Sebastian Saari

TIETOTURVAHAASTEIDEN HUOMIOIMINEN ERP-JÄRJESTELMÄHANKKEISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Saari, Sebastian
Tietoturvahaasteiden Huomioiminen ERP-Järjestelmähankkeissa
Jyväskylä: Jyväskylän yliopisto, 2020, s. 33
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Marttiin, Pentti

Tämän tutkielman tarkoituksena on tunnistaa ja määritellä ERP-järjestelmiä koskevia tietoturvahaasteita ja niiden tietoturvaan vaikuttavia tekijöitä, joita huomioimalla voidaan ERP-järjestelmähankkeissa toteuttaa mahdollisimman turvallisia järjestelmäratkaisuja ja tietoturvan mukaista toimintaa. Lisäksi tutkielmassa perehdytään tietoturvaan ja siihen vaikuttamiseen yleisemmällä tasolla tietoturvaa tavoittelevien organisaatioiden näkökulmasta. ERP-järjestelmät ovat organisaatioiden liiketoiminnan kannalta kriittisiä järjestelmäkokonaisuuksia, joiden arkaluontoisen datan turvaaminen on merkittävää riskien välttämiseksi ja tietoturvan ylläpitämiseksi. Tutkielmassa käsitellään ERP-järjestelmien tietoturvaa pilvipohjaisten ERP-järjestelmien, järjestelmien tietoturvaa edistävien keinojen, ERP-järjestelmän käyttäjien, sekä tietoturvaan vaikuttavien säädösten näkökulmasta.

Asiasanat: Tuotannonohjausjärjestelmä, tietoturva, kyberturvallisuus, ERP-hanke

ABSTRACT

Saari, Sebastian
Identifying information security challenges of ERP-system projects
Jyväskylä: University of Jyväskylä, 2020, pp. 33
Information systems, Bachelor's Thesis
Supervisor(s): Marttiin, Pentti

The goal of this thesis is to identify and define information security challenges as a part of ERP-system projects to develop secure systems and enhance organisational information security. In addition, the thesis aims to generally focus on information security and its different aspects from the perspective of organisations aiming to improve it. ERP- systems are crucial for organisations different business processes that manage critical data, which should not be compromised. The thesis observes information security of ERP-systems from several different perspectives such as security of cloud-based ERP-systems, practical actions that improve information security, security of system users and different standards and policies that affect information security.

Keywords: Enterprise resource planning system, information security, cyber security, ERP- project

KUVIOT

KUVIO 1 Tiedon Sijainti ja riskinhallinnan merkitys 15

TAULUKOT

TAULUKKO 1 Kyberuhkien luokittelu 17

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 4

SISÄLLYS 5

1 JOHDANTO 6

2 ERP-JÄRJESTELMÄT JA TIETOTURVAHAASTEET 9
2.1 Tuotannonohjausjärjestelmä 9
2.2 Tietoturva 10
2.3 ERP-Hankkeet 10

3 PILVIPOHJAISET ERP-JÄRJESTELMÄT 12
3.1 Pilvipohjaiset ERP-järjestelmät 12
3.2 In-house toteutus 13
3.3 Pilvipohjaiset ERP-järjestelmät ja tietoturva 13
3.4 Datan sijainti 14

4 ERP-JÄRJESTELMÄN TIETOTURVAAN VAIKUTTAMINEN 16
4.1 Tietoturvaa koskevien riskien tunnistaminen 16
4.2 Käyttöoikeudet ja tunnistautuminen 18
4.3 Tietoturvapäivitykset 18
4.4 Tietoturvatestaus ja auditointi 19

5 TIETOTURVA JA ERP-JÄRJESTELMÄN KÄYTTÄJÄT 21
5.1 Tietoturvakäytäntö 21
5.2 Tietoturva asenteet ja – tietoisuus 22
5.3 Organisaation sisäiset tietoturvariskit 22
5.4 Tietoturva kouluttaminen 23

6 LAINSÄÄDÄNTÖ JA STANDARDIT 25
6.1 ISO/IEC 27000 25
6.2 Tietosuoja 26
6.3 NIST kyberturvaviitekehys 27

7 YHTEENVETO JA POHDINTA 28

LÄHTEET 30

1 JOHDANTO

Tämän tutkielman tarkoituksena on perehtyä tuotannonohjausjärjestelmien (Enterprice resource planning systems, ERP-systems) tietoturvaan ja siihen vaikuttaviin tekijöihin, sekä tietoturvaan ilmiönä. Nykyään teknologian ja tiedon merkitys kasvaa alati osana yritysten liiketoimintaa. Yhä useammat yritykset ovat riippuvaisia teknologian tarjoamista mahdollisuuksista ja tietojenkäsittelystä osana heidän liiketoimintaansa. Toisaalta tämä ilmiö myös korostaa tiedon saatavuuden ja turvaamisen merkitystä entisestään. Lehto, Limnéll, Innola, Pöyhönen, Rusi ja Salminen (2017) arvioivat vuoden 2017 Suomen kyberturvallisuuden nykytilan kartoituksessaan kyberturvallisuuden roolin korostuvan ja hyökkäyksien lisääntyvän ja monimutkaistuvan entisestään tulevaisuudessa.

Tutkielmassa pohditaan tietoturvaa ERP-järjestelmähankkeiden näkökulmasta, eli mitä eri tietoturvahaasteita organisaatioiden tulee tunnistaa osana hankkeitansa, jotta järjestelmä voidaan kehittää organisaation toimintojen ja niiden tietoturvavaatimuksien mukaiseksi. Tämän lisäksi tutkielmassa perehdytään tietoturvaan yleisesti sen eri tasoilla pääasiassa itse ERP-hankkeita toteuttavien organisaatioiden näkökulmasta. ERP- järjestelmät käsittelevät alati yritysten toiminnan kannalta kriittistä dataa, minkä vääriin käsiin joutuminen tai muuten vaarantuminen voi johtaa vakaviin seurauksiin. ERP-järjestelmät ovat keskeinen osa organisaation avainliiketoimintoja, ja ne käsittelevät paljon liiketoiminnallisesti arkaluontaista dataa, kuten yrityssalaisuuksia, taloudellisia lukuja, sekä työntekijöiden ja asiakkaiden tietoja, minkä vuoksi ne ovat hyviä kohteita potentiaalisille hyökkäyksille (Rîndaşu, 2018).

Tutkielman päätutkimuskysymyksenä toimii, mitä tietoturvaan vaikuttavia tekijöitä organisaatioiden tulee huomioida osana ERP-hankkeitansa kehittääkseen mahdollisimman turvallisia järjestelmäratkaisuja. Täydentävänä kysymyksenä toimii, kuinka organisaatio voi parantaa omaa tietoturvaa koskevaa toimintaansa osana järjestelmien käyttöä ja samalla tunnistaa mahdollisia tietoturvariskejä. Tutkielmassa pyritään huomioimaan tietoturvaa kokonaisvaltaisesti, eikä ainoastaan teknisellä tasolla. Tutkimuskysymys on merkittävä ja

hyödyllinen tietoturvan kehittämisen kannalta lisäämällä siihen ERP-järjestelmien näkökulman ja luomalla monipuolisen kuvauksen sen eri ulottuvuuksista.

Tutkielma toteutettiin kirjallisuuskatsauksena, joka jaoteltiin eri tasoihin. Aluksi perehdyttiin ERP-järjestelmien ja -hankkeiden luonteeseen, jotta voitaisiin paremmin ymmärtää tietoturvan merkitystä osana niitä. Seuraavaksi tutustuin tietoturvaan ja sen eri ulottuvuuksiin kokonaisvaltaisesti pitäen sisällään muun muassa määrittelyn, tekniset ominaisuudet, riskien arvioinnin ja tunnistamisen, käyttäjien merkityksen, sekä sitä koskevat säädökset. Tämän jälkeen siirryin tarkastelemaan suoraan aiheeseen keskittyvää ERP-järjestelmien tietoturvaa koskevaa kirjallisuutta. ERP-järjestelmien turvallisuutta käsittelevää kirjallisuutta on julkaistu melko rajoitettu määrä, ja lähivuosien teokset keskittyvät lähes ainoastaan pilvipohjaisten ERP-ratkaisujen myötä ilmenneisiin haasteisiin, mikä tuotti haasteita kirjallisuuskatsauksen toteutukseen. Lopuksi perehdyin kyseisiä teemoja osittain yhdistävään ja soveltavaan kirjallisuuteen, kuten yleisesti tietojärjestelmien turvallisuuteen, sekä tietojärjestelmien turvallisuusriskejä käsitteleviin teoksiin ja pyrin soveltamaan niitä ERP-järjestelmähankkeiden näkökulmaan. Tutkielmassa tieteellisten lähteiden etsimiseen hyödynnettiin eri tieteellisten julkaisujen tietokantoja kuten IEEE Xplore Digital Library, Google Scholar ja Jykdok, joista suurin osa tutkielmassa hyödynnetystä julkaisuista on peräisin. Lisäksi tutkielmassa hyödynnettiin myös useiden eri teknologiaan erikoistuneiden virastojen ja järjestöjen julkaisuja kuten kansainvälisen standardisoimisjärjestön tietoturva-määritelmiä ja -standardeja, Suomen tietoturvavaltuutetun palveluita sekä EU:n tietosuoja-asetusta. Vähemmän tieteellisiä käytetyistä lähteistä olivat muutamat ERP-järjestelmätoimittajien ja ERP-järjestelmien turvallisuuteen erikoistuneiden yrityksien julkaisut.

Tutkielman ensimmäisessä varsinaisessa luvussa määritellään sen keskeisimmät termit, kuten tuotannonohjausjärjestelmä ja tietoturva. Lisäksi ensimmäisessä luvussa kuvataan myös lyhyesti ERP-järjestelmähankkeiden ominaisuuksia ja luonnetta. Toisessa luvussa käsitellään lähivuosina huomattavasti yleistyneitä pilvipohjaisia ERP-ratkaisuja, sekä verrataan niitä perinteisempiin toteutuksiin ja määritellään näiden vaikutusta tietoturvaan. Pilvipohjaiset ERP-toteutukset käsitellään tutkielman alkuvaiheessa niiden nykyisen merkityksen vuoksi. Kolmannessa luvussa taas käsitellään konkreettisia keinoja, joilla organisaatiot voivat vaikuttaa ERP-järjestelmiensä tietoturvaan, kuten riskien tunnistaminen, käyttöoikeuksien hallinta, tietoturvapäivitykset ja tietoturvatestaaminen. Tämä on tutkielman käytännönläheisin luku. Neljäs luku pitää sisällään ERP-järjestelmien käyttäjiä ja organisaation tietoturvakäytänteitä koskevia aiheita, kuten tietoturva-asenteet, organisaation sisäisitä toimista aiheutuvat riskit, sekä henkilökunnan tietoturvakouluttaminen. Yleensä tietoturvan inhimilliset aspektit jäävät teknisten ominaisuuksien varjoon, minkä vuoksi tutkielmassa pyrittiin huomioimaan niiden eri ominaisuuksia kattavasti. Viidennessä luvussa perehdytään lyhyesti tietoturvan ja tietoturvan kannalta keskeisiin säädöksiin, kuten ISO standardit ja EU:n tietoturva asetus GDPR. Lisäksi kansainvälisen näkemyksen saamiseksi tutkimuksessa perehdytään useaan Yhdysvalloissa toimivan NIST (National Institute of Standards and Technology) viraston julkaisuihin, kuten NIST

kyberturvallisuus viitekehykseen. Kuudennessa sisältöluvussa yhdistetään tutkielman pääpiirteet, sekä pohdin aihetta ja tutkielman toteutusta lyhyesti omasta näkökulmastani. Lopuksi vielä arvioin aihepiirin mahdollisia tulevaisuuden suuntauksia ja listaan tutkielmassa käytetyt lähteet.

