Tampereen yliopisto

Ella Koivisto

ERP-JÄRJESTELMÄN HANKINTAPRO-SESSIN KYBERTURVARISKIT

Kandidaatintyö
Informaatioteknologian ja viestinnän tiedekunta
Kesäkuu 2023

TIIVISTELMÄ

Ella Koivisto: ERP-järjestelmän hankintaprosessin kyberturvariskit
Kandidaatintyö
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Kesäkuu 2023

Toiminnanohjausjärjestelmä (engl. Enterprise Resource Planning systems, ERP) on merkittävä tietojärjestelmä, jota hyödynnetään erilaisissa organisaatioissa. ERP-järjestelmän hankintaprojekti on monimutkainen prosessi, jonka onnistuminen vaatii siinä toimivilta tahoilta erityistä tarkkuutta. Luonteensa ja sisältämänsä informaation vuoksi ERP-järjestelmään liittyvä kyberturvallisuus on erittäin merkittävä osa organisaation kyber- ja tietoturvallisuutta. ERP-järjestelmän hankintaprosessi voidaan jakaa eri vaiheisiin, joista jokainen sisältää erilaisia kyberturvallisuusuhkia, jotka voivat vaikuttaa projektin kulkuun ja koko järjestelmähankkeen onnistumiseen. Tässä työssä pyritään selvittämään, millaisia kyberturvallisuusuhkia näihin erilaisiin vaiheisiin liittyy.

Tämä tutkimus toteutettiin kirjallisuuskatsauksena tutustumalla aihepiirin kirjallisuuteen kuten tutkimuksiin ja tieteellisiin artikkeleihin. Päätutkimuskysymyksenä tässä työssä pohditaan, millaisia kyberturvallisuusuhkia ERP-järjestelmähankkeeseen liittyy. Tämän lisäksi tässä työssä tarkastellaan yleisimpiä ERP-järjestelmäratkaisuja, kuten pilvipohjaista järjestelmää ja tuodaan esille järjestelmien tuomia hyötyjä organisaatioissa. Tässä työssä ERP-järjestelmän hankintaprosessi jaetaan kolmeen osaan: implementointia edeltävään vaiheeseen, implementointivaiheeseen sekä implementoinnin jälkeiseen vaiheeseen. Erilaiset kyberturvallisuusuhat jaetaan organisaation sisäisiin sekä ulkoisiin uhkiin. Tutkimuksen tavoitteena on selvittää erilaiset kyberturvallisuusuhat, jotka vaikuttavat ERP-järjestelmäprojektiin sen hankintaprosessin aikana.

Tehdyn tutkimuksen perusteella ERP-järjestelmän hankintaprosessi on pitkäkestoinen ja monimutkainen ja sen aikana voi ilmetä useita haasteita. Prosessin haastavuudesta huolimatta järjestelmän tuomat hyödyt organisaatioille vaikuttavat huomattavasti niiden toimintaan. ERP-järjestelmän kyberturvallisuudesta huolehtiminen on kriittistä, sillä järjestelmä toimii merkittävässä osassa koko organisaation toimintakykyä. Työn tuloksista voidaan nähdä, että kyberturvallisuusuhat toimivat merkittävänä tekijänä koko ERP-järjestelmähankkeessa ja organisaatioiden tulee huomioida nämä koko hankintaprosessin ajan. Kyberturvallisuusriskejä ilmenee liittyen sekä sosiaalisiin että teknisiin tekijöihin. Näitä ovat esimerkiksi organisaation henkilöstöön liittyvät uhat ja järjestelmän haavoittuvuuksiin liittyvät uhat.

Avainsanat: Toiminnanohjausjärjestelmä, ERP, tietojärjestelmä, kyberturvallisuus, hankintaprosessi

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

ERP (engl. Enterprise Resource Planning systems) Toiminnanohjausjärjestelmä

MRP (engl. Manufactoring Resource Planning) Tuotannonohjausjärjestelmä

IAAS (engl. Infrastructure as a Service) Infrastruktuurin toteutus palveluna

SAAS (engl. Software as a Service) Tietojärjestelmän toteutus palveluna

SOA (engl. Service-oriented architecture) Palvelukeskeinen arkkitehtuuri

PAAS (engl. Platform as a Service) Alustan toteutus palveluna

1. JOHDANTO

Globalisaation sekä tietojärjestelmien lisääntyneen käytön myötä organisaatioiden välinen kilpailu ja koko kilpailukenttä on kasvanut. Resurssienhallinnan laajentuessa ja sen merkityksen kasvaessa sitä on siirretty pois operatiivisten johtajien vastuualueilta kohti tietoteknisempiä ratkaisuja, joihin toiminnanohjausjärjestelmä (Enterprise Resource Planning system, ERP) lukeutuu. Pysyäkseen mukana jatkuvasti muuttuvassa ympäristössä sekä ylläpitääkseen kilpailukykyä organisaatioiden johtajat ovat huomioineet ERP-järjestelmien merkityksen. (Sarkis & Gunasekaran 2003)

Koska ERP- järjestelmät ovat hyvin monimutkaisia tietojärjestelmiä, niiden hankinnan toteuttaminen vaatii organisaatiolta huomattavaa investointia liittyen esimerkiksi kustannuksiin ja aikaan tehden hankkeen onnistumisesta melko hankalan prosessin (Sarkis & Gunasekaran 2003.) Jagoda ym. (2017) jakaa ERP-järjestelmän hankintaprosessin kolmeen vaiheeseen: toteutusta edeltävä vaihe, toteutusvaihe sekä toteutusta seuraava vaihe.

Tietoteknisen kehityksen myötä kyberturvallisuus sekä siihen liittyvät riskit ovat myös nousseet merkittävään rooliin. Organisaatioiden tulisi huomioida kyberturvallisuus tietojärjestelmän koko elinkaaren aikana, mutta tehokkaimmin riskejä voidaan ehkäistä järjestelmän kehitysvaiheen aikana. (Misra ym. 2019) ERP-järjestelmän sisältäessä huomattavasti organisaation toiminnalle merkittävää informaatiota, tulisi kyberturvallisuus huomioida myös sen rakentamisessa sekä käytössä.

Tämän kandidaatintyön tavoitteena on tarkastella ERP-järjestelmän hankintaprosessiin vaikuttavia kyberturvauhkia organisaation näkökulmasta. Riskitekijöitä tarkastellaan prosessin eri vaiheet huomioon ottaen ja ne jaetaan kahteen kategoriaan: organisaation sisäisiin ja ulkoisiin riskeihin. Työssä esitellään myös tapoja, joilla organisaatio voi huomioida näitä erilaisia riskejä ja hieman tarkastellaan myös keinoja ehkäistä kyberturvariskejä. Ehkäisykeinoja ei kuitenkaan laajalti esitellä, jotta työn laajuus pysyy halutussa rajauksessa.

Tutkimuskysymyksenä tässä kandidaatintyössä on:

- Millaisia kyberturvariskejä liittyy ERP-järjestelmän käyttöönottoprosessiin organisaatiossa?

Tätä päätutkimuskysymystä tukemassa olevia alatutkimuskysymyksiä ovat:

- Mitä vaiheita organisaation ERP-järjestelmän käyttöönottoprosessiin kuuluu?
- Missä ERP-järjestelmän käyttöönottoprosessin vaiheissa kyberturvariskejä ilmaantuu ja millaisia ne ovat?

