hallita eri käyttäjien mahdollisuuksia aiheuttaa tietoturvauhkia tietojärjestelmän sisällä. Jokainen työntekijä ei tarvitse pääsyä kaikkeen toiminnanohjausjärjestelmän dataan tai toimintoihin, ja käyttöoikeuksien hallinnalla voidaan varmistaa riittävät muttei ylimääräiset oikeudet nähdä tai käsitellä toiminnanohjausjärjestelmää.

3.3.3 Käyttömallin valinta

Toiminnanohjausjärjestelmän valintaprosessissa tehdään päätös käytettävästä käyttömallista, kuten on-premise-malli tai pilvipalvelumalli. Tietoturvallisuuden kannalta vaikuttaa siltä että kaikkien paitsi suurimpien organisaatioiden kannattaa ehkä suosia pilvipalvelumallilla toimivia toiminnanohjausjärjestelmiä pilvipalveluiden yleisten tietoturvaetujen, kuten hyvän saatavuuden sekä nopean järjestelmäpalautuksen (Abd Elmonem ym., 2016; Johansson ym., 2015; Seethamraju, 2015) vuoksi. PK-yritysten resurssit huomioon ottaen pilvipalvelumalli tarjoaa yleensä kustannustehokkaammin parempaa tietoturvallisuutta PK-yrityksille (Johansson ym., 2015; Seethamraju, 2015).

4 YHTEENVETO

Tässä kandidaatintutkielmassa perehdyttiin toiminnanohjausjärjestelmiin, tietoturvallisuuteen sekä toiminnanohjausjärjestelmiin kohdistuviin tietoturvauhkiin. Tutkielmassa pyrittiin myös löytämään mitigointikeinoja kaikista tyypillisimmille toiminnanohjausjärjestelmiä uhkaaville tietoturvauhille. Tutkielman lopussa käsiteltiin myös muutamia toiminnanohjausjärjestelmien sekä niitä käyttävien yritysten yleistä tietoturvallisuutta parantavia tekijöitä.

Tutkielman alussa motivoitiin tehtävää tutkimusta sekä esiteltiin tutkielman rakenne. Tämän jälkeen siirryttiin käsittelemään toiminnanohjausjärjestelmiä. Tutkielmassa käytiin nopeasti läpi toiminnanohjausjärjestelmien historiaa, millä luotiin pohjaa modernien toiminnanohjausjärjestelmien tarkempaa käsittelyä varten. Moderneista toiminnanohjausjärjestelmistä esiteltiin yleisimpiä moduuleita, käyttömalleja sekä toiminnanohjausjärjestelmien valintaan vaikuttavia tekijöitä, kuten asiakasyrityksen liikevaihdon ja koon vaikutusta valittavaan toiminnanohjausjärjestelmään.

Toiminnanohjausjärjestelmiin keskittyvän luvun jälkeen pohjustettiin tietoturvallisuutta käsitteenä, josta siirryttiin nopeasti toiminnanohjausjärjestelmiä koskevien tietoturvauhkien käsittelyyn. Tietoturvauhkia jaoteltiin kategorioihin, kuten sisäisiin sekä ulkoisiin tietoturvauhkiin, ja näiden kategorioiden sisällä käsiteltiin myös uhkiin sopivia mitigointikeinoja. Oli yllättävää, kuinka vähän lähdekirjallisuutta löytyi tietoturvauhista, jotka koskisivat erityisesti toiminnanohjausjärjestelmiä. Tämä saattaa johtua siitä, että suurin osa toiminnanohjausjärjestelmille tyypillisistä tietoturvauhista koskee myös muita suuria tietojärjestelmiä, joilla käsitellään suuria määriä dataa, ja joilla on useita käyttäjiä saman organisaation sisällä.