2 ERP-JÄRJESTELMÄT JA TIETOTURVAHAASTEET

Tässä luvussa avataan tarkemmin tuotannonohjausjärjestelmän ja tietoturvan määritelmiä ja niihin liittyviä teemoja, sekä avataan lyhyesti ERP- hankkeita ja niille ominaisia piirteitä. Alan kirjallisuudessa voidaan käsitellä varsinkin tietoturvallisuutta erittäin laajasti ja vaihtelevasti, minkä vuoksi on keskeistä rajata sen määritelmä tutkimuksen ja ERP-järjestelmien kannalta merkitykselliseksi. Tietoturvallisuudella on myös sivuavia ja päällekkäisiä termejä, kuten kyberturvallisuus, joten sen suhde tietoturvaan tulee myös määrittää osana tutkielmaa.

2.1 Tuotannonohjausjärjestelmä

ERP- lyhenne viittaa englannin kielen sanoihin enterprise resource planning, mikä tarkoittaa tuotannonohjausta. Yleisesti tuotannonohjausjärjestelmät kuvataan olevan yritysten laajoja järjestelmäkokonaisuuksia, jotka yhdistävät ja mahdollistavat eri liiketoimintaprosesseja. Addo-Tenkorang ja Helo (2011) kuvaavat ERP-järjestelmän tarjoavan yritykselle mahdollisuuden integroida kaikki keskeiset liiketoimintaprosessit parantaakseen tehokkuutta ja ylläpitääkseen parempaa kilpailullista asemaa. Nykyisessä liiketoimintaympäristössä datan ja sen käsittelyn merkitys korostuu osana perinteisiä liiketoiminnallisia toimintoja, kuten raaka-aineiden ja komponenttien valmistusta, varastonhallintaa, kirjanpitoa, henkilöstön hallintoa, sekä jakelukanavia. Paitsi, että ERP- järjestelmät mahdollistavat ja yhdistävät näitä toimintoja, tarjoavat ne myös kattavasti informaatiota paremman päätöksenteon, kilpailukyvyn ja logistiikan saavuttamiseksi (Rashid, Syracuse, Patrick, 2002). Alciviar ym. (2015) vuorostaan kuvaa ERP-järjestelmien hyötyjen olevan tarpeettoman datan väheneminen, reaaliaikaisen informaation saaminen, prosessien standardisointi, sekä tiedon virtaamisen ja kommunikaation paraneminen henkilökunnan välillä. ERP-ohjelmistoilla on maailmanlaajuisesti valtavat markkinat. Vuonna 2018 ERP-järjestelmämarkkinoiden arvioitu arvo oli yhteensä yli 91 miljardia dollaria ja sen on arvioitu nousevan vuoteen 2023 mennessä lähes 97 miljardiin dollariin (Statista, 2019). Vuonna 2007 julkaistussa tutkimuksessaan She ja Thuraisingham (2007) määrittelevät merkittävimmäksi ERP-toimittajaksi SAP:in, sekä arvioivat myös Oraclen ja Microsoftin olevan noususSa ERP-markkinoiden huipulle. Yli vuosikymmentä myöhemmin voidaan heidän arvionsa todeta onnistuneeksi. Ohjelmistoalan teknologiamarkkinoita tutkiva yritys listasi suurimpia ERP-toimittajia markkinaosuuden perusteella, joista suurimpana toimi yhä SAP ja toiseksi suurimpana Oracle. Myös Microsoftilla oli yhä suuri osuus muiden kilpailijoidensa joukossa. (AppsRunTheWorld, 2018)

2.2 Tietoturva

Tietoturvaa voidaan Whitmanin ja Mattordin (2011) mukaan kuvata informaation ja sen käsittelyyn käytettävien kriittisten elementtien turvaamisena. Näitä elementtejä voivat olla metodit tallentaa ja siirtää tietoa, tai esimerkiksi tietojen käsittelyyn käytetyt järjestelmät ja laitteisto. Yleisemmällä tasolla kansainvälinen standardisoimisjärjestö ISO määrittää tietoturvan olevan informaation luottamuksellisuuden, yhtenäisyyden, eheyden ja saatavuuden ylläpitoa. (ISO 20252, 2019). ISO on myös määrittänyt lukuisia yleisiä standardeja tietoturvan ylläpitämiseen. Yleisesti tietoturva käsittelee nimenomaan itse datan turvaamista.

Toinen keskeinen tietoturvaan liittyvä termi on kyberturvallisuus. Kyberturvallisuus määritellään yleensä laajempana kokonaisuutena, joka keskittyy muihinkin alueisiin kuin itse dataan. Kansainvälinen televiestintäliito ITU määrittää kyberturvallisuuden olevan kokoelma työkaluja, käytäntöjä, konsepteja, ohjeita, riskinhallintamenetelmiä, toimintoja, koulutusta, parhaita käytänteitä ja teknologioita, joita voidaan käyttää suojaamaan kyberympäristöä, organisaatioita ja käyttäjien tietoja (ITU, 2020). ISO vuorostaan määrittelee kyberturvallisuuden yksinkertaisemmin olevan IT-järjestelmien suojaamista hyökkäyksiltä, laitteiston vaurioitumiselta, ohjelmiston vahingoittumiselta, informaation vahingoittumiselta, sekä palveluiden häirinnältä tai väärinkäytöltä (ISO 27000, 2018). Tietoturvalla on siis paljon päällekkäisyyttä ja yhtäläisyyttä kyberturvallisuuden kanssa. Tässä tutkimuksessa keskitytään erityisesti tietoturvaan, mutta sivutaan myös kyberturvallisuuden eri ominaisuuksia.

2.3 ERP-Hankkeet

ERP-järjestelmähankkeet ovat pitkäkestoisia ja monimutkaisia prosesseja, joissa yleisesti ilmenee haasteita. Koska ERP-järjestelmät ovat erittäin tärkeitä liiketoiminnan kannalta, voi epäonnistuneella hankkeella olla suuria vaikutuksia organisaation taloudelliseen toimintakykyyn (Wong et.al, 2005). Phaphoom, Qu, Khaeksong ja Saelee (2018) kuvaavat ERP-hankkeita haastaviksi ja paljon organisaation resursseja kuluttaviksi. Heidän mukaansa keskeisiä syitä hankkeiden epäonnistumisille ovat ongelmat organisaation rakenteessa, projektien epärealistinen ajoittaminen, sekä projektin aikana ilmenneet uudet vaatimukset ja projektin laajuus. Tutkimuksessaan Ahmad, Pinedo ja Cuenca (2013) vuorostaan määrittelevät ERP-implementoinnin onnistumiseen liittyviksi keskeisimmiksi kriittisiksi menestystekijöiksi johdon tuen, projektitiimitaidot, työkulttuurin muutoksen, vaatimusten riittävän määrittelyn, onnistuneen viestinnän, sekä kokeneiden projektipäällikköjen ja konsulttien hyödyntämisen.

ERP-hankkeissa järjestelmän implementointi voidaan toteuttaa usean eri strategian kautta, riippuen järjestelmän ja projektin ominaisuuksista. Perinteisesti strategiat on jaoteltu ”Big Bang” implementointiin, jossa uusi järjestelmä otetaan käyttöön kerralla, vaiheittaiseen (phased) implementointiin, jossa

järjestelmä otetaan käyttöön toiminto kerrallaan ja eri aikaan organisaation eri alueilla (Nagpal ym. 2015). Khanna ja Arneja (2012) määrittelevät myös näiden lisäksi mahdollisia implementointistrategioita olevan päällekkäinen (parallel) käyttöönotto, jossa uutta ja vanhaa järjestelmää käytetään samaan aikaan hankkeesta seuraavien riskien minimoimiseksi; prosessiketjun mukainen (process line) implementointi, jossa järjestelmä otetaan käyttöön organisaation tuotteiden ja niiden tuotannon mukaan vaiheittain; sekä hybridi-strategia, jossa voidaan hyödyntää useita eri strategioita organisaation ja projektin vaatimusten mukaan.

3 Pilvipohjaiset ERP-järjestelmät

ERP-hankkeiden alkutaipaleella on hyvä määrittää, mitkä ovat organisaation järjestelmätarpeet. Tässä luvussa käydään läpi eroavaisuuksia ERP-järjestelmätoteutuksien välillä, sekä niiden mahdollisia vaikutuksia tietoturvaan. Yleisesti ERP-toteutukset voidaan jaotella perinteisiin in-house ratkaisuihin, sekä alati yleistyviin pilvipohjaisiin ratkaisuihin, sekä näitä yhdistäviin hybridiratkaisuihin. Erilaisilla ja erikokoisilla organisaatioilla voi olla hyvinkin erilaisia tarpeita järjestelmälle. Tietoturvan kannalta yksi keskeisimmistä painopisteistä koskee datan tallettamista ja sen sijaintia. Erilaisissa ratkaisuissa voidaan dataa tallettaa tarpeen mukaan eri sijainteihin, sekä käsitellä sitä erilaisilla toimintamalleilla.