Työssä johdantoluvun jälkeen esitellään tutkimusmenetelmä sekä pääosassa oleva tutkimusaineisto. Luvussa kolme tutustutaan tarkemmin ERP-järjestelmiin määrittelemällä ne ja tuomalla esille erilaisia mahdollisia toteutustapoja. Tämän lisäksi luvussa käsitellään ERP-järjestelmän merkitystä sekä tuomaa arvoa organisaatiolle. Luvussa neljä tutustutaan ERP-järjestelmän käyttöönottoprosessiin organisaatiossa jakamalla se kolmeen päävaiheeseen: kehitysvaiheeseen, käyttöönottovaiheeseen ja käyttöönottoa seuraavaan vaiheeseen. Työn viides luku käsittelee ERP-järjestelmän hankintaprosessiin vaikuttavia kyberturvauhkia. Luvussa tuodaan esille organisaation keinoja tunnistaa sekä huomioida erilaisia kyberturvariskejä ja jaetaan näitä riskejä organisaation sisäisiin sekä ulkoisiin riskeihin. Työn viimeinen luku on yhteenveto tutkimuksesta. Tässä luvussa esitellään saadut tulokset ja näistä tehdyt päätelmät.

2. TUTKIMUSMENETELMÄ

Tämä työ on toteutettu kirjallisuuskatsauksena, johon on systemaattisesti etsitty tutkimusmateriaalia liittyen ERP-järjestelmiin yleisesti, niiden toimintaan organisaatiossa sekä niihin liittyviin kyberturvauhkiin. Tiedonhaku suoritettiin aiheen rajauksen ja tutkimuskysymyksen valinnan jälkeen erilaisia tietokantoja hyödyntäen. Tässä tutkimuksessa käytettyjä hakukantoja ovat ProQuest, ResearchGate sekä Tampereen yliopiston oma Andor-palvelu. Näistä tietokannoista eniten lähteitä on haettu ProQuest-tietokannasta. Toimivaksi tavaksi hakea aineistoa todettiin myös tutkimusten lähdeluetteloiden tarkasteleminen ja tätä kautta lähdekirjallisuuden löytäminen.

Yleisesti ERP-järjestelmien kyberturvallisuutta on käsitelty kirjallisuudessa melko paljon ja trendi on viime aikoina ollut kasvavassa suunnassa. Kyberturvallisuuden merkityksen kasvaminen viime aikoina on vaikuttanut siihen, kuinka sen yhteyttä organisaatioiden erilaisiin toimiin sekä tietojärjestelmiin on käsitelty lisääntyvässä määrin.

Tiedonhakuun valitut hakulausekkeet muovautuivat sekä tarkentuivat työn aiheen suunnittelun edetessä. Hakulausekkeita myös tarkennettiin saatujen tulosten määrän perusteella rajatummaksi, jotta tiedonhaku olisi tehokkaampaa sekä tuottaisi relevantimpia tuloksia. Hakulausekkeiden yhteydessä käytettiin apuna erilaisia Boolen operaattoreita, kuten esimerkiksi AND- ja OR-operaattoreita.

Tiedonhaussa hakusanojen lisäksi on tehty erilaisia rajauksia, joiden avulla tulosten määrää on saatu rajoitettua. Käytetyn materiaalin kielenä on englanti ja työhön valittu kirjallisuus on pääosin julkaistu viimeisen reilu 10 vuoden aikana. Tämä päätös on tehty sen vuoksi, että esimerkiksi kyberturvallisuudessa sekä tietoturvallisuudessa on tapahtunut isojakin muutoksia sekä kehitystä viimeisen kymmenen vuoden aikana ja tähän työhön haluttiin näiden muutoksien vuoksi valita mahdollisimman tuoreita julkaisuja. Yleisesti ERP-järjestelmiä käsittelevät lähteet ovat vanhempia julkaisuja, mutta nämä on päätetty ottaa mukaan tiedon relevanttiuden perusteella. Vaikka ERP-järjestelmien toteutustavat tai sisällöt ovat muuttuneet myös, on pääosin teoreettinen kirjallisuus sekä tutkimukset pysyneet siten samana, että vanhempaakin materiaalia tässä työssä on päätetty hyödyntää.

Löydettyä lähdekirjallisuutta on rajattu lisää esimerkiksi otsikoiden sekä niiden tutkimuskysymykseen tuoman arvon perusteella. Eräänä tarkastelukriteerinä tiedonhaussa on myös ollut kirjallisuudessa käytetty aiheen tarkastelunäkökulma. Suorittamalla systemaattisesti tätä tekniikkaa, on lopulta päädytty tässä työssä käytettyyn kirjallisuuteen.

3. ERP-JÄRJESTELMÄ

Tässä luvussa perehdytään ERP-järjestelmiin teknologiana ja tarkastellaan erilaisia mahdollisia järjestelmiä ja toteutustapoja sekä näissä ilmeneviä yksittäisiä trendejä. Myös ERP-järjestelmän tuomia etuja, kuten esimerkiksi organisaation tehokkuudessa sekä taloudessa näkyviä hyötyjä pohditaan tässä luvussa.

ERP-järjestelmä on koko organisaation laajuinen tietojärjestelmä, jonka avulla organisaation tärkeitä ydinprosesseja voidaan seurata ja kontrolloida (Addo-Tenkorang & Helo 2011). ERP-järjestelmä pohjautuu aikaisemmin organisaatioissa laajalti käytössä olleista tuotannonohjausjärjestelmistä MRP (engl. Manufactoring Resource Planning). Nykyisin ERP-järjestelmä sisältää erilaisia moduuleja, jotka yhdistävät tuotannon ja logistiikan toimintoihin esimerkiksi rahoitukseen ja kirjanpitoon liittyvät toiminnot. (Hall 2002) ERP-järjestelmä siis integroi yhteen organisaation ydinprosesseja (She 2007).

ERP-järjestelmä voi tuoda organisaatiolle arvoa ja tehostaa sen toimintaa (Ragowsky ym. 2005). ERP-järjestelmän teknologinen sisältö voi kuitenkin vaihdella huomattavan paljon erilaisissa organisaatioissa, jonka vuoksi sen määritelmää on hankalaa taas tältä kantilta rakentaa. Monimutkaisen luonteen ja koko informaation määrän vuoksi ERP-järjestelmän käyttö ei kuitenkaan ole aina helppoa tai onnistunutta. Järjestelmän hankinta on organisaatiossa suuri investointi, jonka vuoksi siihen yhdistyy aina erilaisia riskitekijöitä (Ragowsky ym. 2005).

3.1 Erilaisia ERP-järjestelmiä

ERP-järjestelmän toteutustapoja on erilaisia ja organisaatio valitsee tarpeidensa sekä resurssiensa perusteella omaan toimintaan sisällöltään sekä teknologialtaan sopivan ratkaisun. Tässä työssä ERP-järjestelmäratkaisut jaetaan perinteisiin ERP-järjestelmiin sekä pilvipohjaisiin järjestelmiin. Tarkasteluun tuodaan myös organisaation sisäisen sekä ulkoisen ratkaisun näkökulmat sekä näiden vaihtoehtojen tuomia vaikutuksia järjestelmään ja organisaatioon.