Tyypillisimmiksi toiminnanohjausjärjestelmiin kohdistuviksi tietoturvauhiksi todettiin tutkielmassa ihmislähtöiset uhat, niin sisäiset kuin ulkoiset. Ihmislähtöiset tietoturvauhat koettiin muutamassa tutkimuksessa (Sumner, 2009) todennäköisimmiksi tietoturvauhiksi, ja tietoturvauhkia käsittelevää lukua varten löydetty lähdekirjallisuus tukee tätä tulosta jossain määrin. Pilvipalvelumalli tuo myös uusia tietoturvahaasteita toiminnanohjausjärjestelmiin, mutta samaan aikaan pilvipalvelumallia hyödyntämällä etenkin pienet ja keskisuuret

yritykset voivat ulkoistaa tietoturvallisuudesta huolehtimista isoille pilvipalvelutarjoajille, jotka investoivat paljon resursseja tietoturvallisuuteen (Johansson ym., 2015).

Toiminnanohjausjärjestelmien ja niitä käyttävien yritysten yleistä tietoturvallisuutta kohottavia tapoja ja valintoja löydettiin useita. Tietoturvakulttuurin iskostaminen organisaatioon, käyttöoikeuksien roolipohjainen hallinta sekä sisäisen hallinnan viitekehyksen käyttöönotto olivat esimerkkejä näistä tavoista ja keinoista.

Hyvänä jatkotutkimuskohteena tutkielman aihepiiriin liittyen voisi olla erityisesti toiminnanohjausjärjestelmiä kohtaavien tietoturvauhkien tutkimusta. Tällaisista ERP-spesifeistä tietoturvauhista löytyi melko vähän lähdekirjallisuutta, ja olisi hyvin mielenkiintoista perehtyä aiheeseen enemmän. Olisi myös kiinnostavaa nähdä lisätutkimusta siitä, miten toiminnanohjausjärjestelmien jatkuvasti suositumpi pilvipalvelumalli vaikuttaa toiminnanohjausjärjestelmien tietoturvallisuuteen.

LÄHTEET

Abd Elmonem, M. A., Nasr, E. S., & Geith, M. H. (2016). Benefits and challenges of cloud ERP systems – A systematic literature review. *Future Computing and Informatics Journal*, *1*(1), 1–9. https://doi.org/10.1016/j.fcij.2017.03.003

Aptean. (2021). Ready for Digital Transformation with Aptean ERP Solutions. Noudettu 5. marraskuuta 2021, osoitteesta Aptean.com website: https://www.aptean.com/en-US/solutions/erp

Boehm, H. (2020). The Difference Between MRP I and MRP II. Noudettu 31. lokakuuta 2021, osoitteesta Software Connect website: https://softwareconnect.com/manufacturing/mrp-i-vs-mrp-ii/

Boru, D., Kliazovich, D., Granelli, F., Bouvry, P., & Zomaya, A. Y. (2015). Energy-efficient data replication in cloud computing datacenters. *Cluster Computing*, *18*(1), 385–402. https://doi.org/10.1007/s10586-014-0404-x

Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, *51*(2), 187–205. https://doi.org/10.1016/j.im.2013.11.002

Chou, S.-W., & Chang, Y.-C. (2008). The implementation factors that influence the ERP (enterprise resource planning) benefits. *Decision Support Systems*, *46*(1), 149–157. https://doi.org/10.1016/j.dss.2008.06.003

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Duan, Z., Yuan, X., & Chandrashekar, J. (2008). Controlling IP Spoofing through Interdomain Packet Filters. *IEEE Transactions on Dependable and Secure Computing*, *5*(1), 22–36. https://doi.org/10.1109/TDSC.2007.70224

Gupta, S., & Misra, S. C. (2016). Compliance, network, security and the people related factors in cloud ERP implementation. *International Journal of Communication Systems*, *29*(8), 1395–1419. https://doi.org/10.1002/dac.3107

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

Jacobs, F. R., & Weston, F. C. T. (2007). Enterprise resource planning (ERP)—A brief history. *Journal of Operations Management*, *25*(2), 357–363. https://doi.org/10.1016/j.jom.2006.11.005