3.1 Pilvipohjaiset ERP-järjestelmät

Duanin, Fakerin, Fesastin ja Sturatin (2013) mukaan pilvipohjaiset ERP-järjestelmät toteutetaan yleisesti SaaS (software as a service) mallin mukaan, missä palveluntarjoaja tarjoaa organisaatiolle verkon välityksellä käyttöön koko ERP- sovelluksen, joka vuorostaan pyörii palveluntarjoajan omien resurssien varassa. Pilvitoteutus voidaan myös erikseen luokitella julkiseen-, yksityiseen- ja hybridipilveen. Julkisen pilven ratkaisuissa on pilven infrastruktuuriin jaettu useampien tahojen dataa ja se on helpommin saatavilla. Yksityisessä pilvessä vuorostaan data sijaitsee muista erillisessä infrastruktuurissa. Hybridipilvitoteutuksessa voidaan vuorostaan yhdistää näitä molempia, joissa arkisemmat tarpeet toteutetaan julkisessa pilvessä ja arkaluontoisemmat ja kriittisemmät toiminnot toteutetaan yksityisessä pilvessä. Pilvipohjaisten ratkaisujen vahvuutena on niiden vaivattomampi ylläpito, skaalautuvuus, sekä vähäisemmät kustannukset. (Duan ym., 2013)

Nykyään on paljon ERP-hankkeita, joissa pyritään siirtämään perinteisiä ERP-järjestelmäratkaisuja pilveen. Myös Guptan, Misran ja Akashin(2017) mukaan pilvipohjaisten järjestelmien suosio on noussut niiden kustannustehokkuuden ja helpon ylläpidon vuoksi, mikä vapauttaa organisaation resursseja muiden tavoitteiden saavuttamiseen. Heidän mukaansa pilvipohjaisissa palveluissa on tietoturvan näkökulmasta suuri vastuu palveluntarjoajalla, sillä datan hallinnointi on heidän vastuullaan (Gupta, Misra, Akash, 2017). Saeed, Juell-skielse, Gustaf ja Uppströn (2012) käsittelevät tutkimuksessaan ERP-järjestelmien siirtämistä pilveen ja sen mukanaan tuomia haasteita. Tutkimuksessa pilveen siirtymiseen ajaviksi tekijöiksi mainitaan esimerkiksi pilvipalveluiden tuoma liiketoiminnallinen joustavuus, sekä palveluntarjoajan toimesta toteutuva järjestelmän jatkuva kehitys ja laajennus ilman monimutkaisia hankkeita. Lisäksi myös he painottavat pilvipalveluiden ylläpidon vaivattomuutta ja kustannustehokkuutta, sekä skaalautuvuutta organisaation tarpeiden mukaisiksi.

3.2 In-house toteutus

Duan ym. (2013) tutkimuksen mukaan perinteisemmällä mallilla ERP-järjestelmä voidaan toteuttaa paikallisesti (on-premise) organisaation sisällä. Tässä mallissa ohjelmistot ja palvelimet pyörivät organisaation omilla laitteistoilla ja palvelimet sijaitsevat organisaation omien tilojen sisällä. Perinteinen toteutus voidaan tehdä myös siirtämällä palvelimien ylläpito ulkoiselle taholle (hosted), tai hybridiratkaisuna pitämällä osa toiminnoista talon sisällä ja osa pilvessä. Perinteisemmille toteutuksille on ominaista suuremmat mahdollisuudet kustomoida järjestelmää. (Duan ym., 2013) Pilvipohjaisiin järjestelmätoteutuksiin siirtyessä in-house toteutuksia koskevia haasteita ovat Saeed ym. (2012) mukaan riippuvuus vanhojen järjestelmien toiminnasta, sekä järjestelmiä päivittäessä ilmenevät muutosta koskevat haasteet. Myös datan saatavuus ja riippuvuus palveluntarjoajasta voivat olla syitä perinteisiin järjestelmiin pitäytymiselle.

3.3 Pilvipohjaiset ERP-järjestelmät ja tietoturva

Perinteisellä- ja pilviratkaisuilla on tietoturvan näkökulmasta omat vahvuutensa ja heikkoutensa. Yleisesti suuremmilla yrityksillä on käytössään arkaluonteisempaa dataa, minkä vuoksi on pilveen siirtymisen myötä ilmeneviin tietoturva haasteisiin keskittyminen niille kriittisempää ja suurempi haaste (Duan ym., 2013). Saa ym. (2017) lisäävät tähän, että suuremmat yritykset ovat yleisesti varovaisempia siirtäessään kriittisiä toimintojaan pilveen, sekä yleensä hyödyntävät sisäisiä tietoturvaasiantuntijoita luodakseen itselleen mahdollisimman turvallisia ratkaisuja. Sekä Saan ym. (2017), että Guptan & Misran (2016) tutkimukset toteavat, pienten ja keskisuurten yrityksien voivan hyötyä enemmän pilvipohjaisista ratkaisuista suurempiin yrityksiin verrattuna. Syitä tälle on pk-yritysten rajoitetut taloudelliset resurssit, rajatut mahdollisuudet infrastruktuurille ja yleisesti toimintojen yksinkertaisuus.

Yksi suurimmista eroista ratkaisujen välillä on pilvipalvelupohjaisessa ERP-järjestelmissä ilmenevä organisaation vähäinen mahdollisuus vaikuttaa datan valvontaan. Pilvipohjaisten ERP-ratkaisujen tietoturvahaasteita käsittelevässä tutkimuksessaan Saa ym. (2017) toteaa pilviratkaisujen myötä ilmeneviksi haasteiksi muun muassa datan saatavuuden kannalta suuren riippuvuuden palveluntarjoajasta, sekä mahdolliset eheys ja turvallisuushaasteet, joita voi seurata arkaluontoisen datan tallennuksen ja käsitellyn valvonnan vähäisyydestä. Myös äärimmäisissä tilanteissa on mahdollisuus datan vuotamiseen kolmansille osapuolille palveluntarjoajan toimesta, tai laajojen datavuotojen kautta, johon organisaation on vaikea itse päästä vaikuttamaan. Näiden riskien minimoimiseen Saa ym. (2017) esittävät suosituksia yrityksille, jotka ovat siirtämässä ERP-toimintojaan pilveen, kuten tarkkojen palvelutasosopimusten ja käytänteiden määrittelyn palveluntarjoajan kanssa, joissa ilmenee tarkat vaatimukset ja määrittelyt datan luonteelle ja salaukselle. He myös korostavat palveluntarjoajan ja organisaation

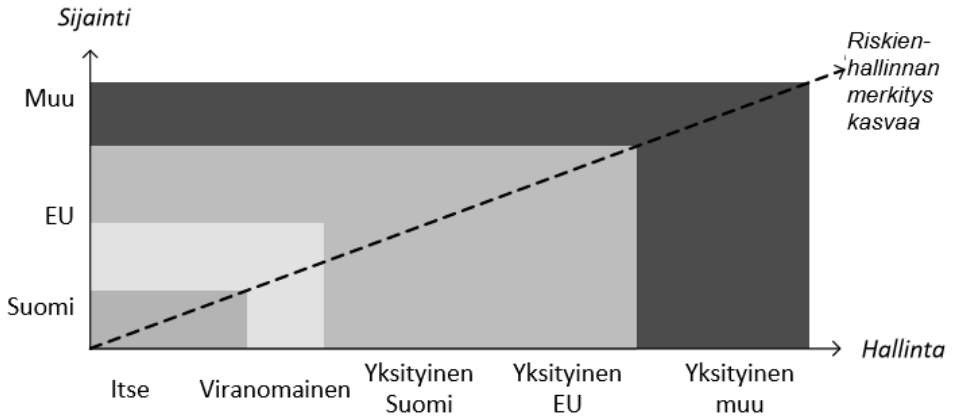
välisen yhteistyön ja luottamuksen merkitystä. Lisäksi he kehottavat hyödyntämään organisaation sisäisiä turvallisuus asiantuntijoita ja tiimejä arvioidessa palveluntarjoajan luotettavuutta ja toimintamalleja. Lopuksi he painottavat myös organisaation sisäisen henkilökunnan tietoturva koulutuksen merkitystä. Näiden lisäksi pilvipohjaisiin ERP-järjestelmiin siirtyessä Rîndaşu (2019) kehottaa organisaatiota hyödyntämään nykyisiä tietoturvatoiminnan parhaita käytänteitä, sekä luomaan organisaatioon tehokkaan riskinhallinnan datavuotojen kaltaisien tilanteiden varalle. Hän myös toteaa pilvipohjaisten ratkaisujen olevan vielä suhteellisen nuori teknologia, minkä vuoksi tulevaisuudessa todennäköisesti ilmenee uudenlaisia haavoittuvaisuuksia niihin liittyen. Vielä näihin lisätäkseen Saeed ym. (2012) toteavat turvallisuus ja yksityisyys riskien olevan yksi keskeisimmistä haasteista pilvipalveluihin siirtyessä, niiden tarjotessa uusia mahdollisuuksia väärinkäytölle ja organisaatioiden ollessa vielä kokemattomia niiden toiminnan suhteen. Myös yleensä organisaation koettu turvallisuus saattaa laskea kriittisten tietovarantojen ylläpidon siirtyessä ulkopuolisille tahoille. Lisäksi riippuvuus palveluntarjoajasta voi johtaa tilanteeseen, jossa palveluntarjoajan vaihtaminen voi olla erittäin työlästä ja riskialtista. He myös korostavat tietoturvariskien yltämistä myös teknologisen ulottuvuuden ulkopuolelle muun muassa laillisiin ja organisaationaalisiin aihepiireihin.

3.4 Datan sijainti

Pilvipohjaisia ratkaisuja toteuttaessa on hyvä kiinnittää huomiota käytettyjen tietovarastojen sijaintiin. Eri maantieteellisillä alueilla sijaitsevien datakeskuksien hyödyntäminen voi vaikuttaa datan tietoturvaan ja sen käsittelytoimenpiteisiin. Lisäksi sijainti vaikuttaa myös yleisesti datakeskuksen toimintaan ja täten myös datan saatavuuteen. Padhy, Patra ja Sapapathy (2011) toteavat pilvipalveluiden tietoturvaongelmia käsittelevässä tutkimuksessaan, että yksi sijaintia koskeva haaste on mahdollinen epävarmuus datan tarkasta sijainnista, sekä tietämättömyys dataan fyysisestä käsiksi pääsystä. Suurimmilla palveluntarjoajilla on datakeskuksia maailmanlaajuisesti. Maantieteellisesti vaihtelevat lainsäädännöt ja määräykset voivat tuottaa ongelmia esimerkiksi koskien yksityisyyttä tai sellaista arkaluonteista dataa, jonka ei haluta päätyvän tietyille maantieteellisille alueille esimerkiksi EU:n ulkopuolelle. Haasteita voi ilmetä myös erilaisissa oikeudellisissa toimenpiteissä, riippuen siitä toteutetaanko tietojen käsittelymaan vai tietojen sijaintimaan lainsäädäntöä. (Padhy, Patra & Apapathy, 2011)

Saeed ym. (2012) kertovat eri valtiolla olevan omat linjauksensa datan sijaintia ja sen turvallista tallettamista koskien. He mainitsevat epävarmuuden datan sijainnista olevan yksi keskeisimmistä syistä välttää pilvipohjaisiin ERP-järjestelmiin siirtymistä. Esimerkkinä he mainitsevat Ruotsin lainsäädännön, joka rajoittaa tiukasti yritysten datan tallettamista EU:n ulkopuolelle. Suomessa asiaa käsittelevä valtiovarainministeriön linjaus ”Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta” (2018) määrittelee julkisen hallinnon tiedonkäsittelyä ja

sen sijoittamista eri maantieteellisille alueille. Yleisesti linjauksen tarkoituksena on hallita pilvipalveluiden käyttöä ja sitä koskevia riskejä. Linjauksessa luokitellaan riskienhallinnan merkitystä suhteessa tiedon tallentamissijaintiin ja tietoa tallentavaan organisaation. Linjauksessa julkaistussa yksinkertaisesta kuviosta 1. ilmenee tiedon sijainnin ja sen vaativan riskienhallinnan tarpeen kasvu siirtyessä Suomen sisäisistä toimijoista EU:n ulkopuolelle. Luontaisesti mitä etäämmäksi data siirretään, sitä enemmän mahdollisia riskejä ilmenee esim. datan saatavuuteen ja säädöksiin liittyen, mikä vuorostaan lisää tarvetta kattavalle riskien hallinnalle.