Perinteinen ERP-järjestelmä on ohjelmisto, joka sisältää yleensä yksittäisen tietokannan, johon organisaation eri toimintojen dataa säilötään keskitetysti. Tällainen perinteinen palvelinpohjainen ERP-järjestelmä toimii itsensä sekä asiakkaan välillä. Perinteisen ERP-järjestelmän tietokanta toimii tiedon ja datana säiliönä sekä jakamisvälineenä organisaation eri osa-alueiden välillä. Perinteiset ERP-järjestelmät ovat yleensä melko raskaita ja niiden implementointiprosessi on monimutkainen ja erittäin pitkäaikainen. (Al-Ghofaili &

Al-Mashari 2014) Perinteiset ERP-järjestelmät yleensä on hankittu organisaation sisäisesti ja näin niitä myös ylläpidetään sekä hallitaan organisaation oman henkilöstön kautta.

Kasvavana trendinä perinteisissä ERP-järjestelmissä on palvelukeskeisen arkkitehtuurin käyttö (engl. Service-oriented architechture, SOA). SOA on tietojärjestelmien suunnittelun, toteutuksen ja käyttöönoton lähestymistapa, jossa tietojärjestelmän erilliset komponentit toimivat itsenäisinä palveluina, jotka toteuttavat organisaation liiketoiminnallisia toimintoja. Tällä arkkitehtuuritason suunnittelutavalla voidaan mahdollistaa joustavampi tietojärjestelmäratkaisu, joka ei ole yhtä monimutkainen mutta taas ketterämpi vastaamaan ympäristön erilaisiin muutoksiin. (Addo-Tenkorang & Helo 2011)

Perinteisten ERP-järjestelmien rinnalle on noussut pilvipohjaiset ratkaisut, jotka organisaatio yleensä hankkii ulkoiselta toimijalta. Vaikka vuosien varrella perinteisiin ERP-järjestelmiin on tehty erilaisia muutoksia esimerkiksi liittyen viestintätekniikoihin sekä informaatioarkkitehtuuriin, eivät nämä järjestelmät välttämättä sovellu onnistuneesti joillekin organisaatioille, jolloin niiden tuomien haittojen riskit nousevat suuremmiksi kuin mahdollisesti niistä saatavat hyödyt (Al-Ghofaili & Al-Mashari 2014). Pilvipalveluilla tarkoitetaan sellaista järjestelmäsuunnittelua, jossa sovellukset, palvelut tai järjestelmät ovat saatavilla verkon kautta pilvialustan myötä. Pilvipohjainen ratkaisu tarjoaa palvelun yleensä matalammalla kustannuksella sekä tekee järjestelmästä skaalautuvamman, saatavuudeltaan paremman sekä osittain myös luotettavamman. (Ali ym. 2017) Kun ERP-järjestelmä tehdään pilvipohjaisesti, se yleensä hankitaan ulkoiselta palveluntoimittajalta.

Pilvipohjaisia ERP-järjestelmiä on karkeasti jaoteltuna kahdenlaisia: palveluna tarjottava tietojärjestelmä (engl. Software as a Service, SaaS) sekä palveluna tarjottava infrastruktuuri (engl. Infrastructure as a Service, IaaS) (Al-Ghofaili & Al-Mashari 2014). Ali ym. (2017) tuo esille näiden lisäksi myös palveluna tarjottavan alustan (engl. Platform as a Service, PaaS). SaaS-pohjainen ERP-järjestelmä toimitetaan pilven kautta siten, että järjestelmää käsitetään organisaation toimittajalta tilaamana palveluna (Ali ym. 2017). IaaS-toimitustapa taas tarkoittaa sitä, että organisaation järjestelmävalvojille toimitetaan laitteistot sekä pilvialusta ulkoisen toimittajan myötä, mutta itse organisaation vastuulle jää ERP-järjestelmäpaketin hankinta, implementointi sekä asennus (Al-Ghofaili & Al-Mashari 2014). Tätä toimitustapaa voidaan hyödyntää silloin, kun ERP-järjestelmä halutaan rakentaa sekä ylläpitää oman organisaation sisäisesti. Viimeisenä, PaaS tarkoittaa taas sitä, että palvelutoimittaja antaa organisaatiolle tarvittavat työkalut sekä palvelut, jotta organisaatiolla itsellään on mahdollista rakentaa näiden avulla oma SaaS-ERP-järjestelmä (Ali ym. 2017).

Merkittävä ero organisaation sisäisesti rakennetun ratkaisun tai ulkoiselta toimittajalta hankitun järjestelmän välillä on se, ketkä sitä ylläpitävät ja hallitsevat. Riippuen organisaation resursseista, tarpeista sekä esimerkiksi taloudellisesta tilanteesta, valitaan sille toimivin tapa tuottaa ja hankkia ERP-järjestelmä. Siinä, missä suurempien organisaatioiden kannalta oma sisäisesti tuotettu järjestelmä voi olla turvallisempi ja järkevämpi valinta, on esimerkiksi pienempien ja ehkä taloudellisesti epätasapainossa olevien organisaatioiden taas järkevämpi valita pilvipohjainen, ulkoisesti hankittu ERP-järjestelmä (Al-Ghofaili & Al-Mashari 2014).

3.2 Toiminnanohjausjärjestelmän merkitys organisaatiolle

ERP-järjestelmän merkitys organisaatiolle on erittäin suuri ja järjestelmää voidaan pitää yhtenä kriittisimmistä tekijöistä organisaatioiden liiketoiminnassa. Oikein toimitettuna, rakennettuna sekä käytettynä ERP-järjestelmä voi parantaa organisaation päätöksentekoa, tehokkuutta sekä vähentää sen kuluja ja näin vaikuttaa organisaation kilpailukykyyn. (Sheik & Sulphey 2020) Vaikka ERP-järjestelmien kompleksisuuden vuoksi niiden mukana ilmenee usein erilaisia ongelmia sekä jopa epäonnistumisia organisaatioissa, on niiden hankinnan sekä käytön nähty olevan vahvasti yhteydessä organisaation parantuneeseen suorituskykyyn sekä erilaisiin aineellisiin ja aineettomiin hyötyihin (Ram ym. 2014).

Merkittävänä ERP-järjestelmän tuomana etuna organisaatiolle voidaan pitää kilpailukyvyn parantamista. Toisaalta, jotta tämä toteutuisi, tulee organisaation tehdä toimia ERP-järjestelmän ympärillä siten, että hyödyn saaminen on mahdollista. Tämä tarkoittaa esimerkiksi tiedon ja datan laadusta huolehtimista, koko ERP-järjestelmän laadusta huolehtimista sekä organisaation toimintaympäristön ymmärrystä liittyen esimerkiksi asiakkaisiin ja muihin organisaation sidosryhmiin. (Ram ym. 2014)

Kilpailukykyyn voidaan ERP-järjestelmän hankinnan myötä vaikuttaa esimerkiksi tiedon jaon tehostamisen, organisaation toimien tehostamisen sekä kustannusten alentamisen myötä.

4. ERP-JÄRJESTELMÄN KÄYTTÖÖNOTTO

ERP-järjestelmän hankintaprosessi on monimutkainen ja vaatii organisaatiolta runsaasti resurssien käyttöä. Se on erittäin stressaava liittyen esimerkiksi organisaation ajallisiin sekä rahallisiin resursseihin ja onkin melko yleistä, että hankinta- ja käyttöönottoprosessi ei onnistukaan lopulta vastaamaan täydellisesti asiakkaan toiveita ja odotuksia. (Mahmood & Miller 2017)

Tässä työssä ERP-järjestelmän käyttöönottoprosessi on jaoteltu kolmeen osaan: käyttöönottoa edeltävään vaiheeseen, käyttöönottovaiheeseen sekä käyttöönottoa seuraavaan vaiheeseen. Seuraavaksi käsitellään näitä vaiheita sekä niiden sisältöä organisaation näkökulmasta. Implementointiprosessi on hieman erilainen riippuen siitä, millaisen ERP-järjestelmän organisaatio hankkii. Esimerkiksi tämän työn aikaisemmassa luvussa esitellyt organisaation sisäiset järjestelmäratkaisut sekä ulkopuoliselta toimittajalta hankitut pilvipohjaiset ratkaisut eroavat hankintaprosessiltaan jonkin verran, mutta tässä työssä hankintaprosessia käsitellään enemmän yleisellä tasolla.

4.1 Käyttöönottoa edeltävä vaihe

Implementaatiota ja käyttöönottoa edeltävä vaihe on erittäin kriittinen, sillä tässä vaiheessa tehdyt päätökset sekä valinnat tulevat merkittävästi vaikuttamaan myös seuraaviin ERP-järjestelmän hankintaprosessin vaiheisiin (Mahmood & Miller 2017). Käyttöönottoa edeltävän vaiheen käynnistää yleisesti organisaation päätös uudistaa nykyistä järjestelmää tai hankkia kokonaan uusi ERP-järjestelmä. Kuitenkin tarpeen lisäksi hankinnan käynnistäminen vaatii organisaation johdon vahvan tuen. (Poon & Yu 2010)

Ensimmäisenä vaiheena tässä kohtaa hankintaprosessia organisaation tulee määrittää esimerkiksi suunnitelma teknologiahankinnan sulauttamiseksi osaksi organisaatiota (Mahmood & Miller 2017). Tämän lisäksi erittäin tärkeänä tehtävänä pidetään erillisen projektitiimin valitsemista toteutusprosessia varten. Jos organisaation oma osaaminen tai resurssit eivät tähän riitä, on hyvin yleistä palkata tilalle esimerkiksi konsultteja hoitamaan projektin eteenpäin viemistä. (Poon & Yu 2010)

Kun organisaatio on nimittänyt projektitiimin joko sisäisesti tai ulkoisten konsulttien avulla, tulee tämän projektitiimin yhdessä organisaation ylemmän johdon määrittää projektille vaatimukset, eli ne reunaehdot, jotka hankittavaa ERP-järjestelmää määrittävät (Jagoda & Samaranayake 2017). Koska ERP-järjestelmä integroidaan merkittäväksi

osaksi organisaation toimintaa, on tärkeää, että järjestelmä hankitaan yrityksen liiketoimintamallia sekä strategiaa noudattaen. ERP-järjestelmän hankintaan liittyy myös tietynlaisia rajoitteita, jotka liittyvät esimerkiksi tekniikkaan, aikaan sekä henkilöstöön. Nämä rajoitteet huomioiden yhdessä organisaation haluamien toiminnallisuuksien tai muiden vaatimusten kanssa määrittävät, minkälaiseen järjestelmäratkaisuun yritys lopulta päätyy. Lopulta organisaation tulee määrittää tärkeimmät kriteerit ja arvioida näiden perusteella mahdollisia järjestelmätoimittajia sekä erilaisia ratkaisuja. (Poon & Yu 2010)

Käyttöönottoa edeltävässä vaiheessa organisaation tulee valita, rakennetaanko tai päivitetäänkö järjestelmä organisaation sisäisesti, vai hyödynnetäänkö tässä ulkoisia toimittajia tai esimerkiksi pilviratkaisuja. Kun tämä päätös on tehty, voidaan organisaatiossa siirtyä hankintaprosessin vaiheeseen, jossa järjestelmä implementoidaan ja myöhemmin otetaan myös käyttöön organisaatiossa.

On hyvin tavallista, että ERP-järjestelmää hankkiva organisaatio ei löydä sellaista ratkaisua, joka toteuttaisi kaikki organisaation asettamat kriteerit. Viimeisenä käyttöönottoa edeltävässä vaiheessa organisaatio arvioi saatavilla olevat vaihtoehdot, valitsee parhaiten sopivan toimittajan ja myös parhaiten sopivan ERP-järjestelmän. (Poon & Yu 2010) Poon & Yu (2010) esittelevät arviointikriteereitä järjestelmän toimittajille, joita ovat esimerkiksi:

- Maine
- Vakavaraisuus
- Palvelun laatu ja aikataulu
- Käyttöönotossa tarjottava tuki.

Tutkimuksessaan Poon & Yu (2010) myös tuovat esille itse järjestelmän arvioimiseen liittyviä kriteereitä, kuten esimerkiksi:

- Järjestelmän toiminnallisuudet
- Hinta, luotettavuus sekä skaalautuvuus
- Kustomoinnin tarve
- Odotetut teknologiset sekä yrityksen toimintaan vaikuttavat muutokset.

Organisaation tulee siis valita vaihtoehdoista paras, jonka toimittajan kanssa siirtyy toivottavasti sopimukseen. Toimittajan sekä järjestelmän valinta on erittäin kriittinen osa hankintaprosessia (Jagoda & Samaranayake 2017).

ERP-järjestelmän päivittäminen tai hankinta saa aina muutoksia aikaan myös organisaation toimintatavoissa tai prosesseissa, joten tärkeää on huolehtia myös asenteista sekä mahdollisesta muutosvastarinnasta näitä uudistuksia kohtaan (Mahmood & Miller 2017).

4.2 Käyttöönotto- ja implementointivaihe

Kun käyttöönottoa edeltävän vaiheen valmistelut ja päätökset on saatu valmiiksi, ja sopimus ERP-järjestelmän päivityksestä tai hankinnasta on tehty, on organisaation aika siirtyä järjestelmän implementointi- ja käyttöönottovaiheeseen. Käyttöönottovaiheeseen vaikuttaa aina se, millaisen järjestelmäratkaisun organisaatio on päättänyt hankkia.

Pituudeltaan implementointi- ja käyttöönottovaihe saattaa olla hyvinkin pitkä, sillä järjestelmän kehityksen ja rakentamisen lisäksi siihen sisältyy sen integroiminen osaksi organisaation toimintaa. Tähän aikaikkunaan vaikuttaa esimerkiksi hankinnan suuruus ja se, onko kyseessä pieni vai huomattavan suuri organisaatio. (Mahmood & Miller 2017)

Tärkeää on ennen eteenpäin siirtymistä käydä läpi suunnitteluvaihe uudelleen, jotta esimerkiksi kaikki tehdyt päätökset ja valinnat ovat yhäkin ajantasaisia. Implementointivaihe vaatii onnistuakseen sen, että aikaisempi vaihe on tehty tarpeiden mukaisesti. Myös riippuen aikaisemmasta implementointia edeltävästä vaiheesta, yleensä ensimmäisenä implementointivaiheessa valitaan haluttu järjestelmä ja tehdään mahdolliset kustomoinnit. Organisaation tuleekin tätä varten selvittää tärkeimmät vaatimuksensa tietojärjestelmälle ja näiden lisäksi esimerkiksi erilaisia liiketoimintavaatimuksia, joita tietojärjestelmältä halutaan. Tämä voidaan tehdä hyödyntämällä esimerkiksi kahta erilaista strategiaa: liiketoimintastrategian luominen tietojärjestelmän infrastruktuuria painottamalla tai keskittymällä tiettyjen, spesifiin liiketoimintaan vaadittavien ominaisuuksien selvittämiseen. (Umble ym. 2003) Joka tapauksessa, organisaatio tarvitsee strategian siihen, kuinka tietojärjestelmä integroidaan osaksi sen toimintaa. Ennen järjestelmän käyttöönottoa, tulee organisaation myös analysoida tietojärjestelmämuutoksesta mahdollisesti tapahtuvia riskejä ja hyödyntää tähän esimerkiksi riskienhallinnan kehysmalleja (Mahmood & Miller 2017).

Valittuaan ja kustomoituaan ERP-järjestelmän oman suunnitelmansa mukaisesti, siirtyy organisaatio implementaatiovaiheessa järjestelmän testaamiseen sekä tätä seuraavaan asentamiseen. Jotta järjestelmä voidaan ottaa organisaatiossa käyttöön, tulee olla varmuus siitä, että järjestelmä toimii odotetusti ja on luotettava. (Umble ym. 2003) Asennusta seuraava käyttäjäkoulutus on tärkeää aloittaa välittömästi, jotta erilaisia testaukseen käytettäviä pilottitapauksia voidaan järjestää. Testausvaiheessa käytävä käyttäjä-

koulutus voi myös tehostaa myöhemmin käyttöönottoa seuraavassa vaiheessa tapahtuvaa käyttökoulutusta, sillä osa organisaation henkilöstöstä on jo työskennellyt uuden järjestelmän parissa.

Käyttöönottovaiheen lopussa organisaation on tärkeää huolehtia erilaisista sopimuksista liittyen esimerkiksi turvallisuuteen sekä käyttöoikeuksiin. Tämän lisäksi otettaessa käyttöön uutta järjestelmää vanhan järjestelmän tilanne, tulee organisaation sekä projektitiimin huolehtia siitä, että vanhan järjestelmän data siirretään oikeassa muodossa luotettavasti uuteen järjestelmään. (Umble ym. 2003) Dataa voidaan siirtää esimerkiksi tehokkaasti automatisoidusti tai joissakin tapauksissa manuaalisesti.

Kun tarvittavat järjestelyt, koulutukset sekä testaus on tehty, voi organisaatio siirtyä implementaatiovaiheessa järjestelmän viralliseen käyttöönottoon ja integrointiin osaksi organisaation toimintaa. Lopulliseen käyttöönottoon on olemassa kaksi yleistä tapaa: joko kerralla tehtävä täysi siirtymä tai asteittain toteutettava muutos. Totaalinen siirtymä toteutetaan siten, että koko organisaatio varustautuu järjestelmän kerralla tehtävään käyttöönottoon. (Umble ym. 2003) Tämä voidaan toteuttaa esimerkiksi loma-aikana tai muuten sellaisena ajankohtana, jolloin käyttöönotosta seuraavat mahdolliset häiriöt vaikuttavat organisaation toimintaan mahdollisimman vähän. Asteittain toteutettava käyttöönotto taas tarkoittaa sitä, että järjestelmän moduulit tai osat otetaan peräkkäin vähän kerrallaan käyttöön (Umble ym. 2003) ja esimerkiksi uutta järjestelmää käytetään päällekkäin vanhan järjestelmän ohella. Tällöin järjestelmän käyttöönottoprosessi on rauhallisempi ja saattaa aiheuttaa vähemmän häiriötä, mutta se on myös huomattavasti pitkäaikaisempi. Valittu käyttöönottotapa vaikuttaa järjestelmän elinkaaren tuleviin vaiheisiin, jotka ilmenevät käyttöönottoa seuraavassa vaiheessa (Law ym. 2010).

4.3 Käyttöönottoa seuraava vaihe

Järjestelmän implementaatio ja käyttöönotto ei ole ERP-järjestelmäprosessin loppu, vaan erittäin suuri paino on myös tätä hankintaa ja käyttöönottoa seuraavalla vaiheella, jossa järjestelmää aletaan käyttämään. Käyttöönottoa seuraavaan vaiheeseen kuuluu esimerkiksi käyttökoulutusta sekä järjestelmän tehokkuuden ja tuoman hyödyn testaamista ja mittaamista. (Mahmood & Miller 2017)

ERP-järjestelmän käyttöönottoa seuraava vaihe voidaan jakaa kahteen tasoon: rutiini ja infuusio. Rutiinilla tarkoitetaan sitä vaihetta, jossa järjestelmä liitetään osaksi organisaation toimintaa ja erityisesti rutiinitoimintoja. Infuusiolla taas tarkoitetaan sitä, että organisaatiossa etsitään uutta innovaatiota tai keskitytään haittatilanteiden, kuten esimerkiksi bugien tai vanhentuneiden osien korjaamiseen. Erityisesti infuusiovaihe on merkittävä,

sillä sen avulla järjestelmää voidaan päivittää muuttuvien tarpeiden tai vaatimusten mukaisesti ja huolehtia siitä, että se toimii luotettavasti ja halutulla tavalla. (Law ym. 2010) Rutiinivaiheessa merkittävässä osassa on käyttäjille järjestetty järjestelmän käyttökoulutus ja tätä voidaankin järjestää joko organisaation sisäisesti tai esimerkiksi implementointiprosessiin hankittujen konsulttien avulla.

Kun järjestelmä on organisaatiossa käytössä, tulee myös tarkkailla sekä mitata sen tehokkuutta sekä organisaatiolle tuomaa arvoa. Myös erilaisten ongelmien seuraaminen sekä etsiminen on olennainen osa järjestelmän käyttöönoton elinkaarta, sillä näin tarkkaillaan, halutaanko järjestelmää ehkä päivittää lisää tai vaihtaa kenties kokonaan uuteen järjestelmään.

5. ERP-JÄRJESTELMÄN KÄYTTÖÖNOTON KYBERTURVALLISUUS

Terminä kyberturvallisuus on hyvin laaja. Kyberturvallisuus kattaa alleen kaikki ne erilaiset rakenteet, toimintatavat ja prosessit, joilla pyritään turvaamaan sekä ylläpitämään organisaation tietojärjestelmät tapahtumilta, jotka niiden turvallisuutta voisivat heikentää (Craigen ym. 2014). Kyberturvallisuuden määrittelytapa riippuu sen kontekstista ja esimerkiksi organisaation omasta käsityksestä ja tavasta harjoittaa sitä. Kyberturvallisuus on nykyisin hyvin pinnalla oleva aihe, johon organisaatioiden tulee keskittyä. Teknologian sekä organisaatioiden kehittyessä nopeasti eteenpäin, tulee organisaatioiden onnistua reagoimaan sekä nopeasti että tehokkaasti kyberturvallisuuteen sekä siihen liittyviin erilaisiin muutoksiin.

ERP-järjestelmä on merkittävässä osassa organisaation toimintaa, jonka vuoksi sen turvaaminen erilaisia kyberturvallisuusriskejä vastaan on tärkeää. Näitä järjestelmiä käytetään erilaisilla jopa kriittisillä toimialoilla, kuten esimerkiksi terveydenhuollossa tai turvallisuusalalla, jolloin sen turvaaminen on erittäin tärkeää (She & Thuraisingham 2007). ERP-järjestelmän luonteen sekä sen sisältämän datan vuoksi kyberturvallisuus on tärkein sen turvallisuuden osa-alue (Hrischev 2020).

5.1 ERP-järjestelmän kyberturvariskien tiedostaminen ja ehkäisy

ERP-järjestelmien kehittyessä yhä eteenpäin on organisaatioille erittäin tärkeää muodostaa tavat tiedostaa riskejä sekä tämän myötä myös ehkäisykeinot näille riskeille. Tämän lisäksi organisaatioilla tulee olla järkevät ja toimivat toimintasuunnitelmat riskien toteutumisen varalle. Esimerkiksi erilaisten kehysmallien avulla organisaatiot voivat tunnistaa osa-alueita, jotka vaativat turvaamista tai jotka voivat olla haavoittuvia.

Tämän lisäksi on tärkeää käyttää erilaisia apuohjelmia, jotka testaavat järjestelmiä haavoittuvuuksien varalta. Tällaisia voivat olla esimerkiksi Acunetix tai WireShark. Myös erilaisten omien testien, kuten esimerkiksi penetraatiotestien tai tietokantatestien suorittaminen auttaa organisaatiota ymmärtämään oman järjestelmän turvallisuutta. Ohjelmistojen lisäksi konsulttipalveluiden tai esimerkiksi valkohattuhakkereiden palkkaaminen auttaa organisaatiota tunnistamaan mahdollisia riskikohtia. (Ali Süzen 2020)

She & Thuraisingham (2007) tuovat esille muutamia malleja, joiden avulla ERP-järjestelmän turvallisuutta voidaan tarkastella. Näitä malleja voidaan käyttää myös hyväksi

mahdollisten riskien tunnistamisessa. Erityisen tärkeää on ymmärtää se, mistä ja miten erilaiset hyökkäykset voidaan tehdä, sillä hyvin iso osa hyökkääjistä hyödyntää juuri organisaation sokeita pisteitä ja heikkouksia vahingon tekemiseen (Osman ym. 2019).

Iso osa ERP-järjestelmään liittyvistä riskeistä voidaan sulkea pois luomalla siihen tarkka seuranta siitä, kuka voi mitäkin järjestelmässä tehdä. Organisaation rakentaessa suunnitelmaa järjestelmän kyberturvariskien varalle, on käyttäjien seuranta sekä annetut luvat ja rajoitteet tärkeä osa sitä (She & Thuraisingham 2007). Rajoitteita tekemällä voidaan pyrkiä ehkäisemään kyberturvallisuusuhkia liittyen esimerkiksi tietovuotoihin tai käyttäjän tekemiin virheisiin. Tähän liittyen, esimerkiksi käyttäjän tunnistautumista vaatimalla voidaan myös vaikuttaa siihen, kuka pystyy järjestelmässä mitäkin tekemään ja varmistua myös siitä, että järjestelmää käyttävät juuri ne henkilöt, jolla siihen on oikeus.

Useita ongelmia voidaan myös ehkäistä tekemällä järjestelmästä sellainen, että se tarkistaa pakolliset vaatimukset eri toimintoja tehtäessä. Tämä tarkoittaa sitä, että ennen kuin jokin toiminto suoritetaan, tarkastaa järjestelmä, että siihen vaadittavat pakolliset vaatimukset on täytetty ja ilman tätä toimintoa ei suoriteta. Samaa käytäntöä voidaan hyödyntää siten, että järjestelmä varmistaa prosessien statuksen ja ympäristön tilanteen ennen suoritettuja toimenpiteitä. (She & Thuraisingham 2007)

Myös datan siirtyminen ja tiedon jakamisen tulee olla järjestelmässä turvattua ja esimerkiksi dokumenttien salattuja. ERP-järjestelmän laajentuessa ja muuttuessa monimutkaisemmaksi, tulee organisaation huolehtia myös siihen liittyvien eri komponenttien, kuten esimerkiksi käyttöliittymän ja tietokannan turvallisuudesta ja varmistaa se, että näistä mihinkään ei liity haavoittuvuuksia, jotka voisivat johtaa koko järjestelmän vaarantumiseen. Pilvipohjaisten järjestelmien yleistyessä tulee myös huomioida näihin liittyvät turvallisuuspiirteet. (She & Thuraisingham 2007)

Tärkeä osa kyberturvallisuusuhkien ehkäisyä on myös tietojärjestelmän päivittäminen sekä huolehtiminen siitä, että komponentit eivät ole vanhentuneita. Myös tietoturvapäivitysten tekeminen mahdollisten haavoittuvuuksien löytyessä vie tietojärjestelmää yhä turvallisemmaksi.

5.2 Sisäiset riskit

ERP-järjestelmään liittyvillä organisaation sisäisillä riskeillä tarkoitetaan niitä riskejä, jotka ilmenevät organisaation omista, sisäisistä toimista. Näihin riskeihin ei vaikuta ulkoiset toimijat vaan organisaatio sekä sen jäsenet. Tässä työssä sisäisiin riskeihin on otettu mukaan myös itse järjestelmään sekä sen kehitykseen liittyvät riskit.

5.2.1 Sisäiset tekniset kyberturvariskit

Iso osa tärkeistä ERP-järjestelmän kyberturvauhista voidaan välttää itse järjestelmän implementaatiovaiheessa. Tässä vaiheessa järjestelmästä voidaan tehdä turvallinen ja kestävä erilaisilta haavoittuvuuksilta. Järjestelmää suunniteltaessa tulee huolehtia, että sen sisältämä data liikkuu turvallisesti oikeissa paikoissa ja pysyy muuttumattomana. Tietoon liittyvänä riskinä voidaan myös pitää sitä, jos data ei ole saatavilla silloin kun sille on tarvetta.

Jos ERP-järjestelmässä ei ole käytössä erilaisia tunnistukseen tai todentamiseen liittyviä prosesseja tai algoritmeja, vaikuttaa se huomattavasti myös ulkoisten kyberturvariskien muodostumiseen, sillä järjestelmä saattaa jäädä helposti haavoittuvaksi ja näin helpoksi kohteeksi esimerkiksi kyberturvahyökkäyksille. Myös erilaisten salausalgoritmien käytön puute johtaa siihen, että data on haavoittuvaa. (Ali Süzen 2020)

Järjestelmän kehitysvaiheessa riskejä liittyy erityisesti juuri itse tietojärjestelmän implementaatioon, mutta myös järjestelmän käyttäjien luomiseen sekä näiden käyttöoikeuksien luomiseen. Tässä vaiheessa suurena riskinä on se, että jos rajoituksia ei luoda niin käyttöönottovaiheessa käyttäjät saattavat esimerkiksi inhimillisten virheiden myötä aiheuttaa suuriakin ongelmia järjestelmän turvallisuudessa. Ilman käyttörajoitteita nousee myös suuri riski liittyen tietoturvallisuuteen sekä tiedon päätymiseen vääriin käsiin. Tällöin käyttäjä, jolla ei välttämättä ole tarvittavia oikeuksia voi päästä käsiksi haavoittuvaan tai arkaluontoiseen organisaation dataan. Tällöin myös riski erilaisista tietovuodoista kasvaa, sillä käyttäjä voi tahattomasti tai tahallaan jakaa tätä tietoa eteenpäin tahoille, joille se informaatio ei kuulu. (Hrischev 2020).

5.2.2 Sisäiset sosiaaliset kyberturvariskit

Sosiaalisina riskeinä tässä työssä pidetään sellaisia, jotka liittyvät suoraan järjestelmää käyttäviin henkilöihin. Kun kyseessä on organisaation sisäisiä, sosiaalisia riskejä, puhutaan siis esimerkiksi organisaation työntekijöihin tai muihin sisäisiin sidosryhmiin liittyvistä riskeistä. Järjestelmän käyttäjien tekemät vahingot tai virheet liittyen ulkopuolisiin hyökkäyksiin kuten esimerkiksi tietojenkalasteluun, käsitellään vasta seuraavassa alaluvussa.

Edellisessä alaluvussa esiin nousseet käyttäjien inhimilliset vahingot tai tahalliset teot ovat erittäin merkittävä osa sosiaalisia riskejä. Merkittävin riskitekijä käyttäjiin liittyen syntyy siitä, jos organisaatio ei huolehdi työntekijöiden riittävästä koulutuksesta kyberturval-

lisuuteen liittyen. Osaamaton ja kyberturvallisuutta ymmärtämätön käyttäjä saattaa vahingossa saattaa järjestelmän huomattavaan vaaraan. Tiedotus esimerkiksi turvallisista salasanoista ja yhtenäisistä toimintaperiaatteista liittyen esimerkiksi ohjelmistojen käyttöön tai fyysiseen kyberturvaan, kuten laitteiden oikeaoppiseen sulkemiseen on erittäin tärkeää, jotta käyttäjien virheiltä vältyttäisiin. Toisaalta virheiden sattuminen on normaalia, joten näitä varten organisaatiolla tuleekin olla oikeanlaiset protokollat ja toimintaperiaatteet seurauksien minimoimiseksi.

Organisaation sisäisesti tulee huolehtia siitä, että työntekijät ymmärtävät esimerkiksi salassapitovelvollisuuden ja sen, että organisaation informaatiota ei voi jakaa ulkopuolisille henkilöille. Toisaalta tulee myös huolehtia siitä, että tieto ei itse organisaationkaan sisällä välttämättä leviä hallitsemattomasti, sillä tällöin riski vääriin käsiin joutumisesta kasvaa yhä suuremmaksi. (Yuchong & Qinghui 2021)

5.3 Ulkoiset riskit

Tässä alaluvussa käsitellään ERP-järjestelmään vaikuttavia ulkoisia kyberturvariskejä, jotka aiheutuvat ulkoisen vaikuttajan toimesta. Ulkoisia hyökkääjiä voivat olla esimerkiksi hakkerit ja hakkeriryhmät, toiset organisaatiot tai valtiot jopa kyberterrorismia harjoittavat toimijat (Yuchong & Qinghui 2021). Tähän sisältyy siis niitä riskejä, joita aiemmassa alaluvussa ei ole käsitelty. Kyberriskien mahdollisuuksien kasvaessa jokainen järjestelmä ja organisaatio voi olla vaarassa (Ostrowski 2021), joten niiden huomioiminen on erittäin tärkeää.

5.3.1 Kyberhyökkäykset

Ehkä yleisin ulkoinen kyberturvariski, joka tietojärjestelmiin ja myös ERP-järjestelmään liittyy, on erilaiset kyberhyökkäykset. Koska teknologiat ovat nousseet yhä merkittävämpään asemaan yhteiskunnissa on myös kybersodankäynti ja kyberhyökkäykset yleisestikin nousseet merkittävämmäksi uhaksi.

Ali Süzen (2020) esittelee kaksi erilaista kyberhyökkäystyyppiä: palvelunestohyökkäykset sekä haittaohjelmat. Palvelunestohyökkäyksillä tarkoitetaan hyökkäyksiä, jotka estävät järjestelmän käytön kokonaan. Tämä voidaan suorittaa esimerkiksi kuormittamalla järjestelmän liikennettä niin paljon, että käyttö estyy. (Yuchong & Qinghui 2021) Haittaohjelmia voivat taas olla esimerkiksi erilaiset virukset, vakoiluohjelmat tai näppäilytallentimet (Ali Süzen 2020). Tällaisten ohjelmien avulla ulkoinen hyökkääjä voi joko kerätä järjestelmän tapahtumia tai dataa itselleen tai päästä muuten käsiksi järjestelmän sisäi-

seen informaatioon. Tällaisia kyberhyökkäyksiä voi toteuttaa joko verkon kautta hakkeroimalla tai esimerkiksi käyttäjien sähköpostiin lähetettyjen hyökkäysten kautta. Käyttäjien kautta suoritetut hyökkäykset ovat erittäin suuri riski etenkin silloin, jos organisaation jäsenillä ei ole tietoa vaarallisista viesteistä tai esimerkiksi siitä, kuinka epäluotettavia linkkejä tai tiedostoja ei tule avata.

Yleinen kyberrikollisten myös käyttämä tekniikka on Man-in-the-Middle-hyökkäys, jossa hakkeri tunkeutuu viestijöiden väliin salakuuntelemaan tai keräämään dataa esittämällä olevansa toinen viestinnän osapuoli (Yuchong & Qinghui 2021).

Organisaation tulee myös huolehtia eri teknologioiden yhteensopivuudesta ja kaikkien saman verkon laitteistojen turvallisuudesta, sillä hyökkäys ERP-järjestelmään voidaan suorittaa myös toisen järjestelmän kautta levittämällä haitallista koodia eteenpäin (Osman ym. 2019).

5.3.2 Muita ulkoisia kyberuhkia

Perinteisten kyberhyökkäysten sekä virusten levittämisen lisäksi organisaatioiden tulee ERP-järjestelmiä hankkiessa huomioida myös muut ulkoiset uhat. Tietojenkalastelu on ehkä yleisin ulkoisten hyökkääjien käyttämä tapa pyrkiä saamaan käsiinsä dataa tai informaatiota, jota voi organisaation haitaksi käyttää. Tietojenkalastelussa hyökkääjä saattaa esiintyä esimerkiksi organisaation sisäisenä tahona tai muuna virallisena tahona ja pyrkiä huijaamaan käyttäjiä antamaan tätä kautta luottamuksellisia tietoja. Yleinen tapa tehdä tätä on esimerkiksi sähköpostiviestien tai muun viestintävälineen kautta. (Yuchong & Qinghui 2021) Hyökkääjä voi myös tarkkailla verkkoliikennettä vakoiluohjelman avulla, jolloin esimerkiksi salasanat ja muut käyttäjätunnukset voivat olla vaarassa (Osman ym. 2019).

Ulkoisena uhkana voidaan myös pitää fyysisiä hyökkäyksiä, joissa esimerkiksi pyritään tuhoamaan tai saamaan pääsy organisaation ERP-järjestelmään. Toisaalta sosiaalinen uhka syntyy myös siten että ulkopuolinen henkilö pyrkii urkkimaan tietoa organisaation jäseniltä erilaisilla keinoilla, joihin ei välttämättä liity huijausviestit tai varsinaiset kyberhyökkäykset.

YHTEENVETO JA POHDINTA

Tässä tutkielmassa esitettiin erilaisia ERP-järjestelmiä sekä näiden hankintaprosessiin liittyviä kyberturvallisuusuhkia. Työssä on myös tarkasteltu hieman erilaisia tapoja ennakoida ja varautua erilaisiin ERP-järjestelmän hankintaprosessin aikana ilmeneviin kyberturvariskeihin. Näiden lisäksi esille on tuotu myös joitakin tapoja, joiden avulla organisaatiossa voidaan pyrkiä ehkäisemään todennäköisimpiä kyberturvallisuusuhkia. Tutkielman tavoitteen mukaisesti aineistosta on onnistuttu tässä työssä löytämään erilaisia kyberturvallisuusuhkia, jotka ovat joko organisaation sisäisiä tai ulkoisia tekijöitä, ja jotka voivat vaikuttaa ERP-järjestelmän toimintaan.

ERP-järjestelmät sekä näihin liittyvät kyberturvallisuusuhat ovat melko suuressa huomiossa tällä hetkellä, sillä organisaatioiden kaikkien tietojärjestelmien muuttuessa yhä kompleksisemmiksi ja moniulotteisemmiksi kasvaa myös niihin liittyvien uhkien todennäköisyys. Koska ERP-järjestelmät ovat sisältämänsä datan vuoksi erittäin tärkeä osa organisaatioiden toimintaa, ovat ne myös löydetyn aineiston perusteella melko suuressa riskissä esimerkiksi kyberhyökkäyksille.

Tarkastellun aineiston perusteella ERP-järjestelmään liittyvää kyberturvaa on käsitelty vielä kuitenkin melko pintapuolisesti kyberturvallisuuden vasta viime aikoina kasvaneen merkityksen vuoksi. Vaikka kyberturvallisuus on ollut esillä, on ERP-järjestelmien kohdalla sitä käsitelty kuitenkin melko pintapuolisesti. Tehdyt tutkimukset perustuvat enemmän esimerkiksi yleisesti organisaatioiden tietojärjestelmien kyberturvallisuuteen eikä esimerkiksi ERP-järjestelmän modulaarisuuden tuomia mahdollisia uhkia tai vaikeuksia ole kovin paljoa käsitelty. Kuitenkin aineistot käsittelevät kyberturvallisuutta tietojärjestelmätasolla niin laajasti, että tätä on pystytty hyödyntämään myös ERP-järjestelmää tarkasteltaessa.

Tämän työn aiheen voidaan todeta olevan ajankohtainen ja tärkeä ERP-järjestelmien kriittisyyden vuoksi. Tutkimuksen sekä tietämyksen lisääntyessä voidaan kyseisten järjestelmien turvallisuutta parantaa yhä ennestään ja organisaatioiden osaamisen kasvaessa voidaan jatkuvasti kehittyviin kyberuhkiin vastata entistä paremmin.

Tutkielman vahvuutena on erilaisten kyberturvauhkien esittely sekä ERP-järjestelmän hankintaprosessin laaja tarkastelu. Hankintaprosessin monimutkaisuuden ymmärtäminen on erittäin merkittävä osa koko hankinnan onnistumista, mutta myös parantaa tässä kontekstissa organisaation valmistautumista erilaisten kyberturvaongelmien ehkäisyyn.

Tässä työssä heikkoutena kuitenkin on kyberuhkien melko pintapuolinen esittely. Todellisuudessa kyberturvallisuuteen liittyviä uhkia on lukematon määrä ja nykyisin niitä voi muodostua hyvinkin erilaisissa tilanteissa sekä organisaation sisällä että ulkopuolella. Työn laajuuden rajoituksen vuoksi näitä kaikki kyberturvallisuusuhkia ei kuitenkaan voitu käydä kovin perusteellisesti läpi. Tähän vaikuttaa myös aineiston haussa esiin ilmennyt seikka: kyberuhkia ei selitetä aineistoissa kovin perusteellisesti, vaan usein nämä on oletettu lukijan tietävän jo etukäteen. Osa-alueiden pääkohdat sekä tärkeimmät tekijät on kuitenkin tässä työssä esitelty riittävällä tasolla.

Jatkossa uskon kyberturvallisuuden nousevan yhä merkittävämmälle tasolle organisaatioiden tietojärjestelmissä kuten myös ERP-järjestelmässä. Uskon myös, että kyberrikolliset tulevat omalta osaltansa kehittymään myös taitavammiksi ja erilaiset hyökkäykset tulevat olemaan yhä hankalempi torjua. Kuitenkin, pitämällä tieto- ja kyberturvallisuuden teknologioiden sekä tietojärjestelmien kehityksen yhtenä merkittävimpänä osa-alueena voidaan näitä kasvavia uhkia pyrkiä ehkäisemään sekä myös torjumaan.

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 (WCECS 2011).

Ali, M., Nasr, E. & Gheith, M. (2017). Benefits and Challenges of Cloud ERP Systems - A Systematic Literature Review. Future Computing and Informatics Journal. 1.

Ali Süzen, A. (2020) A Risk-Assesment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. International Journal of Computer Network and Information Security. Vol. 15(1), pp. 1-12.

Al-Ghofaili, A.A. & Al-Mashari, M.A. (2014). ERP system adoption traditional ERP systems vs. cloud-based ERP systems. Fourth edition of the International Conference on the Innovative Computing Technology (INTECH 2014). pp. 135-139.

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining cybersecurity. Technology innovation management review. Vol. 4(10), pp. 13-12.

Hall, R. (2002) Enterprise resource planning systems and organizational change: transforming work organization? Strategic Change. Vol. 11 (5), pp. 263.

Hrischev, R. (2020) ERP systems and data security. IOP Conference Series. Materials Science and Engineering. 878(1).

Jagoda, K. & Samaranayake, P. (2017) An integrated framework for ERP system implementation. International Journal of Accounting and Information Management. Vol. 25 (1), pp. 91-109.

Law, C.H.C., Chen, C.C & Wu, J.P.B. (2010) Managing the full ERP life-cycle: Considerations of maintenance and support requirements and IT governance practice as integral elements of the formula for successful ERP adoption. Computers in Industry. Vol. 61(3), pp. 297-308.

Mahmood, A. & Miller, L. (2017) ERP system implementation in large enterprises – a systematic literature review. Journal of Enterprise Information Management. Vol. 30(4), pp. 666-692.

Misra, S.C. & Bisui, S. (2019) Security Determinants in ERP Systems: Modeling and Analysis. Software Quality Professional. Vol. 22 (1), pp. 9-22.

Poon, P. & Yu, Y.T. (2010) Investigating ERP systems procurement practice: Hong Kong and Australian experiences. Information and Software Technology. Vol. 52(10), pp. 1011- 1022.

Osman, A., Rehman, A. & Habib, A. (2019) Industrial control system cybersecurity best practices. Barrington. Vol. 66(5), pp. 24-26.

Ostrowsky, S. (2021) ERP system security. Cleveland. Vol. 32(10), pp. 36.

Ragowsky, A., Somers, T.M. & Adams, D.A. (2005) Assessing the Value Provided by ERP Applications Through Organizational Activities. Communications of the Association for Information Systems. Vol. 16, pp. 18.

Ram, J., Corkindale, D. & Wu, M. (2014) ERP adoption and the value creation: Examining the contributions of antecedents. Journal of Engineering and Technology Management. Vol. 33, pp. 113-133.

Sarkis, J. & Gunasekaran, A. (2003) Enterprise resource planning—modeling and analysis. European journal of operational research. Vol. 146 (2), 229–232.

She, W. & Thuraisingham, B. (2007) Security for Enterprise Resource Planning Systems. Information Systems Security. Vol. 16 (3), pp. 152-163.

Sheik, P.A. & Sulphey, M.M. (2020) Enterprise Resource Planning (ERP) As a Potential Tool for Organizational Effectiveness. Webology. Vol. 17(2), pp. 317-327.

Umble, E.J., Haft, R.R & Umble, M.M. (2003) Enterprise resource planning: Implementation procedures and critical success factors. European Journal of Operational Research. Vol. 146 (2), pp. 241-257.

Yuchong, L & Qinghui L. (2021) A comprehensive review study of cyberattacks and cyber security; Emerging trends and recent developments. Energy Reports. Vol. 7, pp. 8176-8186.