Johansson, B., Alajbegovic, A., Alexopoulo, V., & Desalermos, A. (2015). Cloud ERP Adoption Opportunities and Concerns: The Role of Organizational

Size. *2015 48th Hawaii International Conference on System Sciences*, 4211–4219. https://doi.org/10.1109/HICSS.2015.504

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Klaus, H., Rosemann, M., & Gable, G. G. (2000). What is ERP? *Information Systems Frontiers*, *2*(2), 141–162. https://doi.org/10.1023/A:1026543906354

Li, W., Yang, Y., & Yuan, D. (2011). A Novel Cost-Effective Dynamic Data Replication Strategy for Reliability in Cloud Data Centres. *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 496–502. https://doi.org/10.1109/DASC.2011.95

Luo, W., & Strong, D. M. (2004). A framework for evaluating ERP implementation choices. *IEEE Transactions on Engineering Management*, *51*(3), 322–333. https://doi.org/10.1109/TEM.2004.830862

Mabert, V. A., Soni, A., & Venkataramanan, M. A. (2003). The impact of organization size on enterprise resource planning (ERP) implementations in the US manufacturing sector. *Omega*, *31*(3), 235–246. https://doi.org/10.1016/S0305-0483(03)00022-7

Martins, A., & Elofe, J. (2002). Information Security Culture. Teoksessa M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Toim.), *Security in the Information Society: Visions and Perspectives* (ss. 203–214). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-35586-3_16

Panorama Consulting Group. (2021). *2021 ERP Report*.

Panorama Consulting Solutions. (2017). *2017 ERP Report*.

Panorama Consulting Solutions. (2019). *2019 ERP Report*.

Ptak, C. A. (1991). MRP, MRP II, OPT, JIT, and CIM - Succession, Evolution, or Necessary Combination. *Production and Inventory Management Journal*, *32*(2), 7.

Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). Cloud Computing Features, Issues, and Challenges: A Big Picture. *2015 International Conference on Computational Intelligence and Networks*, 116–123. https://doi.org/10.1109/CINE.2015.31

Saa, P., Costales, A. C., Moscoso-Zea, O., & Lujan-Mora, S. (2017). Moving ERP Systems to the Cloud—Data Security Issues. *Journal of Information Systems Engineering & Management*, *2*(4). https://doi.org/10.20897/jisem.201721

Seethamraju, R. (2015). Adoption of Software as a Service (SaaS) Enterprise Resource Planning (ERP) Systems in Small and Medium Sized Enterprises (SMEs). *Information Systems Frontiers*, *17*(3), 475–492. https://doi.org/10.1007/s10796-014-9506-5

She, W., & Thuraisingham, B. (2007). Security for Enterprise Resource Planning Systems. *Information Systems Security*, *16*(3), 152–163. https://doi.org/10.1080/10658980701401959

Shehab, E. M., Sharp, M. W., Supramaniam, L., & Spedding, T. A. (2004). Enterprise resource planning: An integrative review. *Business Process Management Journal*, *10*(4), 359–386. https://doi.org/10.1108/14637150410548056

Shen, Y.-C., Chen, P.-S., & Wang, C.-H. (2016). A study of enterprise resource planning (ERP) system performance measurement using the quantitative balanced scorecard approach. *Computers in Industry*, *75*, 127–139. https://doi.org/10.1016/j.compind.2015.05.006

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, *26*(1), 2–12. https://doi.org/10.1080/10580530802384639

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

von Solms, R. (1998). Information security management (3): The Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*, *6*(5), 224–225. https://doi.org/10.1108/09685229810240158

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

Wang, L., von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud Computing: A Perspective Study. *New Generation Computing*, *28*(2), 137–146. https://doi.org/10.1007/s00354-008-0081-5

Weng, F., & Hung, M.-C. (2014). Competition and Challenge on Adopting Cloud ERP. *International Journal of Innovation, Management and Technology*. https://doi.org/10.7763/IJIMT.2014.V5.531

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security*. Cengage Learning.