KUVIO 1 Tiedon Sijainti ja riskinhallinnan merkitys, Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta (2018)

Vaikka linjaus koskeekin julkisen sektorin tiedontallennusta, on myös yksityisellä sektorilla omia linjauksia ja määrityksiä datan tallennussijaintia koskien. ERP- järjestelmien käsittelemää arkaluontoista dataa tuskin halutaan sijoittaa poikkeuksellisen kauas tai vieraiden lainsäädäntöpiirien vaikutusvallan alaisiksi. Lähivuosina on ilmennyt useita ristiriitaisia tapauksia esimerkiksi Kiinassa tapahtuvaa tietojenkäsittelyä kohtaan, mikä on ilmennyt kiinalaisten palveluiden välttelynä.

4 ERP-järjestelmän tietoturvaan vaikuttaminen

ERP- järjestelmän käsittelemää tietoa voidaan suojata huomioimalla tietoturva osana järjestelmän kehitystä ja käyttöönoton jälkisiä toimenpiteitä. Tässä luvussa käsitellään konkreettisia tekijöitä, joiden on todettu vaikuttavan ERP-järjestelmien turvallisuuteen, sekä pyritään määrittelemään keinoja tunnistaa ERP-järjestelmää koskevia tietoturvariskejä. Suuri osa ERP-järjestelmien turvallisuutta koskevista teknisistä ratkaisuista on riippuvaisia järjestelmätoimittajan toteutuksesta ja täten vähemmän organisaation vaikutusvallan alaisena. She ja Thuraisingham (2007) toteavat ERP-turvallisuutta käsittelevässä tutkimuksessaan suurimman osan ERP-toimittajista tarjoavan järjestelmään integroidun turvallisuusratkaisun. Tämä voi itsessään toimia hyvin, mutta kokonaisvaltaisen turvallisuuden saavuttamiseksi järjestelmä vaatii myös erillisiä toimenpiteitä kuten tietoturvakäytännön kehittämistä, käyttöoikeuksien ja tunnistautumisen hallinta, järjestelmän käytön ajallinen rajoittamista, sekä tietokantojen ja verkon turvallinen toteutusta ja ylläpitoa. ERP-järjestelmien turvallisuuspuolta käsittelevässä tutkimuksessaan Paul, Mridha ja Hasan (2014) vuorostaan mainitsevat yleisiä järjestelmien kehityksessä huomioitavia turvallisuustekijöitä, kuten turvallisten palvelimien ja verkkojen hyödyntämisen, ERP-järjestelmien eri komponenttien yhtenäisyyden huomioimisen niitä erikseen kehitettäessä, järjestelmän kannalta selkeiden tietototurvavaatimusten määrittelyn ja huomioimisen koko kehitysprosessissa, ajankohtaisten tietoturvaa koskevien parhaiden käytänteiden hyödyntämisen kehityksessä, sekä lopuksi järjestelmän kattavan turvallisuustestauksen.

4.1 Tietoturvaa koskevien riskien tunnistaminen

ERP-hankkeissa on yhtenä kriittisenä menestystekijänä pidetty riittävää vaatimusten määrittelyä järjestelmätoteutukselle (Ahmad ym. 2013). Tietoturvan näkökulmasta on ERP-järjestelmää koskevien eri tekijöiden aiheuttamien tietoturvariskien tunnistaminen merkittävää, jotta järjestelmälle voidaan asettaa tarpeeksi tiukat tietoturvakriteerit. Cebula ja Young (2010) kuvaavat nykyään organisaatioiden olevan riippuvaisia teknologiasta ja sen toiminnasta osana liiketoimintaa ja kriittisten liiketoiminnallisten tavoitteiden saavuttamisessa, minkä vuoksi näitä voimavaroja koskevien riskien hallitseminen ja tunnistamisen on avaintekijä organisaation menestymiselle. He muodostavat tutkimuksessaan luokittelun (taxonomy) kyberuhille ja niiden lähteiden tunnistamiselle. He jaottelevat riskit neljään kategoriaan, jotka ovat ihmisten aiheuttamat, järjestelmien ja teknologian häiriöt, epäonnistuneet prosessit ja ulkoiset tapahtumat. (Taulukko 1). Ihmisten aiheuttamat riskit voidaan jakaa tahallisiin tekoihin kuten hyökkäyksiin tai petoksiin, tahattomiin kuten virheisiin ja erehdyksiin, sekä toimettomuuteen kuten tietoturva käytäntöjä vastaan toimimisen ja koulutuksen puutteeseen. Teknologiasta aiheutuvat riskit he puolestaan jakavat laitteiston,

ohjelmistojen ja järjestelmien välille. Prosessit vuorostaan on jaoteltu suunnitteluun ja toteutukseen, prosessien hallintaan ja tukiprosesseihin. Lopuksi ulkoiset tapahtumat on jaoteltu onnettomuuksiin, laillisiin tekijöihin, liiketoiminnallisiin vaikeuksiin ja ulkoisiin palveluihin, joista organisaatio on riippuvainen. Nämä alaryhmät voidaan vuorostaan jakaa entistä rajatumpiin riskeihin. Tämä luokittelu luo kattavan pohjan erilaisien turvallisuusriskien tunnistamiselle. Luokittelu avataan kokonaisuudessaan taulukossa 1. Luokittelua voidaan hyödyntää kokonaisvaltaisesti organisaation kyberuhkien tunnistamiseen osana muita riskinhallintakäytänteitä. Cebula ja Young mainitsevat yhtenä luokittelun kanssa toimivana viitekehyksenä NIST (National Institute of Standards and Technology) julkaisemat ohjeistukset ja viitekehykset. Näitä avataan tutkielmassa myöhemmin kohdissa 4.2 Testaus, sekä 6.3 NIST kyberturva viitekehys.

1. **Ihmisten aiheuttamat**	**2. Järjestelmien ja teknologian häiriöt**	**3. Epäonnistuneet sisäiset prosessit**	**4. Ulkoiset tapahtumat**
1.1 Tahaton 1.1.1 Vahingot 1.1.2 Virheet 1.1.3 Välttäminen	2.1 **Laitteisto** 2.1.1 Kapasiteetti 2.1.2 Toimintakyky 2.1.3 Ylläpito 2.1.4 Vanheneminen	3.**1 Suunnittelu ja toteutus** 3.1.1 Prosessien kulku 3.1.2 Dokumentaatio 3.1.3 Roolit ja vastuut 3.1.4 Ilmoitukset 3.1.5 Tiedonkulku 3.1.6 Ongelmien paheneminen 3.1.7 Palveluntasosopimukset 3.1.8 Tehtävien siirto	4.1 **Onnettomuudet** 4.1.1 Sää 4.1.2 Tuli 4.1.3 Tulva 4.1.4 Maanjäristys 4.1.5 Levottomuudet 4.1.6 Pandemia
1.2 Tahallinen 1.2.1 Petos 1.2.2 Sabotaasi 1.2.3 Varkaus 1.2.4 Vandalismi	2.2 **Ohjelmisto** 2.2.1 Yhteensopivuus 2.2.2 Kokoonpano 2.2.3 Muutoshallinta 2.2.4 Turva-asetukset 2.2.5 Ohjelmointi käytänteet 2.2.6 Testaus	**3.2 Prosessien hallinta** 3.2.1 Tilan valvonta 3.2.2 Mittarit 3.2.3 Ajallinen arviointi 3.2.4 Prosessien omistus	**4.2 Lailliset tekijät** 4.2.1 Säädökset 4.2.2 Lainsäädäntö 4.2.3 Oikeudenkäynti
1.3 Toimettomuus 1.3.1 Taidot 1.3.2 Tiedot 1.3.3 Ohjeistus 1.3.4 Saatavuus	2.3 **Järjestelmät** 2.3.1 Suunnittelu 2.3.2 Määrittelyt 2.3.3 Integraatio 2.3.4 Monimutkaisuus	3.**3 Tukiprosessit** 3.3.1 Henkilöstö 3.3.2 Rahoitus 3.3.3 Koulutus ja kehitys 3.3.4 Hankinnat	**4.3 Liiketoiminnalliset vaikeudet** 4.3.1 Toimittajan virhe 4.3.2 Markkinoiden tila 4.3.3 Taloudelliset olosuhteet
			4.4 Palveluista riippuvaisuus 4.4.1 Hyödykkeet 4.4.2 Hätäpalvelu 4.4.3 Polttoaine 4.4.4 Liikkuminen

Taulukko 1 Kyberuhkien luokittelu, (Cebula & Young, 2010)

4.2 Käyttöoikeudet ja tunnistautuminen

Organisaation sisällä ERP-järjestelmän toimintoja voi hyödyntää suuri määrä erilaisia käyttäjiä johtoportaasta tuotannon tasolle. Kriittisen datan turvaamiseksi on tärkeää määrittää, mitkä tahot pääsevät käsiksi eri toimintoihin ja tietoihin. Yksi keino tämän toteuttamiseksi on roolipohjainen pääsynhallinta (Role-Based Access Control). Cruz, Kaji ja Yanai (2018) kuvaavat sen olevan mekanismi saatavuuden hallitsemiseen, jossa organisaatio määrittelee eri käyttäjille rooleja, jotka vuorostaan ovat suhteessa eri palveluiden ja toimintojen kanssa. Vain tietyn roolin saaneilla käyttäjillä on mahdollisuus päästä käsiksi tiettyihin toimintoihin. Roolipohjainen pääsynhallinta on yleinen keino säätää organisaation sisäistä toimintaa. Tutkimuksessaan he kiinnittävät erityistä huomiota menettelytavan haasteisiin organisaatioiden välisessä toiminnassa, kun eri käyttäjien roolien varmistaminen on haastavampaa ja roolien väärentäminen on yleisempää. Tähän mahdolliseksi ratkaisuksi he esittävät roolien hallintaa älysopimusten pohjalta, jolloin roolien varmistus toteutetaan lohkoketjuteknologian pohjalta, minkä vuoksi erillisten organisaatioiden välinen roolien varmennus on luottamuksellisempaa. ERP-järjestelmien toteutuksissa on lähivuosina alettu hyödyntämään lohkoketjuja ja niiden toiminta sisältää yleisesti organisaatioiden välistä toimintaa eri sidosryhmien kanssa, minkä vuoksi roolien tehokkaampi varmentaminen organisaatioiden välillä voisi tukea toiminnan turvallisuutta.

Tietoturvan saavuttamiseksi on myös käyttäjien käyttöoikeuksien lisäksi keskeistä todentaa kriittiseen dataan käsiksi pääsevät käyttäjät oikeiksi. Käyttäjien tunnistautumiseen on olemassa lukuisia eri työkaluja ja yleensä se on luontaisesti osa ERP-järjestelmätoteutusta jo valmiiksi. Derbyn yliopiston Class of Enterprise Systems 2011–12 (2012) julkaiseman ERP-järjestelmien haasteita koskevan tutkimuskokoelman mukaan perinteinen ja vahva keino tunnistautumiseen myös ERP-järjestelmissä on kaksiosainen tunnistautuminen, jossa käyttäjä tarvitsee perinteisen salasanatunnustuksen lisäksi toisen tunnistautumiskeinon esimerkiksi käyttäjän omistaman fyysisen objektin kautta. Lisäksi kokoelmassa määritellään ERP-järjestelmän käyttäjien tunnistautumisen olevan avaintekijä käyttäjien saatavuuden ja oikeuksien hallintaan, sekä myös keino käyttäjien toiminnan seurantaan ja kirjaamiseen. Tunnistautumisella voidaan havaita eri tahojen toimesta tehtyjä tietoturvarikkeitä ja näin ehkäistä niitä.

4.3 Tietoturvapäivitykset

Uusia uhkia tietoturvalle ilmenee alati, minkä vuoksi on tärkeää päivittää järjestelmätoteutusta vastaamaan niiden myötä ilmeneviin haasteisiin. Norjalaisten tutkijoiden Bjelland ja Haddara (2018) julkaisemassa tutkimuksessa käsitellään ERP-järjestelmien järjestelmäpäivityksiä ja niiden merkistä erityisesti pilvipohjaisten ratkaisujen näkökulmasta. He kuvaavat ERP-järjestelmien vaativan säännöllisiä päivityksiä virheiden korjaamiseen, turvallisuuden korottamiseen,

toimintojen lisäämiseen ja kehittämiseen, sekä toiminnan muokkaukseen ulkopuolisten säädöksien mukaiseksi. Ero pilvipohjaisten ja paikallistoteutettujen ERP-järjestelmien päivittämisen välillä on se, että pilviratkaisuissa päivitykset voidaan toteuttaa reaaliaikaisesti tarpeen vaatiessa, sekä yksinomaan palveluntarjoajan toimesta, kun taas paikallisratkaisuja päivittäessä toimittaja informoi organisaatiota mahdollista päivityksistä, jonka jälkeen järjestelmän käyttäjät voivat vaikuttaa sen asennukseen. Yleisesti paikallisjärjestelmien päivittämisen koetaan olevan monimutkainen ja resursseja vaativa toimenpide, joka voi vaatia organisaation sisäisiä asiantuntijoita. Toisaalta pilvijärjestelmien päivityksissä on organisaatiolla vähemmän vaikutusvaltaa ja ne voivat tuntua pakotetuilta, kun niiden ajankohtaan ja sisältöön on vaikeampi vaikuttaa. (Bjelland & Haddara, 2018)

ERP-toimittaja SAP julkaisee yleensä päivityksiä kuun toisena tiistaina, joiden osana korjataan mahdollisia haavoittuvuuksia SAP-tuotteissa. He muistuttavat asiakkaillensa päivityksien tärkeydestä ja suosittelevat niiden asentamista viiveettä järjestelmäympäristöjen suojaamiseksi. (SAP, 2020)

4.4 Tietoturvatestaus ja auditointi

Paremman tietoturvan aikaansaamiseksi voidaan järjestelmätoteutusta testata monella eri tavalla. NIST (National Institute of Standards and Technology) julkaisemassa suosituksessa Scarfone, Souppaya, Cody ja Orebaugh (2008) käsittelevät tietoturvan testausta ja arviointia. Yksi keino testata kuinka järjestelmä suoriutuisi mahdollisia hyökkäyksiä vastaan on penetraatiotestaus. Siinä järjestelmän arvioijat jäljittelevät oikeita hyökkäyksiä ja kohdentavat niitä järjestelmään selvittääkseen mahdollisia haavoittuvaisuuksia, määrittääkseen mahdollisilta hyökkääjiltä vaadittavan tason, kehittääkseen lisätoimenpiteitä hyökkäyksiä vastaan, sekä kehittääkseen organisaation kykyä havaita hyökkäyksiä ja reagoida niihin. Lisäksi haavoittuvuuksia löytämällä voidaan luoda yhteyksiä niiden myötä paljastuvien mahdollisten uusien haavoittuvuuksien välille. Organisaation henkilökunnan toimintaa voidaan testata vuorostaan sosiaalisella manipuloinnilla (social engineering), jossa henkilökuntaa yritetään huijata paljastamaan tietoja, joita voidaan hyödyntää järjestelmiin tai verkkoihin hyökätessä. Tällä voidaan testata organisaation tietoturvakäyttäytymisen ja -asenteiden vahvuutta, sekä käytänteiden seuraamista. Manipulointi tavanomaisesti kohdistuu merkittäviin henkilöihin organisaation sisällä, joilla on pääsy arkaluontoisiin tietoihin. Manipulointia testatessa on hyvä huomioida, että mahdollinen onnistuminen voi johtaa yksittäishenkilöiden aseman heikkenemiseen, minkä vuoksi on tärkeää keskittyä yksilöinnin sijaan organisaation tietoturvan parantamiseen kokonaisvaltaisesti.

Tietoturva auditointi on keino määrittää organisaation tietoturvatasoa tunnistamalla ja testaamalla sen eri osa-alueita ja havaitsemalla niistä mahdollisia kehityskohteita. Onwubiko (2009) kuvaa tietoturva auditoinnin olevan keino organisaation tiedon turvallisuuden selvittämiseen toteuttamalla

kokonaisvaltainen auditointi organisaation toimintaan ja järjestelmiin, minkä perusteella mitataan organisaation valmiutta suojata arvokkaita resurssejaan. Hänen mukaansa auditoinnissa perehdytään muun muassa organisaation tietoturvakäytäntöön, teknisiin toteutuksiin, toimintoihin ja käytänteisiin, joita arvioimalla pyritään määrittelemään organisaatiolle vaadittava tietoturvataso. Lisäksi auditointi voidaan toteuttaa uhkien ennaltaehkäisyä varten, jotta organisaation toiminta voidaan mukauttaa sille määritellylle tietoturvatasolle tai sitten vastareaktiona jo mahdollisen tietoturvahaasteen ilmennettyä, minkä seurauksena tarve auditoinnille on havaittu. Kokonaisvaltaisen ja onnistuneen auditoinnin toteuttamiseen on olemassa monia linjauksia ja ohjeita, joihin voi perehtyä esimerkiksi sertifikaatin muodossa. Myös ISO-27001 linjauksessa on tarkat linjaukset kattavan ja onnistuneen tietoturva-auditoinnin toteuttamiseen.

5 Tietoturva ja ERP-järjestelmän käyttäjät

Tässä luvussa käsitellään tietoturvaa ja sen huomioimista ERP-järjestelmien käyttäjien näkökulmasta. Yleisesti organisaation tietoturvaan vaikuttavat monet inhimilliset tekijät, jotka jäävät joskus teknologien ominaisuuksien varjoon. Luvussa määritellään organisaation tietoturvakäytänteitä ja niiden merkitystä, käsitellään tietoturvatietoisuuden ja -asenteiden merkitystä, käydään läpi esimerkkejä organisaation sisäisistä tietoturvariskeistä, sekä esitetään mahdollisia toimintamalleja kehittää organisaation tietoturvatoimintaa. Tuotannonohjausjärjestelmät ovat alati vuorovaikutuksessa eri käyttäjiensä kanssa. Organisaation sisällä eri tahot ovat riippuvaisia järjestelmän tarjoamista toiminnoista ja tiedonkäsittelystä. Tämän vuoksi on tietoturvan kannalta erittäin tärkeää huolehtia organisaation sisällä henkilökunnan tietoturva taidoista ja asenteista, sekä yleisistä turvallisuus toimintamalleista. Shaw, Chen, Harris ja Huan (2009) toteavat heikon tietoturvatietoisuuden omaavien käyttäjien olevan yksi merkittävimmistä aukoista organisaation tietoturvassa. Safa, Solms ja Furnell (2015) vuorostaan kuvaavat käyttäjien laiminlyönnin, tietämättömyyden, tietoisuuden puutteen, välinpitämättömyyden tai haitallisten aikeiden olevan yleisiä syitä tietovuodoille. He myös painottavat, kuinka teknologialla ei voida yksinomaan varmistaa organisaation turvallisuutta ja, että käyttäjien toimintaa tulisi pitää kriittisenä turvallisuuteen vaikuttavana tekijänä.

5.1 Tietoturvakäytäntö

Yrityksillä tulee olla olemassa kokonaisvaltaiset tietoturvakäytänteet ja -ohjeistukset. ERP-hankkeiden kannalta nämä korostuvat entisestään, sillä kun organisaation liiketoiminnalliset toimintatavat muuttuvat uusien järjestelmähankintojen myötä, tulee myös tietoturvakäytänteiden muuttua niiden mukaisiksi. ISO määrittelee tietoturvakäytännön (information security policy) olevan keino johdolle määrittää liiketoiminnalle riittävät tietoturvaa koskevat vaatimukset ja säädökset. (ISO 27002, 2013) Flowerdayn ja Tuyikezeen (2016) mukaan tekijöitä tehokkaiden ja toimivien tietoturvakäytänteiden luomiseen ovat uusien teknologien tuomien haasteiden huomioiminen, yleisien säädöksien noudattaminen, sekä keskeisten sisäisten ja ulkoisten uhkien tunnistaminen. Lisäksi he keskittyvät johdon tuen merkitykseen käytäntöjen kehittämisessä ja niiden toteuttamisessa, sekä henkilökunnan asenteiden ja käyttäytymisen rooliin käytänteiden toteutumisessa. ERP-hankkeiden näkökulmasta Doherty ja Fulford (2006) kuvaavat hankkeiden mukanaan tuovan muutoksen vaativan kattavaa arviointia tietoturvan ja organisaation strategian näkökulmasta. Organisaation tietoturvakäytänteitä määrittäessä tulee huomioida ERP-järjestelmän myötä ilmenevä mahdollinen tiedon rajoittaminen sen levitessä laajemmalle alueelle ja useammille käyttäjille organisaation sisällä, riittävä tiedon saatavuus ja mahdollinen riippuvuus

järjestelmästä, sekä riittävä tiedon salaus. He myös suosittelevat ERP-järjestelmän myötä ilmenevien uusien toimintojen arvioimista ja vertausta olemassa oleviin tietoturvakäytänteisiin, sekä tarvittaessa päivittää käytänteitä tai mahdollisesti poistaa käytänteiden vastaiset komponentit käytöstä kokonaan ja luoda niiden tilalle käytänteiden mukaiset uudet vastineet.

5.2 Tietoturva asenteet ja – tietoisuus

Tietoturvatietoisuudella (information security awarness) viitataan tilaan, jossa organisaatiossa toimivat käyttäjät ovat tietoisia, sekä toivotusti sitoutuneita toimimaan organisaation turvallisuuslinjausten mukaisesti (Siponen, 2013). Shaw ym. (2009) vuorostaan kuvaa tietoturvatietoisuuden olevan käyttäjien ymmärryksen taso koskien tietoturvan merkitsevyyttä, sekä heidän vastuutansa pitääkseen oman toimintansa tietoturvan kannalta riittävällä tasolla suojatakseen organisaation kriittisiä toimintoja. Koska käyttäjät syöttävät ja tulkitsevan suuria määriä kriittistä dataa ERP-järjestelmien kautta, on henkilökunnan toimintaan vaikuttavilla asenteilla ja tietoisuudella tietoturvallisesta toiminnasta suuri vaikutus organisaation kokonaisturvallisuuteen. Tietoisuuden ja asenteiden merkitys korostuu Ahmad ym. (2016) tutkimuksessa, jonka mukaan korkeat tietoturvataidot omaavien henkilöiden kyvyt eivät välttämättä johda heidän taitojensa tasoiseen toimintaan, mikä selittyy heikoilla tietoturva-asenteilla.

5.3 Organisaation sisäiset tietoturvariskit

Henkilökunnan puutteellinen tietoturvaosaaminen ja huono tietoisuus ja asenne tietoturvaa kohtaan altistavat organisaation tietoturvariskejä aiheuttavalle toiminnalle. Safa, Solms ja Furnell (2015) painottavat kuinka hakkerit voivat enemmänkin kohdistaa hyökkäyksiä ihmisiin, tietokoneiden sijaan. He myös listaavat perinteisiä esimerkkejä tietoturvariskeille altistavasta toiminnasta kuten sosiaalitunnuksien käyttäminen salasanana tai käyttäjänimenä, salasanojen kirjoittaminen muistiin esim. paperille, kirjautumistietojen jakaminen kollegoiden kesken, tuntemattomien sähköpostien ja liitteiden avaaminen, sekä epäluotettavien ohjelmien lataaminen verkosta. Tällöin siis organisaation sisäinen käyttäytyminen luo ulkopuolisille tahoille mahdollisuuksia hyötyä heikosta tietoturvatoiminnasta. Toisessa tutkimuksessa Safa, Maple, Watson ja Solms (2018) käsittelevät organisaation sisäisiä turvallisuusuhkia. He painottavat kuinka perinteisesti on keskitytty tietoturvan saavuttamiseen teknologisesta näkökulmasta, vaikka myös inhimilliset tekijät ovat keskeisessä roolissa organisaation kokonaisturvallisuuden takaamisessa. Sisäiset riskit eivät ole välttämättä tahattomia ja huolimattomuudesta johtuvia. Yleinen syy tietoturvariskeille voi olla organisaation sisäisen luotetun toimijan toimesta tapahtunut tahallinen tiedon vuotaminen tai väärin käsittely. Tämä tapahtuu yleensä taloudellista hyvitystä vastaan.

Esimerkkejä vastaavasta toiminnasta ovat tietojen luvaton poistaminen, monistaminen, välittäminen ja muokkaus organisaatiolle haitallisin tavoin. Keskeisimmät tekijät vastaavassa toiminnassa ovat tekijän motiivi tietoturvan vastaiseen toimintaan, sekä toiminnalle luodut mahdollisuudet. Uhkien vähentämiseksi he suosittelevat vaikuttamaan henkilökunnan asenteisiin ja huomioimalla heitä osana tietoturvatoimintaa, sekä yleisesti karsimalla mahdollisuuksia mahdollisille rikkeille esim. käyttöoikeuksien tarkan valvonnan myötä. Yleisesti organisaation sisäisten tietoturvariskien huomioiminen on oleellisia myös ERP-järjestelmän näkökulmasta, sillä ne tarjoavat mahdollisuuden suurelle määrälle käyttäjiä päästä käsiksi ja muokata organisaation kannalta kriittistä dataa.

5.4 Tietoturvakouluttaminen

On tärkeää, että organisaatio toimii aktiivisesti parantaakseen henkilökuntansa tietoturvaa koskevia taitoja, sekä pyrkii vaikuttamaan heidän tietoturva-asenteisiinsa, sekä täten myös -käyttäytymiseen. Tähän on olemassa monia erilaisia toimintamalleja ja prosesseja. Amankwa, Loock ja Kritzinger (2014) ovat jaotelleet tietoturvan kehittämisen organisaatiossa tietoturvan opettamiseen(education), koulutukseen (training), sekä tietoisuuteen ja asenteisiin vaikuttamiseen(awareness). Näistä opettaminen keskittyy tietoturvadokumentteihin ja linjauksiin perehtymiseen, sekä ymmärtämiseen. Tietoturvakoulutuksella puolestaan pyritään varmistamaan, että työntekijät osaavat heidän tehtävänsä kannalta vaadittavat tietoturvataidot ja -toimintamallit. Heidän mukaansa asenteisiin ja tietoisuuteen vaikuttamalla taas pyritään takaamaan, että työntekijät ymmärtävät roolinsa ja vastuun tietoturvan kannalta, sekä toimivat sen mukaisesti.

Safa ym. (2015) mukaan tietoturvatietoisuuden parantaminen vaatii oikeanlaisia harjoituksia ja toimintaa, jotta voidaan saavuttaa parempaa tietoturvakäyttäytymistä. Esimerkkejä toimintatavoista tietoisuuden ja taitojen parantamiseksi organisaatiossa ovat erilliset tietoturvakurssit, tietoturvaa koskevat formaalit esitykset, tietoturvan parantamista koskevat kokoukset, tietoisuutta luovat objektit kuten julisteet, näytönsäästäjät, kynät yms., suorat sähköpostit käyttäjille tai tietoturvaa koskevat pelit. Näitä keinoja voidaan hyödyntää kokonaisvaltaisissa tietoisuuskampanjoissa, joilla pyritään vaikuttamaan organisaation asenteisiin ja tietoisuuteen. Heidän mukaansa oleelliset ja ajankohtaiset kampanjat ovat avain onnistuneeseen tietoturvatietoisuuden kehittämiseen. (Safa ym., 2015) Siponen (2015) esittää tutkimuksessaan viitekehyksen ja keinoja tietoturvatietoisuuden kehittämiseen organisaatioiden sisällä. Tutkimus painottaa motivaation ja tietoturvaan suhtautumisen merkitystä osana tietoturva-asenteita. Hän toteaa perinteisten tietoturvaan vetoavien kampanjoiden voivan teoriassa olla tehokas ratkaisu asenteiden kehittämisessä, mutta niillä voi olla myös odottamattomia vaikutuksia ja vaihteleva vaikutus motivaatioon, mikäli ne koetaan turhauttaviksi ja pakonomaisiksi. Tietoturvatietoisuuden kehittäminen Siposen mukaan vaatii myös opettamiseen ja kouluttamiseen, jossa opetus kehittää käyttäjien motivaatiota ja ymmärrystä tietoturvan merkitykseen, kun taas koulutus

parantaa käyttäjien taitoja ja pätevyyttä. Tietoturvatietoisuuden vaikuttamiseen pyrkiessä hän käsittelee useita käyttäytymiseen ja motivaatioon vaikuttavia tekijöitä, kuten käyttäjien toimintaa ohjaava logiikka, tunteet, moraalit, hyvinvointi, turvallisuuden kokeminen ja rationaalisuus. Hän myös painottaa tietoisuuteen vaikuttavien henkilöiden omien tietoisuutta koskevien asenteiden ja ominaisuuksien merkitystä vaikuttamisen uskottavuuden kannalta. (Siponen, 2013)

Tutkimuksessaan Gurnani, Pandey ja Rai (2014) käsittelevät kyberturvaharjoitusten (Cyber security exercise) hyödyntämistä organisaation tietoturvan parantamiseksi. Näissä harjoituksissa pyritään tutustuttumaan käyttäjiä mahdollisesti heidän organisaatioonsa kohdistuvia hyökkäyksiä vastaan luomalla ja arvioimalla lavastettuja hyökkäystapahtumia. Erilaisia tapahtumia toteuttamalla voidaan kartoittaa henkilöstön tietoturvatoimintaa, sekä samalla myös kehittää sitä. Vastaavilla harjoituksilla saadaan myös toteutettua tietoturvatoimintaa myös käytännössä, minkä vuoksi työntekijät ovat valmiimpia hallitsemaan oikeita tilanteita. Harjoituksilla voidaan myös testata ja kehittää koko organisaation toimintamallien ja linjausten toteutumista. Haasteena harjoituksissa on niiden monimutkainen luonne, minkä vuoksi niiden kehittäminen vaatii resursseja, sekä asiantuntijoita. (Gurnani ym., 2014)

ERP-järjestelmien tietoturvan kannalta on myös merkittävää, että loppukäyttäjät koulutetaan käyttämään järjestelmää oikein. Uusien järjestelmähankkeiden myötä saattaa yrityksen toiminnassa ilmetä uusia toimintamalleja, jotka käyttäjien tulee osata ja ymmärtää. Alcivar & Abad (2016) mukaan käyttäjien onnistunut kouluttaminen on yksi ERP-käyttöönoton keskeisimmistä kriittisistä menestystekijöistä. Järjestelmän käytön kouluttamiseen on olemassa monia perinteisiä työkaluja kuten virtuaaliset oppitunnit, ohjekirjat, opetusohjelmat, sekä opetusvideot. Näiden lisäksi Alcivar & Abad esittävät tutkimuksessaan ERP käytön kouluttamista pelillistämistämistä (gamification) hyödyntäen, jolloin käyttäjä pääsee harjoittelemaan järjestelmän käyttöä käytännönläheisemmin ja mielekkäämmin verrattuna perinteisiin koulutustapoihin, mikä vuorostaan johtaa parempiin oppimistuloksiin ERP-järjestelmän käyttöä koskien. ERP-järjestelmien turvallisuutta kuvaavassa viitekehyksessään Marnewick ja Labuschagne (2005) vuorostaan painottavat riittävää resurssien käyttöä käyttäjien koulutukseen, jotta nämä ymmärtäisivät järjestelmän toiminnan ja sitä ympäröivän turvallisuuden merkityksen. He myös mainitsevat johdon sitoutumisen, sekä muutoksenhallinnan merkityksen ERP-hankinnoissa.

6 Lainsäädäntö ja standardit

Tässä luvussa käsitellään erilaisia säädöksiä ja standardeja, jotka saattavat vaikuttaa ERP-järjestelmän tietoturvatoteutukseen. Yleisesti tietojärjestelmähankkeita toteuttaessa on tärkeää huomioida erilaisia niiden tiedonkäsittelyä koskevia säädöksiä. Nämä säädökset voivat käsitellä esimerkiksi järjestelmän yleistä tietoturvatoteutusta ja -toimintaa. Lisäksi ERP-järjestelmille on ominaista käsitellä mahdollisia henkilötietoja, minkä vuoksi on syytä keskittyä myös lähivuosina esillä olleisiin tietosuojasäädöksiin.

6.1 ISO/IEC 27000

ISO 27000 on kansainvälisen standardisoimisjärjestön (ISO) julkaisema joukko tietoturvastandardeja. Ne koostuvat tietoturvaa koskevista parhaista käytänteistä ja toimintaohjeista. Näistä keskeisimpänä toimii ISO 27001, joka käsittelee toimivien tietoturvan johtamisjärjestelmien (ISMS) käyttöönottoa, toimintaa, valvomista, arvioimista, ylläpitoa, sekä kehittämistä. Standardissa määritellään vaatimuksia tietoturvajohtamisjärjestelmän ohjauksen toteuttamiseen erillisten organisaatioiden tarpeiden mukaisiksi. Tähän kuuluu vaadittavat toiminnot tietoturvariskien tunnistamiseksi ja ehkäisemiseksi suhteessa niihin prosesseihin, joita organisaatio haluaa suojata. ISO 27002 vuorostaan esittää yleisesti hyväksyttyjä tietoturvan hallintatoimintoja sekä parhaita käytänteitä organisaation tieturvan toteuttamiseen käytännössä. Näiden lisäksi ISO 27000 sisältää myös useita standardeja ja suosituksia muun muassa organisaation tietoturvatoiminnan tehokkuuden arvioimiseen ja mittaamiseen, riskienhallintaan, tietoturva-auditointiin, toiminnan valvomiseen, tietoturvan taloudellisen ulottuvuuden tunnistamiseen, tietoturva-asiantuntijoiden kyvykkyyksien tunnistamiseen, sekä tietoturvaa koskevaan viestintään. (ISO 27000, 2018)

ISO 27000 sisältää paljon yleisesti päteviä toimintamalleja, joita ERP-hankkeissa huomioimalla voidaan mahdollisesti kehittää koko organisaation sekä samalla itse järjestelmän tietoturvaa. SAP-järjestelmien kyberturvallisuuteen erikoistuva ERPScan suosittelee ISO 27000-standardin mukaisen toiminnan toteuttamista ERP-järjestelmien kriittisten liiketoimintaprosessien turvaamiseksi. He suosittelevat ERP-järjestelmän riittävää auditointia tietoturvanjohtamisjärjestelmän mukaisessa ympäristössä, kriittisten tietovarojen tunnistamista ja niiden käyttöoikeuksien hallintaa, toimintamallia haavoittuvuuksien tunnistamiseen ja korjaamisen, riskien arviointia ja hallitsemista, sekä järjestelmän ja organisaation toiminnan yleistä seurantaa, jotta ne toimivat vaatimuksien määrittelevällä tasolla. (ERPScan, 2020)

6.2 Tietosuoja

ERP-järjestelmät voivat käsitellä suuria määriä henkilötietoja esimerkiksi asiakastietojen ja henkilökunnan tietojen muodossa, minkä vuoksi on ERP-hankkeiden kannalta merkittävää perehtyä tietosuojaan ja sen toteuttamiseen ennen järjestelmän käyttöönottoa. Suomen tietosuojalain noudattamista valvova tietosuojavaltuutettu kuvaa tietosuojan olevan: ”Perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.” Lisäksi aina henkilötietoja käsitellessä tulisi toiminta perustaa lakiin. Suomessa tietosuojaa säätelee muun muassa tietosuojalaki, EU:n yleinen tietosuoja-asetus, rikosasioiden tietosuojadirektiivi ja rikosasioiden tietosuojalaki. Lisäksi henkilötietojen käsittelyä säätelee laki sähköisen viestinnän palveluista, työelämän tietosuojalaki ja luottotietolaki. Valtuutettu myös erottaa tietoturvan ja tietosuojan kuvaamalla tietoturvaa tietosuojan toteuttamisen keinoksi, jossa organisaationallisilla ja teknisillä toimenpiteillä varmistetaan tiedon saatavuus, luottamuksellisuus ja eheys. Hyvin toteutetulla tietoturvalla voidaan siis osittain varmistaa henkilötietojen asianmukainen käsittely, eli tietosuojan toteutuminen. (Tietosuojavaltuutetun toimisto, 2020)

EU:n yleinen tietosuoja-asetus eli GDPR on 2018 voimaan astunut asetus, jonka tavoitteena on EU:n sisällä vahvistaa säännöt luonnollisten henkilöiden henkilötietojen suojelulle ja henkilötietojen vapaalle liikkumiselle, sekä tukea perusoikeutta henkilötietojen suojaan. Asetuksessa esitetään kattavasti vaatimuksia EU:n sisällä tapahtuvalle henkilötietojen käsittelyä sisältävälle toiminnalle. Vaatimukset koskevat esimerkiksi henkilötietojen käsittelyn periaatteita ja lainmukaisuutta eri tilanteissa, sekä rekisteröidyn henkilön suostumusta henkilötietojen käsittelyyn ja hänelle vaatimusten mukaisten tietojen käsittelyä koskevien tietojen ilmoittamiseen, kuten esimerkkeinä mihin tietoja käytetään, kenelle tiedot päätyvät ja kuinka henkilöllä on pääsy niihin. ((EU) 2016/679, 2016)

Tietoturvan näkökulmasta GDPR määrittelee asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen turvalliseen käsittelyyn, kuten tietojen riittävä pseudonymisointi ja salaus, kyky taata järjestelmän luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, tietojen saatavuuden palauttaminen fyysisen tai teknisen vian sattuessa, sekä toiminta, jolla arvioidaan säännöllisesti tietoturvaa koskevien toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. Lisäksi asetus määrittää turvallisuustasoa arvioidessa keskeisimmäksi huomion kohteeksi tietojen käsittelyn mahdolliset riskit, kuten henkilötietojen vahingollisen tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai asiattoman tietoihin käsiksi pääsemisen. Rekisterinpitäjän tulee myös varmistaa, että henkilötietojen parissa toimivat henkilöt toimivat asetuksen mukaisesti. Mahdollisen tietoturvaloukkauksen tapahtuessa tulee asetuksen mukaan loukkauksesta ilmoittaa valvontaviranomaiselle sekä vaadittaessa myös itse rekisteröidylle. ((EU) 2016/679, 2016)

6.3 NIST kyberturvaviitekehys

NIST (National Institute of Standards and Technology) on Yhdysvalloissa toimiva virasto, joka pyrkii edistämään teknologiaa ja teollisuutta, sekä pyrkii samalla määrittämään standardeja. NIST on julkaissut kyberturvaviitekehyksen, joka pyrkii edistämään Yhdysvaltojen turvallisuutta ja taloutta määrittelemällä toimintamalleja kriittisten infrastruktuurien suojaamiseen tunnistamalla, arvioimalla ja hallitsemalla kyberuhkia kustannustehokkaalla tavalla, erilaisten organisaatioiden tarpeiden mukaan. Viitekehys keskittyy hyödyntämään liiketoiminnan päätoimintoja ja tavoitteita ohjatakseen turvallisuustoimenpiteitä ja tunnistamaan mahdollisia riskejä osana niitä. Vaikka viitekehitys on alun perin kehitetty kriittisen infrastruktuurin turvaamiseen, voidaan sitä hyödyntää joustavasti organisaatioissa, jotka ovat riippuvaisia teknologiaratkaisujensa toiminnasta. (Barrett, 2018)

Viitekehys jakautuu kolmeen pääalueeseen, jotka ovat viitekehyksen ydinosa (core), toteutustasot (implementation tiers) ja profiili. Ydinosassa määritellään vaadittavat toimenpiteet tunnistettujen kyberturvallisuustavoitteiden saavuttamiseksi. Turvallisuustoimenpiteiden systemaattiseen järjestelyyn ja määrittelyyn viitekehys esittää viisi pääfunktiota, jotka ovat tunnista (identify), suojaa (protect), havaitse (detect), reagoi (respond) ja palaudu (recover). Näitä funktioita hyödyntämällä kyberuhkien torjunnassa organisaatio pystyy tehokkaammin tekemään päätöksiä, käsittelemään uhkatilanteita ja parantamaan toimintaansa oppimalla aikaisemmista aktiviteeteistä. Viitekehyksen toteutustasojen tarkoituksena on vuorostaan jakaa organisaation eri alueita ja toimintoja neljän tason mukaan, jotka kuvaavat vaadittavien kyberturvatoimenpiteiden vakavuutta ja monimutkaisuutta. Profiilissa taas määritellään kyseessä olevan organisaation ominaisuuksia, kuten toimintoja, liiketoiminnan vaatimuksia, riskin sietokykyä ja resursseja. Näitä hyödyntämällä kyetään rajaamaan ja vähentämään kyberuhkia niin, että toiminta on asetettujen tavoitteiden ja mahdollisten lakisääteisten vaatimuksien ja toimialan parhaiden käytänteiden mukaisia. (Barrett, 2018)

ERP-järjestelmähankkeiden näkökulmasta voidaan NIST-kyberturvaviitekehystä hyödyntää sen joustavuuden ja yleistettävyyden ja liiketoiminnallisen painotuksen vuoksi. Toinen NIST:in julkaisema viitekehys on riskinhallintaviitekehys tietojärjestelmille ja organisaatioille, ja sen käyttö voidaan yhdistää NIST-kyberturvaviitekehykseen. Tietojärjestelmien viitekehys on tarkoitettu riskienhallinnan yhdistämiseen osaksi organisaation eri järjestelmien toimintaa. Viitekehys tarjoaa muun muassa tietoturvan riskien luokittelutyökaluja, ohjeita tietoturvatoimintojen valitsemiseen, käyttöönottoon ja arviointiin, sekä keinoja järjestelmän seurantaan. Näitä voidaan vuorostaan hyödyntää osana organisaation päätöksentekoa ja riskienhallintaviitekehyksen jalkauttamista. (Force, 2018)

7 Yhteenveto ja pohdinta

Tutkielmassa esitettiin tietoturvan eri ulottuvuuksia, joita huomioimalla organisaatio pystyy parantamaan ERP-järjestelmiensä ja koko organisaation tietoturvaa. Tutkielmaa toteuttaessani huomasin ERP- järjestelmien ja tietoturvan välillä vahvan yhteisen teeman: ne ovat molemmat kattavasti esillä organisaation eri tasoilla ja osana lukuisia organisaation toimintaan vaikuttavia tekijöitä. Ne molemmat myös vaativat paljon huomiota osana organisaation kriittistä päätöksentekoa ja toiminnan ohjausta.

Tietoturva on moniulotteinen ilmiö. ERP-järjestelmien kaltaisten monimutkaisten järjestelmäkokonaisuuksien näkökulmasta tietoturva käsittää monipuolisemman aihepiirin, kuin osasin odottaa. Vaikka itse järjestelmän toteutuksessa turvallisuuden huomioiminen ja sen ylläpitoon käytetyt toimenpiteet, kuten päivitykset ja tunnistautuminen ovat yhä erittäin keskeisessä roolissa, on kriittistä nähdä myös raudan ja koodin ulkopuolelle. ERP-järjestelmät toimivat ympäristöissä, joissa niiden toimintaan vaikuttavat lukuiset tekijät, kuten käyttäjät, lainsäädäntö ja organisaatioiden välinen yhteistyö. Tietoturvan kannalta merkittävä riskitekijä saattaa istua vieressäsi toimiston kahvipöydässä. Myös tiedon määrän ja merkityksen kasvaessa ihmisiä kiinnostaa enemmän, mitä heidän tietojansa käsitellään ja hyödynnetään, mikä on lähivuosina ollut esillä myös ERP-maailmassa.

Tässä vaiheessa voidaan todeta tutkielman käsittelevän aiheen hyödyllisyyttä ja merkitsevyyttä. ERP-järjestelmät ovat kriittisiä lukuisien organisaatioiden liiketoiminnan jatkuvuudelle ja itsessään mahdollistavat liiketoimintaprosesseja ja niiden yhdistämistä kokonaisuuksiksi, minkä vuoksi on niiden toimintaan liittyvien tietoturvahaasteiden tunnistaminen avaintekijä kokonaisvaltaisen tietoturvan ylläpitämiseksi. Tutkielmassa yhdistetään tieteenalan kannalta keskeisiä teemoja, joista voi olla hyötyä sekä tietoturvaansa, että ERP-järjestelmiään kehittämään pyrkiville organisaatioille.

Niin tutkielman vahvuutena kuin heikkoutena toimivat sen kokonaisvaltainen näkemys tietoturvaan. Tietoturvaa käsitellään perinteisesti hyvin teknologiapainotteisesta näkökulmasta, minkä vuoksi tutkielman kokonaisvaltainen katsaus aiheeseen tuo esiin seikkoja, jotka mahdollisesti muuten jäisivät huomioimatta. Lisäksi tämä mahdollisti kirjallisuuskatsauksen toteuttamisen laajemmin ja suurempaan aihepiiriin tutustuen. Toisaalta tutkielman kannalta olisi ollut hyvä keskittyä enemmän myös järjestelmän konkreettisen toteutuksen teknisiin ratkaisuihin, sillä niiden merkitys järjestelmän turvallisuuden kannalta on erittäin suuri. Aiheesta on kuitenkin haastava löytää lähteitä ERP-järjestelmätoteutuksien välisten erojen, monimutkaisuuden ja vähäisen tutkimuksen vuoksi ja se olisi voinut saada liian suuren painoarvon suhteessa tutkielman muihin aiheisiin. Myös tutkielmassa esitettyjen tietoturvanäkökulmien määrän vuoksi jää niiden käsittely melko pinnalliselle tasolle, kuitenkin tiivistäen aiheiden pääkohdat ytimekkäästi ja tutkielman tutkimuskysymyksen kannalta riittävällä tasolla.

ERP-järjestelmiä ja tietoturvaa yhdistävä kirjallisuus on lähiaikoina keskittynyt pääasiassa pilvipohjaisten palveluiden mukana ilmenneisiin haasteisiin, mikä on luonnollista niiden yleistymisen seurauksena. Tämä entisestään vähentää keskittymistä järjestelmän tekniseen turvallisuustoteutukseen, sillä se on pääosin palveluntarjoajan vastuulla. Uskon, että tulevaisuudessa kirjallisuus tulee yhä enemmän keskittymään pilvipohjaisiin ratkaisuihin, sekä perinteisten järjestelmien siirtämiseen pilveen ja kyseisten projektien kriittisiin menestystekijöihin. Yleisesti uskon tietoturvan ja kyberturvallisuuden merkityksen korostuvan paitsi ERP-järjestelmiä koskien myös yleisellä tasolla tulevaisuudessa uhkien kehittyessä ja nuorten ja haavoittuvien teknologioiden tarjotessa uusia liiketoiminnallisia mahdollisuuksia. Lisäksi uskon yksityisyyskysymyksen kiristyvän entisestään, kun suuria datamääriä aletaan hyödyntämään entistä tehokkaammin. Lehto ym. (2017) painottavat Suomen tilannekartoituksessaan ennaltaehkäisyn merkitystä tulevaisuudessa. He toteavat kuinka järjestelmiä kehittäessä turvallisuus tulisi rakentaa järjestelmien sisäänrakennetuksi ominaisuudeksi, eikä jälkeenpäin ”päälle liimatuksi” ominaisuudeksi. He painottavat myös yleisen tietoisuuden ja osaamisen lisäämisen tarpeen ja järjestelmien kestokyvyn merkitystä kyberuhkien ennaltaehkäisyssä. Myös tulevaisuuden älykkäät tuotannonohjausjärjestelmät tulee rakentaa turvallisina ja ennaltaehkäisevinä, sillä tulevaisuuden mahdolliset uhkat voivat olla ennalta-arvaamattomia ja entistäkin vakavampia.

LÄHTEET

Addo-Tenkorang, R., & Helo, P. (2011). Enterprise resource planning (ERP): A review literature report. *Proceedings of the World Congress on Engineering and Computer Science, October 2011 (Vol. 2)*, pp. 19-21).

Ahmad, M. M., & Cuenca, R. P. (2013). Critical success factors for ERP implementation in SMEs. *Robotics and computer-integrated manufacturing*, *29(3)*, 104-111.

Ahmad, Z., Norhashim, M., Song, O. T., & Hui, L. T. (2016). A typology of employees' information security behaviour. *2016 4th International Conference on Information and Communication Technology (ICoICT)*, *May 2016* (pp. 1-4). IEEE.

Alcivar, I., & Abad, A. G. (2016). Design and evaluation of a gamified system for ERP training. *Computers in Human Behavior, 58*, 109-118.

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014) December 2014*, (pp. 248-252). IEEE.

AppsRunTheWorld, (2018). Top 10 ERP Software Vendors, Market Size and Market Forecast 2018-2023 https://www.appsruntheworld.com/top-10-erp-software-vendors-and-market-forecast/

Barrett, M. P. (2018). NIST Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep.

Bjelland, E., & Haddara, M. (2018). Evolution of ERP systems in the cloud: A study on system updates. *Systems, 6(2)*, 22.

Cebula, J. L., & Young, L. R. (2010). A taxonomy of operational cyber security risks (No. CMU/SEI-2010-TN-028). Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Class of Enterprise Systems 2011-12 (2012). *Emerging Issues and Technologies for ERP Systems. First Edition* (May 28, 2012)

Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *Ieee Access, 6*, 12240-12251.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & security, 25(1)*, 55-63.

Duan, J., Faker, P., Fesak, A., & Stuart, T. (2013). Benefits and drawbacks of cloud-based versus traditional ERP systems. Proceedings of the 2012-13 course on Advanced Resource Planning.

ERPScan (2020). SAP Compliance with ISO27001, https://erpscan.io/solutions/by-compliance/sap-compliance-iso-27001/

EU:n yleinen tietosuoja-asetus (EU) 2016/679, (2016)

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & security, 61*, 169-183.

Force, J. T. (2018). NIST Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Final Public Draft) (*No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft))*. National Institute of Standards and Technology.

Gupta, S., & Misra, S. C. (2016). Moderating effect of compliance, network, and security on the critical success factors in the implementation of cloud ERP. *IEEE Transactions on Cloud Computing, 4(4)*, 440-451.

Gupta, S., Misra, S. C., Singh, A., Kumar, V., & Kumar, U. (2017). Identification of challenges and their ranking in the implementation of cloud ERP. *International Journal of Quality & Reliability Management, 34(7)*, 1056-1072

Gurnani, R., Pandey, K., & Rai, S. K. (2014, March). A scalable model for implementing Cyber Security Exercises. *2014 International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 680-684). IEEE.

ISO/IEC 20252 (2019) Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements.

ISO/IEC 27000 (2018) Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27002 (2013) Information technology – Security techniques – Code of practice for information security controls.

ITU (2020) Definition of cybersecurity, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Khanna, K., & Arneja, G. P. (2012). Choosing an appropriate ERP implementation strategy. *IOSR journal of Engineering, 2(3)*, 478-483.

Lehto ,M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen, M., (2017) Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.

Marnewick, C., & Labuschagne, L. (2005). A security framework for an ERP system. ISSA.

Nagpal, S., Khatri, S. K., & Kumar, A. (2015). Comparative study of ERP implementation strategies. In 2015 Long Island Systems, *Applications and Technology, May 2015* (pp. 1-9). IEEE.

Onwubiko, C. (2009). A security audit framework for security management in the enterprise. *International Conference on Global Security, Safety, and Sustainability, September 2009* (pp. 9-17). Springer, Berlin, Heidelberg.

Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2)*, 136-146.

Paul, D., Mridha, M. R., & Hasan, M. R. (2014). Performance Evaluation and Operation of Enterprise Resource Planning (ERP) Software Security System. *International Journal of Intelligent Information Systems. 3. 45*. 10.11648/j.ijiis.20140305.11.

Phaphoom, N., Qu, J., Kheaksong, A., & Saelee, W. (2018). An Investigation of ERP implementation:: A Comparative Case Study of SME and Large Enterprises in Thailand. In 2018 *16th International Conference on ICT and Knowledge Engineering (ICT&KE), November 2018* (pp. 1-6). IEEE.

Rashid, M. A., Hossain, L., & Patrick, J. D. (2002). The evolution of ERP systems: A historical perspective. *Enterprise Resource Planning: Solutions and Management (pp. 35-50)*. IGI global.

Rîndaşu, S. M. (2018). Information security challenges-vulnerabilities brought by ERP applications and cloud platforms. *Audit Financiar, 16(149)*, 131-139.

Saa, P., Moscoso-Zea, O., Costales, A. C., & Luján-Mora, S. (2017). Data security issues in cloud-based Software-as-a-Service ERP. *12th Iberian Conference on Information Systems and Technologies (CISTI), June 2017* (pp. 1-7). IEEE.

Saeed, I. & Juell-Skielse, Gustaf & Uppström, Elin. (2012). Cloud enterprise resource planning adoption: *Motives & barriers. Advances in Enterprise Information Systems II*. 99-122. 10.1201/b12295-45.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications, 40*, 247-257.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security, 56*, 70-82.

SAP, (2020). SAP Security Notes & News, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). NIST Technical guide to information security testing and assessment. *NIST Special Publication, 800(115),* 2-25.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52(1),* 92-100.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security. 8(1),* 31-41

Statista (2020)Enterprise resource planning (ERP) software market revenues worldwide from 2018 to 2023, https://www.statista.com/statistics/605888/worldwide-enterprise-resource-planning-market-forecast/

Tietosuojavaltuutetun toimisto (2020), Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä https://tietosuoja.fi/tietosuoja

Valtiovarainministeriö (2018) Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta.

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

Wong, A., Scarbrough, H., Chau, P., & Davison, R. (2005). Critical failure factors in ERP implementation. *Pacis 2005 Proceedings*, 40.