Jenni Juola

TIETOTURVATASON KEHITTÄMINEN PK-YRITYKSISSÄ

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tuotantotalouden koulutusohjelma
Syyskuu 2017

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Syyskuu 2017	**Tekijä/tekijät** Jenni Juola
Koulutusohjelma Tuotantotalous		
Työn nimi TIETOTURVATASON KEHITTÄMINEN PK-YRITYKSISSÄ		
Työn ohjaaja FM Joni Jämsä		**Sivumäärä** 42 + 2
Työelämäohjaaja FM Anita Rättyä		

Opinnäytetyön toimeksiantaja oli CyberWI-tietoturvahanke, jonka kansallisena koordinaattorina toimii Centria-ammattikorkeakoulu. Opinnäytetyön aiheena oli tietoturvallisuuden kehittäminen pienissä ja keskisuurissa yrityksissä. Työn tavoitteena oli laatia tietoturvapolitiikka ja tietoturvaohjeet hankkeen asiakasyritykselle. Lisäksi tavoitteena oli muodostaa asiakasyritykseen laadittujen ohjeiden pohjalta kehys tietoturvaohjeiden laatimiseen. Tätä kehystä voitaisiin hyödyntää hankkeessa muissakin asiakasyrityksissä.

Työn teoriaosuudessa käsiteltiin aluksi tietoturvallisuuden peruskäsitteitä ja osa-alueita sekä tietoturvallisuutta ohjaavia lakeja ja standardeja. Tämän jälkeen tarkasteltiin pienten ja keskisuurten yritysten näkökulmasta yritysjohdon tärkeimpiä tehtäviä ja työkaluja tietoturvallisuuden kehittämisessä. Lopuksi selvitettiin, miten henkilökunta voi omalla toiminnallaan vaikuttaa tietoturvallisuuden toteutumiseen.

Esitetyt periaatteet todennettiin opinnäytetyön käytännön osiossa tekemällä hankkeen asiakasyritykselle tietoturvapolitiikka ja tietoturvaohjeet. Tietoturvapolitiikan laadinnassa käytettiin valmista kehystä, mutta sisältö muokattiin vastaamaan yrityksen tarpeita. Laaditut dokumentit liitettiin osaksi yrityksen laadunhallintajärjestelmää. Lisäksi opinnäytetyöprojektin tuloksena tietoturvahankkeen käyttöön muodostui muokattava tietoturvaohjepankki, jonka avulla tietoturvaohjeiden laatiminen tuleville asiakasyrityksille on tulevaisuudessa helpompaa.

Asiasanat
laatu, riskienhallinta, tietosuoja, tietoturva, tietoturvaohjeet, tietoturvapolitiikka

ABSTRACT

Centria University of Applied Sciences	Date	Author
	September 2017	Jenni Juola
Degree programme Industrial Management		
Name of thesis DEVELOPMENT OF INFORMATION SECURITY LEVEL IN SME BUSINESSES		
Instructor M.Sc. Joni Jämsä		**Pages** 42 + 2
Supervisor M.Sc. Anita Rättyä		

This thesis was commissioned by CyberWI –cyber security project which is coordinated by Centria University of Applied Sciences. The theme of this thesis was to develop cyber security in small and medium sized enterprises. The aim of the thesis was to create information security policy and instructions to the client company of the project. The target was also to create a common template for customer specific security instructions which could be utilized in the other companies.

The theory section of the thesis firstly introduces the basic terms and subareas of information security and also information security laws and standards. After that the thesis discusses the most important tasks and tools of company management for improving information security in small and medium sized companies. Finally, the thesis describes how employees can affect a company's cyber security by their own way of working.

In the practical part of the thesis information security policy and instructions were created for the client company. The information security policy was modified from a ready made framework to meet the client's specific needs. The created documents were attached as a part of the client's quality management system. Another task carried out in the practical part was creating a common modifiable information security instructions pool which could be utilized while creating client specific information security instructions in the future.

Key words
data protection, information security, information security instructions, information security policy, quality, risk management

KÄSITTEIDEN MÄÄRITTELY

Biometrinen tunnistus	Tunnistusmenetelmä, joka perustuu ihmisen fyysiseen ominaisuuteen, esimerkiksi sormenjälki, silmän iiris tai kasvojen muoto
DoS	Denial of Service, palvelun esto
Haavoittuvuus	Alttius turvallisuutta uhkaaville tekijöille, voi johtua esimerkiksi turvatoimien ja suojausten puutteesta tai heikkoudesta
Haittaohjelma	Ohjelma, jonka tarkoituksena on aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä
Henkilötieto	Luonnollista henkilöä tai hänen ominaisuuksiaan kuvaava merkintä, joka voidaan tunnistaa häntä tai hänen perhettään koskevaksi
ISO/IEC 9000	Laadunhallintaa käsittelevä standardiperhe
ISO/IEC 27000	Tietoturvallisuutta käsittelevä standardiperhe
Rekisterinpitäjä	Taho, jonka käyttöä varten henkilörekisteri perustetaan
Riski	Todennäköisyys uhkan toteutumiselle, ilmaistaan usein tapahtuman seurausten ja toteutumisen todennäköisyyden yhdistelmänä
Riskienhallinta	Toiminta, jolla organisaation toimintaa ohjataan riskien osalta
Tietoriski	Riski, joka aiheutuu tiedosta tai kohdistuu tietoon
Tietosuoja	Ihmisen yksityisyyden suoja henkilötietoja käsiteltäessä
Tietoturvallisuus	Tiedon käytettävyyden, eheyden ja luottamuksellisuuden varmistaminen

Tietoturvapolitiikka	Yrityksen johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta
Uhka	Mahdollinen tapahtuma, josta voi seurata vahinkoa organisaatiolle tai järjestelmälle
Vahinko	Toteutunut riski, mitattavissa rahallisena kustannuksena

1 JOHDANTO

Kaikissa yrityksissä on liiketoiminnan jatkuvuuden kannalta merkittävää tietoa, mutta siitä huolimatta useissa pienissä ja keskisuurissa yrityksissä ei ole kiinnitetty riittävästi huomiota tietoturvallisuuteen. Tietoturvan merkitys korostuu entisestään teknologian jatkuvan kehityksen myötä. Tietoturva koetaan usein monimutkaiseksi asiaksi, joka kuuluu ensisijaisesti tietotekniikasta vastaaville henkilöille. Tietoturvallisuus on kuitenkin paljon muutakin kuin teknologiaa, ja siitä on vastuussa yrityksen johto. Henkilöstön toiminnalla on tietoturvallisuuden toteutumisessa merkittävä rooli ja jokainen työntekijä voi omalla toiminnallaan edistää tietoturvallisuuden toteutumista yrityksessä.

Yrityksen tietoturvallisuudelle asettavat vaatimuksia niin sisäiset kuin ulkoisetkin tekijät, ja niiden tulisi ohjata tietoturvan kehittämistä yrityksessä. Vaatimustenmukaisuuden varmistamiseksi yrityksen on tunnistettava sen toimintaan vaikuttavat lait ja asetukset, joista uusimpana EU:n tietosuoja-asetus. Lakien ja asetusten lisäksi yrityksen tietoturvallisuuden kehittämistä ohjaa asiakkaiden ja yhteistyökumppanien vaatimukset sekä yrityksen johdon määrittelemä taso tietoturvallisuudelle. Tietoturvallisuuden kehittäminen voi tuoda yritykselle kilpailuetua ja vahvistaa sen imagoa.

Opinnäytetyön toimeksiantaja oli CyberWI –tietoturvahanke, jonka kansallisena koordinaattorina toimii Centria-ammattikorkeakoulu. Vaikka hankkeessa keskeistä on teollisen internetin laitteiden suojaaminen, on tavoitteena lisäksi sellaisten tietoturvaan liittyvien sovellusta tai palveluiden tuottaminen, joita myös pienten ja keskisuurten yritysten on helppo hyödyntää. Työskennellessäni opiskelija-assistenttina hankkeessa, sain projektipäälliköltä aiheen opinnäytetyölle. Opinnäytetyön tavoitteena oli tietoturvan kehittäminen pienissä ja keskisuurissa yrityksissä ja aiheen oli tarkoitus muotoutua tarkemmin asiakasyrityksen tarpeisiin. Selvityksessä kävi ilmi, että asiakasyritys on halukas kehittämään tietoturvallisuuden tasoaan. Yrityksessä ei ollut tietoturvapolitiikkaa eikä henkilöstön tietoturvaohjeistusta, joten opinnäytetyön tavoitteeksi otettiin niiden luominen. Tarkoituksena oli myös saada aikaan yleinen tietoturvaohjeistus, jota voitaisiin tulevaisuudessa muokata hankkeessa eri yritysten tarpeisiin. Asiakasyrityksen toimitusjohtajaa mietitytti EU:n tietosuoja-asetuksen vaatimat toimenpiteet yrityksessä. Opinnäyte-

työn teoriaosassa käsitelläänkin EU:n tietosuoja-asetuksen vaikutuksia PK-yrityksen näkökulmasta, jotta yrittäjä saa tietoa uudistuksesta, mutta yritykseltä vaadittavien toimenpiteiden selvittämistä päätettiin jatkaa opinnäytetyön ulkopuolella.

Tietoturvallisuus on aiheena laajuutensa vuoksi haastava mutta silti mielenkiintoinen ja ajankohtainen. Tietoturvallisuutta käsittelevää materiaalia on saatavilla erittäin paljon ja sitä hyödynnetään työssä monipuolisesti. Useimmat lähteet käsittelevät tietoturvallisuutta suuren organisaation näkökulmasta, mikä luo haasteita PK-yrityksen tarpeiden huomioimiselle aiheen käsittelyssä. Opinnäytetyössä käytettiin lähteinä alan kirjallisuutta, tietoturvastandardeja, lehtiartikkeleita sekä sähköisiä materiaaleja.

Opinnäytetyön luvussa 2 määritellään tietoturvallisuuden käsite sen kolmen ulottuvuuden sekä kahden lisämääritelmän avulla. Tämän jälkeen tietoturvallisuutta tarkastellaan sen osa-alueiden kautta. Kolmannessa luvussa käsitellään lyhyesti yrityksen tietoturvallisuutta ohjaavia lakeja sekä standardeja ja muita ohjeistuksia. Lisäksi luvussa käsitellään EU:n tietosuojauudistuksen merkittävimpiä vaatimuksia. Neljänteen lukuun on koottu PK-yrityksen näkökulmasta merkittävimpiä tietoturvallisuuden kehittämiseen liittyviä johdon toimenpiteitä. Lisäksi luvussa esitellään työkaluja tietoturvallisuuden kehittämiseen ja jatkuvuudenhallintaan sekä pohditaan tietoturvallisuuden ja laadun yhteneväisyyksiä. Viidennessä luvussa käsitellään tietoturvallisuuteen liittyviä asioita, joita henkilöstön tulisi arjessa huomioida. Kuudennessa luvussa kerrotaan työn käytännön toteutuksesta ja luku 7 sisältää johtopäätökset ja pohdintaa.

2 TIETOTURVA

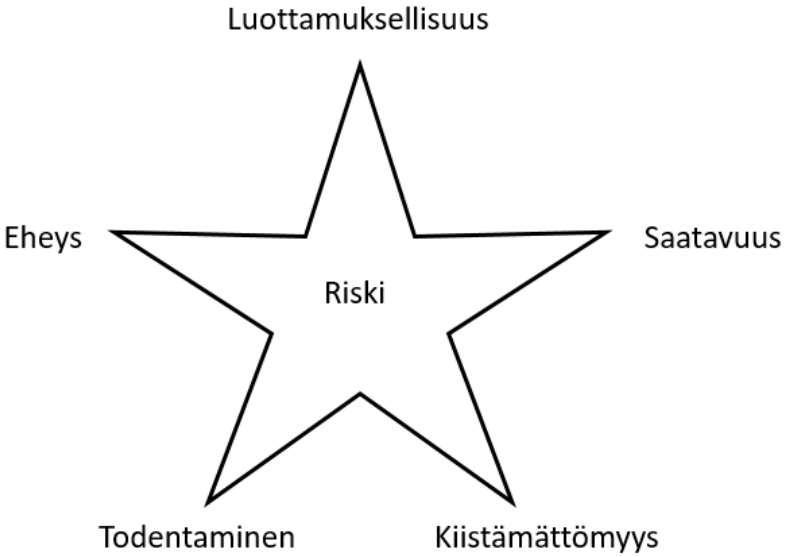
Tietoturvallisuuden tarkoituksena on tukea yrityksen liiketoiminnan tarpeita sekä täyttää sille asetetut sisäiset ja ulkoiset vaatimukset. Usein tietoturva nähdään vain ylimääräisiä kustannuksia aiheuttavana pakotteena. Asianmukaisesti hoidettu tietoturva tuo kuitenkin yritykselle kilpailuetua ja antaa edellytyksiä liiketoiminnan jatkuvuudelle. Tietoturvallisuuden perinteinen määritelmä keskittyy tiedon kolmen perusominaisuuden - eheyden, luottamuksellisuuden ja saatavuuden - turvaamiseen. (Laaksonen, Nevasalo & Tomula 2006, 17-18.)

Luottamuksellisuudella tarkoitetaan luokitellun tai salassa pidettävän tiedon käytön rajaamista vain niille tahoille, joilla on siihen tiedonsaanti- ja käyttöoikeus. Luottamuksellisuus voidaan toteuttaa tietojärjestelmissä esimerkiksi käyttöoikeuksien hallinnalla, jolloin käyttäjälle annetaan vain tehtävien hoitamiseen tarvittavat oikeudet. Tiedon hallussapitoa loukataan, jos ulkopuolinen taho käyttää yrityksen toimintaan liittyvää luottamuksellista tietoa luvattomasti hyväkseen. Tiedon luottamuksellisuuden menettäminen voi aiheuttaa yritykselle merkittäviä taloudellisia vahinkoja. (Rousku 2014, 47; Miettinen 1999, 25.)

Miettisen (1999, 26) mukaan tiedon eheydellä tarkoitetaan, että tietoa ei synny tai katoa itsestään ja se pysyy alkuperäisessä muodossaan koko elinkaaren ajan. Tiedon eheyden voi menettää esimerkiksi tietojärjestelmän toimintahäiriön, tietokannan vioittumisen tai tietojen luvattoman muuttamisen vuoksi. Rousku (2014, 47) keskittyy tiedon eheyden määrittelyssään siihen, ettei tieto saa muuttua hallitsemattomasti. Tiedon eheys voidaan varmistaa sillä, että tietoa saavat muokata vain sellaiset henkilöt, joilla on siihen käyttöoikeus. Tärkeimpien tietojen tulee olla kaikissa tilanteissa palautettavissa. (Rousku 2014, 49; Miettinen 1999, 26.)

Tiedon saatavuudella pyritään varmistamaan, että tiedot ovat niitä tarvitsevien käyttäjien saatavilla. Tiedon saatavuutta voivat uhata esimerkiksi palvelunestohyökkäykset (DoS, Denial of Service). (Rousku 2014, 50.) Tietojen saatavuus menetetään, jos niitä ei voida käyttää silloin kun niitä tarvittaisiin. Saatavuus voidaan menettää joko tahattomasti, esimerkiksi teknisen vian vuoksi tai tarkoituksellisen toiminnan takia. Tiedon saatavuutta voi rajoittaa myös tarpeettoman tiukat suojaustoimet. (Miettinen 1999, 28.)

Edellä esitettyyn kolmeen ulottuvuuteen perustuvaa määritelmää pidetään usein riittämättömänä. Hakala, Vainio & Vuorinen (2006, 4) ja Raggad (2010, 22) laajentavat tiedon määritelmää kiistämättömyyden ja pääsynvalvonnan avulla. Raggadin (2010, 22) esittämässä tähtimallissa (KUVIO 1) tietoturvallisuutta kuvataan kolmen perusulottuvuuden lisäksi näillä kahdella lisämääritelmällä. Mallissa tähden ydin muodostuu riskiperusteisesta johtamistavasta ja jokainen sakara kuvaa tietoturvallisuuden tavoitetta. Pääsynvalvonnan eli todentamisen avulla varmistetaan, että käyttäjällä on oikeus päästä tietoihin. Useimmiten todentamiseen käytetään käyttäjätunnusta ja salasanaa. Kiistämättömyys tarkoittaa sitä, että järjestelmää käyttävän henkilön tiedot voidaan tunnistaa ja tallentaa. Tiedonsiirrossa kiistämättömyydellä tarkoitetaan sitä, ettei tiedon lähettäjä voi kiistää lähettämistä eikä tiedon vastaanottaja viestin saapumista. Tiedonsiirrossa kiistämättömyys varmistetaan usein digitaalisella allekirjoituksella. (Hakala ym. 2006, 5; Raggad 2010, 22.)



KUVIO 1. Tietoturvallisuuden tähtimalli. (mukaillen Raggad 2010, 22)

2.1 Tietoturva osana yrityksen kokonaisturvallisuutta

Tietoturvallisuus tulisi ymmärtää osana yrityksen kokonaisturvallisuutta, jonka tarkoituksena on edistää yrityksen kilpailukykyä ja parantaa tuottavuutta. Yrityksen kokonaisturvallisuudella pyritään varmistamaan liiketoiminnan jatkuvuus, turvallisuus ja vaatimuksenmukaisuus kaikissa tilanteissa. Elinkeinoelämän keskusliitto on kehittänyt yritysturvallisuusmallin (KUVIO 2), joka toimii perustana yrityksen turvallisuuden tarkasteluun. Kokonaisturvallisuuden osa-alueet ovat osin päällekkäisiä, ja tietoturvallisuuden yhteydessä tarkastellaankin usein myös henkilöstöturvallisuutta ja toimitila- ja kiinteistöturvallisuutta, vaikka ne eivät varsinaisesti tietoturvallisuuden osa-alueita olekaan. (Elinkeinoelämän keskusliitto)

KUVIO 2. Yritysturvallisuusmalli. (mukaillen Elinkeinoelämän keskusliitto)

Tietoturvallisuus on laaja kokonaisuus, minkä vuoksi se jaetaan usein käsittelyn helpottamiseksi osa-alueisiin. Nämä osa-alueet helpottavat tietoturvallisuuden kokonaisuuden ymmärtämistä ja auttavat käytännön toimenpiteiden suunnittelussa. Tässä työssä käytetään Hakalan ym. (2006, 10) jaottelua, jossa tietoturva on jaettu seuraaviin osa-alueisiin:

- Hallinnollinen turvallisuus
- Fyysinen turvallisuus
- Henkilöstöturvallisuus
- Tietoaineistoturvallisuus
- Ohjelmistoturvallisuus
- Laitteistoturvallisuus
- Tietoliikenneturvallisuus

Hallinnollisella turvallisuudella tarkoitetaan niitä hallinnollisia keinoja, joilla pyritään tietoturvalliseen toimintaan. Näitä ovat esimerkiksi tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta. (VAHTI 5/2004, 27.) Hallinnolliseen turvallisuuteen kuuluu tietoturvapolitiikan määrittäminen, toiminnan linjaukset, johtaminen ja resursointi sekä ylläpito. Hallinnollinen turvallisuus käsittää kaikki tietoturvallisuuden osa-alueet ja kokoaa ne yhteen. (Miettinen 1999, 18). Organisaation toimintaa koskevien lakien, viranomaisvaatimusten ja standardien perusteella voidaan asettaa tavoitteet ja mittarit tietoturvallisuudelle. (Andreasson, Koivisto & Ylipartanen 2015, 162.)

Fyysisen turvallisuuden avulla organisaatiosta pyritään tekemään turvallinen ja häiriötön toimintaympäristö. Fyysinen turvallisuus pyrkii suojaamaan muun muassa toimitiloja, laitteita, aineistoja ja henkilöitä tuhoilta ja vahingoilta. Fyysiseen turvallisuuteen kuuluvat esimerkiksi kulun- ja tilanvalvonta sekä tulipalojen, sähköhäiriöiden sekä vesivahinkojen torjunta. (VAHTI 3/2007, 59; Laaksonen ym. 2006, 66.) Fyysistä turvallisuutta voidaan toteuttaa esimerkiksi valvontakameroiden, rikosilmoitinten, erilaisten lukitusten sekä kulkuoikeuksien ja kulunvalvonnan avulla. (Järvinen & Rousku 2017, 54.)

Miettisen (1999, 18-19) mukaan henkilöstöturvallisuus käsittää sekä henkilöihin liittyvien tietojen suojaamisen että yrityksen tietojen suojaamisen henkilöiden aiheuttamilta uhilta. Raggadin

(2010, 16) mielestä henkilöstöturvallisuutta tarvitaan ehkäisemään henkilöstön aiheuttamia tietoturvauhkia, niin tahallisia kuin tahattomiakin. Järvisen & Rouskun (2017, 55) mukaan henkilöstöturvallisuuden tarkoitus on huolehtia ihmisten toimintakyvystä ja turvallisuudesta. Henkilöstöturvallisuuteen kuuluu myös varahenkilö- sekä päivystys ja varallaolojärjestelyt niiden henkilöiden osalta, jotka ovat organisaation toiminnan kannalta kriittisiä. (Järvinen & Rousku 2017, 55.) Valtiovarainministeriön Vahti-ohjeissa (3/2007, 57) henkilöstöturvallisuus määritellään henkilöstöstä johtuvaksi riskienhallinnaksi. Osaava ja sitoutunut henkilöstö muodostaa henkilöstöturvallisuuden perustan. Uuden henkilön rekrytointi on keskeinen asia henkilöstöturvallisuudessa. Rekrytoitavan henkilön osaaminen, sopivuus ja tausta tulee selvittää ennen palkkaamista, tehtävien vaativuus ja luottamuksellisuus huomioon ottaen. Tietoturvallisuuden toteutumiseen vaikuttaa merkittävästi myös henkilöstön riittävä määrä, työtyytyväisyys ja motivaatio. (VAHTI 3/2007, 57.)

Tietoaineistoturvallisuus keskittyy tietojen säilyttämiseen, varmistamisen ja palauttamiseen sekä tuhoamiseen liittyviin asioihin. Tietoaineistoturvallisuudessa tulee ottaa huomioon niin sähköinen kuin manuaalinenkin tietoaineisto. (Hakala ym. 2006, 11.) Tietoaineistoturvallisuus käsittää muun muassa tietoaineistojen luokittelun, turvallisen käsittelyn ja säilytyksen, varmuuskopioinnin sekä tärkeiden asiakirjojen, tietovarastojen ja yksittäisten tietojen suojaamisen (Laaksonen ym. 2006, 67). Tieto tulisi luokitella sen mukaan, kuinka arvokasta se organisaatiolle on (Raggad 2010, 6). Luokittelun avulla hallitaan tietoaineistojen eheyttä ja luottamuksellisuutta sekä saatavuutta ja käytettävyyttä. Valtionhallinnon organisaatioissa salassa pidettävä tieto luokitellaan neljään suojaustasoon. PK-yrityksissä tietojen luokittelu näin tarkasti ei useinkaan ole tarkoituksenmukaista, jolloin tiedot voidaan luokitella julkisiin ja salassa pidettäviin tietoihin. Salassa pidettävistä tiedoista voidaan tarvittaessa erottaa organisaation sisäiset tiedot ja yhteistyötahoille luovutettavat tiedot. (Järvinen & Rousku 2017, 46.) Tietojen luokittelun tavoitteena on varmistaa riittävä suojaustaso, joka määräytyy tiedon merkittävyyden perusteella. Tiedon luokittelun tulisi perustua lakisääteisiin vaatimuksiin, tiedon arvoon ja kriittisyyteen sekä sen luvattoman paljastumisen tai muokkaamisen aiheuttamiin vaikutuksiin. (SFS-EN ISO 27002 2017, 23.)

Ohjelmistoturvallisuudessa keskitytään käyttöjärjestelmien, ohjelmistojen ja sovellusten ylläpitoon ja päivitykseen liittyviin turvallisuustoimenpiteisiin. Ohjelmistoturvallisuuteen kuuluu myös tunnistamis- ja suojausominaisuudet sekä valvonta- ja lokimenettelyt. Ohjelmistoturvallisuutta voidaan parantaa kiinnittämällä huomiota muun muassa käyttöjärjestelmän ja ohjelmistojen

asetuksiin sekä käyttäjien koulutukseen ja ohjeistukseen. (VAHTI 3/2007, 69.) Ohjelmien määrityksessä tulisi ottaa huomioon liiketoiminnan tarpeet sekä lain asettamat vaatimukset. Ohjelmat voivat kerätä tietoa tarpeettomasti, mikä voidaan käytännössä ehkäistä oletusasetuksia muuttamalla. (Laaksonen ym. 2006, 67.) Ohjelmistoturvallisuuden avulla pyritään varmistamaan mm. ohjelmistojen sopivuus käyttötarkoitukseen, keskinäinen yhteensopivuus sekä toiminnan virheettömyys ja luotettavuus. Ohjelmistoturvallisuutta voidaan parantaa esimerkiksi ohjelmistojen testauksella. (Hakala ym. 2006, 11.)

Laitteistoturvallisuuteen tarkoituksena on turvata laitteisto koko sen elinkaaren ajan. Laitteistoturvallisuuteen sisältyy muun muassa laitteistojen suojaus, asennus, ylläpito ja poisto sekä niihin liittyvä hallinnointi. (VAHTI 3/2007, 63.) Laitteistoturvallisuutta voidaan yrityksessä edistää ottamalla käyttöön vain sellaisia laitteita, joiden tietoturvallisuus on huomioitu asianmukaisesti jo valmistusvaiheessa. Parhaimmillaan turvallisuusasiat on huomioitu laitteistoissa jo niiden suunnittelussa, valmistuksessa ja kokoonpanossa. (Miettinen 1999, 21.) Hakala ym. (2006, 12) listaa laitteistoturvallisuuteen muun muassa tietokoneiden toiminnan testauksen, huollon järjestämisen sekä laitteiden kulumiseen ja vanhentumiseen varautumisen. Laitteiden käytöstä johtuvien vaaratekijöiden arviointi ja minimointi kuuluvat myös laitteistoturvallisuuteen. (Hakala ym. 2006, 12.)

Tietoliikenneturvallisuuden avulla pyritään turvaamaan yritykselle kriittisten tietojen liikkuminen verkossa ja ehkäisemään tietojen luvaton paljastuminen, muokkaaminen ja tuhoaminen (Raggad 2010, 19). Tietoliikenneturvallisuuden tavoitteena on yrityksen tietoliikenteen jatkuvan ja häiriöttömän toiminnan turvaaminen kaikissa tilanteissa (Miettinen 1999, 20). Tietoliikenteen turvallisuutta voidaan parantaa verkon salauksella. Suljetun verkon avulla voidaan ehkäistä tietoliikenteen paljastuminen ulkopuolisille ja tiedon muuttaminen ja tuhoaminen ulkopuolisten toimesta. Salaus tulisi toteuttaa niin, ettei se häiritse viestintäverkkojen ja viestintäpalveluiden toimintaa tai käyttöä. (Laaksonen ym. 2006, 66.)

2.2 Tietosuoja

Tietosuojan tarkoituksena on turvata henkilötietojen tarkoituksen- ja vaatimustenmukainen käyttö. Tietosuoja vaatii toteutuakseen tietoturvallisuutta. Tietoturvallisuuden avulla voidaan varmistaa, ettei henkilötietoja voida käyttää tai muokata hallitsemattomasti, eivätkä ne joudu

sellaisten tahojen haltuun, joilla ei ole niihin käyttöoikeutta. Henkilötietoja ovat nimen, osoitteen ja syntymäajan lisäksi kaikki merkinnät, jotka kuvaavat ihmisten ominaisuuksia ja toimintaa. Henkilötietoja kerätään esimerkiksi markkinointia varten, mutta niistä ovat kiinnostuneet myös verkkorikolliset. Tämän vuoksi omien ja yrityksen työntekijöiden henkilötietojen suojaaminen on tärkeää. EU-maissa henkilötietojen käsittelyn turvallisuutta pyritään yhdenmukaistamaan EU:n tietosuojauudistuksen avulla. (Järvinen & Rousku 2027, 18-19; Järvinen 2012, 12.)

Perinteinen tilinpäätös on jokaiselle yrittäjälle tuttu, mutta tietotilinpäätös on monelle yhä tuntematon. EU:n tietosuoja-asetuksen osoitusvelvollisuuden myötä tietotilinpäätöksen merkitys on kasvamassa. Tietotilinpäätös on johdon sisäisestä tarkastelun seurauksena syntyvä raportti, jossa käsitellään muun muassa tietovarantoja, tietojohtamista, tietojenkäsittelyä sekä tietoturvallisuutta. Tietotilinpäätöksessä voidaan kuvata esimerkiksi yrityksen hallussa olevat tietovarannot, yrityksen toimintaan liittyvät tietovirrat ja niiden toimivuus yhdessä tietojenkäsittelyn kanssa. Lisäksi tietotilinpäätöksessä voidaan kuvata miten tietosuoja ja tietoturva toteutuvat yrityksessä ja miten niihin liittyvä riskienhallinta on toteutettu. Tietotilinpäätös toimii yrityksessä suunnittelun, toiminnan ohjauksen, raportoinnin sekä johtamisen tukena ja sen avulla voidaan varmistaa, että sovellettavaa lainsäädäntöä noudatetaan. Dokumentin avulla voidaan tarkastella tietojenkäsittelyn nykytilaa yrityksessä. Lisäksi tietotilinpäätös auttaa EU:n tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa. Suoraa velvoitetta tietotilinpäätöksen tekemisestä tietosuoja-asetuksesta ei löydy, mutta sen katsotaan olevan ”paras käytäntö” osoitusvelvollisuuden toteuttamiseen. (Tietosuojavaltuutetun toimisto 2012; Haukkovaara 2017.)

3 LAIT, STANDARDIT JA SOPIMUKSET

Lainsäädäntö asettaa yrityksille sekä suoria että epäsuoria velvoitteita tietoturvallisuuteen liittyen. Velvoitteet ovat useimmiten yleisluontoisia, jolloin käytännön toteutus ja riittävän tietoturvatason määrittäminen on yrityksen vastuulla. Yrityksen kannalta on olennaista selvittää toimintaa koskevat yksittäiset säädökset, jotka asettavat vaatimuksia tietoturvan suunnittelulle, ylläpidolle ja kehittämiselle. Tietoturvavelvoitteita tai –oikeuksia ei ole Suomessa säännelty erillisen tietoturvaa koskevan lain avulla, vaan tietoturvaa koskevia säädöksiä on käsitelty useissa eri laeissa. Keskeisimpiä tietoturvallisuutta koskevia lakeja ovat muun muassa henkilötietolaki, sähköisen viestinnän tietosuojalaki sekä julkisuuslaki. Tietoturvan käytännönläheisyyden ja tekniikan nopean kehityksen vuoksi yritykset toivovat viranomaisilta erillisen lainsäädännön sijaan ohjeita tietoturvallisuutta edistävien ja ylläpitävien toimintojen toteuttamisesta. Toisaalta tietoturvallisuutta koskevien velvoitteiden hajaantuminen eri lakien sisältöihin vaikeuttaa tietoturvatyön toteuttamista käytännössä. (Laaksonen ym. 2006, 18-23; Rousku 2014, 126.)

Organisaatiota voivat lakien ja asetusten lisäksi velvoittaa erilaiset turvallisuussopimukset muiden organisaatioiden kanssa. Esimerkiksi toimittajien, alihankkijoiden tai muun yhteistyöorganisaation kanssa solmittu sopimus voi edellyttää, että yrityksen omien tietojen lisäksi huolehditaan tietoturvan toteutumisesta myös yhteistyöorganisaatioiden luottamuksellisten tietojen osalta. Sopimuksen laiminlyönnistä voi seurata jopa yhteistyön loppuminen, mistä aiheutuu organisaatiolle taloudellisen menetyksen lisäksi mainevahinkoja. (Rousku 2014, 126)

3.1 EU:n tietosuojauudistus

EU:n laajuinen tietosuojauudistus on säädöspaketti, joka sisältää GDPR-tietosuoja-asetuksen (General Data Protection Regulation) sekä direktiivin lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta. Uudistus astui voimaan huhtikuussa 2016 ja henkilötietojen käsittelyn tulee olla asetuksen mukaista kahden vuoden siirtymäajan jälkeen, toukokuussa 2018. Uudistus päivittää ja nykyaikaistaa vuonna 1995 hyväksytyn tietosuojadirektiivin säännöt. Yhtenäisen ja ajantasaisen lainsäädännön avulla voidaan muun muassa mahdollistaa digitaalitalouden kehitys, tehostaa rikollisuuden ja terrorismin torjuntaa sekä taata henkilötietojen suoja perusoikeutena. (Eurooppa-neuvosto)

Tietosuojauudistuksella tavoitellaan yhdenmukaista lainsäädäntöä kaikissa EU:n jäsenmaissa sekä niissä valtioissa, joissa käsitellään EU:n kansalaisen henkilötietoja. Asetuksella pyritään edistämään liiketoimintamahdollisuuksia lisäämällä kuluttajien luottamusta digitaalisiin palveluihin. Lisäksi sen avulla pyritään vahvistamaan yksilön vapauksia ja oikeuksia, takaamaan riittävän korkea tietosuojan taso, vahvistamaan sisämarkkinoita sekä parantamaan pk-yritysten toimintaedellytyksiä. (Enroth & Neuvonen, 2017.)

Yrityksen kannalta uudistus lisää sääntelyä sekä hallinnollisia velvoitteita. Erityisesti uudistus koskee henkilötietoja laajamittaisesti käsitteleviä yrityksiä, mutta se lisää velvoitteita myös kaikille henkilötietoja käsitteleville yrityksille. Yrityksissä henkilötietoja käsitellään usein erilaisten asiakasrekisterien ja sähköisen henkilöstön hallinnan muodossa. (Enroth & Neuvonen, 2017.)

Tietosuoja-asetukseen valmistautuminen kannattaa yrityksessä aloittaa henkilötietojen käsittelyn nykytilan kartoituksella. Nykytilan kuvaamiseen voi käyttää esimerkiksi tietotilinpäätöstä. Kun tiedetään henkilötietojen käsittelyn nykytila, voidaan ryhtyä selvittämään, mitä muutoksia ja toimenpiteitä tietosuoja-asetus kyseisen yrityksen kohdalla vaatii. Monet rekisterinpitäjiä koskevat vaatimukset vastaavat henkilötietolain vaatimuksia, joten jos tietosuoja on yrityksessä hoidettu aiemmin huolella, asetuksen vaatimukset on helpompi toteuttaa. (Oikeusministeriö 2017.)

Asetuksen keskeisimmät, rekisterinpitäjiä koskevat vaatimukset käsittelevät muun muassa tietosuojaperiaatteita, riskiperusteista lähestymistapaa, vaikutustenarviointia sekä rekisteröityjen oikeuksia. Asetuksen tietosuojaperiaatteet ovat osittain samankaltaisia kuin henkilötietolain periaatteet. Nämä periaatteet tulisi uuden asetuksen mukaan olla sisäänrakennettuja eli niiden tulisi olla osa kaikkia niitä toimintoja, joissa henkilötietoja käsitellään. Henkilötietolaista poiketen uusi asetus sisältää osoitusvelvollisuuden. Organisaation on siis pystyttävä osoittamaan, että tietosuojaperiaatteita noudatetaan. Käytännössä tietosuojaperiaatteiden noudattaminen voidaan ilmaista dokumentoimalla tietojen käsittelyyn liittyvät prosessit sekä tietosuojaperiaatteiden käytännön toteuttaminen. Asetukseen sisältyy myös riskiperusteinen lähestymistapa, joka tarkoittaa velvoitteiden ja suojatoimien suhteuttamista henkilötietojen käsittelystä aiheutuvaan riskiin. Esimerkiksi pelkän nimen ja sähköpostiosoitteen suojaamiseen ei ole tarpeen käyttää yhtä vahvoja suojaustoimia kuin arkaluontoisempien tietojen, esimerkiksi terveystieto-

jen suojaamiseen. Uusi tietosuoja-asetus lisää huomattavasti rekisteröidyn oikeuksia, ja asetuksen mukaan yksi rekisterinpitäjän velvollisuuksista on rekisteröidyn oikeuksien toteuttaminen. (Oikeusministeriö 2017.)

3.2 Standardit, suositukset ja toimintamallit

Tietoturvallisuuden kehittämisen ja hallinnan avuksi on kehitetty useita erilaisia standardeja ja toimintamalleja. Suomessa tunnetuimpia ohjeistuksia ovat ISO 27000 –standardisarja, kansallinen turvallisuusauditointikriteeristö (KATAKRI) sekä valtionhallinnon tietoturvallisuuden johtoryhmän kehittämä VAHTI-ohjeistus.

ISO 27000 on standardisarja, joka on kehitetty tietoturvallisuuden hallintajärjestelmän tueksi. Se sisältää tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin liittyviä suosituksia, joiden avulla voidaan suojata muun muassa taloudellista informaatiota ja työntekijöiden henkilötietoja. ISO 27000 –sarjaan sisältyy standardeja esimerkiksi sanastoon, vaatimuksiin, menettelyohjeisiin, toteuttamisohjeisiin, mittaamiseen sekä tietoturvariskien hallintaan liittyen. Noudattamalla tietoturvallisuuden hallintajärjestelmästandardeja, yrityksessä voidaan taata tieto-omaisuuden hallinnan perusedellytysten toteutuminen sekä niiden jatkuva kehittäminen. (SFS)

Katakri on tietoturvallisuuden auditointityökalu, joka pohjautuu lainsäädännön ja tietoturvallisuusvelvoitteiden asettamiin vaatimuksiin. Katakri jakautuu kolmeen osa-alueeseen; turvallisuusjohtamiseen, fyysiseen turvallisuuteen ja tekniseen tietoturvallisuuteen. Katakri on tarkoitettu pääasiassa yrityksen turvallisuusjärjestelyjen ja viranomaisten tietojärjestelmien turvallisuuden arviointiin, mutta sitä voidaan käyttää apuna myös yritysten tietoturvallisuuden kehittämisessä. Katakrin sisältäminen turvallisuusjärjestelyjen avulla pyritään saavuttamaan riittävä turvallisuustaso uhkiin suhteutettuna. (Katakri 2015, 3.)

VAHTI-ohjeet ovat valtionhallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) kehittämiä tieto- ja kyberturvallisuuteen liittyviä ohjeita parhaista käytännöistä. Ohjeet on tarkoitettu ensisijaisesti valtionhallinnon organisaatioille, mutta ohjeita voi käyttää sovellettuna myös PK-yrityksissä. VAHTI-ohjeet käsittelevät kaikkia tietoturvallisuuden osa-alueita, ja niistä löytyy myös käytännön neuvoja tietoturvallisten toimintatapojen toteuttamiseen. (Valtiovarainministeriö)

4 JOHDON TEHTÄVÄT JA TYÖKALUT

Tietoturvallisuuden kehittäminen yrityksessä edellyttää johdon sitoutumista. Päätös tietoturvan kehittämisestä on ensimmäinen askel kohti parempaa tietoturvaa. Porvarin (2012, 97) mukaan PK-yrityksissä ei usein ole käytettävissä merkittäviä resursseja tietoturvallisuuden kehittämiseen, minkä vuoksi on välttämätöntä kohdistaa ne oikein. Resurssien tehokas hyödyntäminen edellyttää tärkeiden toimintojen, ja niitä uhkaavien tekijöiden tunnistamista. Riskienhallinnan avulla voidaan löytää yritystoiminnan kannalta merkittävimmät riskit, jolloin kehittämistoimenpiteiden järkevä kohdistaminen on helpompaa. Johdon sitoutuminen on tietoturvan kehittämisessä ensiarvoisen tärkeää. Tietoturvapolitiikan avulla johto voi ilmaista sitoutumisensa tietoturvallisuuteen, ja se toimii myös pohjana henkilöstön ohjeistukselle. (VAHTI 3/2007, 15; VAHTI 2/2011, 21.)

Tähän lukuun on pyritty kokoamaan useiden eri lähteiden pohjalta tärkeimpiä asioita tietoturvan kehittämisessä. Tietoturvan hallinnan avuksi on kehitetty useita erilaisia oppaita, kuten Vahtiohjeiden ”Johdon tietoturvaopas” (2/2011). PK-yrityksen näkökulman huomioimiseksi oli kuitenkin tarpeen tutkia myös erityisesti PK-yrityksille tarkoitettuja ohjeita. Luvussa käsitellään myös tietoturvallisuuden yhteydessä käytettäviä johdon työkaluja, PDCA-mallia (Plan-Do-Check-Act) sekä vuosikelloa. Näiden työkalujen avulla tietoturvallisuuden jatkuvuutta voidaan edistää.

4.1 Suojattavan pääoman tunnistaminen

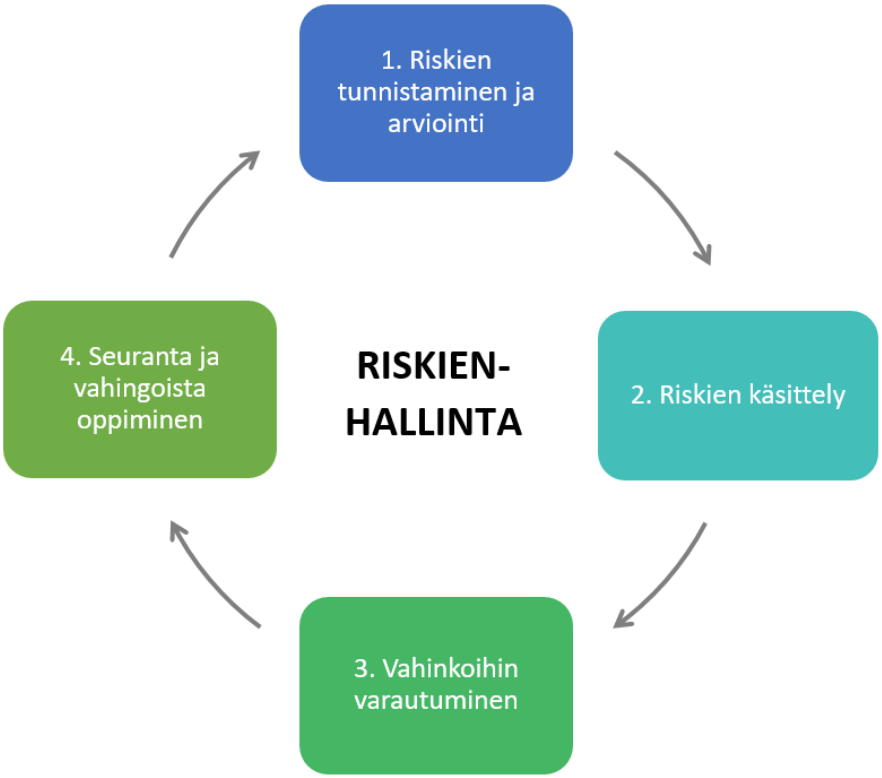
Suojaustoimenpiteiden toteuttamisen kannalta on olennaista tunnistaa yritykselle kriittiset prosessit ja resurssit. Kaikkien kohteiden suojaaminen yhtä vahvasti ei ole taloudellisesti järkevää ja erityisesti PK-yrityksissä niukkojen resurssien kohdistaminen oikein on välttämätöntä. Kriittisiä prosesseja voi toimialasta ja yrityksestä riippuen olla esimerkiksi tuotanto- ja varastotilat, valmistusprosessi, keskeiset alihankkijat, tuotekehitystieto ja tietojärjestelmä, kuten sähköposti tai toiminnanohjausjärjestelmä. Kriittisille prosesseille on ominaista, että niiden toimimattomuus aiheuttaa yritykselle merkittäviä kustannuksia tai mainevahinkoa. Suojattavan pääoman tunnistamisen ja priorisoinnin jälkeen esimerkiksi riskien- ja jatkuvuudenhallinnan kohdistaminen on helpompaa. (Cybricon Oy & Tietoturvaamo Oy 2015, 4.)

4.2 Riskienhallinta

Riskienhallinta liittyy läheisesti tietoturvallisuuteen. Riskienhallinnan avulla voidaan selvittää yritystoiminnan kannalta olennaiset uhkatekijät. Arvioimalla uhkien seurausvaikutuksia, voidaan hahmottaa niiden mahdollinen vaikutus päivittäiseen yritystoimintaan. Riskien hallinnan tavoitteena on ymmärtää yritystoimintaan kohdistuvat riskitekijät sekä määrittää hyväksyttävä riskitaso, jolloin riskejä voidaan pyrkiä alentamaan hyväksyttävälle tasolle. (Miettinen 1999, 50.)

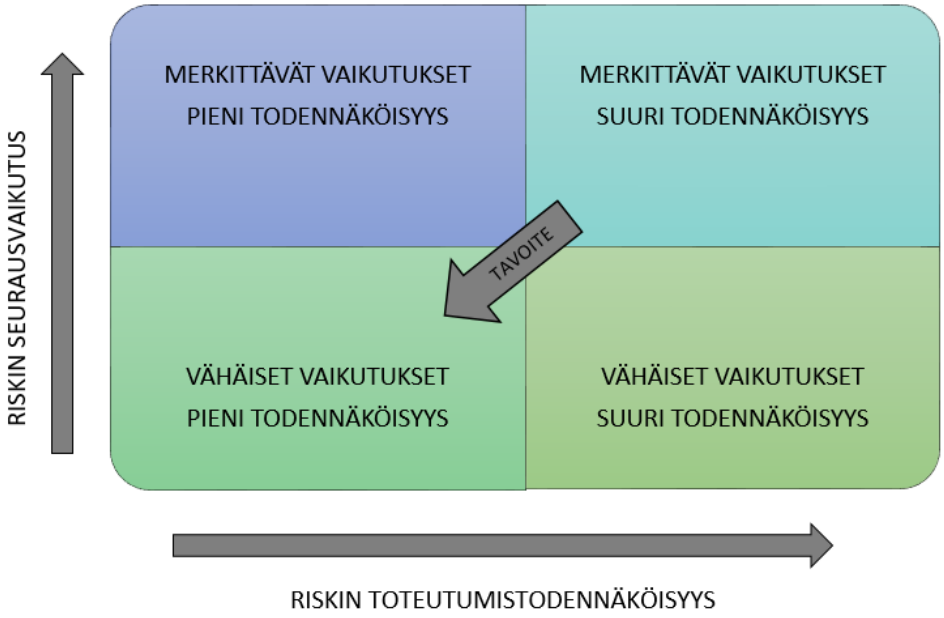
Riskienhallinnan avulla voidaan vähentää häiriöitä ja toimintakatkoja kriittisissä prosesseissa, minkä seurauksena riskienhallinnasta seuraa sekä taloudellista että maineellista hyötyä. Riskienhallinta tulisi saada osaksi yrityksen normaalia toimintaa. Kertaluontoinen tai ulkopuolisen suorittama riskienhallinta ei palvele yritystä optimaalisesti. Riskienhallintatoimet tulisi kohdistaa ensisijaisesti kriittisiksi tunnistettuihin prosesseihin. (Cybricon Oy & Tietoturvaamo Oy 2015, 5.)

Suomen Riskienhallintayhdistyksen ylläpitämällä, PK-yrityksille suunnatulla riskienhallintasivustolla kuvataan riskienhallintaprosessin päävaiheet (KUVIO 3). Riskienhallintaprosessista on löydettävissä yhteneväisyyksiä PDCA-malliin. Riskienhallinta aloitetaan riskien tunnistamisella ja arvioinnilla. Käytännössä suojattavaan kohteeseen liittyviä mahdollisia riskejä mietitään ja ne listataan. Riskit tulisi järjestää niiden suuruuden mukaan, jotta käytettävissä olevat resurssit voidaan kohdistaa merkittävimpiin riskeihin. Riskien suuruutta voidaan arvioida esimerkiksi kertomalla riskin todennäköisyys sen aiheutumisesta seuraavilla vahingoilla. Toisessa vaiheessa mietitään, miten riskin toteutumisesta aiheutuvat vahingot voidaan välttää tai miten niitä voidaan pienentää. Monilla pienilläkin käytännön toimenpiteillä voidaan pienentää riskejä merkittävästi. Tietoturvariskeihin liittyviä suojaustoimenpiteitä ovat esimerkiksi tekniset ratkaisut sekä työntekijöiden toiminta. Kaikkia riskejä ei voida poistaa, vaan ne täytyy hyväksyä. Tämän vuoksi on tarpeellista varautua vahinkoihin. Näin voidaan taata kriittisten prosessien toiminnan jatkuminen myös häiriötilanteissa. Neljännessä vaiheessa riskienhallintakeinojen toimivuutta seurataan ja sitä kehitetään tarvittaessa. Riskienhallintatoimintaa organisoidaan ja kehitetään jatkuvasti prosessin aikana. Riskienhallintatyöstä saadaan tehokkaampaa, kun koko henkilöstö osallistutetaan siihen. Työntekijä voi tunnistaa sellaisiakin riskejä, joista johdolla ei ole käsitystä. (Suomen Riskienhallintayhdistys; Cybricon Oy & Tietoturvaamo Oy 2015, 5.)



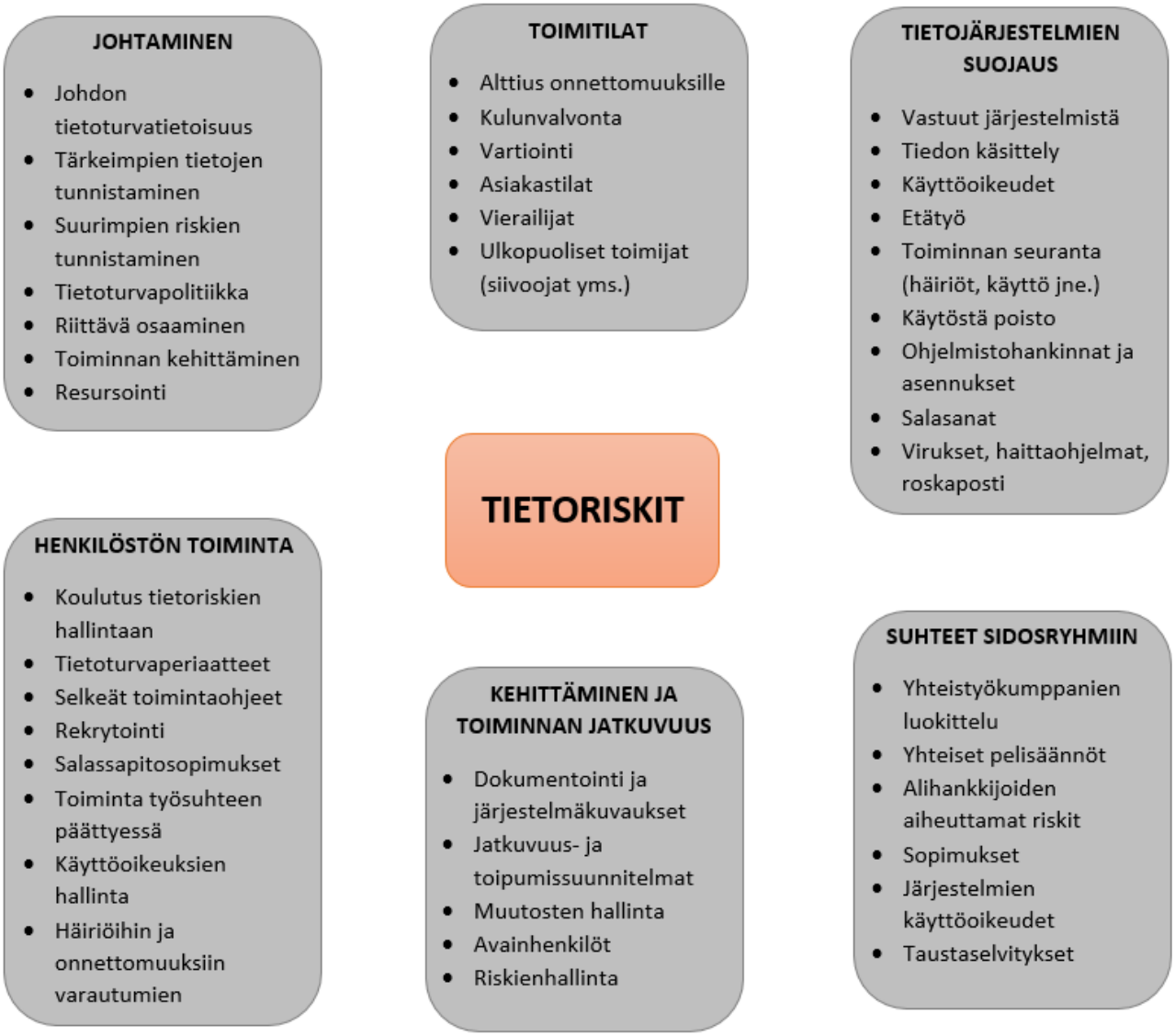
KUVIO 3. Riskienhallintaprosessi. (mukaillen Suomen Riskienhallintayhdistys)

Tietoturvallisuusriskien merkittävyyttä voi tarkastella esimerkiksi oheisen kuvion avulla (KUVIO 4). Pystyakseli kuvaa seurausvaikutuksia, joita tietoturvallisuusriski toteutuessaan aiheuttaa. Vaaka-akseli kuvaa todennäköisyyttä sille, että kyseinen riski toteutuu. Malli on jaettu neljään osaan riskien suuruuden määrittämiseksi. Vasempaan yläkulmaan sijoitetaan riskit, joilla on toteutuessaan merkittäviä seurausvaikutuksia mutta joiden toteutuminen on epätodennäköistä. Näiden riskien seurannan tulisi olla jatkuvaa, jotta voidaan varmistua siitä, että toteutumistodennäköisyys pysyy pienenä. Oikean alakulman riskit eivät aiheuta merkittäviä rahallisia tai maineellisia vahinkoja, mutta niiden toteutuminen on todennäköistä. Näistä riskeistä voi kuitenkin kertyä merkittäviä vahinkoja, mikäli ne toistuvat useasti. Riskienhallinnan toimenpiteet tulisi kohdistaa ensisijaisesti oikeaan yläkulmaan sijoitettuihin riskeihin, joilla on vakavat seuraukset ja joiden toteutuminen on todennäköistä. Riskienhallinnan tavoitteena on, että kaikki riskit lähestyvät tilannetta, jossa riskin seuraukset ovat vähäisiä ja toteutumistodennäköisyys on pieni. (Miettinen 1999, 58-59.)



KUVIO 4. Riskien arviointi. (mukaillen Miettinen 1999, 58)

Tietoturvariskien hallinnassa on olennaista tunnistaa keskeiset tietoon liittyvät riskit. PK-yrityksessä tietoriskien kartoittamiseen voidaan käyttää esimerkiksi tietoriskikarttaa (KUVIO 5), jossa on lueteltu olennaisia huomioon otettavia asioita muun muassa johtamiseen, toimitiloihin, tietojärjestelmien suojaukseen ja henkilöstön toimintaan liittyen. Tietoriskikartta on eräänlainen muistilista niistä asioista, joiden huomioiminen on tietoriskien hallinnan kannalta olennaista. Kaikki tietoriskikartassa olevat asiat eivät välttämättä kosketa kaikkia yrityksiä, jolloin ne eivät vaadi toimenpiteitä. Tietoriskikartan avulla voidaan arvioida, mitkä asiat edellyttävät yritykseltä toimenpiteitä ja mitkä asiat ovat jo kunnossa. (Vuori ym. 2004.)



KUVIO 5. PK-yrityksen tietoriskikartta. (mukaillen Suomen Riskienhallintayhdistys)

4.3 Tietoturvapolitiikan laadinta

Tietoturvapolitiikka toimii pohjana tietoturvan toteuttamiselle, ja siitä käy ilmi yrityksen johdon linjaukset, tavoitteet ja vastuut yleisellä tasolla. Politiikkaa tulee päivittää tarvittaessa. Tietoturvapolitiikan avulla johto voi osoittaa henkilöstölle, että on halukas kehittämään tietoturvallisuutta ja tukemaan siinä myös koko henkilöstöä. Tietoturvapolitiikka toimii pohjana tietoturvaohjeiden laadinnalle. Tietoturvapolitiikkaa tulee katselmoida säännöllisesti, ja sitä tulee päivittää tarvittaessa. (Laaksonen ym. 2006, 146-147.)

Tietoturvapolitiikka tulisi aina määrittää yrityskohtaisesti, ettei siitä muodostu liian yleisluonteinen. Tietoturvapolitiikan laadinnassa voi kuitenkin käyttää kehyksenä valmiita malleja, mutta sisältö tulee tarkentaa yrityksen johdon linjausten mukaiseksi. Valtiovarainministeriön VAHTI-ohjeen mukaan yrityksen tietoturvapolitiikka voi sisältää esimerkiksi seuraavia asioita: tietoturvapolitiikan tavoite, toimintaa ohjaavat lait ja standardit, tietoriskien hallinta, tietoturvallisuuden merkitys organisaatiolle ja tietoturvavastuut. Tietoturvapolitiikan sisältö vaihtelee organisaation koon ja toimintaympäristön mukaan. (Hakala ym. 2006, 8; VAHTI 3/2007, 85-86).

4.4 Henkilöstön kouluttaminen ja ohjeistus

Yrityksen johto on vastuussa siitä, että työntekijät ymmärtävät tietoturvallisten toimintatapojen merkityksen yritykselle ja sen maineelle. Työntekijöiden tulisi olla tietoisia yrityksen tietoturvapolitiikasta, tietoturvallisuuden parantamisen vaikutuksista sekä siitä, miten työntekijä voi omalta osaltaan vaikuttaa tietoturvallisen työympäristön luomiseen. Yrityksen johto voi omalla esimerkillään viestiä henkilöstölle, että yrityksessä sitoudutaan noudattamaan tietoturvallisia toimintatapoja. (SFS-EN ISO 27001 2017, 16; Laaksonen ym. 2006, 258.)

Yle Savon toteuttaman tietoturvakyselyn mukaan 52 prosenttia Pohjoissavolaisista kyselyyn vastanneista yrityksistä ja työnantajista pitivät entisiä ja nykyisiä työntekijöitä suurimpana tietoturvauhkana. Vasta toiseksi suurimpana uhkana pidettiin ulkopuolisia tekijöitä kuten hakkereita, rikollisia, kansainvälisiä toimijoita sekä yleistä ilkivaltaa. Tietoturvaa oli yrityksissä parannettu henkilöstön seurantaa ja ohjeistusta lisäämällä. (Lötjönen, 2013.) Centria-ammattikorkeakoulun vuonna 2016 tekemän selvityksen mukaan alueen yrityksissä olisi kehitettävää henkilöstön kouluttamisessa ja ohjeistamisessa.

Laaksosen ym. (2006, 249) mukaan työntekijän tietoturvakäyttäytymiseen vaikuttavat muun muassa toimintaohjeet ja koulutus, muiden työntekijöiden toiminta, henkilökohtainen asenne sekä tietoturvallisuutta edistävien toimien vaatima työmäärä. Tietoturvapolitiikan pohjalta voidaan laatia työntekijöille tietoturvaohjeet, joiden tulisi ohjata työntekijän käyttäytymistä. Tietoturvakoulutuksella voidaan lisätä työntekijöiden tietoturvatietoisuutta, mikä edesauttaa ohjei-

den noudattamista. Tietoturvaohjeiden laadinnassa tulisi kiinnittää huomiota ohjeiden selkeyteen sekä siihen, miten ohjeista voidaan tehdä mahdollisimman helposti toteutettavia. (Laaksonen ym. 2006, 249-250.)

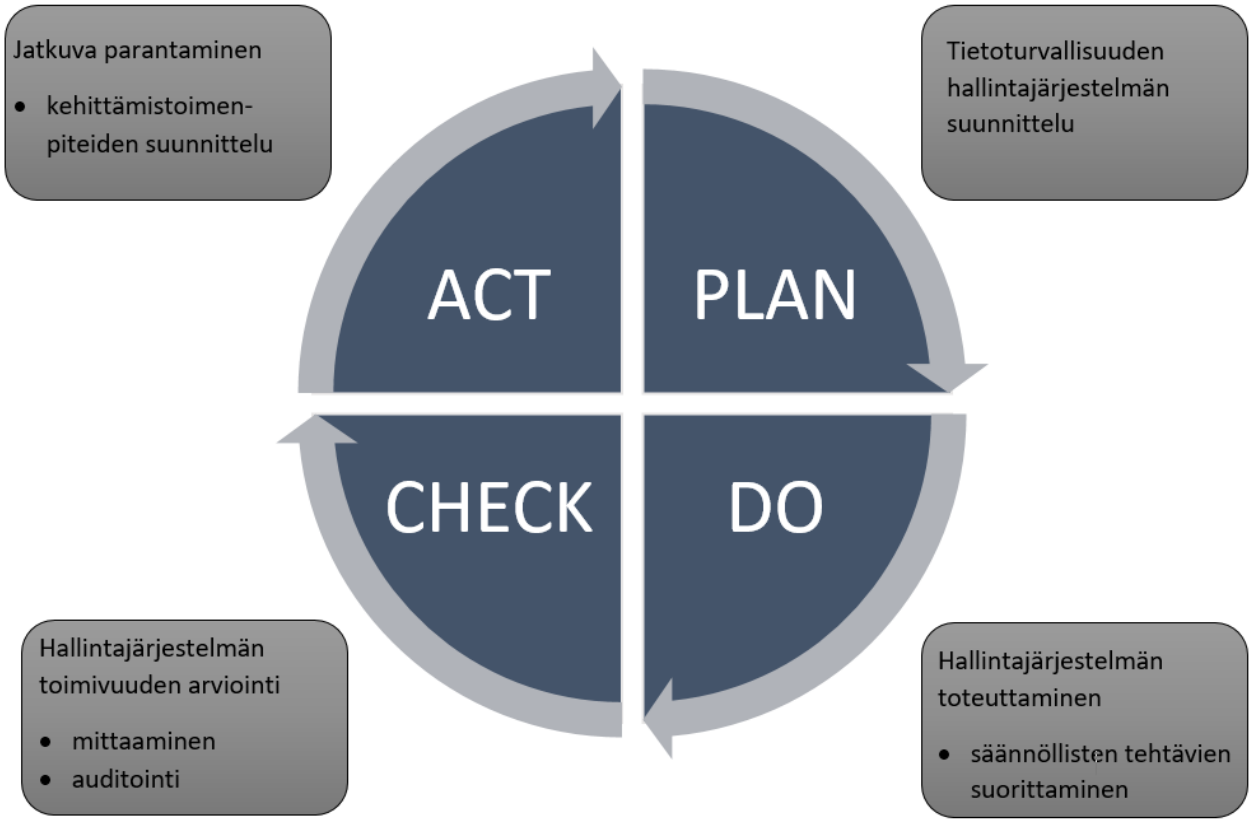
4.5 Jatkuvuuden hallinta

Jatkuvuuden hallinnan tavoitteena on turvata tärkeiden prosessien toiminta häiriötilanteissa. Erilaiset tekniset viat, luonnonilmiöt ja ihmisten aiheuttamat tahalliset ja tahattomat toimet voivat aiheuttaa häiriöitä liiketoiminnalle. Jatkuvuuden hallinnan avulla pyritään vähentämään näiden häiriöiden vaikutusta, nopeuttamaan häiriöstä palautumista sekä pitämään häiriöstä aiheutuvat vahingot mahdollisimman pieninä. Jatkuvuuden hallinnan toimenpiteet tulisi kohdistaa ensisijaisesti kriittisiin prosesseihin. (Cybricon Oy & Tietoturvaamo Oy 2015, 6; Rousku 2014, 60-61.)

Häiriötilanteisiin varautumisessa voidaan käyttää apuna jatkuvuus- ja toipumissuunnitelmia. Nämä suunnitelmat sisältävät käytännön toimintaohjeita häiriötilanteiden varalle, minkä vuoksi niiden dokumentoiminen on tarpeellista. Jatkuvuussuunnitelmassa kuvataan, miten häiriötilanteisiin varaudutaan ennakkoon ja miten liiketoimintaa jatketaan esimerkiksi tietojärjestelmiin kohdistuvan häiriön aikana. Toipumissuunnitelmassa kuvataan toimenpiteitä kriittisen järjestelmän palauttamisesta toimintakuntoon. (Cybricon Oy & Tietoturvaamo Oy 2015, 7.)

4.6 PDCA-malli

Tietoturvallisuuden hallinta tulisi ymmärtää jatkuvana prosessina. Hyvä tietoturvallisuuden hallinta edellyttää jatkuvaa parantamista, jossa voidaan käyttää apuna PDCA-mallia (KUVIO 6) (Plan-Do-Check-Act), jonka suomenkielinen vastine on Suunnittele-Toteuta-Arvioi-Toimi. Suunnitteluvaiheessa rakennetaan tietoturvallisuuden hallintajärjestelmä, johon kuuluu muun muassa suojattavien kohteiden tunnistaminen, tietoturvatason määrittäminen sekä tietoturvapolitiikan luominen ja riskien arviointi. Toisessa vaiheessa suunnitellut toimenpiteet toteutetaan käytännössä. Kolmannessa vaiheessa toteutettujen toimenpiteiden onnistumista arvioidaan ja seurataan. Neljäs vaihe sisältää saavutetun tietoturvatason ylläpidon sekä kehittämiskohteiden tunnistamisen jatkuvan parantamisen takaamiseksi. (Hakala ym. 2006, 106-111; Mehan 2014, 192-193; VAHTI 2/2014,15.)



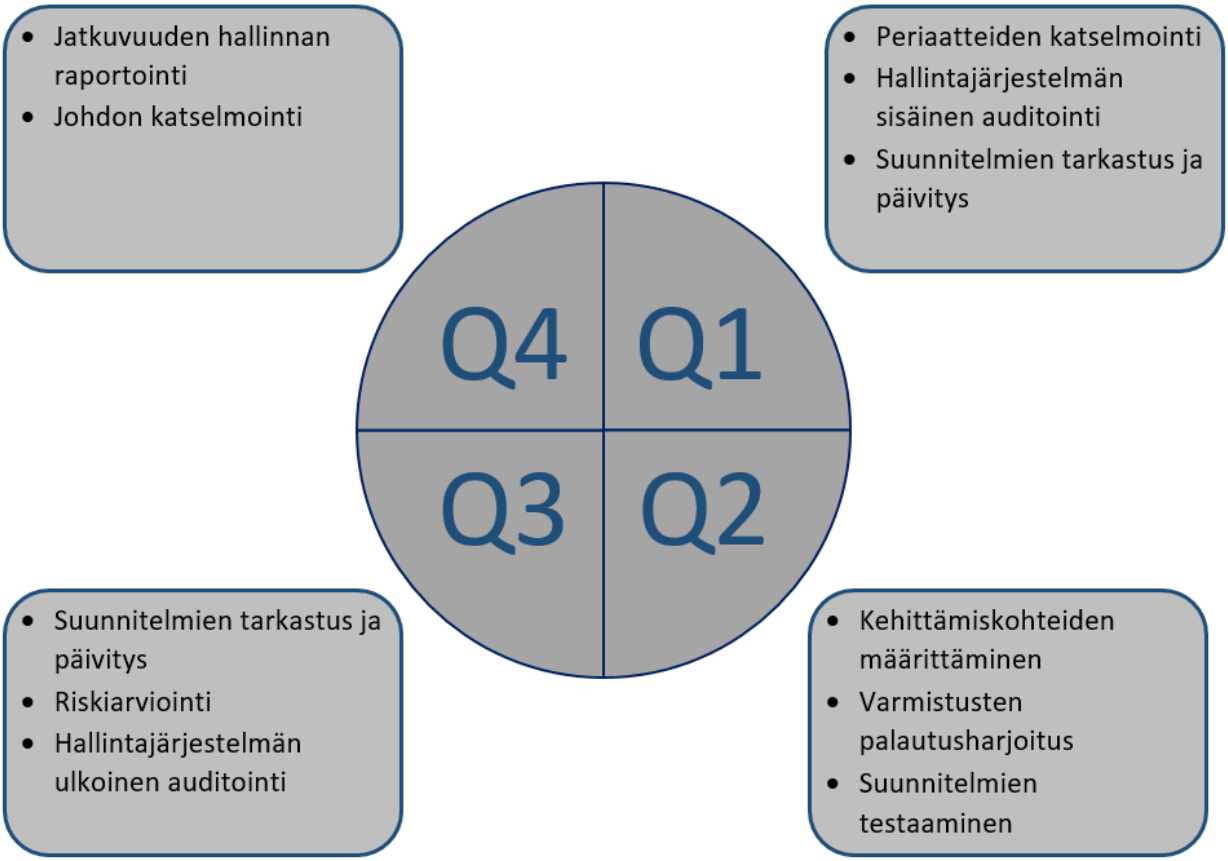
KUVIO 6. Tietoturvallisuuden PDCA-malli. (mukaillen VAHTI 2/2015, 15.)

PDCA-mallia (KUVIO 6) voidaan soveltaa myös tietoturvariskien hallintaprosessissa. Suunnitteluvaiheeseen kuuluu muun muassa riskien arviointi ja suunnitelma niiden käsittelystä. Toteutusvaiheessa aiemmin laadittu riskienkäsittelysuunnitelma otetaan käyttöön toteuttamalla toimenpiteet, joita vaaditaan riskin saamiseksi hyväksyttävälle tasolle. Tietoturvariskit muuttuvat jatkuvasti, minkä vuoksi niiden seuranta ja arviointi on tärkeää. Arviointivaiheessa tarkastellaan sitä, onko riskien käsittelyä ja arviointia tarpeen muuttaa. Neljäs vaihe sisältää riskien hallintaprosessin ylläpidon ja parantamisen. (SFS-EN ISO 27005 2013, 24.)

4.7 Vuosikello

Vuosikello on yrityksissä yleisesti käytetty johdon työkalu, jota voidaan soveltaa myös tietoturvallisuuden hallinnassa. Vuosikellossa esitetään vuoden aikana tehtävät toimenpiteet, ja se voidaan toteuttaa joko sanallisesti tai kuvana. Vuosikello helpottaa säännöllisesti toistuvien

tehtävien ajoittamista ja muistamista. Vuosikelloa tulee ylläpitää ja päivittää säännöllisesti. Tietoturvallisuuteen liittyvät toimenpiteet voidaan liittää osaksi yrityksen yleistä vuosikelloa tai vaihtoehtoisesti tietoturvallisuudelle voidaan luoda oma vuosikello. VAHTI –julkaisussa 2/2016 on esitetty esimerkki jatkuvuudenhallinnan vuosikellosta (KUVIO 7), joka on tarkoitettu valtionhallinnon organisaatioille. PK-yrityksissä ei usein ole tarpeen tehdä erillisiä vuosikelloja eri toiminnoille, vaan tietosuojaan ja tietoturvaan liittyviä toimenpiteitä voidaan merkitä jo käytössä olevaan, esimerkiksi laadunhallinnan vuosikelloon. Tietoturvallisuuden vuosikelloon voidaan sisällyttää esimerkiksi riskienhallintaan, jatkuvuudenhallintaan, poikkeamien seurantaan ja henkilöstön koulutukseen liittyviä toimenpiteitä. (Matkailualan tutkimus- ja koulutusinstituutti 2010; VAHTI 2/2016, 26.)



KUVIO 7. Jatkuvuudenhallinnan vuosikello. (mukaillen VAHTI 2/2016, 67.)

4.8 Tietoturvallisuus ja laatu

Monissa yrityksissä on käytössä sertifioitu laatujärjestelmä, jonka avulla pyritään vähentämään esimerkiksi toimintatavoista ja henkilöistä johtuvia virheitä. Laatujärjestelmille on ominaista,

että laatu ja sen valvonta ovat osa jokapäiväistä toimintaa ja kaikki henkilöt osallistuvat laatutyöhön. Tietoturvallisuuden tulisi olla samalla tavalla osa yrityksen arkea. Tietoturvallisuuden johtaminen on monilla tavoin samankaltaista laatujohtamisen kanssa. Sekä laadunhallintajärjestelmissä että tietoturvallisuuden hallintajärjestelmissä keskeisiä asioita ovat johtaminen, resurssienhallinta, prosessienhallinta sekä jatkuva kehittäminen. Laadunhallintajärjestelmät ja tietoturvallisuuden hallintajärjestelmät sisältävät monia yhtäläisyyksiä, mutta siitä huolimatta niiden yhdistämisen toimivuudesta ei ole juuri lainkaan käytännön kokemuksia. Yhteisen hallintajärjestelmän toteuttaminen laadulle ja tietoturvalle vaatii yrityskohtaista tarkastelua. Yhteisen hallintajärjestelmän avulla on mahdollista säästää resursseja esimerkiksi päällekkäisien tehtävien poistamisella. (Laaksonen ym. 2006, 112-114.)

Tietoturvallisuus käsitetään usein osaksi laatua, ja joissain tapauksissa asiakas tai yhteistyökumppani voi asettaa vaatimuksia laadun lisäksi myös tietoturvallisuudelle. Laatuasiat on monissa yrityksissä viety pitkälle, eikä tietoturvaa ole syytä erottaa laadukkaan tuotteen tai palvelun muodostamisessa. Optimaalisessa tilanteessa sekä tietoturvallisuus että laatu ovat keskeisiä liiketoimintaa tukevia tekijöitä, joiden edistämiseen kiinnitetään huomiota päivittäisessä toiminnassa. Molemmissa tavoitteena on tyypillisesti yrityksen toimintaprosessin kehittäminen, huomioimalla samalla asiakkaan tarpeet ja vaatimukset. (Miettinen 1999, 63-64.)

Tietoturvallisuuden taso tulisi määrittää siten, että se täyttää yrityksen ja asiakkaan asettamat vaatimukset. Ylilaadusta puhutaan silloin, kun tietoturvallisuuden laatutaso on huomattavasti korkeampi kuin sille asetetut vaatimukset. Kuten tiedon saatavuuden käsittelyn yhteydessä on mainittu, tietoturvallisuuden liian korkea taso voi vaikeuttaa työtehtävien hoitamista, jos esimerkiksi suojaukset on toteutettu liian monimutkaisesti tarvittavaan suojaustasoon nähden. (Miettinen 1999, 65.)

5 HENKILÖSTÖN ROOLI TIETOTURVALLISUUDESSA

Lähes jokaisen yrityksen toiminta on riippuvaista tietojen käsittelystä ja siirrosta, minkä vuoksi on tärkeää toimia niiden periaatteiden mukaisesti, joilla pyritään turvaamaan toiminnan jatkuvuus. Jokainen työntekijä voi omalla toiminnallaan vaikuttaa tietoturvallisuuden toteutumiseen ja koko henkilöstöllä on vastuu tietoturvallisista toimintatavoista. Esimerkiksi kiire ja työntekijän huolimattomuus voivat aiheuttaa merkittäviä riskejä tietoturvallisuudelle. Yrityksen tietoturvakäytänteiden omaksuminen ja noudattaminen on ensiarvoisen tärkeää, jotta työntekijä voi omalta osaltaan vaikuttaa arjessa tietoturvan toteutumiseen. Tietoturvatietoisuuden lisääntyminen helpottaa ohjeiden ymmärtämistä ja lisää motivaatiota niiden noudattamiseen. (VAHTI 4/2013, 17-19; Järvinen & Rousku 2017, 45.)

Tutkimuksen mukaan tietoturvaohjeiden noudattamiseen vaikuttavat sekä työntekijän omat kokemukset että ulkoa tulevat vaatimukset. Mikäli työntekijät kokevat, että voivat omalla toiminnallaan edistää yrityksen tietoturvallisuutta, he todennäköisemmin noudattavat ohjeita. Tästä johtuen on tärkeää, että työntekijöiden tietoturvatietoisuutta lisätään. Merkittävin ulkoinen tekijä työntekijöiden tietoturvakäyttäytymisessä on johdon valvonta ja suhtautuminen tietoturvaohjeiden noudattamiseen. (Herath & Rao 2009, 21.)

Tässä luvussa on pyritty käsittelemään niitä asioita, joiden huomioiminen henkilöstön jokapäiväisessä toiminnassa on tietoturvallisuuden kannalta merkittävintä. Tiedot on koottu muun muassa Henkilöstön tietoturvaohjeen (VAHTI 4/2013), Viestintäviraston tietoturvaohjeiden sekä Rouskun (2014) ja Järvisen & Rouskun (2017) kirjojen pohjalta. Käsittelyssä on pyritty huomioimaan erityisesti PK-yritysten tarpeet sekä resurssit.

5.1 Sähköposti

Sähköpostista on tullut useimmille yrityksille välttämätön, päivittäinen viestinnän työkalu. Sähköpostin turvallinen käyttö edellyttää käyttäjältä huolellisuutta. Sähköpostin kautta leviää paljon roskapostia, joka voi sisältää viruksia tai muuta haitallista aineistoa. Luottamuksellista tietoa tulisi lähettää sähköpostilla vain salatussa muodossa. (Viestintävirasto 2015b)

Työsähköpostia tulisi lähtökohtaisesti käyttää vain työasioiden hoitamiseen. Epäilyttäviltä vaikuttavien sähköpostiviestien kanssa tulisi noudattaa erityistä varovaisuutta. Haittaohjelmat voivat levitä sähköpostiviestien tai niiden liitetiedostojen kautta. Sähköpostiviestit voivat sisältää myös linkkejä, jotka ohjaavat käyttäjän haittaohjelmasivustolle. Liitetiedoston tai linkin avaaminen voi johtaa koneen saastumiseen. Tutulta lähettäjältä tulleen epäilyttävän viestin oikeellisuus kannattaa varmistaa lähettäjältä puhelimitse. Viestintäviraston mukaan sähköpostin kautta leviävissä haittaohjelmissa yleisiä tiedostopäätteitä ovat .COM, .EXE, .SHS, .PIF ja .VBS. (Vahti 4/2013, 32-33; Viestintävirasto 2015b.)

Salaamattomalla sähköpostilla voi lähettää vain julkista tietoa. Sähköpostilla välitettävä salassa pidettävä tieto tulee salata. Organisaation sisäisessä viestinnässä on usein käytössä salattu yhteys, mutta jos salassa pidettävää tietoa sisältävä sähköposti lähetetään suojaamattoman yhteyden ulkopuolelle, tarvitaan erillinen sähköpostin salaus. Sähköpostin salaamiseen on useita keinoja. Sähköpostiviesti voidaan esimerkiksi lähettää turvapostina tai se voidaan salata varmenteen tai julkisen avaimen avulla. (Rousku 2014, 284-287.)

Sähköpostin perillemenoon luotetaan välillä liiankin vankasti. Kriittisten asioiden hoidossa ei tulisi luottaa pelkästään sähköpostiin. Sähköpostin perillemenosta voi varmistua vasta siinä vaiheessa, kun viestiin vastataan. Mikäli sähköpostiviesti vaatii nopeaa toimintaa vastaanottajalta, viestin perillemeno tulisi varmistaa esimerkiksi lukukuittauksen tai puhelinsoiton avulla. Lukukuittausominaisuus löytyy useimmista sähköpostiohjelmista. (Rousku 2014, 176.)

5.2 Salasanat

Palveluiden ja tietojärjestelmien käyttäjät tunnistetaan ja todennetaan usein käyttäjätunnuksen ja salasanan avulla. Salasanan tarkoitus on suojella käyttäjätiliä luvattomalta käytöltä. Muistettavien käyttäjätunnusten ja salasanojen määrä kasvaa jatkuvasti, ja usein muistamista pyritään helpottamaan tinkimällä salasanan laadusta. Mikäli käyttäjän tunnistamiseen käytetään vain yhtä tapaa, puhutaan heikosta käyttäjätunnistamisesta. Salasanan ollessa ainoa tunnistus- ja todennusmenetelmä, salasanan laatu vaikuttaa suoraan palvelun tietoturvaan. (Viestintävirasto 2014b.)

Valtiovarainministeriön mukaan salasanojen kanssa tulee noudattaa varovaisuutta. Henkilökohtaista salasanaa ei saisi koskaan luovuttaa ulkopuoliselle. Saman salasanan käyttöä eri palveluissa tulisi välttää, ja erityisesti tulisi erottaa työhön sekä vapaa-aikaan liittyvät salasanat. (VAHTI 4/2013, 13.)

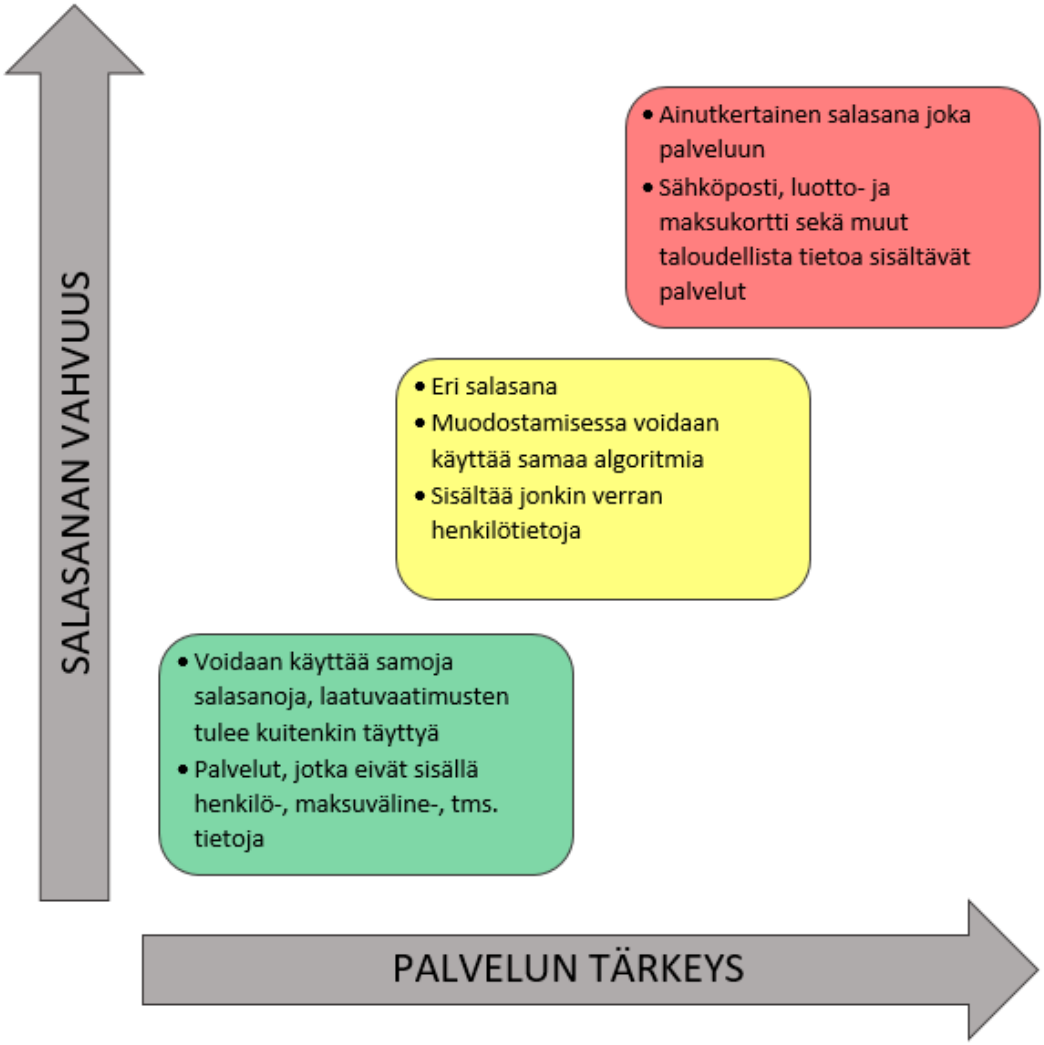
Osa palveluista voi edellyttää salasanalta tiettyjä laatuvaatimuksia jo rekisteröitymisvaiheessa. Yleisten ohjeistusten mukaan salasana on sitä vahvempi, mitä pidempi se on. Myös käytetyillä merkeillä on väliä. Salasanan murtaminen on sitä vaikeampaa, mitä useampaa merkkisarjaa ja merkkiä siinä käytetään. Salasana ei myöskään saisi muodostua minkään kielen järjellisestä sanasta ja se tulisi vaihtaa säännöllisesti. (Rousku 2014, 179.)

Vahvalle salasanalle asetetaan siis melko tarkkoja vaatimuksia. Vahvan salasanan muistaminen useisiin, jopa kymmeniin palveluihin on käytännössä mahdotonta. Salasanojen muistamista helpotetaan usein kirjoittamalla palvelu ja käytetty salasana paperille, ja pahimmassa tapauksessa säilytetään paperia tietokoneen lähistöllä. Mikäli salasana halutaan kirjoittaa ylös, tulisi huolehtia siitä, että paperista ei käy ilmi minkä palvelun salasana on kyseessä. Salasana voidaan kirjoittaa paperille vain osittain, mikä helpottaa muistamista mutta ei paljasta koko salasanaa. Paperia tulisi säilyttää turvallisesti, poissa tietokoneen välittömästä läheisyydestä. Salasana voidaan tallentaa tietokoneelle, kunhan se on salatussa muodossa. Salasanojen hallintaan on kehitetty myös sovelluksia, jotka tallentavat salasanat salatussa muodossa joko pilvipalveluun tai laitteelle, jolle sovellus on asennettu. Salasanojen hallintaa tarjoavia sovelluksia ovat muun muassa Keepass ja F-Secure Key. (Viestintävirasto 2014b.)

Petteri Järvinen pohtii blogissaan ”Havaintoja digimaailmasta” salasanojen tiheän vaihtamisen tarpeellisuutta. Teoriassa salasanan vaihtamisella voidaan saada mahdollinen tunkeutuja ulos järjestelmästä. Järvisen mukaan käytännössä edes päivittäinen salasanan vaihtaminen ei riitä, koska tunkeutuja ehtii kerätä tietoja jo muutamassa tunnissa. Lisäksi useiden vahvojen salasanojen muistaminen on erittäin vaikeaa, mikä voi johtaa huonojen salasanojen valitsemiseen. Järvinen kehottaakin vaihtamaan salasanan vain silloin, kun sen tiedetään paljastuneen. (Järvinen 2017.)

Rouskun (2014, 184) mukaan käytettävät salasanat voidaan jakaa esimerkiksi kolmeen kategoriaan palvelun kriittisyyden mukaan. Kuviossa 8 esitetään palvelun sisältämän tiedon kriittisyyden ja salasanan vahvuuden välinen yhteys. Mitä kriittisempi palvelu on, sitä vahvempi ja

ainutkertaisempi salasanan tulisi olla. Tärkeimpien ja arkaluontoisinta tietoa sisältävien palveluiden salasanojen tulisi olla ainutkertaisia jokaisessa palveluissa. Salasanojen muodostamisessa voidaan käyttää samaa kaavaa, jos palvelut sisältävät vain jonkin verran henkilötietoja. Palveluissa, jotka eivät sisällä varsinaisia henkilö-, maksuväline yms. tietoja, voidaan käyttää samoja salasanoja. Näissäkin palveluissa käytettävien salasanojen laatuvaatimukset, esimerkiksi pituuden ja erikoismerkkien osalta, tulee täyttyä. (Rousku 2014, 184.)



KUVIO 8. Salasanakategoriat. (mukaillen Rousku 2014, 184.)

5.3 Työpiste

Yrityksen tiloissa voi liikkua työajan ulkopuolella ulkopuolisia henkilöitä, esimerkiksi siivoojia ja vartijoita. Nämä henkilöt voivat nähdä vahingossa heille kuulumatonta tietoa, mikäli arkaluontoisia papereita jätetään työpöydälle ja tietokonetta ei lukita. Tämän vuoksi työpaikalla tulisi ottaa käyttöön puhtaan pöydän ja puhtaan näytön periaate. Puhtaan pöydän periaatteella tarkoitetaan sitä, että paperilla tai sähköisillä tallennusvälineillä olevaa salassa pidettävää tietoa säilytetään työpöydällä vain silloin, kun sitä tarvitaan. Muina aikoina salassa pidettävää tietoa tulisi säilyttää lukitussa paikassa. Turvallinen säilytystila voi suojata tietoa myös esimerkiksi tulipalolta. Siisti työpiste edistää tietoturvallisuuden lisäksi työn tehokkuutta ja viihtyvyyttä. Puhtaan näytön periaatteeseen kuuluu, että tietokone lukitaan silloin, kun työpisteeltä poistutaan. Puhtaan pöydän ja puhtaan näytön periaatteen avulla pyritään ehkäisemään tiedon häviäminen ja vahingoittuminen sekä tiedon päätyminen ulkopuolisille. (SFS-EN ISO 27002 2017, 46; Laaksonen ym. 2006, 169-170.)

5.4 Sosiaalinen media

Sosiaalisen median käyttö on lisääntynyt yrityksissä viime vuosina merkittävästi. Sosiaalinen media on ilmiönä melko uusi, mistä johtuen sen tuomia riskejä ei välttämättä osata yrityksessä huomioida. Tällaisia riskejä ovat esimerkiksi virheellisen tiedon leviämisestä johtuva mainevahinko ja huolimattomuudesta tai tietämättömyydestä johtuva tietovuoto. Käyttäjän toiminta on merkittävässä asemassa sosiaalisessa mediassa, minkä vuoksi riskien tiedostaminen ja käyttäjien ohjeistaminen on ensiarvoisen tärkeää. (VAHTI 4/2010, 11-12.)

Sosiaalisen median hyödyntäminen yritystoiminnassa tulisi aina olla johdon tietoinen päätös. Sosiaalisen median käytön tulisi pohjautua yrityksen ydintoimintojen tukemiseen ja sille tulee asettaa riittävät resurssit. Sosiaalisessa mediassa yritys voi muun muassa tavoittaa uusia ja palvella olemassa olevia asiakkaita sekä lisätä myyntiä. Parhaimmillaan sosiaalinen media on yritykselle erinomainen myynti- ja markkinointikanava. Yritykselle tuleva palaute on sosiaalisessa mediassa useimmiten heti kaikkien nähtävillä, mikä voi olla yrityksen maineelle vahingollista. Yrityksen hyvän maineen ylläpitämiseksi palautteisiin tulisi reagoida nopeasti ja riittävällä vakavuudella. (Cybricon Oy & Tietoturvaamo Oy 2015, 14.)

Sosiaalisen median käytöstä on hyvä sopia työpaikalla. Usein työnantaja rajoittaa sosiaalisen median käyttöä, jotta siitä ei ole haittaa työtehtävien hoitamiselle. Sosiaalisen median käyttö työkoneella edellyttää erityistä varovaisuutta. Esimerkiksi Facebookissa leviää usein haitallisia linkkejä, joiden avaamisesta voi seurata harmia. Sosiaalisessa mediassa julkaistut kuvat ja kirjoitukset voivat levitä laajalle ja niiden poistaminen jälkeenpäin voi olla mahdotonta. (Järvinen & Rousku 2017, 130-131.)

5.5 Ohjelmistot

Haittaohjelmat leviävät tietokoneeseen useimmiten verkkosivujen tai sähköpostin liitetiedostojen kautta. Haittaohjelmistojen torjunnassa auttaa varovaisuuden lisäksi päivitysten asentaminen, torjuntaohjelman käyttäminen sekä vain tarpeellisten ohjelmien käyttäminen. Erityisesti työpaikan koneella tulisi käyttää vain sellaisia ohjelmia, joita työtehtävien hoitaminen edellyttää. Tietoturvan kannalta erityisen kriittisiä ovat Java-sovellukset sekä Flash- ja Silverlight-laajennukset. Työkoneissa ohjelmien asennuksen voi estää rajoittamalla käyttöoikeuksia. Käyttöoikeuksien rajoittaminen voi ehkäistä myös tahattomia vahinkoja. (Järvinen & Rousku 2017, 90-91.)

Ohjelmistopäivitysten tarkoituksena on parantaa ohjelmistojen turvallisuutta korjaamalla niistä löytyneitä virheitä ja haavoittuvuuksia. Verkkorikolliset voivat hyödyntää käyttöjärjestelmistä ja ohjelmistoista löytyneitä tietoturva-aukkoja, minkä vuoksi päivitysten asentaminen on tärkeää. Käyttöjärjestelmän ja ohjelmistojen päivittäminen voi olla kokonaan tai osittain työntekijän vastuulla tai siitä voi huolehtia yrityksen tietohallinto. Monissa tilanteissa päivitysten automatisointi voi olla tarpeen, jolloin päivitysten asentamisesta ei aiheudu ylimääräistä työtä. (Järvinen & Rousku 2017, 103.)

5.6 Varmuuskopiointi

Tietojen varmuuskopiointi on osa liiketoiminnan riskien ja jatkuvuuden hallintaa. Jokaisella yrityksellä on sellaista tietoa, jonka häviäminen vaarantaa liiketoiminnan jatkumisen. Tiedon häviäminen voi aiheutua esimerkiksi tietomurrosta, inhimillisestä virheestä, käyttäjän huolimattomuudesta, kiristyshaittaohjelmasta, varkaudesta, tulipalosta tai tallennuspaikan toiminnan häi-

riöstä. Tämän vuoksi yritykselle tärkeät tiedot tulisi suojata varmuuskopioinnin avulla. Varmuuskopioinnissa kaikki liiketoiminnan kannalta tärkeät tiedot kopioidaan sijaintiin, josta ne voidaan tarvittaessa palauttaa. (Rauhala Yhtiöt Oy.)

Varmuuskopiointi voidaan toteuttaa automaattisesti, jolloin työntekijälle ei aiheudu varmuuskopioinnista ylimääräistä työtä. Mikäli varmuuskopiointi tehdään manuaalisesti, tulisi kaikilla työntekijöillä olla riittävät tiedot ja taidot varmuuskopioinnin suorittamiseen. Varmuuskopioinnin voi ostaa myös ulkoisena palveluna, jolloin yrityksen tärkeät tiedot tallentuvat palveluntarjoajan palvelimelle tai pilvipalveluun. Varmuuskopiointi tulisi suorittaa säännöllisesti ja riittävän tiheästi, jotta viimeisimmät versiot tiedoista saadaan palautettua. Varmuuskopioitujen tiedostojen palauttamista tulee testata säännöllisesti, koska varmuuskopioinnin hyödyt katoavat, jos tiedostot eivät ole tarvittaessa saatavilla. Varmennettavien tietojen laajuus ja tallennuspaikkojen määrä tulee määritellä tapauskohtaisesti. (Rauhala Yhtiöt Oy.)

5.7 Etätyö

Työtehtävien hoitaminen työpaikan ulkopuolella on lisääntynyt huomattavasti. Töitä voidaan tehdä niin kotona kuin työmatkoillakin. Töiden tekeminen on pääsääntöisesti turvallisinta yrityksen työtiloissa, mikä tulisi huomioida erityisesti silloin, kun työtehtävien hoitaminen edellyttää salassa pidettävän tiedon käsittelyä. Yrityksen johdon tulisi laatia etätyötä koskevat ohjeet, mikäli etätyön tekeminen sallitaan. Työntekijöiden tehtäväksi jää ohjeiden sisäistäminen ja noudattaminen. (Järvinen & Rousku 2017, 48; Rousku 2014, 174.)

Työntekijän toiminta vaikuttaa merkittävästi etätyön turvallisuuteen, minkä vuoksi etätyön ohjeistaminen on tärkeää. Viestintävirasto listaa seitsemän turvallisuusohjetta etätyöhön liittyen. Viruksentorjuntaohjelmistojen, käyttöjärjestelmien ja muiden sovellusten päivitykset tulisi olla ajan tasalla erityisesti etätyötä tehtäessä. Vieraiden verkkojen käyttö lisää etätyön riskejä, joten suojaamattomien langattomien verkkojen sijaan tulisi käyttää esimerkiksi puhelimen verkkoyhteyttä. Työmatkoilla laitteista ja asiakirjoista tulisi huolehtia ja kiinnittää huomiota myös siihen, onko ympäristö sopiva työasioista puhumiseen. Kotona työskenneltäessä tulisi huolehtia kotiverkon turvallisuudesta vaihtamalla oletussalasana. Työpaikan tietokone on tarkoitettu lähtö-

kohtaisesti vain työtehtävien hoitamiseen, ei vapaa-ajan toimintaan tai muiden perheenjäsenten käyttöön. Vastavuoroisesti omien laitteiden käyttö työtehtävissä ei ole suotavaa, mikäli siitä ei ole erikseen sovittu. (Viestintävirasto 2015a.)

5.8 Mobiililaitteet

Mobiililaitteet eli älypuhelimet, tabletit ja muut vastaavat laitteet sisältävät nykyään käyttäjän omien tietojen lisäksi myös yrityksen tietoja. Esimerkiksi työsähköpostia käytetään usein myös oman mobiililaitteen kautta. Mobiililaitteiden käyttöjärjestelmät ovat hyvin suojattuja, mutta laitteiden käytössä tulee kuitenkin olla huolellinen. Mobiililaitteiden turvallisuutta edistää se, että käytettävät sovellukset täytyy ladata sovelluskaupasta, jossa niiden tietoturvallisuuteen on kiinnitetty huomiota. Mobiililaitteisiin liittyvä merkittävin uhka on niiden joutuminen vääriin käsiin. Mobiililaitteiden lukituksella pyritään estämään laitteen luvaton käyttö. Lukituksen avaamiseen on käytössä erilaisia menetelmiä. Perinteisesti lukitus avataan salasanan, numerokoodin tai lukituskuvion avulla. Nykyteknologia mahdollistaa käyttäjän tunnistamisen biometrisen menetelmän avulla, esimerkiksi käyttämällä sormenjälkeä tai silmän iiristä. Salasanan, numerokoodin tai lukituskuvion syöttämisen voi nähdä vierestä, minkä takia biometriset tunnistusmenetelmät ovat turvallisempia. (Järvinen & Rousku 2017, 117.)

Mobiililaitteiden tiedot varmuuskopioidaan usein laitevalmistajan omaan pilvipalveluun. Tällöin tiedot ovat tallessa vaikka laite hajoaa tai katoaa. Pilvipalvelun käyttö mahdollistaa tietoihin murtautumisen ilman laitteen hallintaa, joten käytettävän salasanan tulee olla erityisen vahva. Sovelluksia ladatessa kannattaa perehtyä sovelluksen pyytämiin käyttöoikeuksiin. Kaikki toiminnot, joihin sovellus pyytää käyttöoikeutta eivät ole välttämättä tarpeellisia. Henkilötiedot, osoitekirja ja sijaintitiedot antavat paljon tietoa käyttäjästä ja auttavat oikeanlaisten mainosten kohdistamisessa. Käyttöoikeuksia voi kuitenkin rajata myös asennuksen jälkeen. Mobiililaitteen kadotessa se voidaan lukita, paikantaa tai tyhjentää valmistajan nettisivujen kautta. Turvaominaisuudet eivät ole käytössä automaattisesti, joten niihin tulee perehtyä laitekohtaisesti. (Järvinen & Rousku 2017, 119-127.)

5.9 Pilvipalvelut

Pilvipalveluiksi kutsutaan palveluja, jotka tarjoavat tietojenkäsittelyä, tallennusta ja tietoliikennepalveluita verkkoyhteyden välityksellä. Pilvipalvelut voivat helpottaa tietojen käytettävyyttä monessa tilanteessa, koska tietojen käyttö ei ole sidonnainen tiettyyn paikkaan tai laitteeseen. Pilvipalveluiden käyttöön liittyy kuitenkin myös tietoturvallisuuteen liittyviä haasteita, jotka tulisi ottaa huomioon sopimusta tehdessä. (Viestintävirasto 2014a.)

Pilvipalvelut luokitellaan usein sen mukaan, millaista palvelumallia tarjotaan. Ohjelmistoresurssi –palvelumalliksi (engl. Software as a Service, SaaS) kutsutaan palvelua, jossa käyttäjälle tarjotaan esimerkiksi verkon yli käytettävää tallennussovellusta. Useimmiten asiakasta veloitetaan tallennustilan käytön mukaan. Tällaisen palvelun käyttöönotto on helppoa, mutta käyttäjä ei voi juurikaan vaikuttaa palvelun tekniseen tietoturvaan. Alustaresurssipalvelut (engl. Platform as a Service, PaaS) mahdollistavat omien ohjelmistojen ja niiden tietoturvan toteuttamisen. Infrastruktuuriresurssipalvelu (engl. Infrastructure as a Service, IaaS) tarjoaa asiakkaalle tallennustilaa, laskentatehoa ja verkkoyhteyksiä. Tällöin asiakkaalla on suurin vastuu tietoturvan kehittämisestä mutta myös suurin toimintavapaus ohjelmistojen toteuttamiseen. Pilvipalvelu voidaan hankkia vain tietyn organisaation tai organisaatiojoukon omaan käyttöön. Vaihtoehtoisesti voidaan käyttää julkista pilvipalvelua. Yrityksessä tulisi miettiä, mikä pilvipalvelumalli tukee parhaiten yrityksen toimintaa ja vastaa yrityksen tarpeisiin. (Viestintävirasto 2014a.)

Pilvipalveluiden tarjoajia ja sopimusten sisältöjä tulisi vertailla ennen sopimuksen tekemistä. Esimerkiksi turvallisuuteen vaikuttavat tekijät voivat vaihdella eri palveluntarjoajien välillä huomattavasti. Palveluntarjoajan fyysisen sijainnin selvittäminen on tärkeää, koska se voi vaikuttaa siihen, mitä tietoja palveluun voi tallentaa. Paikallinen lainsäädäntö voi asettaa rajoituksia erityisesti henkilötietojen tallennussijainnille. Pilvipalveluiden hyötyjä tulisi peilata sen aiheuttamiin riskeihin. Joillekin yrityksille pilvipalveluiden käyttö voi aiheuttaa niin paljon riskejä, ettei se ole kannattavaa. Riskejä voidaan pienentää esimerkiksi käyttämällä pilvipalveluita julkisen, tai sellaisen tiedon kanssa, jonka paljastuminen ei aiheuta merkittäviä vahinkoja. Riskejä voidaan osittain pienentää myös tarkasti laaditulla sopimuksella palveluntarjoajan kanssa. (Viestintävirasto 2014a.)

6 KÄYTÄNNÖN OSUUDEN TOTEUTUS

Aloitin opinnäytetyön tekemisen toukokuussa 2017 ollessani harjoittelijana CyberWI-tietoturvahankkeessa. Hankkeen yksi tavoite on pyrkiä tuottamaan sellaisia sovelluksia tai palveluja, joita myös pienten ja keskisuurten yritysten on helppo hyödyntää. Tällaisia sovelluksia ja palveluita pyritään kehittämään Centrian tietoturvalaboratoriossa. Tuotantotalouden opiskelijana minulla ei ollut kattavaa tietämystä teknisestä tietoturvasta, joten laboratorion kehittämistoimi löytyi hallinnollisen tietoturvan puolelta. Opinnäytetyön keskeiseksi aiheeksi valikoitui ”Ohjeistus tietoturvan toteuttamiseksi PK-yrityksissä”. Aiheen oli tarkoitus ohjautua tarkemmin asiakasyrityksen tarpeisiin. Selvityksessä kävi ilmi, ettei asiakasyrityksellä ollut tietoturvapolitiikkaa eikä tietoturvaohjeistusta, joten opinnäytetyön aihe osoittautui asiakasyrityksen näkökulmastakin tarpeelliseksi. Opinnäytetyön teoreettinen viitekehys rakentui kesän 2017 aikana, ja käytännön osa toteutettiin syksyn 2017 aikana.

6.1 Tavoitteet

Tietoturvan toteuttamista yrityksissä ohjaavat muun muassa lait ja asetukset sekä hyväksi todetut käytännöt. Tietoturvan toteuttaminen vaatii johdon tukea, joka ilmenee konkreettisesti tietoturvan johtamisessa ja tietoturvapolitiikassa. Henkilöstölle asetetut vastuut ja velvollisuudet määritellään tietoturvapolitiikassa, jonka pohjalta laaditaan ohjeistus tietoturvan toteuttamiseksi jokapäiväisessä toiminnassa. Tietoturvaohjeiden avulla henkilöstön on helpompi toimia yrityksen johdon asettamien periaatteiden mukaisesti. Lisäksi uusien työntekijöiden perehdyttäminen on tehokkaampaa. Tietoturvan toteutumisen kannalta on olennaista, että uusi työntekijä omaksuu tietoturvallisuuden vastuut ja velvollisuudet heti työsuhteen alussa.

Tämän työn tavoitteena oli kehittää yleiset ja selkeät tietoturvaohjeet, joita voidaan soveltaa useimmissa yrityksissä. PK-yrityksissä ei usein ole käytettävissä merkittäviä resursseja tietoturvan kehittämiseen, minkä vuoksi ohjeiden laadinnassa pyritään huomioimaan juuri PK-yritysten tarpeet. Tietoturvaohjeet tulee aina räätälöidä yrityskohtaisesti, joten ohjeiden ei ole tarkoitus soveltua sellaisenaan yritysten käyttöön. Yleisten tietoturvaohjeiden tavoitteena on helpottaa yritysten tietoturvatyötä sekä lisätä kustannustehokkuutta. Yrityskohtaisten ohjeiden laatiminen valmiiseen kehykseen pohjautuen vähentää tarvittavia resursseja.

6.2 Tietoturvapolitiikan laadinta

Tietoturvaohjeistuksen laatimiseksi on tarpeen luoda yritykselle tietoturvapolitiikka, josta käy ilmi muun muassa johdon linjaukset sekä työntekijöiden vastuut ja velvollisuudet. Tietoturvapolitiikan avulla johto voi osoittaa henkilöstölle, että on sitoutunut kehittämään tietoturvallisuutta yrityksessä. Tietoturvapolitiikan laatiminen yhdessä asiakasyrityksen johdon kanssa oli osa opinnäytetyön käytännön osiota.

Tietoturvapolitiikan valmistelussa voidaan Hakalan ym. (2006, 8) mukaan käyttää apuna valmista kehystä, mutta sisältö täytyy tarkentaa yrityksen johdon linjausten mukaiseksi. Asiakasyrityksen tietoturvapolitiikka laadittiin hankkeen käyttöön valmistellun tietoturvapolitiikan pohjalta. Tietoturvapolitiikan laadinnan yhteydessä yritykseen nimitettiin tietoturvatyöryhmä, johon kuuluu johdon lisäksi muun muassa yrityksen tietoturvavastaava. Tietoturvatyöryhmä toimii tietoturvallisuuden kehittäjänä yrityksessä ja osallistui myös tietoturvapolitiikan laadintaan.

Laaksosen ym. (2006, 146-147) mukaan tietoturvapolitiikkaa tulee katselmoida säännöllisesti, ja sitä tulee päivittää tarvittaessa, esimerkiksi silloin, kun yrityksen prosesseissa tapahtuu muutoksia. Asiakasyrityksessä on käytössä ISO 9001 –laatujärjestelmä, ja laatuasioita hoitaa ulkoistettu laatupäällikkö. Laatupäällikön kanssa sovittiin, että yrityksen laatukäsikirjaan sisällytetään kuvaus tietoturvapolitiikasta sekä varsinaisen tietoturvapolitiikan sijaintipaikka. Laatujärjestelmän yhteydessä vuosikellosta oli tullut yrityksen johdon käyttämä työkalu. Laatupäällikön ja toimitusjohtajan kanssa keskusteltuamme tulimme siihen tulokseen, että tietoturvallisuuteen liittyviä asioita, kuten tietoturvapolitiikan katselmointi, sisällytetään vuosikelloon. Näin varmistetaan, että tietoturvapolitiikan katselmointi ja päivitys tulee hoidettua.

6.3 Tietoturvaohjeiden laadinta

Internetissä on saatavilla useita erilaisia malleja henkilöstön tietoturvaohjeista. Osa ohjeista on selkeitä ja ytimekkäitä, toiset taas laajoja ja yksityiskohtaisia. Näissä kaikissa ohjeissa on kuitenkin ongelmana niiden yleisluontoisuus. Tietoturvaohjeiden laatimiseksi tarvitaan tietoa yrityksen käytännöistä ja toimintatavoista, jotta tietoturvaohjeista saadaan tarkoituksenmukaiset juuri kyseiseen yritykseen. Tietoriskikartoituksen avulla voidaan arvioida, mitkä ohjeet ovat kaikkein merkittävimpiä tietoturvallisuuden toteutumisen kannalta.

Opinnäytetyön osana oli tuottaa yleisluontoiset henkilöstön tietoturvaohjeet, joita voidaan tarpeen mukaan muokata yrityskohtaisiksi. Palvelutoiminnan tarpeiden perusteella parhaimmaksi ratkaisuksi katsottiin eräänlaisen ohjepankin laatiminen. Ohjeiden laadinnassa käytettiin apuna luotettavien lähteiden, kuten Viestintäviraston ja Valtiovarainministeriön linjauksia. Ohjepankki sisältää monipuolisesti tietoturvaohjeita, joista voidaan koostaa yrityksen toiveiden ja tarpeiden mukaiset tietoturvaohjeet. Ohjepankin on tarkoitus toimia palvelutoiminnan työkaluna, jota voidaan päivittää ja laajentaa tarpeiden mukaan. Tietoturvaohjepankin sisällysluettelo on liitteessä 2.

Asiakasyrityksen tietoturvaohjeiden laadinnassa huomioitiin yrityksen nykyiset käytännöt sekä johdon linjaukset. Toiveena oli, että ohjeet pidettäisiin selkeänä ja melko lyhyenä. Tarvittaessa yksityiskohtaisempia ohjeistuksia annettaisiin työntekijöille henkilökohtaisesti. Tämän vuoksi ohjeisiin ei sisällytetty tarkempia perusteluja tai laitekohtaisia ohjeistuksia. Laaditut ohjeet käytiin läpi yrityksen tietoturvavastaavan kanssa, jotta varmistuttiin ohjeiden sopivuudesta kyseiseen yritykseen. Asiakasyrityksen tietoturvaohjeiden laadinnassa tuli hyvin esille se, että yleiset ohjeistukset eivät sovi sellaisenaan yritysten käyttöön. Lähes kaikki ohjeet riippuvat yrityksen käytännöistä ja johdon linjauksista. Esimerkiksi etätyöhön liittyvät ohjeistukset voidaan toteuttaa laajana erillisenä ohjeena. Jos etätyötä ei yrityksessä tehdä juuri lainkaan, laajojen ohjeistusten laatiminen ei ole tarkoituksenmukaista.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyön aiheena oli tietoturvallisuuden kehittäminen PK-yrityksissä. Opinnäytetyön toimeksiantajana oli CyberWI-tietoturvahanke ja tavoitteena oli laatia asiakasyritykselle tietoturvapolitiikka sekä käytännönläheiset ja selkeät henkilöstön tietoturvaohjeet. Lisäksi tavoitteena oli, että käytännön työn pohjalta voitaisiin laatia hankkeen käyttöön yleinen tietoturvaohjeistus, jonka avulla ohjeiden laatiminen tulevaisuudessa muissa asiakasyrityksissä olisi helpompaa. Teoriaosassa käsiteltiin myös EU:n tietosuoja-asetuksen vaikutuksia yleisesti PK-yrityksen näkökulmasta, vaikka käytännön toteutusta päätettiin jatkaa opinnäytetyön ulkopuolella. Opinnäytetyön tuloksena CyberWI-tietoturvahankkeen asiakasyritys sai tietoturvapolitiikan ja henkilöstön tietoturvaohjeet. Lisäksi hankkeen käyttöön muodostui tietoturvaohjepankki, jota voidaan laajentaa ja päivittää tarpeen mukaan. Ohjepankki helpottaa hanketyötä tulevaisuudessa asiakasyritysten tietoturvaohjeiden laatimisen osalta.

Tietoturvallisuudesta on viimekädessä aina vastuussa yrityksen johto ja sen tehtävänä on määrittää yrityksen tietoturvallisuuden taso niin, että sekä sisäiset että ulkoiset vaatimukset täyttyvät. Erityisesti pienissä ja keskisuurissa yrityksissä tekninen tietoturva on useiden lähteiden mukaan hyvin hoidettu, mutta hallinnolliseen tietoturvaan on kiinnitetty vähemmän huomiota. Työni aikana pohdin useaan otteeseen mistä kyseinen ilmiö johtuu. Tietoturvallisuuden kehittäminen vaatii yritykseltä resursseja ja tekninen tietoturva on helppo hoitaa kuntoon esimerkiksi ulkoistettuna palveluna. Pienten yritysten johdolla on usein valtavasti erilaisia tehtäviä, eikä tietoturvaan perehtymiseen ole välttämättä aikaa. Heikko tietoturvatietoisuus voi johtaa siihen, että tietoriskejä ei osata ottaa huomioon tai niitä ei pidetä yritystoiminnan kannalta merkittävinä. Tällöin tietoturvallisuuden kehittäminen voidaan helposti luokitella vähemmän tärkeäksi asiaksi.

Tietoturvallisuus on kokonaisuutena erittäin laaja ja monet lähteet käsittelevät tietoturvallisuutta suurten yritysten tai valtionhallinnon näkökulmasta. Tietoturvallisuuden toteuttaminen yhtä korkealla tasolla ei ole PK-yritysten näkökulmasta useinkaan mahdollista eikä edes tarpeellista, vaan jo pienillä toimenpiteillä tietoturvatasoa voidaan nostaa merkittävästi. Riittävän tietoturvatason varmistamiseksi olisi tärkeää, että yrityksen johdolla olisi riittävä ymmärrys tietoturvallisuudesta. Mielestäni pystyin opinnäytetyön toisessa luvussa käsittelemään riittävän

kattavasti tietoturvallisuuteen liittyvät määritelmät ja osa-alueet, tietoturvallisuuden peruskäsitteiden ja laajuuden ymmärtämiseksi. Lakien, standardien ja sopimusten käsittelyssä painotettiin EU:n tietosuojauudistusta aiheen ajankohtaisuuden vuoksi. Käsittelyn näkökulma on yleisluontoinen, mutta siitä ilmenee mitkä ovat uudistuksen merkittävimmät henkilötietolaista poikkeavat muutokset.

Tietoturvapolitiikka toimii Laaksosen ym. (2006, 146-147) mukaan pohjana tietoturvallisuuden toteuttamiselle ja siinä käydään läpi yleisellä tasolla tavoitteet, vastuut ja johdon linjaukset. Tietoturvapolitiikka voi helposti kuulostaa turhalta dokumentilta, mutta huolellisesti toteutettuna se on mielestäni erittäin toimiva tapa käydä läpi ja dokumentoida linjauksia, tavoitteita ja vastuita. Hakalan ym. (2006, 8) mukaan tietoturvapolitiikan laadinnassa voi käyttää kehyksenä valmiita malleja, mutta tietoturvapolitiikan sisältö tulee määrittää yrityskohtaiseksi. Tietoturvapolitiikan laadinnassa käytettiin hankkeen käyttöön aiemmin valmisteltua mallia, mutta sisältö muokattiin vastaamaan asiakkaan näkemyksiä. Mielestäni tämä oli onnistunut ratkaisu tietoturvapolitiikan laadintaan. Valmis kehys auttoi mm. siinä, että kaikki tarpeelliset asiat tulee käytyä läpi. En usko, että tietoturvapolitiikasta muodostui liian yleisluontoinen dokumentti, koska asiat käytiin huolellisesti läpi asiakasyrityksen johdon kanssa.

Erityisesti PK-yrityksissä tietoturvallisuuden kehittämiseen ei useinkaan ole käytössä merkittäviä resursseja. Tämän vuoksi on välttämätöntä kohdistaa ne oikein. (Porvari 2012, 97.) Vähäisten resurssien kohdistamisessa auttaa esimerkiksi suojattavan pääoman tunnistaminen sekä riskienhallinta. Näiden toimenpiteiden suorittaminen pitäisi mielestäni hoitaa yrityksen sisällä, koska yrityksen kriittisten toimintojen ja prosessien hyvä tunteminen on välttämätöntä. Ulkopuolinen taho voi tietysti ohjeistaa esimerkiksi tietoriskien laajuudesta, jotta riskejä osataan huomioida mahdollisimman monipuolisesti. PK-yrityksille suunnatun riskienhallintasivuston mukaan riskien pienentäminen ei välttämättä vaadi merkittäviä resursseja. Tietoturvariskeihin liittyviä suojaustoimenpiteitä ovat esimerkiksi työntekijöiden toiminta sekä tekniset ratkaisut (Suomen Riskienhallintayhdistys). Kerätyn teoriatiedon pohjalta uskallan väittää, että henkilöstön ohjeistaminen ja ohjeiden noudattamisen seuraaminen ovat tärkeimpiä keinoja, joilla voidaan pienentää tietoturvariskejä.

Suurimmat vaikeudet opinnäytetyön tekemisen aikana liittyivät aiheen rajaamiseen. Tietoturvallisuus on aiheena erittäin laaja ja se kytkeytyy moniin muihin osa-alueisiin. Tietoturvan ke-

hittäminen tulisi yrityksessä toteuttaa asteittain, koska useassa tapauksessa jonkin toimenpiteen toteuttaminen vaatii toisen toimenpiteen tekemistä. Esimerkiksi tietoturvaohjeistuksen laatiminen vaatii johdon linjauksia, jotka käsitellään tietoturvapolitiikassa. Tietoturvapolitiikan laatimisen kannalta on olennaista tunnistaa muun muassa kriittiset prosessit ja liiketoiminnan kannalta merkittävimmät riskit.

Opinnäytetyön alussa tuntui haasteelliselta, että asiakasyritys, jolle tietoturvapolitiikka ja henkilöstön tietoturvaohjeet laadittiin, ei ollut minulle entuudestaan tuttu. Mielestäni tietoturvapolitiikasta ja tietoturvaohjeista saatiin siitä huolimatta laadittua tarpeeksi yrityskohtaiset. Toisaalta oli hyvä, että en tuntenut yritystä tarkemmin, koska työn tavoitteena oli laatia tietoturvaohjeet, joita voidaan jatkossa hyödyntää hankkeen palvelutoiminnassa. Jos olisin laatinut tietoturvaohjeet itselleni tuttuun yritykseen, en välttämättä olisi osannut tarkastella asiaa sellaisesta näkökulmasta, josta olisi ollut työn tilaajalle hyötyä.

Tietoturvaohjeiden laatimisen aikana tasapainoilin laajuuden ja ytimekkyyden välillä. Laajoissa ohjeissa voidaan käsitellä erilaisia tilanteita tarkasti, ja voidaan myös esittää perusteluita sille, miksi kyseisen ohjeen noudattaminen on tärkeää. Vaarana kuitenkin on, että laajoja ohjeistuksia ei ehditä tai viitsitä yrityksessä lukea. Ohjeita laatiessa huomasin, että ohjeistus lähtee helposti laajenemaan liikaa, mikäli ohjeen noudattamisen tärkeyttä alkaa perustella. Asiakasyrityksen toiveesta ohje pyrittiin pitämään ytimekkäänä ”huoneentauluna”. Hankkeen käyttöön tuleva ohjepankki sisältää sen sijaan myös perusteita ohjeiden noudattamisen tärkeydelle sekä yksityiskohtaisempia ohjeistuksia. Tulevaisuudessa ohjepankkia tullaan mahdollisesti päivittämään myös laitekohtaisilla ohjeilla.

Herathin & Raon (2009, 21) mukaan työntekijät noudattavat ohjeita todennäköisemmin, mikäli he kokevat, että voivat omalla toiminnallaan edistää yrityksen tietoturvallisuutta. Tämän vuoksi työntekijöiden tietoturvatietoisuuden lisääminen on ohjeiden noudattamisen kannalta olennaista. Tietoturvaohjeistuksen yhteydessä kehotetaankin usein toteuttamaan tietoturvakoulutus, joka olisi syytä uusia vuosittain. Tietoturvaohjeiden laadinnassa tulisi huomioida se, miten paljon annetut ohjeet vaikeuttavat työntehtävien suorittamista, koska se on varmasti merkittävä tekijä ohjeiden noudattamisessa.

Olen opiskeluaikanani usein pohtinut työntekijöiden suhtautumista muutoksiin sekä roolia muutoksessa. Joskus työntekijöiden asenne muutoksiin on kielteinen ja lähtökohtaisesti ajatellaan,

että uuden toimintatavan käyttöönotto on hankalaa. Esimerkiksi tuotannon kehittämisprojektissa asiantuntija on varmasti ammattitaitoisin henkilö kertomaan muun muassa mitä muutoksia vaaditaan, mutta ajattelen kuitenkin, että jokainen työntekijä on ammattilainen omassa työssään. Luulen, että mikäli työntekijät otetaan mukaan esimerkiksi tuotannon kehittämisprojektiin, voidaan uusien toimintatapojen löytämisen lisäksi vaikuttaa työntekijöiden asenteeseen muutoksen osalta. Sama ajatus voisi toimia myös tietoturvallisuuden kehittämisessä. Työntekijät löytävät varmasti parhaat tietoturvalliset toimintatavat omissa työtehtävissään, mikäli heille annetaan siihen mahdollisuus. Tietoturvallisten toimintatapojen löytäminen vaatii kuitenkin riittävän tietoturvatietoisuuden, jotta ymmärtää työntekijän toiminnan tärkeyden tietoturvallisuudessa. Ohjeiden jalkauttaminen, tietoturvatietoisuuden lisääminen ja työntekijöiden asenteet ohjeiden noudattamisessa olisivat mielenkiintoisia jatkotutkimusaiheita.

Mielenkiintoisinta opinnäytetyöprojektin aikana oli tietoturvaan liittyvien asioiden implementointi olemassa olevaan laatujärjestelmään. Tietoturvallisuus voidaan usein käsittää osaksi tuotteen tai palvelun laatua. Tietoturvallisuutta käsittelevä ISO27001 -standardi ja laatua käsittelevä ISO9001 –standardi sisältävät useita samankaltaisia kohtia ja hallintatyökaluja. Sekä laadunhallinnan että tietoturvajohtamisen yhteydessä puhutaan esimerkiksi riskien- ja jatkuvuudenhallinnasta, vuosikellosta ja PDCA-mallista. Opinnäytetyön tekemisen aikana heräsi kysymys siitä, onko tietoturvallisuuden ja laadun hallinta järkevä pitää pienemmissä yrityksissä erillisinä osa-alueina vai voisiko niitä järkevästi yhdistää. Laaksonen ym. (2006, 112-114) toteaa, että yhteisen hallintajärjestelmän avulla on mahdollista säästää resursseja, mutta sen toteuttaminen vaatii aina yrityskohtaista tarkastelua. Mielestäni tietoturvapolitiikan liittäminen osaksi laatujärjestelmää sekä sen päivittämisen liittäminen osaksi vuosikelloa olivat asiakasyrityksessä erittäin toimivia ratkaisuja. Erityisesti PK-yrityksissä on mielestäni järkevää hyödyntää johdolle tuttuja hallinnan työkaluja sekä hoitaa hallinnolliset toimenpiteet keskitetysti, jotta kokonaisuuden hallitseminen on helpompaa. Tietoturvallisuuden hallinnan liittäminen laatujärjestelmään laajemmassa mittakaavassa olisi hyödyllinen ja mielenkiintoinen jatkotutkimuskohde. Voitaisiinko implementoinnilla saada aikaan se, että laadun lisäksi myös tietoturvallisuus olisi yhä useammassa yrityksessä osa jokapäiväisiä toimintaa ja työntekijöiden toimintatapoja?

Tuotantotalouden opiskelijana minulla ei ollut juurikaan pohjatietoa tietoturvallisuudesta ennen opinnäytetyön aloittamista. Opinnäytetyön tekemisen aikana tietoturvatietouteni kasvoi merkittävästi, ja luulen, että oppimistani tiedoista on minulle tulevaisuudessa erittäin paljon hyötyä.

Tietämyksen lisääntymisen ohella erittäin tärkeä oppimani asia oli se, mistä tietoa löytää. Monet asiat varmasti unohtuvat, jollei niitä päivittäin tarvitse ja lisäksi tietoturva muuttuu teknologian kehityksen myötä. Jatkossa osaan kuitenkin etsiä tietoturvaan liittyvää tietoa luotettavista lähteistä ja ymmärrän tietoturvallisuuden laajuuden ja kokonaisvaltaisuuden.

Saatujen tulosten perusteella voidaan mielestäni todeta, että opinnäytetyölle asetetut tavoitteet saavutettiin kiitettävästi. Opinnäytetyö toteutui kesälomista aiheutuneista viivästyksistä huolimatta aikataulun mukaisesti. Tietoturvaohjepankki täytti hankkeen tarpeet yleisestä tietoturvaohjeistuksesta ja asiakasyritykselle laaditut dokumentit parantavat tietoturvallisuuden tasoa ja helpottavat tietoturvan jatkokehitystä. Asiakasyritykselle laaditun tietoturvapolitiikan sisällysluettelo on liitteessä 1 ja tietoturvaohjepankin sisällysluettelo liitteessä 2.

Kaiken kaikkiaan opinnäytetyön tekeminen oli opettavainen prosessi, eikä sen loppuun vieminen olisi ollut mahdollista ilman Filosofian Maisteri Anita Rättyän asiantuntevaa ohjausta ja tukea opinnäytetyön aikana eteen tulleiden haasteiden selvittämisessä.

LÄHTEET

Alexander, P. 2005. Is Your Biz Safe From Internet Security Threats? Saatavissa: https://www.entrepreneur.com/article/78616. Viitattu 12.5.2017.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma.

Cybricon Oy & Tietoturvaamo Oy. 2015. PK-yrityksen kymmenen tietoturvakäskyä. Saatavissa: https://www.kirkkonummi.fi/instancedata/prime_product_julkaisu/kirkkonummi/embeds/kirkkonummiwwwstructure/60308_Tietoturva_opas_sivuittain.pdf. Viitattu 15.5.2017.

Elinkeinoelämän keskusliitto. Saatavissa: https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/. Viitattu 6.6.2017.

Enroth, T. & Neuvonen, R. 2017. EU:n tietosuoja-asetuksen yritysvaikutukset. Valtioneuvoston selvitys- ja tutkimustoiminta. Saatavissa: http://tietokayttoon.fi/documents/1927382/2116852/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset/7f043abc-2068-45f2-8470-0b2df19f7189?version=1.0. Viitattu 9.6.2017.

Eurooppa-neuvosto. Tietosuojan uudistus. Saatavissa: http://www.consilium.europa.eu/fi/policies/data-protection-reform/. Viitattu 8.6.2017.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Haukkovaara, O. 2017. Tietotilinpäätös – Johtamisen työkalu, EU-vaatimusten helpottaja. Alma Talent Oy. Saatavissa: http://www.tivi.fi/Kumppanit/Sofigate/tietotilinpaatos-johtamisen-tyokalu-eu-vaatimusten-helpottaja-6652925. Viitattu 2.8.2017.

Herath, T. & Rao, H. R. 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Saatavissa: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/HerathRao2009_DSS_PenalitesPressures.pdf. Viitattu 10.7.2017.

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

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

Järvinen, P. Havaintoja digimaailmasta. Älä vaihda turhaan – salasanat ovat psykologiaa, ei tekniikkaa. Saatavissa: http://pjarvinen.blogspot.fi/2017/04/ala-vaihda-turhaan-salasanat-ovat.html. Viitattu 7.6.2017.

Katakri – Tietoturvallisuuden auditointityökalu viranomaisille. 2015. Saatavissa: http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf. Viitattu 20.7.2017.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja – Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.
Lötjönen, K. 2013. Työntekijät ovat suurin tietoturvauhka yrityksille – Henkilöstön ohjeistusta aiotaan tiukentaa. Yle. Saatavissa: http://yle.fi/uutiset/3-6941588. Viitattu 15.5.2017.

Matkailualan tutkimus- ja koulutusinstituutti. 2010. Työkaluja ideointiin: Vuosikello. