Sara Carlsson

TIETORISKIEN HALLINTA PK-YRITYKSEN DIGITALISOITUMISESSA

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tuotantotalouden koulutusohjelma
Huhtikuu 2020

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Huhtikuu 2020	**Tekijä/tekijät** Sara Carlsson
Koulutusohjelma Tuotantotalous		
Työn nimi TIETORISKIEN HALLINTA PK-YRITYKSEN DIGITALISOITUMISESSA		
Työn ohjaaja FM Joni Jämsä		**Sivumäärä** 34
Työelämäohjaaja Ins.AMK Minna Sipilä		

Opinnäytetyön toimeksiantaja oli Centria-ammattikorkeakoulun tietoturvan kehittämishanke. Opinnäytetyön tarkoituksena oli laatia digitalisoituvien pk-yritysten tarpeisiin kolme riskienkartoituskuviota eri tilanteisiin. Tavoitteena oli selvittää, minkälaiset tietoriskit yrityksiä uhkaavat ja kuinka niitä vastaan voidaan varautua.

Opinnäytetyön teoriaosuudessa käsiteltiin digitalisaatiota sekä sen vaikutuksia yritysten toimintaan ja sen mahdollistamiin uusiin toimintatapoihin. Tämän lisäksi teoriaosuudessa käsiteltiin tietoturvaa, tietosuojaa sekä riskienhallintaa erityisesti tietoriskien näkökulmasta.

Käytännön osuus toteutettiin teoriaosion sekä kirjallisuuden ja sähköisten artikkeleiden pohjalta. Opinnäytetyön tuloksena selvisi, että tietoturva on enemmän riippuvaista hallinnollisista toimenpiteistä kuin teknisistä. Tärkeintä on henkilöstön osaaminen ja tietoturvakäytänteiden laatiminen. Tarvittaessa tilaamalla järjestelmät toimittajalta, pk-yritykset eivät tarvitse niin paljon omaa järjestelmä osaamista ja voivat sen avulla suojautua myös tietoriskeiltä.

Asiasanat
Digitalisaatio, riskienhallinta, tietoriski, tietosuoja, tietoturva

ABSTRACT

Centria University of Applied Sciences	Date	Author
	April 2020	Sara Carlsson

Degree programme
Industrial Management

Name of thesis
INFORMATION RISK MANAGEMENT IN THE DIGITALIZATION OF SMES

Instructor	Pages
M.Sc. Joni Jämsä	34

Supervisor
B.Sc. Minna Sipilä

This thesis was commissioned by the information security development project of Centria University of Applied Sciences'. The purpose of the thesis was to form three risk mapping figures for small and medium-sized enterprises to different situations. The aim was to examine what kinds of information risks threaten companies and how to prepare for them.

The theoretical part of the thesis discusses digitalization and its effects on the operations of companies and the new ways of operating made possible by it. In addition to this, the theoretical part discuss data security, data protection and risk management, especially from the perspective of data risks.

The practical part was executed on the basis of the theoretical part as well as literature and electronic articles. As a result of the thesis, it became clear that information security is more dependent on administrative measures than on technical ones. The most important thing is the competence of the personnel and the development of information security practices. If necessary, by ordering the systems from a supplier, small and medium-sized enterprises do not need so much expertise of their own and can also protect themselves against data risks.

Key words
Digitalization, data protection, information risk, information security, risk management

KÄSITTEIDEN MÄÄRITTELY

Alustatalous	Digitaalisen alustan kautta tapahtuvaa kaupankäyntiä
Digitalisaatio	Tiedonkäsittely tietokoneen ymmärtämässä muodossa, mutta käsite kattaa myös laajemman yhteiskunnallisen muutoksen.
Digitalisoituminen	Fyysisesti tehtävä asia muutetaan digitaalisesti tehtäväksi
GDPR	(General Data Protection Regulation) EU:n yleinen tietosuoja-asetus
Henkilötietojen käsittelijä	Henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun
ISO 31000	Standardi riskienhallintaan
Liiketoimintamalli	Kuvaa sitä, miten yrityksen ansainta tapahtuu
Palvelunestohyökkäys	Verkkopalvelun palvelinten lamauttaminen kohdistamalla niihin suuri määrä dataa tai häiritsemällä muilla keinoin niiden toimintaa
Pitkä häntä	Tuotevalikoiman vähän myyvä, mutta monipuolistava osuus
Pk-yritys	Yritys, jossa on alle 250 työntekijää tai, jonka liikevaihto on vähemmän kuin 50 miljoonaa euroa vuodessa
Rekisteröity	Yksityishenkilö, jonka henkilötietoja käsitellään
Rekisterinpitäjä	Henkilö, yritys, tai muu yhteisö, joka määrittelee henkilötietojen käsittelyn keinot sekä tarkoitukset

SME	(Small and Medium-sized Enterprise) Pk-yritys, jossa on alle 250 työntekijää tai, jonka liikevaihto on vähemmän kuin 50 miljoonaa euroa vuodessa
Tietoturvallisuus	Tiedon luotettavuuden, eheyden sekä saatavuuden takaaminen
Tietosuoja	Yksilön oikeus omiin tietoihinsa ja henkilötietojen vaatimuksenmukainen käsittely
Tietoriski	Yrityksen tietoihin kohdistuvat uhkat
VPN	(Virtual Private Network) Virtuaalinen erillisverkko
Yksityisyydensuoja	Henkilön oikeus yksityisyyteen tietojenkäsittelyssä ja omassa yksityiselämässään. Yksityisyydensuoja on perustuslain turvaama oikeus

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVIOT

1 JOHDANTO

Digitalisaatio on muuttanut jokaisen ihmisen arkea. Yritysten kilpailukenttä on muuttunut ja turvatakseen toimintansa jatkuvuuden, yritysten on otettava käyttöön uusia tietojärjestelmiä sekä lisättävä digitaalisia palveluita asiakkaille. Jotta digitalisaatio on mahdollista, täytyy tietoturva-asiat ottaa huomioon. Digitalisaation myötä tietoturvariskit ovat kasvava uhka yrityksille. Myös yritysten vastuu tietosuojasta on kasvanut. Euroopan unionin tietosuoja-asetus on lisännyt kuluttajien oikeuksia tietää, mitä tietoja heistä kerätään. Pk-yrityksissä harvemmin on tietoturvavastaavaa, mutta tietoturva on siitä huolimatta merkittävä osa yrityksen kokonaisturvallisuutta. Suurin rooli tietoturvasta on ihmisten käsissä, tekninen puoli on vähemmistöä.

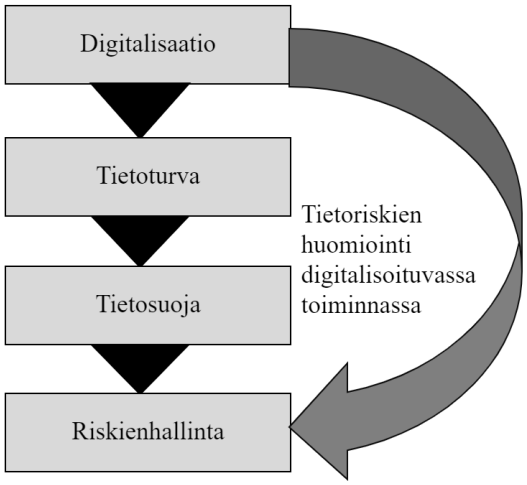
Opinnäytetyöni on Centria-ammattikorkeakoulun tietoturvan kehittämisprojektin toimeksianto. Projektin tavoitteena on kannustaa pk-yrityksiä riskienottoon, rohkaista niitä digitalisoimaan toimintaansa sekä lisätä pk-yritysten valmiuksia kansainväliseen toimintaan. (Centria-ammattikorkeakoulu 2018.) Opinnäytetyöni tutkimusongelma on: Mitä tietoriskejä pk-yrityksen tulee huomioida digitalisoidessaan toimintaansa ja kuinka niihin tulee varautua? Pyrin valitsemaan tutkimukseni aiheet sen mukaan, mitkä olisivat pk-yrityksille helppoja ja mahdollisia toteuttaa sekä myös ajankohtaisia. Tutkimus ongelma rajataan koskemaan alla mainittuja tapauksia:

1. Verkkokaupan tietoriskit
2. Etätyöskentelyn tietoriskit
3. Toimitusketjun hallinnan digitalisoitumisen tietoriskit

Opinnäytetyön käytännön osuus toteutettiin teoriaosioon sekä lähdekirjallisuuteen ja sähköisiin artikkeleihin nojautuen. Käytännön osuudessa tavoitteenani on kartoittaa riskejä edellä mainituille tapauksille ja tehdä havainnollistava kuvio tietoriskeistä sekä niiden torujumisesta. Riskit rajataan koskemaan ainoastaan tietoriskejä sekä niitä esitetään neljästä viiteen kustakin tapauksesta. Opinnäytetyöni tuloksena syntyy kolme riskikartoituskuviota eri tilanteisiin.

Opinnäytetyöni aihe on laaja ja lähdemateriaalia oli paljon saatavissa. Käytin opinnäytetyön teoriaosiossa lähteenä alan kirjallisuutta sekä sähköisiä materiaaleja. Opinnäytetyön teoreettinen viitekehys on esitettynä kuviossa 1. Luvussa kaksi käsitellään digitalisaatiota sekä sen vaikutuksia yritysten toimintaympäristöjen muutoksiin. Yritysten toimintaympäristöt ovat muuttuneet merkittävästi niin asiakkaiden

muuttuneen käyttäytymisen kuin kilpailuympäristön muutoksen seurauksena. Digitalisaation seurauksena yritysten on kehitettävä liiketoimintamallejaan, jotta ne pysyvät elinvoimaisena. Teoriaosuuden luvussa kolme käsittelen tietoturvaa sekä sen eri osa-alueita sekä mitkä tekijät vaikuttavat siihen. Luvussa neljä selvitän, mitä tarkoitetaan tietosuojalla ja käyn läpi toukokuussa 2018 velvoittavaksi muuttuneen Euroopan unionin tietosuoja-asetuksen keskeisimmän sisällön. Luvussa viisi käyn läpi riskienhallinnan prosessia yleisellä tasolla sekä esittelen tietoriskit, joita yrityksien tulisi ottaa huomioon toiminnassaan. Kuudennessa luvussa esittelen opinnäytetyön käytännön osuuden ja viimeisessä luvussa on johtopäätökset ja pohdinta.



KUVIO 1. Opinnäytetyön teoreettinen viitekehys

2 DIGITALISAATIO

Digitalisaatio alkoi 1990-luvun puolessa välissä verkkoselainten kehittymisen seurauksena, joka mahdollisti tiedon vapaamman saatavuuden yhä useammalle (Gerdt & Eskelinen 2018, 13). Kehittynyt tietotekniikka ja teknologia sekä sen käyttömahdollisuudet yhä useammalla elämän osa-alueella ovat digitaalisen murroksen taustalla. Digitalisaatio tekee mahdolliseksi ensisijaisesti datan nopeamman sekä helpomman jakamisen, käsittelyn sekä prosessoinnin. Tulevaisuudessa yritysten menestys pohjautuu ohjelmistojen tehokkaaseen hyödyntämiseen vuorovaikutuksessa yhteistyökumppanien, asiakkaiden sekä muiden sidosryhmien kesken. (Hämäläinen, Maula & Suominen 2016, 21-22.)

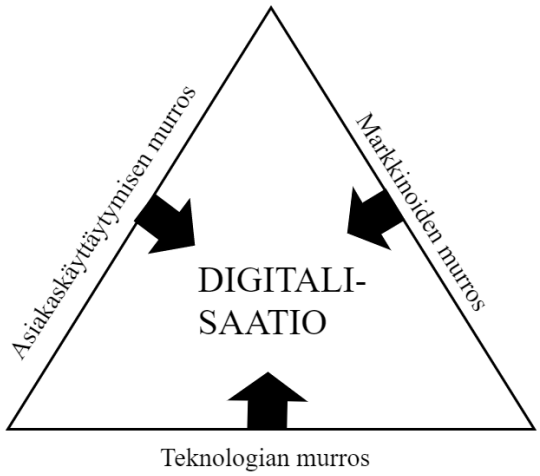
Digitalisaatiota on hankalaa määrittää yksiselitteisesti ja perimmäinen syy digitalisaation taustalla on digitalisoituminen (Ilmarinen & Koskela 2015, 22). Digitalisoitumista tapahtuu, kun fyysinen tuote tai prosessi muutetaan verkossa, eli digitaalisesti toimivaan tai tehtävään (Ilmarinen & Koskela 2015, 22; Hämäläinen ym. 2016, 21). Selkeitä esimerkkejä digitalisoitumisesta ovat muun muassa tavaratalojen muuttuminen verkkokaupoiksi sekä CD-levyjen sijaan kuluttajat ostavat suoratoistopalveluita. Edellä mainittujen lisäksi yritykset digitalisoivat myös liiketoimintaprosessejaan. (Ilmarinen & Koskela 2015, 22.) Tilastokeskuksen (2017, 6.) määritelmän mukaan digitalisaatiolla tarkoitetaan seuraavaa:

> Digitalisaatio tarkoittaa tiedon tallentamista, siirtämistä ja käsittelyä tietokoneiden ymmärtämässä muodossa, mutta käsitteellä viitataan myös laajemmin taloudelliseen ja yhteiskunnalliseen muutosprosessiin.

Digitalisaatiosta puhuttaessa tarkoitetaan usein koko toimintaympäristön muutosta. Yrityksille tämä tarkoittaa täysin uudenlaista tapaa tehdä liiketoimintaa, ei pelkästään myyntikanavan muutosta. Digitalisaatiossa kyse on digitaalitekniikan hyödyntämisestä, asiakaslähtöisyydestä sekä innovaatioista. (Hämäläinen ym. 2016, 21.) Ilmarisen & Koskelan (2015, 23) mukaan digitalisaatiosta voidaan puhua silloin, kun ihmisten käyttäytyminen, markkinat sekä yritysten ydintoiminta muuttuvat digitalisoitumisen seurauksena. Digitalisaatio onkin aikamme merkittävin muutosvoima. Tapamme hankkia tietoa ja tuotteita, kuluttaa palveluja sekä olla vuorovaikutuksessa muiden kanssa ovat muuttuneet merkittävästi. Yritysten näkökulmasta tarkasteltuna digitalisaatio muuttaa niiden toimintaympäristöä kilpailun koventumisen myötä sekä toimialarajojen hämärtyessä. Yrityksissä tarvitaan uudenlaista osaamista ja toimintatapoja. (Ilmarinen & Koskela 2015, 13.)

2.1 Digitalisaation murrokset

Digitalisaation murros on merkitykseltään verrattavissa teolliseen vallankumoukseen ja se vaikuttaa maailmanlaajuisesti yhteiskuntiin sekä talouteen ja näiden myötä vääjäämättä myös yritysten toimintaan (Hämäläinen ym. 2016, 21). Digitaalinen murros on muuttanut muun muassa yrityksien kilpailukenttää sekä toimialojen rakenteita. Lisäksi se on vaikuttanut kuluttajien käyttäytymiseen sekä työmarkkinoihin ja työelämään kohdistuviin odotuksiin. (Hämäläinen ym. 2016, 14.) Digitalisaation murros on muuttanut myös jokaista yritysten toimintoa, kuten myyntiä, markkinointia, johtamista sekä tuotteiden tai palvelujen tuottamista (Ilmarinen & Koskela 2015, 52). Ilmarinen & Koskela (2015, 52) ovat jakaneet digimurroksen alueet markkinoiden, teknologian sekä asiakaskäyttäytymisen murrokseen (KUVIO 2).



KUVIO 2. Digitalisaation murrokset (mukaillen Ilmarinen & Koskela 2015, 52)

Ilmarinen & Koskela (2015, 58) mukaan asiakaskäyttäytymisen murros on merkittävin digitalisaatiota kiihdyttävä voima. Digitaaliset innovaatiot ovat muuttaneet asiakaskäyttäytymistä, niin asiakkaiden tavat kuin tottumukset ovat muuttuneet (Hämäläinen ym. 2016, 24). Asiakaskäyttäytymisen murros pakottaa yritykset oppimaan uusille tavoille. Asiakkailla on yhä enemmän päätösvaltaa, miten, missä, milloin he haluavat asioida. Digitalisaation myötä asiakkaille on tarjolla enemmän vaihtoehtoja ja kilpailijat voivat tulla mistäpäin maailmaa tahansa. Helppous, nopeus, edullisuus sekä laatu ovat olleet kilpailuvaltteja yrityksille jo ennen internettiäkin. Nyt digitalisaatio mahdollistaa asiakkaiden saataville maailmanluokan yritysten palvelut, jotka toimivat mittareina erinomaiselle palvelulle ja joiden toimintaan verrataan myös kotimaisia yrityksiä. (Ilmarinen & Koskela 2015, 53-54.)

Asiakkaat odottavat palveluiden olevan saatavilla vuorokauden ympäri, silloin kun itselle sopii. Palvelun käytön sekä ostamisen tulisi olla vaivatonta. Lisäksi asiakkaat ovat tottuneet siihen, että asiat tapahtuvat välittömästi ja heidän voi olla vaikea ymmärtää, miksi ulkomainen verkkokauppa kykenee toimittamaan

tilauksen nopeammin kuin kotimainen. Digitaalisuuden aikana kynnys vaihtaa palveluntarjoajaa on pieni. Asiakkaat ovat entistä hintatietoisempia ja hintojen vertailu on helppoa ja nopeaa internetin avulla. Monia palveluita saa myös ilmaiseksi omaan käyttöön, kuten uutiset, musiikki tai mobiilipelit. Yritykset joutuvatkin pohtimaan, mikä on asiakkaalle tarjottava lisäarvo tai -hyöty. (Ilmarinen & Koskela 2015, 54.)

Digitalisaation ovat mahdollistaneet teknologiset innovaatiot sekä niiden sovellukset. Näiden lisäksi laitteiden, ohjelmistojen sekä tiedonsiirron kehittyminen ovat vaikuttaneet digitalisaation syntyyn. Digitaalisen tuotteet muuttuvat jatkuvasti edullisimmaksi sekä niiden saatavuus ja tehokkuus paranevat, jonka seurauksena löytyy uusia osa-alueita, joissa digitaalista teknologiaa on mahdollista sekä kannattavaa hyödyntää. Langattoman tiedonsiirron nopea kehitys on mahdollistanut älypuhelinten ja muiden älylaitteiden kehityksen. Monelle kuluttajalle älypuhelin onkin ensisijainen väline digitaalisten palvelujen käyttöön. (Ilmarinen & Koskela 2015, 59-61.)

Markkinoiden murrokseen vaikuttavia tekijöitä ovat globaali kilpailu, sääntely muutokset, uudet haastajat sekä toimialaliukumat. Digitalisaatio muuttaa yritysten kilpailukenttää, nykyisin paikalliset yritykset kilpailevat globaalien toimijoiden kanssa. Asiakkaan näkökulmasta tarkasteltuna ostoksien teko tai palvelun tilaus on yhtä helppoa tehdä ulkomaiselta toimijalta kuin kotimaiseltakin. EU-lainsäädäntö sekä luottokorttimaksaminen pienentävät asiakkaiden kynnystä tilata tuotteita ulkomailta. Digitalisaation aikana yrityksen menestyminen vaatii uudenlaisia liiketoimintamalleja, ketteryyttä uudistaa liiketoimintaa sekä kykyä vastata asiakkaiden muuttuneisiin odotuksiin. Monelle toimialalle on syntynyt uusia haastajia, koska niiden on helpompi toimia uudella tavalla, kuin perinteisen, asemansa vakiinnuttaneen yrityksen. Toimialarajat liukuvat yritysten hakiessa kasvua ja lisätuloja digitaalisten palvelujen sekä liiketoimintamallien avulla. Digitalisaatio tarjoaa yrityksille keinon laajentaa tuote- tai palveluvalikoimaansa. (Ilmarinen & Koskela 2015, 65-67.)

2.2 Digitalisaation uudet liiketoimintamallit

Digitalisaaton myötä syntyy uusia liiketoimintamalleja. Se aiheuttaa myös toimialaliukumia sekä murtaa vanhoja liiketoimintamalleja. Yleensä markkinoiden uudet toimijat ovat luoneet uusia liiketoimintamalleja, kun taas perinteiset toimijat ovat pyrkineet laajentamaan tulojen hankkimistapojaan digitalisaation avulla. (Ilmarinen & Koskela 2015, 136.) Yritysten sekä toimialojen rajojen murtuminen tuovat haasteita

nykypäivän johtajille. Nykyään liiketoimintamallit muokkaavat teollisuudenaloja, kun aikaisemmin teollisuudenala määritti liiketoimintamallin. Uusien liiketoimintamallien etsiminen on kokeellista sekä sitä tehdään jatkuvasti. (Hämäläinen ym. 2016, 67.) Liiketoimintamallilla tarkoitus on kuvata yrityksen tarjoomaa, potentiaalisia asiakkaita sekä käytännön liiketoiminnan toteuttamista. Liiketoimintamallin tarkoitus on siis kuvata, miten yrityksen ansainta, eli tulojen hankkiminen, tapahtuu. (Tall, Sorama, Tulisalo, Petäjä, & Virkamäki 2013, 37 ;[Pulkkinen 2005.])

Digitalisaatiota hyödyntävillä liiketoimintamalleilla on yhteisiä tekijöitä kuten, skaalautuvuus, kevyt kustannusrakenne, maailmanlaajuinen markkina-alue ja toiminnasta saatavan datan hyödyntäminen. Digitaaliset palvelut saavat skaalautuvuudestaan etua, koska toiminnan kasvaessa muuttuvat kustannukset eivät ole niissä yhtä suuret, sillä ihmisen tekemää työtä ei tarvita niiden tuottamiseen. (Ilmarinen & Koskela 2015, 136.) Liiketoiminnan siirtyminen verkkoon madaltaa uusien toimijoiden kynnystä astua toimialalle. Esimerkiksi nykyään voi perustaa suoraan verkkokaupan perinteisen kivijalkakaupan sijaan. Sovellusten rakentamisen kustannukset ovat pienempiä nykyisin tai oman verkkokaupan voi perustaa jo olemassa olevalle alustalle. Liiketoiminnan aloittaminen ei enää vaadi niin paljon pääomaa kuin ennen. (Hämäläinen ym. 2016, 27.) Perustamalla yrityksen verkkoon voi tavoittaa maailmanlaajuisen markkinan (Ilmarinen & Koskela 2015, 136).

Monet digitalisaatioajan liiketoimintamallit perustuvat verkoston luomiseen sekä ekosysteemi- ajatteluun. Näihin digitaalisiin liiketoimintamalleihin monesti sisältyy ajatus, jossa asiakkaalle tuotettava arvo on sitä suurempi mitä laajempi verkosto on. (Ilmarinen & Koskela 2015, 156.) Tällöin puhutaan myös alustataloudesta. Muita yrityksien liiketoimintamalleihin sekä strategioihin vaikuttaneita ilmiöitä ovat muun muassa datan hyödyntäminen, esineiden internet (Internet of Things), robotiikan yleistyminen sekä sosiaalisen median tarjoamat liiketoimintamahdollisuudet. (Hämäläinen ym. 2016, 49.)

2.2.1 Alustatalous

Alustataloudella tarkoitetaan taloudellista, sosiaalista sekä yhteiskunnallista toimintaa, jonka keskiössä ovat teknologia-alusta sekä sen päälle liitetyt kolmansien osapuolten tarjoamat palvelut (Gerdt & Eskelinen 2018, 47). Hämäläisen ym. (2016, 34) mukaan alustataloudessa liiketoiminnan mahdollistaa teknologinen alusta tai käyttöliittymä, jossa ihmiset tai palvelun tarjoajat sekä ostajat kohtaavat toisensa.

Alustojen rooli jatkaa kasvuaan ja niiden vaikutus on yhä suurempi. Alustatalous lisää epäsuoraa kilpailua melkein jokaisella toimialalla ja siten se muuttaa kilpailua suuresti. Tunnettuja alustatalouden vaikuttajia sekä teknologiayhtiöitä ovat muun muassa Alibaba, Amazon, Facebook sekä Netflix. (Gerdt & Eskelinen 2018, 47-48)

Teknologinen kehitys on ollut viime vuosina nopeaa ja se on tehnyt mahdolliseksi alustojen hyödyntämisen uudella tavalla. Kaupankäynnistä on tullut edullisempaa, helpompaa sekä nopeammin skaalautuvaa, koska ostajien ja myyjien kohtaamisten välittäminen on siirtynyt verkkoon. Digitaalinen alusta tuo vaivattomasti sekä maailmanlaajuisesti ison määrän toimijoita samaan paikkaan. Tämän lisäksi digitaalinen alusta mahdollistaa tiedon keräämisen, suodattamisen sekä analysoinnin, joka tuo lisäarvoa niin alustan käyttäjille kuin omistajille. Alustatalouden liiketoimintalogiikassa keskeisimmät asiat ovat palvelun tarjoajien sekä ostajien muodostaman verkoston johtaminen sekä jäsenten resurssien hyödyntäminen niin, että arvoa kyetään luomaan mahdollisimman paljon koko ekosysteemille. Ekosysteemissä keskeinen ajatus on se, että verkostossa täytyy olla useampi toimija, joiden yhteinen osaaminen, tuotteet sekä vetovoima tekevät verkostosta kiinnostavan. Hyvä alusta myös pienentää kaupankäynnistä aiheutuvia kustannuksia, joita eri toimijoille aiheutuisi muuten. (Hämäläinen ym. 2016, 34-36.)

Eri alustat toimivat eri tavalla, mutta niissä on usein samankaltainen verkostorakenne. Toimijat muodostavat verkoston ja jokaisella toimijalla on oma roolinsa sekä tehtävänsä verkostossa. Verkoston omistajien tehtävä on johtaa sekä ylläpitää ekosysteemiä ja heidän hallussaan on alustan immateriaalioikeudet. Palveluntarjoaja vastaa alustan käyttöliittymästä, palvelun tuottajat vastaavat alustan tarjoomasta ja kuluttajat käyttävät palveluja. Roolit verkostossa voivat muuttua. (Hämäläinen ym. 2016, 36.)

2.2.2 Datan hyödyntäminen liiketoiminnassa

Digitalisaation seurauksena datan määrä kasvaa valtavasti. Dataa on mahdollista seurata sekä analysoida reaaliaikaisesti ja tämä koskee myös ihmisten käyttäytymistä sekä liikkeitä. Tiedon arvo tulee korostumaan entisestään tulevaisuudessa, eikä ole itsestäänselvyys, kuka pääsee käsiksi näihin tietoihin. (Hämäläinen ym. 2016, 49.) Yrityksiä kiinnostava tieto koskee muun muassa asiakkaiden ostokäyttäytymistä, kuten mitä erilaisia tuotteita asiakas ostaa. Kerättyjä tietoja voidaan hyödyntää yrityksen liiketoiminnassa, markkinoinnissa sekä tuotekehityksessä. Näitä tietoja kutsutaan myös big data -nimellä. Big

data voi tulevaisuudessa vaikuttaa tapaan, jolla yrityksissä tehdään päätöksiä sekä miten yritystä johdetaan. (Hämäläinen ym. 2016, 50.)

2.3 Digitalisaation mahdollisuudet ja uhat

Digitalisaation myötä yrityksien on mahdollista tavoittaa uusia asiakkaita, kasvattaa myyntiään, parantaa palveluaan sekä toimia nopeammin. Yrityksien on pystyttävä tekemään uudistuksia sekä hyödyntämään digitaalisia työkaluja, jotta ne pystyvät vastaamaan muuttuneisiin asiakasodotuksiin sekä menestymään kilpailussa. Nykyään digitalisaatio on yritykselle välttämättömyys. (Ilmarinen & Koskela 2015, 14). Sen avulla yritykset pystyvät uudistamaan liiketoimintaansa muun muassa pienentämällä kulujaan, parantamalla laatua sekä tarjoamalla parempaa asiakaskokemusta. Yritysjohtajien tulisi nähdä digitalisaatio liiketoiminnan parantamisen tai uuden liiketoiminnan kehittämisen välineenä. (Ilmarinen & Koskela 2015, 31-32).

Jokainen yritys, niin pieni kuin suuri, joutuu miettimään digitalisaation tuoman kehityksen sekä uusien liiketoimintamallien myötä, miten oman liiketoiminnan perusta muuttuu ja mistä uudet kilpailijat tulevat (Hämäläinen ym. 2016, 89). Yrityksille digitalisaation suurin uhka on sen vaikutuksien aliarviointi ja se, että kilpailijat ehtivät hyödyntämään uudet mahdollisuudet nopeammin (Ilmarinen & Koskela 2015, 14). Tiedosta on tullut yrityksille merkittävä tuotannontekijä uusien teknologisten innovaatioiden ja digitalisaation seurauksena. Tietosuoja sekä tietoturva ovat keskeisiä edellytyksiä sekä mahdollistajia digitalisaation hyödyntämiseen. (Andreasson, Riikonen & Ylipartanen 2019, 22.) Tietoturvariskit on otettava huomioon niin yritysten kuin yksityishenkilöiden arjessa (Hämäläinen ym. 2016, 23).

3 TIETOTURVA

Tietoturvallisen toiminnan kolme tärkeintä tavoitetta ovat tiedon luottamuksellisuuden, eheyden ja saatavuuden takaaminen (Rousku 2014, 47). Luottamuksellisuudella tarkoitetaan sähköpostien, yrityssalaisuuksien sekä henkilötietojen pysymistä poissa julkisuudelta ja pääsy tietoihin tulee olla vain tiettyjen ihmisten saatavilla (Järvinen 2012, 10). Luottamuksellisuus tietojärjestelmissä hoidetaan usein käyttöoikeuksien hallinnalla. Joka tarkoittaa, että käyttäjällä on työn hoitamisen kannalta asianmukaiset oikeudet toimia käytössä olevissa järjestelmissä sekä päästä tarvitsemiinsa tietoihin käsiksi. (Rousku 2014, 47.) Tiedon eheydellä tarkoitetaan sitä, että tieto ei saa muuttua hallitsemattomasti. Tietoja saavat muokata vain siihen oikeutetut käyttäjät. Viimeinen tietoturvan periaate on tiedon saatavuus, joka tarkoittaa, että tiedon tulee olla saatavilla sitä tarvitsevalle käyttäjälle tietojärjestelmässä tai palvelussa. Käytännössä tietojen sekä palveluiden täytyy olla käytettävissä sekä toimia kaiken aikaa, koska yhteiskuntamme on digitalisoitunut ja muuttunut yhä enemmän toimivaksi vuorokauden ympäri (Rousku 2014, 49-50).

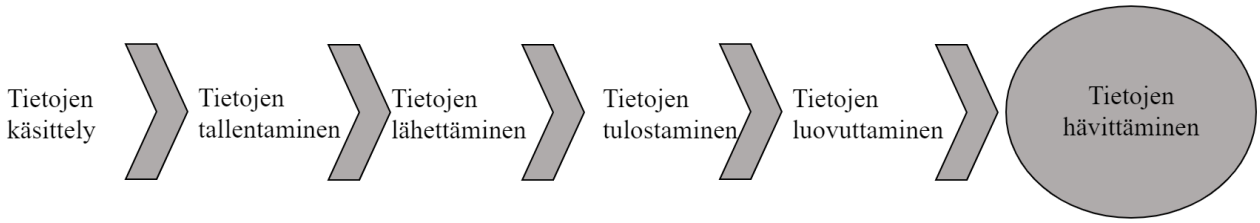
Tietoturvassa pyrkimyksenä on siis tiedon luottamuksellisuuden, eheyden sekä saatavuuden suojaaminen. Tietoturva koostuu niistä teknisistä ratkaisuista ja hallinnollisista prosesseista, joilla suojataan tietoaineistoa. (Rousku 2014, 130.) Päämääränä tietoturvatyössä on turvata toiminnan kannalta tärkeiden tietojärjestelmien sekä tietoverkkojen häiriötön toiminta, estää ulkopuolisten pääsy tietoihin sekä tietojärjestelmiin ja suojata tietoa vääristymiseltä tai tuhoamiselta sekä minimoida toetutuneista riskeistä aiheutuvat vahingot (Andreasson ym. 2019, 21).

3.1 Tietoturvan osa-alueet

Tietoturvallinen työskentely edellyttää, että henkilöstö on tietoinen yrityksen tietoturvakäytännöistä ja työtehtävien kannalta tarpeellisia palveluita osataan käyttää oikein. Tietoturvallisuus koostuu niin hallinnollisista kuin teknisistäkin toimenpiteistä. (Järvinen & Rousku 2017, 45.) Kyberturvallisuuden lehtorin Panu Moilasen mukaan 20 prosenttia tietoturvasta on tekniikkaa ja 80 prosenttia on ihmisen käytöstä (Laitinen 2017, 12). Järvinen & Rousku (2017, 71) mukaan hallinnollinen tietoturvallisuus kattaa tietojen luokittelun sekä niiden asianmukaisen käsittelyn. Muita hallinnollisia turvatoimia ovat toiminta- sekä johtamismallien luominen ja tietoturvapolitiikan laatiminen. Hallinnolliseen puoleen kuuluu myös sovittujen toimintamallien toimeenpano, valvonta ja organisointi, eli valtuutuksien, töiden, tehtävien

vastuiden jako sekä järjestäminen. (Juvonen, Koskensyrjä, Kuhanen, Ojala, Pentti, Porvari & Talala 2014, 156.)

Tietoja tulisi luokitella yrityksessä käytettävän luokituksen mukaisesti. Tietoja luokittelemalla voidaan turvata tiedon eheys sekä saatavuus. Henkilöstön on tärkeää tunnistaa, milloin kyseessä on salaista tietoa ja tietää kuinka toimia sen kanssa. Tietojen luokitus vaikuttaa siihen, miten tietoja tulisi käsitellä kussakin käsittelyn vaiheessa. (Järvinen & Rousku 2017, 45-47.) Tietojen käsittelyn vaiheet ovat esitettynä kuviossa 3. Esimerkiksi henkilöiden, jotka työssään luovat uusia tiedostoja, tulisi selvittää minne salassa pidettävät tiedostot tulisi tallentaa siten, etteivät ne ole kaikkien saatavilla. Useimmin työpaikoilla on verkkolevyasemat tai muu paikka, johon salassa pidettävät tiedostot tallennetaan. (Järvinen & Rousku 2017, 49.)



KUVIO 3. Tietojen käsittelyn vaiheet (mukaillen Järvinen & Rousku 2017, 47)

Käyttöoikeuksien hallinta tapahtuu yrityksissä käyttäjätunnusten sekä salasanojen avulla. Ne ovat tietoturvallisuuden keskeisimpiä asioita, koska niiden avulla rajataan sitä, kuka tai ketkä pääsevät käsiksi toiminnossa olevaan tietoon. Salasanan merkitys on suuri ja siitä on haluttu tehdä entistä turvallisempi, jonka vuoksi kaksivaiheinen tunnistautuminen on yleistynyt palveluissa. Työntekijöitä tulee ohjeistaa myös vahinkojen ilmoittamisesta. Jos työntekijä on kadottanut kannettavan tietokoneensa tai puhelimensa, tulisi hänen ilmoittaa asiasta välittömästi työnantajalleen, jotta tietoturvariski pienenisi. Samoin myös muusta epäilyttävästä toiminnasta on ilmoitettava aina. (Järvinen & Rousku 2017, 57-59)

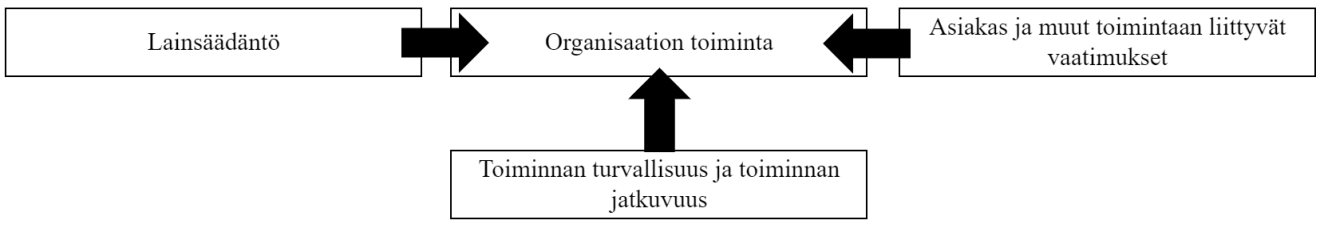
Järvisen & Rouskun (2017, 71) mukaan teknisen turvallisuuden keskiössä ovat päätelaitteet, tietojärjestelmät sekä toimitilat. Tekniseen tietoturvaan vaikuttavia toimenpiteitä ovat käytössä olevien laitteiden sekä ohjelmistojen suojaaminen päivittämällä. Päivittämällä ohjelma, siitä pyritään saamaan turvallisempi sekä korjata mahdollisia haavoittuvaisuuksia. (Järvinen & Rousku 2017, 103) Haavoittuvaisuudet ovat ohjelman heikkoja kohtia, joita hakkerit ja muut rikolliset hyödyntävät. Pitämällä ohjelmat päivitettyinä, haittaohjelmien riski pienentyy. Päivitysten lisäksi keskeinen osa teknistä tietoturvaa on palomuuri. Sen avulla vartioidaan tietokoneen, modeemin sekä tietoverkkojen välistä tietoliikennettä sekä

estetään haittaohjelmien sekä luvattomien käyttäjien tunkeutuminen tietokoneelle verkkoyhteyden välityksellä. (Laitinen 2017, 4.)

Tietoturvallisuus on osa yrityksen kokonaisturvallisuutta. Tietoturvallinen toiminta edellyttää myös toimitila- ja kiinteistö- sekä henkilöstöturvallisuuden alaisia toimenpiteitä. Kiinteistö- ja tilaturvan keskeisimpiä keinoja ovat kulunvalvonta, kulkuoikeudet, lukitukset, varashälyttimet sekä kameravalvonta. Tarkoituksena on turvata sekä taata henkilöstölle ja vierailijoille häiriötön työympäristö. Henkilöstöturvallisuudella huolehditaan niin työntekijöiden turvallisuudesta sekä toimintakyvystä kuin myös yrityksen toiminnan kannalta kriittisten henkilöresurssien varmistamisesta esimerkiksi päivystys sekä varahenkilöjärjestelyllä. Henkilöstöturvallisuuteen liittyviä toimenpiteitä ovat turvallisuusselvitys ja salassapitositoumus. (Järvinen & Rousku 2017, 54-56) Henkilöturvallisuus ja fyysinen turvallisuus ovat esimerkkejä toiminnallisista turvatoimista. Niillä pyritään vaikuttamaan henkilöstön toimintatapoihin sekä tottumuksiin. Lisäksi toiminnallisilla- eli operatiivisilla turvatoimilla vaikutetaan yrityksen turvallisuuskulttuurin muodostumiseen. (Juvonen ym. 2014, 156)

3.2 Tietoturvan vaatimukset

Tietoturvan vaatimukset koostuvat monista osatekijöistä, kuten organisaation toimialasta, lainsäädännöstä sekä asiakasvaatimuksista ja käsiteltävistä tiedoista (Järvinen & Rousku 2017, 31). Yrityksen johdon tehtävä on asettaa tavoitteet sekä vaatimukset tietoturvallisuudelle (Juvonen ym. 2014, 162). Työnantajan tehtävä on huolehtia riskien arvioinnista, tämän lisäksi henkilöstöä tulee ohjeistaa uhkakuvista sekä heille on annettava ohjeet niin työntekoon kuin laitteiden sekä palvelujen käyttöön (Järvinen & Rousku 2017, 31). Kuviossa 4 esitellään yrityksen tietoturvallisuuden vaatimuksia ohjaavia tekijöitä.



KUVIO 4. Tietoturvaa ohjaavat vaatimukset (mukaillen Järvinen & Rousku 2017, 31)

Yritysten on otettava vastuu tietoturvallisuudesta, koska EU:n sekä Suomen lait velvoittavat tekemään niin (Rousku 2014, 125). Toukokuussa 2018 velvoittavaksi tullut EU:n yleinen tietosuoja-asetus lisää

erityisesti henkilötietojen käsittelyä koskevaa sääntelyä. Lainsäädännön rikkomisesta seurauksena voi tulla tutkintapyyntö sekä oikeusprosessi. (Järvinen & Rousku 2017, 31.) Lakien sekä asetusten lisäksi yrityksiä velvoittavat toimittajien, yhteistyökumppanien sekä alihankkijoiden kanssa tehdyt sopimukset. Sopimusten takia yritykset ovat velvollisia huolehtimaan toisten yritysten sekä asiakkaidensa tiedoista omiensa lisäksi. (Rousku 2014, 126.) Jos tietoturva poikkeama pääsee tapahtumaan, eikä sopimusten mukaan ole toimittu, niin yritys voi olla korvausvelvollinen tai seurauksena voi olla muita sanktioita (Järvinen & Rousku 2017, 32).

Toiminnan turvallisuus sekä jatkuvuus vaikuttavat yrityksen tietoturvatoimintaan. Jos tietoturvallisuutta tai henkilötietojen asianmukaista käsittelyä laiminlyödään, seurauksena usein on maineen sekä luottamuksen menetys niin asiakkaiden kuin alihankkijoiden keskuudessa. Mainehaitat ja epäluottamus voivat vaikuttaa yrityksen talouteen ja sen myötä vaarantaa liiketoiminnan jatkuvuuden. Tietoturvallisuuden pettäessä voi tulla katko tiedon saatavuuteen, jolloin yritys voi menettää rahaa. (Järvinen & Rousku 2017, 32.) Yritys voi pyrkiä minimoimaan yleisempien vikatilanteiden aiheuttamia vahinkoja jatkuvuudenhallintasuunnitelmalla. Suunnitelma pohjautuu yrityksen liiketoiminnan jatkuvuuden turvaamiseen ja siinä keskitytään turvaamaan liiketoiminnan kannalta tärkeimmät toiminnot. (Rousku 2014, 61.)

4 TIETOSUOJA

Tietosuojalla tarkoitetaan yksilön oikeutta omiin henkilötietoihinsa sekä yksityisyyden suojaamista henkilötietoja käsiteltäessä. Digitalisoitumisella sekä informaatioteknologialla on merkittävä vaikutus siihen, millä tavoin henkilötietoja käsitellään ja kuinka jokaisen henkilön sekä yrityksen tulisi omassa toiminnassaan tähän suhtautua. (Aalto-Setälä & Viitaila 2018, 4.) Tietosuojan tarkoituksena on varmistaa henkilötietojen oikea, tarkoituksen- sekä vaatimuksenmukainen käyttö. Mitä enemmän palvelut toimivat netissä, sitä enemmän myös henkilötietoja kerätään. Jokaisesta merkinnästä muodostuu tietoja palveluntarjoajan henkilörekisteriin. (Järvinen & Rousku 2017, 18) Tietosuojan pyrkimyksenä on ohjata rekisterinpitäjiä hyviin henkilötietojen käsittely- ja tietosuojakäytäntöihin sekä suojaamaan tiedon kohteen yksityiselämää, etuja, oikeuksia sekä vapauksia. (Andreasson ym. 2019, 20). Tietosuojan avulla huolehditaan, niin yrityksen työntekijän kuin yksityishenkilön, henkilötietojen turvallisesta käsittelystä. Tietoturvallisuuden pettäessä seurauksena on useimmiten tietosuojaongelmia. (Rousku 2014, 52)

4.1 Tietosuoja kilpailutekijänä

Viime vuosina tapahtuneet tietomurrot sekä niistä yrityksille aiheutuneet vahingot ovat vaikuttaneet suuresti yritysten sekä yksityishenkilöiden tietosuojaan suhtautumiseen. Tietomurtojen takia asiakkaat ovat yhä kiinnostuneempia missä ja miten heidän henkilötiedoistaan huolehditaan. Yrityksen toiminnan ja menestyksen kannalta on tärkeää, että asiakkaat voivat luottaa tietojensa pysyvän tallessa. Tietosuoja-asetuksen tarkoituksena on asettaa yrityksille säännöt tietosuojan järjestämiseen sekä turvata asiakkaiden luottamus. (Aalto-Setälä & Viitaila 2018, 4.) Andreasson ym. (2019, 20) mukaan on perusteltua sanoa, että EU:n yleisen tietosuoja-asetuksen seurauksena tietosuojasta, sen organisoinnista sekä henkilöstön tietosuojaosaamisesta tulee yritysten operatiivisen toiminnan menestyksen avain.

4.2 Euroopan unionin yleinen tietosuoja-asetus (GDPR)

Euroopan unionin yleistä tietosuoja-asetusta alettiin soveltaa kansallisesti 25. toukokuuta 2018. Uudistettu tietosuoja-asetus on sellaisenaan sovellettavaa oikeutta ja se on yleispätevä, kaikilta osin velvoittava sekä sitä sovelletaan jokaisessa EU-jäsenvaltiossa, pois lukien mahdolliset kansallisesti säädetyt

poikkeukset. EU:n yleisen tietosuoja-asetuksen tavoitteina ovat sisämarkkina-alueen vahvistaminen, yksilön oikeuksien parantaminen, tietosuojan maailmanlaajuisen ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on myös luoda EU:lle ajantasainen, turvallinen, yhtenäinen sekä kattava tietosuojakehys. Lisäksi määränpäänä on parantaa kansalaisten luottamusta verkkopalveluihin ja siten viedä eteenpäin EU:n digitaalisten sisämarkkinoiden kehittämistä. (Andreasson ym. 2019, 27.)

Yleinen tietosuoja-asetus koskee niin automaattista kuin manuaalista henkilötietojen käsittelyä. Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön, eli rekisteröityyn, liittyvää tietoa, kuten nimi, henkilötunnus tai sijainti. (Andreasson ym. 2019, 28-29.) Arkaluonteisia henkilötietoja ovat muun muassa etnisyys, poliittinen mielipide, uskollinen vakaumus, ammattiliitonjäsenyys sekä terveystiedot. Näiden arkaluontoisten henkilötietoryhmien tietojen käsittely on kiellettyä. Asetuksessa on huomioitu tilanteet, joissa rekisteröity on antanut suostumuksen arkaluontoisten tietojen käsittelyyn tai kun yleinen etu niin vaatii. (Aalto-Setälä & Viitaila 2018, 7.) Asetuksen mukaan kaikessa tietojen käsittelyssä tulisi varmistua siitä, että käsitellään vain käsittelyn puolesta tarpeellisia henkilötietoja (Andreasson ym. 2019, 30).

Rekisterinpitäjän ja henkilötietojen käsittelijän vastuulla on varmistaa tietojen asianmukainen ja tarpeeksi turvallinen käsittely jokaisessa tietojenkäsittelyn vaiheessa (keräys, säilytys, hävittäminen). Molempien on myös ylläpidettävä selostetta jokaisesta vastuullaan olevasta tietojenkäsittelytoimesta. Pyydettäessä rekisterinpitäjä on velvollinen todistamaan, että noudattaa tietosuojavelvoitteitaan. Rekisterinpitäjän on tehtävä kattava riskienarviointi henkilötietojen käsittelyyn liittyvistä riskeistä, erityisen tärkeää tämä on silloin, kun käsitellään arkaluontoisia tietoja. Rekisterinpitäjän velvollisuus on huolehtia suojatoimenpiteistä, joilla vastataan tietosuoja-asetuksen vaatimuksiin. Näitä ovat muun muassa henkilöstön koulutus ja ohjeistus, salassapitositoumukset ja tietojärjestelmien tietoturva. Rekisterinpitäjän tulee itse määritellä asianmukaiset suojatoimet huomioiden oman toimintansa asettamat vaatimukset. Tietosuojaperiaatteita on noudatettava jokaisessa henkilötietojen käsittelyvaiheissa. EU:n yleisen tietosuoja-asetuksen periaatteet ovat:

- lainmukaisuus, kohtuullisuus, läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys

- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus

Asetuksen myötä rekisterinpitäjä on osoitusvelvollinen todistamaan, että se noudattaa tietosuojaperiaatteita. Jos rekisteröidyn tietoturvaa loukataan, niin rekisterinpitäjä on velvollinen ilmoittamaan siitä valvontaviranomaiselle sekä rekisteröidylle. Henkilötietojenkäsittelijän on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle. (Andreasson ym. 2019, 29-32.)

EU:n yleisen tietosuoja-asetuksen mukaan henkilötietoja saa kerätä ainoastaan tiettyä, nimenomaista sekä laillista tarkoitusta varten. Henkilötietojen käsittelyperusteita ovat muun muassa suostumus, arkistointi ja tieteellinen tutkimus. Rekisterinpitäjän on pystyttävä todistamaan, että suostumus henkilötietojen käsittelyyn on annettu. Rekisteröidyllä on myös oikeuksia. Henkilöllä on oikeus saada tietää, mitä tietoja hänestä on kerätty sekä miten tietoa kerätään. Jos rekisteröity huomaa, että henkilötiedoissa on virhe, hänellä on oikeus saada ne korjatuksi. Samoin rekisteröidyllä on oikeus vaatia tietojaan poistettavaksi rekisteristä sekä oikeus tulla tiedotetuksi, jos henkilötietoihin on kohdistunut tietoturvaloukkauksia. Rekisteröidyllä on oikeus siirtää tiedot toiseen järjestelmään sekä rajoittaa henkilötietojensa käsittelyä. (Andreasson ym. 2019, 33-34.)

Asetuksen myötä organisaatioiden tulee arvioida henkilötietojen käsittelykäytäntönsä vaatimuksenmukaisuus muun muassa asiakasprosesseissa, sopimuksissa alihankkijoiden kanssa sekä henkilöstöhallinnossa. Tietosuojan nykytilan kartoituksen voi tehdä laatimalla tarpeeksi laajan tietotilinpäätöksen. Tietotilinpäätös on sisäisen tarkastelun tuloksena laadittu raportti, jossa esitetään tietojenkäsittelyä koskevat keskeiset asiat. Kun tietosuojan nykytila on kartoitettu, tulisi sen pohjalta selvittää tehtävät toimenpiteet organisaation henkilötietojen käsittelylle. Organisaatiossa käsiteltävät henkilötiedot, niihin kohdistuvat riskit sekä nykyiset käytännöt vaikuttavat toimenpiteiden laajuuteen. Organisaation johdon tulee olla tietoinen lainsäädännöstä sekä sen vaikutuksesta omiin toimintoihin. Jatkossa organisaatioiden on pystyttävä myös todistamaan, miten tietosuoja huomioidaan toiminnan suunnittelussa ja toteutuksessa. (Andreasson ym. 2019, 42-43.)

Jos tietosuoja-asetusta rikotaan, siitä voi seurata muun muassa huomautus, varoitus, sertifikaatin menettäminen tai viranomaisen määräämä hallinnollinen sakko, eli hallinnollinen seuraamusmaksu. Seuraamusmaksulla halutaan korostaa tietosuojan merkittävyyttä. Seuraamusmaksu voi olla enintään 20 miljoonaa euroa tai 4 prosenttia yrityksen maailmanlaajuisesta kokonaisliikevaihdosta. Sakon suuruus mää-

räytyy sen mukaan, kumpi edellä mainituista on suurempi. Seuraamusmaksu voidaan määrätä olosuhteista riippuen, joko muiden toimenpiteiden lisäksi tai niiden sijasta. Viranomaisen on otettava huomioon seuraamusmaksua määrätessään eri asioita muun muassa rikkomuksen vakavuus, luonne ja kesto, tahallisuus, toistuvuus sekä organisaation toimet tapahtuneen vahingon lieventämiseksi. (Aalto-Setälä & Viitaila 2018, 34.)

5 RISKIENHALLINTA

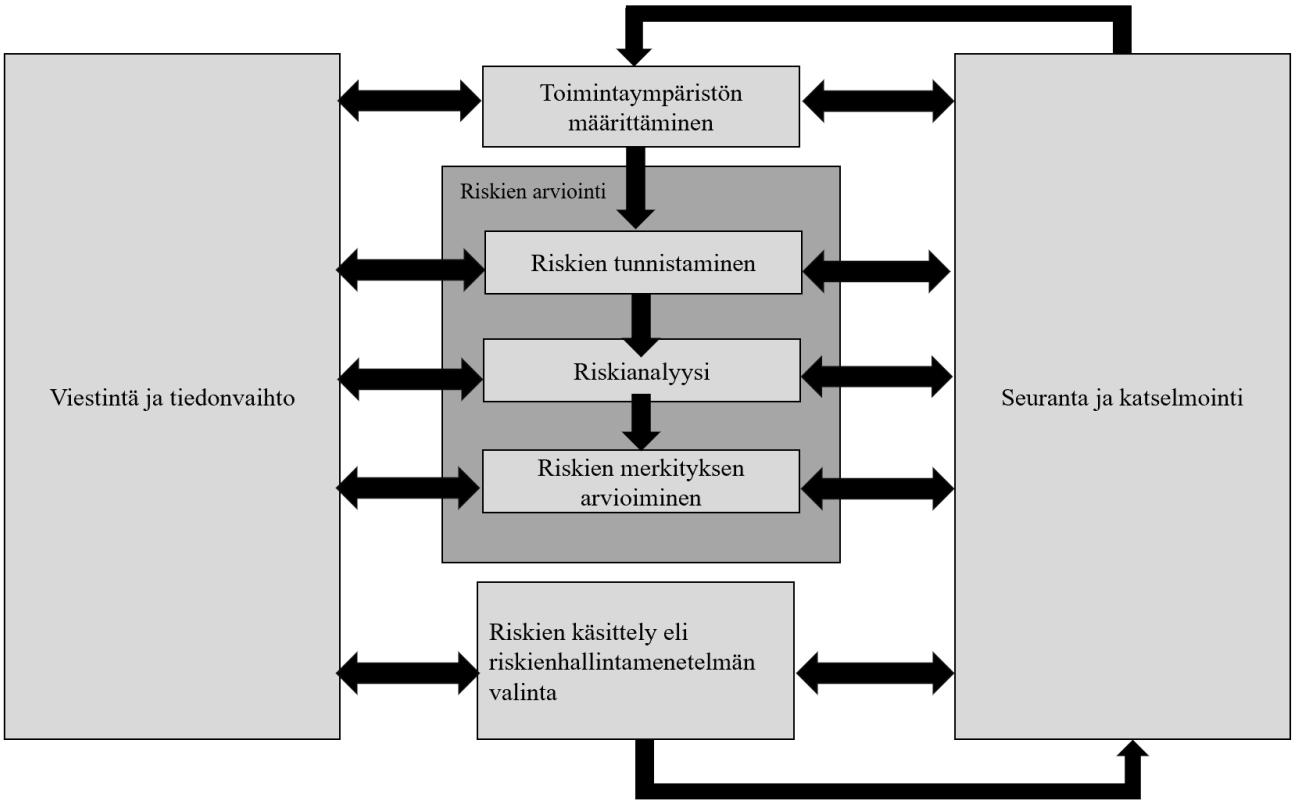
Riskeillä tarkoitetaan yrityksen toimintaa uhkaavia asioita tai tapahtumia. Riskin toteutuessa yrityksen toiminta voi vaikeutua merkittävästi tai pahimmillaan se voi estyä kokonaan. Riskin käsite voi pitää sisällään myös mahdollisuuden. (Juvonen ym. 2014, 7.) Tässä opinnäytetyössä keskityn kuitenkin yrityksiä uhkaaviin riskeihin. Hyvin järjestetylle riskienhallinnalle on tyypillistä toiminnan jatkuvuus. Se mahdollistaa toimintaan liittyvien riskien tunnistamisen etukäteen ja sen myötä niihin osataan myös varautua paremmin. (Andreasson ym. 2019, 57: Juvonen ym. 2014, 7.) Juvosen ym. (2014, 7) mukaan riskienhallinnan tulisi olla osa yrityksen jokaista toimintaprosessia.

Riskienhallinnan avulla yritys voi saavuttaa kilpailuetua useissa eri tilanteissa, eikä sen merkitystä yritykselle pidä vähätellä. Riskienhallinnan yhtenä tavoitteena on estää tekemästä samoja virheitä uudestaan, tulevia riskejä kartoitetaan hyödyntämällä aiemmista tapauksista saatuja tietoja. Vahinkojen ennaltaehkäisy sekä torjuminen on huomattavasti halvempaa kuin niiden selvittely jälkikäteen. (Andreasson ym. 2019, 57.) Riskienhallinta kattaa kaiken tietoturvallisuutta sekä jatkuvuuden hallintaa kehittävän työn. Tärkeintä riskienhallinnassa on tunnistaa todennäköiset sekä vaikutuksiltaan merkittävät riskit yrityksen toiminnalle. Riskien arviointi on tärkeää, koska siten yrityksissä kyetään kohdistamaan resurssit oikeisiin paikkoihin. Jos ei riskienhallintaa tehdä, vaarana on se, että investoinnit turvallisuuteen menevät vääriin kohteisiin. (Rousku 2014, 61.)

5.1 Riskienhallintaprosessi

ISO 31000 -standardin mukaisen riskienhallintatyön vaiheet koostuvat toimintaympäristön määrittelystä, riskien arvioinnista, riskeihin varautumisesta sekä riskienhallinnan seurannasta (KUVIO 5). Liiketoimintaympäristön määrittelyssä huomioidaan niin sisäinen kuin ulkoinenkin toimintaympäristö. Riskien arviointi on toinen riskienhallintaprosessin vaihe. Siihen kuuluu ISO 31000 -standardin mukaan kolme vaihetta, joista merkittävin on riskien tunnistus, koska ainoastaan tunnistettuihin riskeihin pystytään varautumaan. Kun riskit on tunnistettu, tehdään riskianalyysi. Riskianalyysin päämääränä on arvioida riskien suuruus sekä niiden toteutumisen todennäköisyys. Sen avulla ei pystytä poistamaan riskejä kokonaan tai pienentämään niitä, mutta siitä saatavan tiedon avulla riskeihin pystytään varautumaan

paremmin. Puhekielessä riskianalyysillä tarkoitetaan riskien arviointia. Riskien merkityksen arvioiminen on ajankohtaista, kun tehdään kannattavuuslaskelmia eri riskienhallinta keinojen välillä. Jos paljastuu suuruudeltaan merkittäviä riskejä, kannattaa niitä mahdollisuuksien mukaan vakuuttaa, jolloin riski siirtyy pois yritykseltä. (Juvonen ym. 2014 17-20.)



KUVIO 5. ISO 31000 -standardin mukainen riskienhallintaprosessi (mukaillen Juvonen ym. 2014, 18)

Kolmas riskienhallinnan vaihe on menetelmän valinta, eli se, miten riskeihin varaudutaan. Yrityksen toiminnan kannalta suuriin riskeihin tulee varautua mahdollisimman tehokkaasti. Muissa tapauksissa riskeihin varaudutaan taloudellisesti kannattavimmalla tavalla. Viimeinen riskienhallinnan vaihe on seuranta ja katselmointi, jossa ideana on pitää huoli sovittujen käytänteiden toteutuksesta. Seuranta edellyttää järjestelmällistä työskentelyä yritykseltä, tämä sisältää säännöllisen riskien kartoituksen ja lisäksi olisi tärkeää pitää lukua läheltä piti -tilanteista. (Juvonen ym. 2014, 19.)

5.2 Tietoriskit

Digitalisaation seurauksena myös turvallisuutta uhkaavat tekijät ovat kehittyneet. Nämä uudenlaiset uhkatekijät koskettavat sekä palvelun tarjoajia että käyttäjiä. (Ilmarinen & Koskela 2015, 224) Nykyisin niin yhteiskunnan kuin yritysten tärkeimmät prosessit ovat sidoksissa tieto- ja viestintätekniikan järjestelmien toimintaan. Uudet järjestelmät ovat tuoneet mukanaan tietoriskit. Tietojenkäsittely on tärkeä osa liiketoimintaa ja tietojärjestelmät ovat uhattuna esimerkiksi verkkohyökkäyksien muodossa. (Juvonen ym. 2014, 150) Tietoturvan sekä tietosuojan riittävä taso ovat tärkeitä ja yritysten tulisi varautua niitä uhkaaviin riskeihin. Toteutuneet tietoriskit, esimerkiksi tietovuodot, voivat aiheuttaa yrityksille mainehaittojen lisäksi korvausvaatimuksia sekä muita taloudellisia seuraamuksia. (Andreasson ym. 2019, 57.) Juvosen ym. (2014, 150-151) mukaan pk-yritykset harvemmin arvioivat tietoriskejä ja turvatoimien riittämättömyys käy ilmi vasta silloin, kun vahinko tai häiriö on päässyt jo tapahtumaan.

Tietoriskejä voidaan luokitella monella eri tavalla. Luokittelulla pyritään kuvaamaan riskien ominaispiirteitä sekä niistä aiheutuvaa vahinkoa, jonka lisäksi luokittelu auttaa riskien tunnistamisessa sekä arvioinnissa ja turvatoimien suunnittelussa. Tässä työssä käytetään Juvonen ym. (2014, 151.) jaottelua, joissa tietoriskit on jaoteltu seuraavanlaisiin osa-alueisiin:

- omaisuusriskit
- keskeytysriskit
- henkilöstöriskit
- tietoverkkorikollisuus ja muut rikosriskit
- vastuu- ja sopimusriskit
- kehittämisriskit, yhteensopimattomuus, virheet ja laatuongelmat

Tietoturvan näkökulmasta omaisuusriskit kohdistuvat työasemiin, oheis- ja tietoliikennelaitteisiin, palvelimiin, verkon kaapelointiin, ohjelmistoihin, tiedostoihin sekä tietotaitoon. Tietojen katoamisesta, päätymisestä vääriin käsiin tai tuhoutumisesta seurauksena voi olla todella suuria taloudellisia menetyksiä tai muuta vahinkoa. Häiriöt tietojenkäsittelyssä voivat olla seurauksia erilaisista sisäisistä tai ulkoisista tapahtumista. Ulkoisia tapahtumia ovat yleensä onnettomuudet, luonnonilmiöt, varkaudet sekä laitteen rikkoutuminen henkilön toiminnan seurauksena. Sisäiset tapahtumat ovat seurausta yleensä laitteen ku-

lumisesta ajan saatossa, valmistusvirheestä tai huollossa tapahtuneesta virheestä. Laitevahinkojen seurauksena tiedostot sekä ohjelmistot voivat tuhoutua. Tietojen katoamista voi suojata varmuuskopioinnilla. (Juvonen ym. 2014, 151-152)

Keskeytysriskejä tietoturvan näkökulmasta katsottuna ovat tietoliikenteen, palvelimen tai sähkön katkokset. Liiketoiminnalle kriittisiä tietojärjestelmiä ovat muun muassa toiminnanohjaus-, asiakkuudenhallinnan-, toimitusketjujen ja logistiikan järjestelmät. Keskeytysriskit ovat yleensä merkitykseltään suurempia, kuin omaisuusriskit. (Juvonen ym. 2014, 152.) Tieto on liiketoiminnan kannalta merkittävä kilpailutekijä, mutta myös edellytys päivittäisten toimintojen onnistumiselle. Tiedon on oltava saatavissa silloin kuin sitä tarvitaan. Jos ei tiedetä varaston saldoa, asiakkaiden yhteystietoja tai tuotannon tilannetta, yrityksen toiminta voi keskeytyä tai ainakin siihen tulee haasteita. (Myllynen 2005, 243.) Toiminnan keskeytymisen lisäksi keskeytyksistä aiheutuu taloudellisia menetyksiä yritykselle (Juvonen ym. 2014, 152).

Osaavat työntekijät ovat tärkeä tietovoimavara yritykselle, mutta toiminta- ja turvallisuusketjun kannalta myös haavoittuva pala. Henkilöstöriskejä on muun muassa tärkeän henkilön poissaolo, jolloin yrityksessä ei ole tämän henkilön osaamista käytettävissä. (Juvonen ym. 2014, 152) Henkilöstö on merkittävä tietoturvauhka ja tämän takia on tärkeää, että henkilöstöllä on käytössään turvalliset työvälineet ja ohjeistaa heitä niiden käytössä sekä pitää heidät ajan tasalla muuttuneista tietoturvauhista. (Järvinen & Rousku 2017, 44). Henkilöriskit voivat olla tahattomia kuten vahingot ja virheet, mutta myös tahallisuutta sekä väärinkäytöksiä esiintyy (Juvonen ym. 2014, 152).

Tietoverkkorikollisuus ja muut rikosriskit ovat yrityksille jokapäiväisiä uhkia. Ne ilmenevät haittaohjelmina, verkkohyökkäyksinä sekä ilkivaltana. Verkkohyökkäysten pyrkimyksenä on lamaannuttaa yrityksen kriittiset palvelimet, toiminnot sekä tuotanto. Tietoverkkojen kautta on mahdollista tunkeutua yrityksen järjestelmiin sekä ujuttaa haittaohjelmia yrityksen tietokoneisiin tai muihin laitteisiin ja kaapata ne. (Juvonen ym. 2014, 152.) Haittaohjelmat voivat päätyä tietokoneelle muun muassa internet-sivujen tai sähköpostissa olleen liitetiedoston kautta. Haittaohjelma siirtyy käyttäjän koneelle, jos menee sivustolle, johon on asennettu haittaohjelma. (Järvinen & Rousku 2017, 90: Laitinen 2017, 19.) Erilaisia haittaohjelmia ovat kiristys- ja vakoiluohjelmat, tietojenkalastelu sekä palvelunestohyökkäys. Näiden lisäksi netissä liikkuu erilaisia huijauksia ja tilausansoja. (Laitinen 2017, 19.) Kyberuhkien lisäksi palvelimiin sekä työasemiin kohdistuu myös uhkia varkauksille ja fyysiselle ilkivallalle. Tahallisten tekojen motiivina on yleensä rahallinen etu tai vahingon aiheuttaminen. (Juvonen ym. 2014, 152)

Yrityksen vastuuriskeillä tarkoitetaan sitä, että yritys on velvollinen korvaamaan aiheuttamansa vahingon. Mikäli yrityksen tietojärjestelmillä palvellaan vain yritystä itseään, tietojenkäsittelyyn liittyvät vastuuriskit eivät pakosti ole suuret. Muiden tietoja käsiteltäessä on mahdollista, että yritys joutuu korvausvastuuseen tekemistään virheistä. Sopimusriskejä tietoturvan näkökulmasta esiintyy tietojärjestelmien hankinnoissa, käyttöpalvelusopimuksissa sekä tukitoiminoissa. Järjestelmän valmistuminen voi viivästyä tai siinä voi olla puutteita, jolloin sen käyttäminen ei ole mahdollista. Hankittu palvelu voi olla laadultaan heikkoa tai hidasta. (Juvonen ym. 2014, 153.)

Kehittämistyössä on riskejä, projektit voivat myöhästyä tai niiden kustannukset saattavat mennä budjetin yli. Yhteensopimattomuusriskit kohdistuvat laitteistoihin sekä ohjelmistoihin, yhteensopimattomuus voi johtua esimerkiksi standardoinnin puutteesta. Ohjelmistot saattavat sisältää virheitä ja käyttöjärjestelmät, joita ei ole päivitetty, voivat sisältää haavoittuvuuksia. (Juvonen ym. 2014, 153.) Käyttäjän virhe on yleisin tietoriski. Noin puolet tietoriskeistä ovat seurausta käyttäjän virheen sekä ylläpitopuutteiden ja järjestelmävirheiden yhdistelmistä. (Kalliokoski 2003.) Monet riskit vaikuttavat toisiinsa ja toteutuneet riskit aiheuttavat uusia riskejä eri osa-alueille. (Juvonen ym. 2014, 151).

6 RISKIKARTOITUS

Opinnäytetyön tavoitteena on tehdä riskikartoitus kuvioita kolmeen eri tilanteeseen. Tarkoituksena on havainnollistaa niitä riskejä, joita tulisi ainakin ottaa huomioon, kun ollaan digitalisoimassa toimintoja pk-yrityksessä. Valitsin aiheiksi käytännön osioon verkkokaupan, etätyön ja toimitusketjun hallinnan digitalisoinnin. Tavoitteenani oli löytää toimintoja uhkaavia tietoriskejä ja keinot niihin varautumiseen. Valitsemani aiheet ovat ajankohtaisia ja niiden avulla yritys voi parantaa kannattavuuttaan ja turvata työvoiman saatavuuden.

Opinnäytetyöni teoriaosiossa aiemmin olen esitellyt digitalisaation aiheuttamia muutoksia niin yritysten kuin markkinoiden näkökulmasta. Tämän lisäksi teoriaosiossa on käyty läpi tietoturvaa ja -suojaa sekä riskienhallintaa. Myös laki sekä yrityksen asiakkaat odottavat, että tietoturvallisuus otetaan huomioon ja tietosuoja käytännöt ovat hallinnassa ja tämä on välttämätöntä myös yrityksen jatkuvuuden kannalta. Lähden laatimaan riskienkartoituskuvioita teoriaosiossa esittelemiini tietoriskeihin ja tietoturvatoimiin perustuen. Jokaisen yrityksen on digitalisoitava toimintaansa, jos haluaa pitää sen toiminnassa. Turvallisuusuhkien hallinta on yksi digitalisaation perusedellytys (Ilmarinen & Koskela 2015, 224).

6.1 Verkkokauppa

Kaupan ala on suurten muutosten kohteena. Digitalisaation myötä verkkokauppa mahdollistaa kuluttajille enemmän valinnanvaraa palveluntarjoajissa. Kilpailu kiristyy niin Suomessa kuin kansainvälisestikin. Monikanavaiset liiketoimintamallit ovat yleistymässä maailmanlaajuisesti. (Nieminen 2016, luku 9.1.) Monikanavaisuudella tarkoitetaan, että asiakkaat voivat asioida yrityksen kanssa usealla eri tavalla, kuten netissä tai myymälöissä. Monikanavaisuutta tulee kehittää, koska kuluttajat suosivat erilaisia tapoja asioidessaan yrityksen kanssa. Esimerkiksi osa haluaa tutustua tuotteeseen etukäteen netissä sekä vertailla hintoja. Ostoksien tekemisen mieltymykset myös vaihtelevat, osa haluaa nähdä tuotteen fyysisesti ja osa asiakkaista taas haluaa asioida rauhassa verkkokaupassa. (Ilmarinen & Koskela 2015, 109-110.)

6.1.1 Verkkokaupan edut

Perustamalla verkkokaupan yritys saavuttaa monia etuja kivijalkamyymälään verrattuna. Verkossa yritys voi ylläpitää laajempaa tuotevalikoimaa. Fyysisiä tuotteita myytäessä on edelleen huomioitava varaston koko. Digitaalisia tuotteita voi myydä melkein rajattomasti. Digitaalinen tallennuskapasiteetti on edullista, joka mahdollistaa suurten tietomäärien esilläpidon verkkokaupassa. (Alhonen 2015, 19-20.) Verkkokauppa mahdollistaa sellaistenkin tuotteiden valikoimassa pitämisen, joita ei yksittäisen tuotteen osalta myydä paljon. Puhutaan pitkä häntä -tuotteista, jonka käsitteen Chris Andersson on vuonna 2004 julkituonut. Digitalisaatio mahdollistaa yritykselle laajemman, jopa maailmanlaajuisen, asiakaskunnan tavoittamisen, jolloin myös erikoisimmille tuotteille riittää tarpeeksi kysyntää. Pitkä häntä -tuotteiden myynti perustuu verkon tehokkaisiin hakutoimintoihin, jolloin kuluttaja löytää etsimänsä helposti. Yrittäjän ei ole myöskään pakko pitää tuotetta itsellään varastossa, jolloin pääomaa ei sitoudu varastoon. (Ilmarinen & Koskela 2015, 146.) Verkkokauppa tuo joustavuutta toimintaan. Tuotteita voidaan pitää verkkokaupassa esillä ja hakea vasta sitten tavarantoimittajalta, kun asiakas on jo tilannut tuotteen. (Alhonen 2015, 20)

Yritykset kohtaavat globaalin kilpailun digitalisaation myötä, mutta samalla paikallisille yrityksille tarjoutuu mahdollisuus kasvattaa omaa asiakaskuntaa sekä markkinoita sen keinoin. (Ilmarinen & Koskela 2015, 68.) Verkkokauppa on saatavissa kaikkialla ja potentiaalisia asiakkaita ovat kaikki ne ihmiset, jotka käyttävät internettiä. Täysin vapaata verkkokauppakaan ei ole ja sitä rajoittavia tekijöitä muun muassa kielimuuri, toimitustapojen ehdot, puutteellinen verkkomaksaminen sekä paikallinen lainsäädäntö. Verkkokauppaan panostetaan kuitenkin kansainvälisesti ja EU:ssa korostetaan verkkokaupan merkitystä työllisyyden sekä talouskasvun nostattajana. (Alhonen 2015, 20.) EU:n yleisen tietosuoja-asetuksen yhtenä tavoitteena on yhtenäistää EU-jäsenmaiden tietosuoja käytänteitä ja siten tukea digitaalisten sisämarkkinoiden kehitystä EU:n alueella (Andreasson ym. 2019, 27).

Kuluttajien näkökulmasta verkkokaupan etuja ovat hintojen vertaamisen helppous, joka aiheuttaa kauppiaalle paineita pitää hintansa kilpailukykyisinä, sekä vaivaton tuotteiden etsiminen internetin hakutoiminnoilla. Yrittäjän näkökulmasta verkkokauppa on kustannustehokkaampi kuin hyvällä sijainnilla oleva kivijalkamyymälä. Useimmiten verkkokaupan ylläpitokustannukset ovat maksimissaan joitakin satoja euroja. Henkilöstöä ei tarvita verkkokaupan hoitamiseen niin paljon, sillä suurin osa verkkokaupan prosesseista pystytään automatisoimaan. Verkkokauppa on yleistynyt ja niiden myynti on kasvanut viime aikoina, jonka myötä myös palautusprosesseja sekä tuotteiden että rahojen osalta täytyisi automatisoida. (Alhonen 2015, 20-21)

6.1.2 Verkkokaupan tietoriskit

Pk-yrityksillä ei yleensä ole omaa tietoturvasta vastaavaa osastoa. Pk-yritykset ovat kiinnostavia kohteita verkkorikollisille ja erityisesti verkkokauppa on houkutteleva kohde tietomurtoa suunnittelevalle, koska siinä on mahdollisuus hyötyä taloudellisesti. Keskeinen tekijä verkkokaupan menestymiseen on kuluttajien luottamus. (Alhonen 2015, 37) Yrittäjän on kannattavaa olla tietoinen myös asiakkaita uhkaavista tietoturvariskeistä, jotta hän osaa tiedottaa ja neuvoa asiakkaita tilanteiden mukaan. (Alhonen 2015, 138) Kuviossa 6. esitellään verkkokaupan tietoriskejä sekä niihin varautuminen. Olen rakentanut kuvion tähän kappaleeseen käyttämieni lähteiden pohjalta.

Asiakkaisiin kohdistuvia tietoturvariskejä aiheuttavat tietoverkkorikolliset. Tietoverkkorikolliset haluavat saada käsiinsä asiakkaiden käyttäjätunnuksia sekä salasanoja ja luottokorttinumeroita. Asiakkaita yritetään huijata muun muassa erilaisin tietojenkalasteluviestein. Viesteissä voi olla linkkejä verkkokauppaa muistuttavalle sivustolle, johon käyttäjää pyydetään syöttämään tietonsa. Salasanoja vaaditaan nykyisin monessa paikassa ja käyttäjien näkökulmasta ongelmia aiheuttavat heikot salasanat, joita hyökkääjät voivat arvata. Rekisteröityneiltä käyttäjiltä tulisi vaatia tarpeeksi pitkiä sekä eri merkkejä sisältäviä salasanoja verkkokaupan toimesta. (Alhonen 2015, 138-139.)

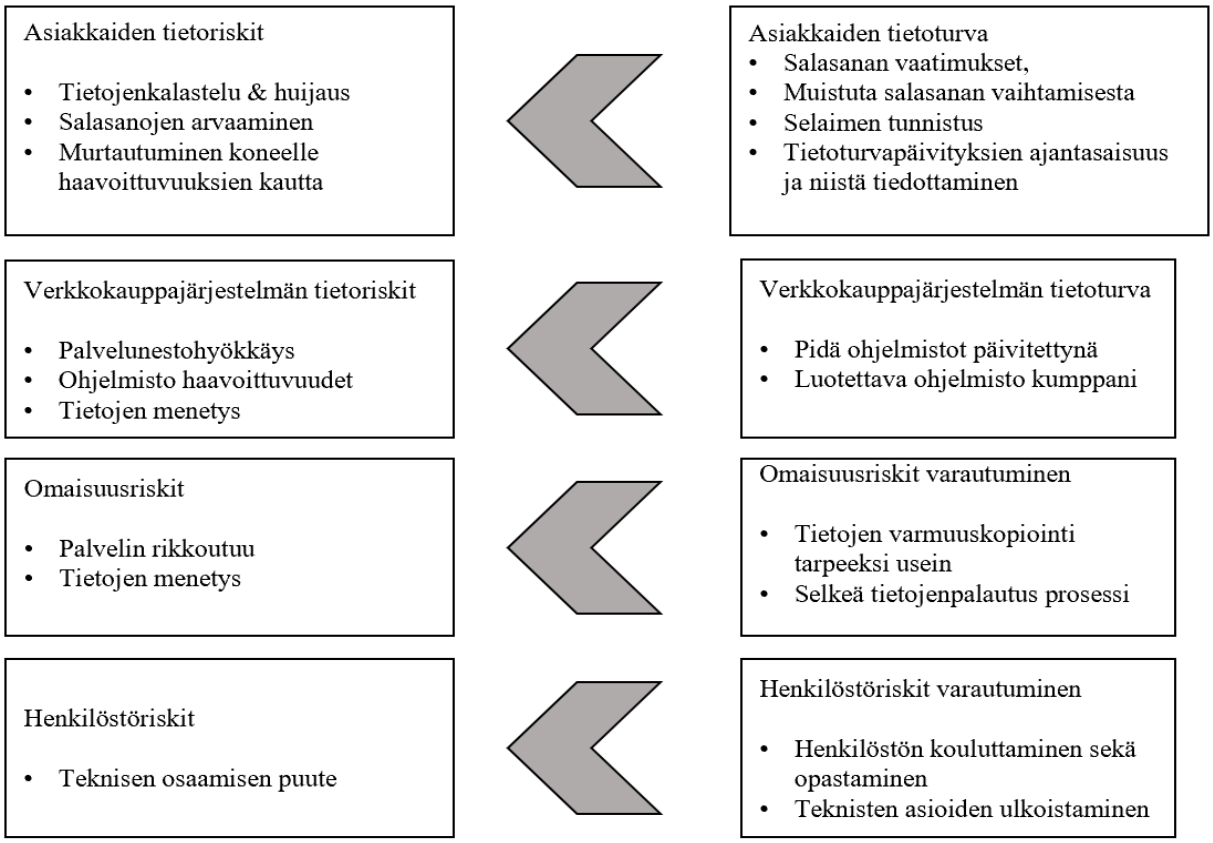
Verkkokauppiaalla on melko vähän mahdollisuuksia vaikuttaa palvelun käyttäjien omaan käytökseen tietoturvan osalta. Asiat, joihin verkkokauppa pystyy vaikuttamaan ovat järjestelmän hyväksymän salasanan pituus ja muistutusviesti salasanan vaihdosta. Tämän lisäksi verkkokaupalla voi olla selaimen tai selainversion tunnistava ohjelma, joka voi suositella asiakkaalle sen päivittämistä. Tietoturvapäivitysten tulee olla ajan tasalla ja niistä on tärkeää tiedottaa asiakkaita. Turvallisuuden tunnetta asiakkaille voi luoda sillä, että yritys ilmoittaa näkyvästi kaupan yhteystiedot. (Alhonen 2015, 142) Yritys voi myös tiedottaa asiakkailleen, mikäli tietojenkalastelu viestejä on liikkeellä yrityksen nimissä.

Verkkokauppajärjestelmään kohdistuvia tietoturvariskejä ovat haittaohjelmat sekä tietoverkkorikollisuus. Verkkokaupalle ikävä uhka on palvelunestohyökkäys, jonka pyrkimys on häiritä verkkopalvelun palvelinta niin, etteivät käyttäjät pääse verkkokauppaan (Alhonen 2015, 140). Tästä aiheutuu yritykselle myynnin menetystä, eli taloudellista vahinkoa. Alhosen (2015,140) mukaan palvelunestohyökkäykseltä suojautuminen on vaikeaa ja mahdollisuudet siihen ovat rajalliset. Ohjelmistohaavoittuvuudet verkkokauppaohjelmistoissa tai palvelimissa antavat hyökkääjälle tilaisuuden aiheuttaa vahinkoa yrityksen toiminnan häiritsemiseksi. Haavoittuvuuksilta voi suojautua huolehtimalla, että verkkokaupan tietoturvapäivitykset ovat ajan tasalla. Tietoturvapäivitysten asentaminen ja haavoittuvaisuuksista tiedottaminen

on verkkokauppa palveluntuottajan vastuulla silloin, kun palvelu on tilattu toimittajalta. (Alhonen 2015, 141.)

Verkkokauppajärjestelmää uhkaa myös tietojen menettäminen. Jos palvelimiin kohdistuu vahinko tai onnettomuus ja se tulee käyttökelvottomaksi, ovat yrityksen tärkeät tiedot vaarassa. Tietojen turvaamiseksi on tärkeää, että verkkokaupan tärkeistä tiedoista otetaan varmuuskopioita säännöllisesti. Yrityksessä on olennaista miettiä selkeä prosessi tietojen palauttamiseksi. Varmuuskopiot tulisi tallentaa palvelimelle, joka sijaitsee eri tilassa. Esimerkiksi tulipalon sattuessa, kaikki tiedot eivät tällöin pääse tuhoutumaan. (Alhonen 2015, 142.) Luokittelin tietojen menettämisen sekä palvelinten vikaantumisen myös omaisuusriskeiksi kuvioon 6.

Henkilöstöriski muodostuu pk-yrityksissä teknisen osaamisen puutteesta. Yrityksessä ei välttämättä ole osaamista verkkokauppaan liittyvistä teknologioista. Henkilöstö resurssit määrittelevät pitkälti sen, mitä kannattaa tehdä itse. Useimmiten yritykset päätyvät ulkoistamaan verkkokauppaohjelmiston, jolloin ohjelmiston tilaajan näkökulmasta moni riskeistä on hallittavissa oikealla toimittajavalinnalla. (Alhonen 2015, 37) Henkilöstöä on tärkeää opastaa sekä kouluttaa tietoturvallisiin toimintatapoihin liittyen (Alhonen 2015,142).



KUVIO 6. Verkkokaupan tietoriskit ja niihin varautuminen

6.2 Etätyöskentely

Tieto- ja viestintätekniikan kehitys mahdollistaa työn tekemisen eri paikoissa. Työ ei ole enää sidoksissa tiettyyn toimipisteeseen. (Kandolin, Ropponen & Tuomivaara 2016, 60.) Yhä useammin töitä tehdäänkin etänä varsinaisen työpaikan ulkopuolella kuten kotoa, työmatkalla tai asiakkaan luona (Järvinen & Rousku 2017, 48). Modernien yhteistyöalustojen sekä järjestelmien avulla pystytään järjestämään kokouksia sekä vaihtamaan tietoja ilman fyysistä siirtymistä. Aikaisemmin neuvotteluihin sekä tapaamisiin täytyi lentää paikan päälle, nykyisin samat neuvottelut hoidetaan sähköisten laitteiden ja erilaisten sovellusten avulla etänä. Nykyiset sovellukset ovat helppokäyttöisiä ja kustannustehokkaita, joten kenelle tahansa on mahdollista järjestää kokous niiden avulla. (Hämäläinen ym. 2016, 24.)

6.2.1 Etätyön edut

Työnantajan näkökulmasta katsottuna etätyön sallimalla on mahdollista rekrytoida laajemmalta alueelta työntekijöitä, jolloin potentiaalisia työntekijöitä on enemmän tarjolla. Etätyöskentely mahdollisuudella voi myös houkutella osaajia töihin sekä sen avulla voidaan pienentää toimistokustannuksia. Yhteiskunnan kannalta etätyö tukee aluekehitystä sekä se helpottaa osatyökykyisten työllistymistä. Lisäksi etätyö vähentää ruuhkia ja päästöjä. (Kandolin ym. 2016, 66)

Työntekijöiden näkökulmasta etätyön etuja ovat muun muassa mahdollisuus vaikuttaa omaan työhönsä, keskeytyksien väheneminen sekä lisääntynyt vapaa-aika työmatkojen jäädessä pois. Myös työtyytyväisyyden katsotaan kasvavan ja henkilöstö on paremmin sitoutunutta työpaikkaansa. (Kandolin ym. 2016, 64-65.) Tyytyväinen ja sitoutunut henkilöstö ei todennäköisemmin vaihda työpaikkaa, joten tietotaito säilyy yrityksellä itsellään.

6.2.2 Etätyön tietoriskit

Etätyössä on monia haasteita ja riskejä hyötyjen lisäksi. Tässä opinnäytetyössä keskityn kuitenkin tietoturvan näkökulmasta riskeihin sekä niiden torjumiseen. Kuviossa 7. on havainnollistettuna etätyöskentelyn tietoriskejä sekä keinoja niiden torujumiseen. Yleisesti ottaen työskentely muualla kuin työpaikalla on riskialttiimpaa, koska silloin henkilö ei ole yrityksen turvatoimien ulottuvilla ja käytössä on jokin muu tietoliikenneyhteys, kuin työpaikan tarjoama. Etätyössä tulisi noudattaa samoja ohjeistuksia, kun

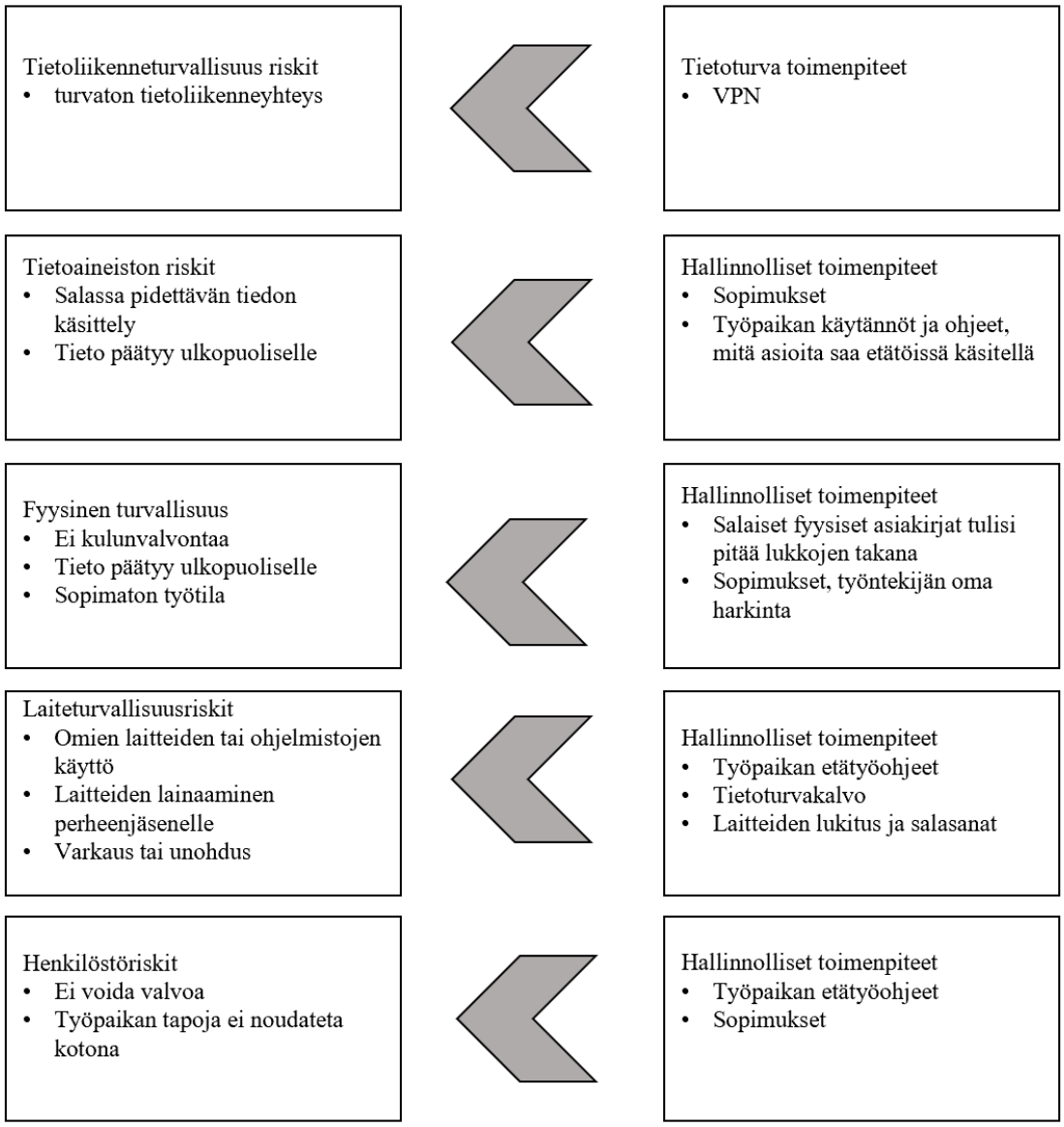
työpaikallakin työskenneltäessä. (Järvinen & Rousku 2017, 47.) Yrityksen tulisi varustaa käytössä olevat tietokoneet VPN-yhteydellä etätyön mahdollistamiseksi. VPN-yhteys toimii siten, että se muodostaa salatun yhteyden avoimen internet-verkon yli yrityksen verkkoon. (Järvinen & Rousku 2017, 68.) VPN-tekniikka mahdollistaa etätyöläisille pääsyn yrityksen suljettuun verkkoon työpaikan ulkopuolelta. VPN ei kuitenkaan torju haittaohjelmia tai tee netin käytöstä täysin turvallista, mutta ainakin turvallisempaa (Solla 2019.)

Rouskun (2014, 173) mukaan etätöiden teossa tulee huomioida tietoaineiston turvallisuus, jota uhkaavat väärinkäytökset sekä hyökkäyksien uhat. Tietojen luokittelu on yksi osa tietoturvallista työskentelyä ja se vaikuttaa myös tietojenkäsittelyn vaatimuksiin. Etätyön tekoon vaikuttavat esimerkiksi tietojen luonne, joita työtehtävässä käsitellään. Sopimukset asiakkaiden kanssa voivat kieltää tietojen käsittelyn työpaikan ulkopuolella tai kodin tietokoneella. Salassa pidettäviä tietoja varten yrityksellä tulisi olla ohjeistus etätyöntekoon. (Järvinen & Rousku 2017, 46-49.) Etätyössä on riskinä se, että salainen tieto voi päätyä yrityksen ulkopuoliselle taholle.

Kandolin ym. (2016, 67) mukaan etätyössä on huomioitava sopiva työtila. Työpaikalla tilan turvallisuuteen voidaan vaikuttaa kulunvalvonnalla, jonka avulla varmistutaan siitä, ettei tiloissa liiku työpaikan ulkopuolisia henkilöitä. Etätyössä on työntekijän omalla vastuulla, että turvallinen työpiste löytyy. Työpaikan tietoaineistoa käsiteltäessä on huolehdittava, ettei salainen tieto leviä työpaikan ulkopuolisille henkilöille. Salassa pidettävät asiakirjat tulisi pitää lukkojen takana eikä salassa pidettäviä tietoaineistoja tulisi hävittää kodin roskakoriin. Työpaikan ulkopuolella työskenneltäessä tulisi muistaa myös, että työasioista puhuttaessa ympäristö olisi syytä ottaa huomioon. Videopalaverin sisältö tai julkisessa liikenteessä puhelun kuulevat myös kanssa ihmiset. Erityisesti salassa pidettävistä asioista tilan sopivuus keskustelulle on arvioitava. (Rousku 2014, 173.)

Etätyöskentelystä aiheutuu väärinkäytön riskejä myös mukana kulkeviin tietoteknisiin laitteisiin. Työntekoon tarkoitettuja laitteita ei saisi antaa perheenjäsenten tai muidenkaan henkilöiden käyttöön. Myöskään omia laitteita ei tulisi käyttää työntekoon, vaikka ne olisivatkin parempia kuin työnantajan tarjoamat. Omien laitteiden käytöstä tulisi aina erikseen sopia ja varmistua, että ne vastaavat tietojenkäsittelyn vaatimuksiin ja ovat tarpeeksi tietoturvallisia. (Rousku 2014, 172-173.) Työnantajan tarjoamiin laitteisiin tulisi asentaa salasanat, sekä automaattinen lukitus (Rousku 2014, 171). Laitteet voidaan myös varastaa tai ne voivat unohtua ottaa mukaan, jos työskennellään liikennevälineessä tai muulla julkisella paikalla. Kannettavan tietokoneen kanssa tulee olla varuillaan ja näyttöä voi suojata ympärillä olevilta ihmisiltä hankkimalla tietoturvakalvon (Rousku 2014, 169).

Työnantaja ei pysty valvomaan etätyötä tekeviä samalla tavalla, kuin toimipisteellä työskenteleviä (Kandolin ym. 2016, 67). Etätyötä varten yrityksillä tulisikin olla selkeät etätyöohjeet, joita henkilöstön tulee noudattaa. (Rousku 2014, 172.) Tämän lisäksi työntekijöiden on noudatettava etätöissä ollessaan myös yrityksen muita normaaleja tietoturvakäytänteitä (Järvinen & Rousku 2017, 47).



KUVIO 7. Etätyön tietoriskit ja niihin varautuminen

6.3 Toimitusketjun hallinta

Toimitusketjun hallinta pitää sisällään yrityksen sekä sen yhteistyökumppaneiden muodostaman verkoston materiaalivirtojen sekä niihin liittyvien tieto- ja rahavirtojen ohjauksen, johtamisen, suunnittelun ja

kehittämisen. Tavoitteena on tuottaa mahdollisimman paljon lisäarvoa asiakkaalle. Toimitusketjun hallinnassa tärkeitä piirteitä ovat luotettavuus, aika sekä läpinäkyvyys. Ketjun osapuolten on tärkeää tehdä yhteistyötä yhteisen tavoitteen eteen. (Logistiikan maailma 2020a.)

Läpinäkyvyys on ensiarvoisen tärkeää ja sen saavuttamiseksi toimitusketjun osapuolien on jaettava tietoa toistensa kanssa. Teknologia mahdollistaa sen, että tavaravirtaa voidaan seurata yhä tarkemmin. Yhteistyön lisäksi toimitusketjun hallinnan kannalta tärkeitä asioita ovat ketteryys sekä riskienhallinta. Riskienhallinta kuuluu jokaiselle toimitusketjun osapuolelle. Prosessien digitalisointi parantaa toimitusketjun ajanhallintaa, tuottavuutta, läpinäkyvyyttä sekä osapuolten välistä luottamusta. (Logistiikan maailma 2020b.)

Teknologia, liiketoimintaprosessit sekä päätöksen teko monimutkaistuvat jatkuvasti, jonka takia yrityksissä on panostettava tiedon hallintaan sekä sen hyödyntämiseen entistä enemmän (Nieminen 2016, luku 8). Toimitusketjun hallinta on alueena erittäin laaja, joten päätin rajata tämän osuuden koskemaan tietojärjestelmiä, kuten toiminnanohjausjärjestelmiä sekä paperin vähentämisen yritysten toimitusketjun prosesseissa. Kuviossa 8 on esiteltynä toimitusketjun hallinnan digitalisoinnin tietoriskejä sekä niihin varautumista.

6.3.1 Toimitusketjun hallinnan digitalisoituminen

Jotta yritys voi menestyä, sen tulee kyetä hyödyntämään sekä hallitsemaan kaikkea tietoa tehokkaasti. Liiketoimintaan liittyvät tiedot koskevat muun muassa tuotteita, prosesseja, toimittajia sekä asiakkaita. Datan määrä lisääntyy jatkuvasti ja haasteena onkin löytää yrityksen toiminnan kannalta tärkeimmät tiedot, joita voidaan hyödyntää päätöksenteossa sekä liiketoiminnan optimoinnissa. Erilaisia tietojärjestelmiä ovat esimerkiksi toiminnanohjaus- sekä tuotetiedon hallinnanjärjestelmät. Näiden lisäksi hankintatoimintaa hyödyttäviä järjestelmiä ovat sähköiset tilausjärjestelmät sekä huutokaupat ja toimittajasuhteiden hallintaan. Tietojärjestelmiä tarvitaan jokaisen liiketoiminnan osa-alueen tueksi. (Nieminen 2016, luku 8.)

Toiminnanohjausjärjestelmän on tarkoitus liittää yhteen yrityksen eri toiminnot, jotta niitä pystytään hallitsemaan. Sen avulla materiaalin fyysinen ohjaus sekä talouden hallinta linkittyvät toisiinsa. Toiminnanohjausjärjestelmän myötä liiketoimintaprosesseja pystytään automatisoimaan sekä sovittamaan yhteen. Järjestelmä koostuu itsenäisistä osista ja yritykset voivat valita osia sen mukaan, mitkä ovat oman

liiketoiminnan kannalta hyödyllisiä. (Nieminen 2016, luku 8.1.) Toiminnanohjausjärjestelmän lisäksi toimitusketjun ohjausjärjestelmiä tarvitaan myös varastonhallinnan ja tuotannonohjauksen prosesseihin. Tuotannonohjauksen tarkoitus on kertoa tuotteiden valmistuminen sekä tuotantokapasiteetin huomioiminen ja varastonhallinnassa varastotasojen ylläpito. (Logistiikan maailma 2020c.) Niemisen (2016, luku 8.1) mukaan toiminnanohjausjärjestelmän avulla tilaus-toimitusketjua saadaan tehostettua sekä yhtenäistettyä ja materiaalivirtauksen ohjausta parannettua.

Prosessien digitalisointi ja tiukat kustannustehokkuustavoitteet ovat myötävaikuttaneet paperittomuuden lisääntymiseen. Paperista aiheutuu yrityksille kustannuksia, kuten postitus- sekä tulostuskuluja, jonka lisäksi paperin käsittely, arkistointi sekä hävitys sitovat henkilöstöä ja hidastavat toimintaa. Myös ympäristöasiat vaikuttavat osaltaan paperin määrän vähentämiseen. Jokaisen digitaalisuuteen tähtäävän yrityksen tavoite tulisi olla paperin määrän vähentäminen. Sitä voi edesauttaa investoimalla sähköiseen asiakirjahallintaan, -sopimiseen, -viestintään sekä -laskutukseen. Paperi estää reaaliaikaisen toiminnan, jonka vuoksi jokaisen digitaalisuutta tavoittelevan yrityksen tulisi päästä paperista eroon. Paperisten dokumenttien digitalisoinnissa oleellisinta olisi luopua asiakirjamuotoisesta tietojen käsittelytavasta, jolloin dokumenttien sekä lomakkeiden sisältöä pystyttäisiin hyödyntämään erilaissa järjestelmissä, palveluissa sekä automatisoiduissa prosesseissa. (Ilmarinen & Koskela 2015, 123-124.)

6.3.2 Toimitusketjun hallinnan tietoriskit

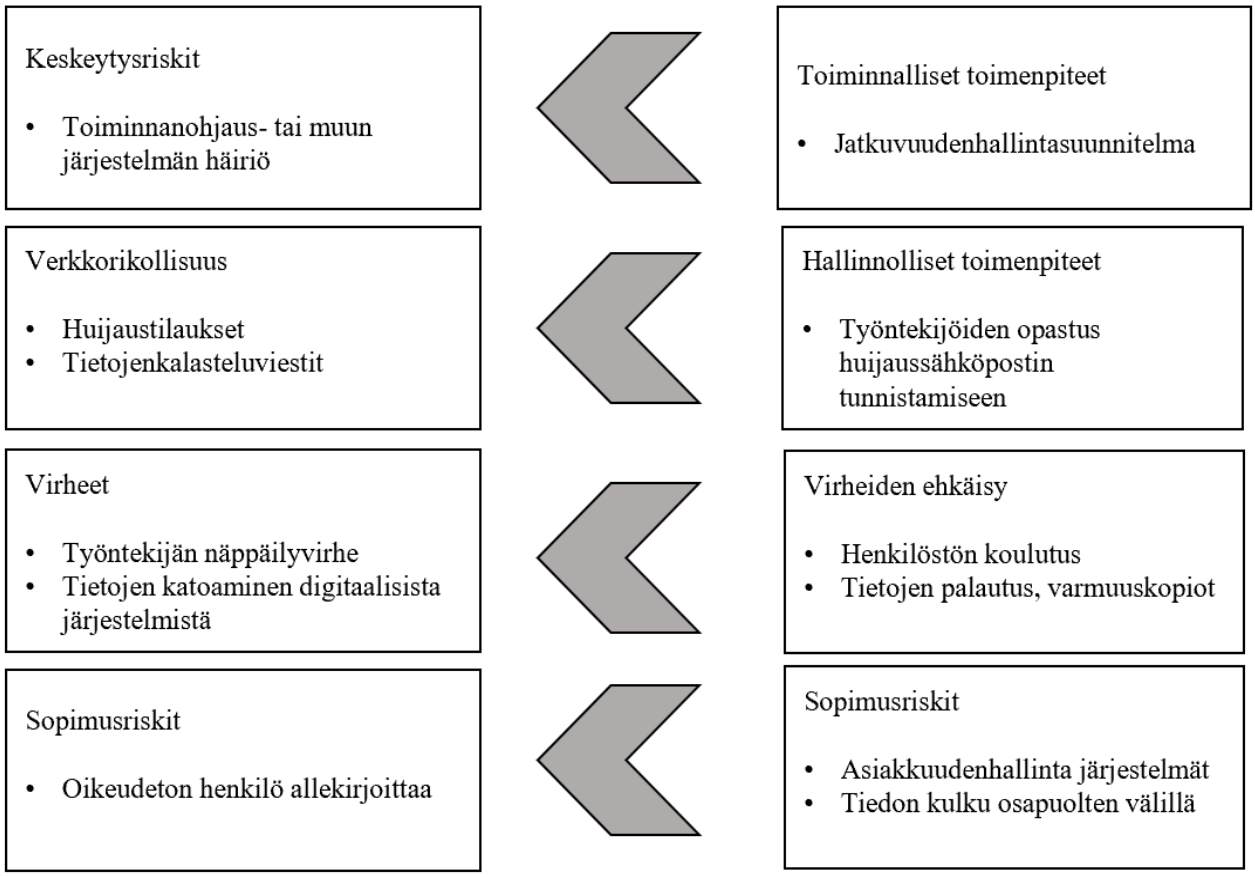
Pk-yrityksillä on toiminnanohjausjärjestelmille erilaisia teknisiä sekä toiminnallisia vaatimuksia kuin suurilla yrityksillä. Useimmissa järjestelmissä rakenne vaatii hierarkkista johtamismallia sekä toimintojen eriytymistä. Koska pk-yrityksissä henkilöstö voi tehdä useammalla alueella sekä tasolla töitä, toiminnanohjausjärjestelmän käyttöönotto on vaikeaa pk-yritykselle. Myös järjestelmätoimittajille on vaikeaa kehittää ohjelmistoja, koska pk-yritysten toiminta on hyvin erilaista keskenään ja asiakkaiden toiveet ja tavoitteet järjestelmän suhteen vaihtelevat. Haasteita ja uhkia aiheutuu, kun järjestelmiä integroidaan keskenään verkostoituvan toiminnan myötä. (Logistiikan maailma 2020c)

Tuotannonohjausjärjestelmille on tavanomaista, että kaikki yrityksen toiminnot käyttävät samaa tietokantaa. Tieto on saatavilla ajantasaisesti jokaiselle työntekijälle, josta aiheutuu vaatimuksia tiedon oikeellisuudelle. Tietojen täytyy olla syötettyinä oikein sekä ajoissa järjestelmään. (Logistiikan maailma 2020d.)

Jos toiminnanohjausjärjestelmään tai muuhun tietojärjestelmään tulee häiriö tai katkos, tieto ei ole saatavissa. Toiminnanohjausjärjestelmän pysähtyminen voikin keskeyttää yrityksen toiminnan kokonaan. Yritysten kannattaakin luoda tärkeille tietojärjestelmille suunnitelma, jotta häiriötilanteessa osataan varautua oikein ja pystytään turvaamaan toiminnan jatkuvuus. Mitä toiminnan kannalta kriittisemmästä järjestelmästä on kyse, sitä laajempia jatkuvuudenhallintasuunnitelmien kuuluisi olla. Jatkuvuudenhallintasuunnitelman tarkoituksena on minimoida yleisimpien häiriötilanteiden vahingot. Perustana suunnitelmalle on turvata liiketoiminnan jatkuvuus. Toimintoja, jotka eivät ole yrityksen toiminnan kannalta välttämättömiä, ei oteta niin paljon huomioon. Lisäksi on tärkeää tunnistaa toimintojen keskinäiset riippuvuudet, jotta varaudutaan oikein. (Rousku 2014, 60-61.)

Kun asiakirjoja digitalisoidaan, mahdollistetaan usein samalla sopimusten sekä muiden oikeustoimien varmentaminen sähköisesti. Tällöin tunnistautumiseen vaaditaan digitaalista vahvistamista tai allekirjoitusta, allekirjoitustapoja ovat esimerkiksi mobiilivarmenne tai pankin verkkopalvelutunnukset. Yritys voi käyttää allekirjoittamiseen joko omaa allekirjoituspalvelua tai ostaa sellaisen toimittajalta. Digitaalinen allekirjoitus sisältää myös haasteita ja esimerkiksi yritysten välisessä liiketoiminnassa on otettava huomioon nimenkirjoitusoikeudet ja niissä mahdollisesti tapahtuvat muutokset. (Ilmarinen & Koskela 2015, 124.) Riskinä on, että tieto ei kulje yritysten välillä, jonka seurauksena oikeudeton henkilö voi allekirjoittaa sopimuksen. Tästä voi aiheutua taloudellisia vahinkoja yritykselle. Toimittaja- tai asiakassuhteiden hallintaan on erilaisia järjestelmiä, jotka tekevät tiedon jakamisesta helpompaa ja parantavat yhteistyökumppanien välistä vuorovaikutusta (Nieminen 2016, luku 8.3). Niistä näkee muun muassa yrityksen yhteyshenkilöt, joiden kanssa asioidaan. Vieraan nimen vastaan tullessa sähköpostissa, on helppoa tarkistaa, onko kyseinen henkilö töissä oikeasti yrityksessä.

Yrityksiä yritetään huijata monin keinoin netissä ja sähköpostissa, esimerkiksi valheellisilla tarjouksilla (Järvinen & Rousku 2017, 81). Yrityksiä uhkaavat rikolliset, väärinkäyttäjät sekä huijarit taloudellisen hyödyn perässä (Rousku 2014, 197). Valetarjouksissa motiiveina voi olla ilkivalta, taloudellinen hyöty tai tietojen, kuten yrityksen myymien tuotteiden hintojen urkkiminen. Yrityksien sähköposteihin voi myös saapua tiedonkalastelu viestejä. Tärkeintä on ohjeistaa työntekijöitä yrityksen käytännöistä sekä opettaa heitä tunnistamaan huijaus viestit. Sähköposteissa tulleita linkkejä tai liitetiedostoja ei tule avata, jos lähettäjä on tuntematon (Rousku 2014, 175).



KUVIO 8. Toimitusketjun digitalisoinnin tietoriskit ja niihin varautuminen

7 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyössäni tavoitteenani oli laatia kolme kappaletta riskikartoituskuvioita, jotka käsittelevät digitaalisessa toiminnassa ilmeneviä tietoriskejä sekä keinot niihin varautumiseen. Valitsin käytännön osion aiheiksi verkkokaupan, etätyöskentelyn sekä toimitusketjun hallinnan digitalisoitumisen tietoriskit. Verkkokaupan tapauksessa merkittäviä riskitekijöitä olivat tietoverkkorikolliset, jotka vaanivat yritystä itseään sekä asiakkaita. Tärkeimpiä rikollisten torjumiskeinoja on huolehtia ohjelmistojen päivityksistä sekä vaatia asiakkailta tarpeeksi vahvoja salasanoja ja tiedottaa tietoturvapäivityksistä. Muut verkkokaupan tietoriskit koskevat omaisuusriskejä, joka kattaa tietojen tuhoutumisen sekä henkilöstöriskit. Henkilöstöriskeihin voidaan käytännössä varautua ulkoistamalla verkkokauppapalvelu alihankkijalle tuotettavaksi, jolloin omalle henkilöstölle riittää, että osaavat käyttää palvelua.

Etätyön tapauksessa yrityksen tulisi tarjota työntekijöilleen VPN-yhteys, jonka avulla työntekijät pääsevät yrityksen salattuun verkkoon. Työpaikan ulkopuolella työskenneltäessä henkilöstön tulisi muistaa noudattaa samoja yrityksen käytänteitä kuin työpaikallakin. Etätyön tietoriskit liittyvät vahvasti siihen, että tieto voi päätyä yrityksen ulkopuolisille henkilöille eikä työntekijä ole työpaikan turvallisuuskontrollien piirissä tai esimiehen valvonnan alla. Tietoriskejä muodostuu työvälineiden lainaamisesta perheenjäsenille tai työväline voi unohtua esimerkiksi liikennevälineeseen. Vastaavasti työpaikan ulkopuolinen henkilö voi kuulla puhelimessa käydyn keskustelun. Selkeiden etätyöohjeiden avulla voidaan ehkäistä virheellistä toimintaa.

Toimitusketjun hallinnan digitalisoinnissa rajasin aiheen koskemaan tietojärjestelmiä sekä paperin vähentämisen yritysten toimitusketjun toiminnoissa. Toimitusketjun kannalta tärkein ja yrityksen toiminnalle kriittisin on toiminnanohjausjärjestelmä, jos se ei ole käytössä yrityksen toiminta voi pysähtyä. Näitä tilanteita varten tulisi tehdä jatkuvuudenhallintasuunnitelma, jossa on toimintaohjeet tilanteiden varalle. Muut toimitusketjua uhkaavat riskit ovat tietojenkalastelu viestit sekä valetilaukset, henkilöstöriskit ja sopimusriskit. Näihin voidaan varautua opastuksella ja vuorovaikutusta lisäämällä kuten myös tietojen palautus käytännöillä ja varmuuskopioinnilla.

Tuotoksistani kävi ilmi ainakin se, että tietoturva ei ole ainoastaan tekniikkaa ja että suurin osa tietoturvasta on yrityksen henkilöstöstä ja viestinnästä kiinni. Tärkeää olisikin kouluttaa henkilöstöä ja laatia yritykseen tietoturvakäytännöt. Pk-yrityksissä kaikkia toimintoja ei ole järkevää tehdä itse ja ohjelmistot

ja muut tietojärjestelmät ovat helpointa ulkoistaa. Opinnäytetyön tekeminen oli opettavaista ja mielenkiintoista. Itselleni tietoturva aiheena oli varsin vieras, mutta tietoa oli saatavissa paljon ja mielestäni onnistuin täyttämään opinnäytetyön tavoitteen, eli tuottamaan riskienkartoituskaaviot. Tietoturvallisuudella on valtava merkitys yrityksen kokonaisturvallisuuteen ja sillä on paljon merkitystä yrityksen maineeseen niin yritysasiakkaiden kuin henkilöasiakkaiden keskuudessa.

LÄHTEET

Aalto-Setälä, M. & Viitaila, M. 2018. Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille. Helsinki: Keskuskauppakamari. Saatavissa: https://kauppakamari.fi/wp-content/uploads/2018/11/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio-1.pdf Viitattu 14.3.2020

Alhonen, A. 2015. Verkkokauppaopas 2015. Anders innovations Oy. Saatavissa: https://tieke.fi/wp-content/uploads/2018/11/Verkkokauppaopas_2015.pdf viitattu 29.3.2020

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki: Tietosanoma Oy.

Centria-ammattikorkeakoulu, 2018. Saatavissa: https://tki.centria.fi/hanke/cynic-business-models-for-digital-innovation-and-cyber-secur/1876 viitattu 6.4.2020

Gerdt, B. & Eskelinen, S. 2018. Digiajan asiakaskokemus. Helsinki: Alma Talent Oy. Saatavissa: https://bisneskirjasto-almatalent-fi.ezproxy.centria.fi/teos/DAEBDXDTEB#kohta:Digiajan((20)asiakaskokemus viitattu 19.3.2020

Hämäläinen, V., Maula, H. & Suominen K. 2016. Digiajan strategia. Helsinki: Alma Talent Oy.

Ilmarinen, V. & Koskela, K. 2015. Digitalisaatio: Yritysjohdon käsikirja. Helsinki: Talentum.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala T. 2014. Yrityksen riskienhallinta. Helsinki: Finanssi- ja vakuutuskustannus Oy

Järvinen, P. 2012. Arjen tietoturva. Vinkit & ratkaisut. Jyväskylä: Docendo

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit. Helsinki: Alma Talent Oy.

Kalliokoski, P. 2003. Ihminen on suurin tietoriski. Kaleva. Julkaistu 21.09.2003. Saatavissa: https://www.kaleva.fi/teemat/digi/ihminen-on-suurin-tietoriski/560451/ viitattu 26.3.2020

Kandolin, I., Ropponen, A. & Tuomivaara, S. 2016. Jousto-opas. Sujuvuutta työhön yksilöllisillä ja yhteisöllisillä ratkaisuilla. Helsinki: Työterveyslaitos. Saatavissa: http://www.julkari.fi/bitstream/handle/10024/131548/Jousto_opas.pdf?sequence=1&isAllowed=y viitattu 31.3.2020

Koistinen-Jokiniemi, P., Koskiniemi, T., Lehtinen, I., Lindroos, V., Martikainen, J., Montonen, S., Savela, O. & Tuomaala, E. 2017. Digitalisaatio ja bkt – Miten digitalisaatio näkyy taloustilastoissa. Tilastokeskus. Saatavissa: https://www.tilastokeskus.fi/static/media/uploads/tup/kantilinpito/digitalisaatio_bkt.pdf viitattu 21.02.2020

Laitinen, J. 2017. Kodin kyberopas, Ohjeita digitaaliseen arkeen. Helsinki: Turvallisuuskomitea. Saatavissa:https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf viitattu 22.03.2020

Logistiikan maailma 2020a. Toimitusketjun hallinta. Saatavissa: http://www.logistiikanmaailma.fi/logistiikka/logistiikka-ja-toimitusketju/ viitattu 02.04.2020

Logistiikan maailma 2020b. Strategisia tavoitteita toimitusketjun hallinnalle. Saatavissa: http://www.logistiikanmaailma.fi/logistiikka/logistiikka-ja-toimitusketju/toimitusketjun-hallintastrategiat/ viitattu 02.04.2020

Logistiikan maailma 2020c. Ohjausjärjestelmät. Saatavissa: http://www.logistiikanmaailma.fi/logistiikka/ohjausjarjestelmat/ viitattu 03.04.2020

Logistiikan maailma 2020d Toiminnanohjausjärjestelmä. Saatavissa: http://www.logistiikanmaailma.fi/logistiikka/ohjausjarjestelmat/toiminnanohjausjarjestelma/ viitattu 04.04.2020

Myllynen, T. 2005. Tietoturva ja riskit tietotekniikassa. Teoksessa H. Kuusela & R. Ollikainen. (toim.) Riskit ja Riskien hallinta. Tampere: Tampere University Press. 242-274.

Nieminen, S. 2016. Hyvä hankinta – Parempi bisnes. Helsinki: Talentum pro. Saatavissa: https://bisneskirjasto-almatalent-fi.ezproxy.centria.fi/teos/FAGBHXCTEB#kohta:8((20)Tietoj((e4)rjestelm((e4)t((20)hankinnan((20)tukena((20)(:8.1((20)Toiminnanohjausj((e4)rjestelm((e4)t((20)/piste:b1226 viitattu 02.04.2020

Pulkkinen, M., Rajahonka, M., Siuruainen, R., Tinnilä, M. & Wendelin, R. 2005. Liiketoimintamallit arvonluojina: ketjut, pajat ja verkot. Helsinki: Teknologiainfo Teknova. Teknologiateollisuuden julkaisu 8.

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum Media Oy.

Solla, K. 06.09.2017 Digitreenit: Mikä ihmeen vpn? Se suojaa nettiyhteyttäsi avoimessa verkossa. 11.02.2019 Saatavissa: https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suojaa-nettiyhteyttasi-avoimessa-verkossa viitattu 31.03.2020

Tall, J., Sorama, K., Tulisalo, P., Petäjä, E. & Virkamäki, A. 2013. Yrittäjyys 2.0 – menestyksen avaimia. Seinäjoki: Seinäjoen ammattikorkeakoulu. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/55178/B69_netti.pdf?sequence=1&isAllowed=y viitattu 20.3.2020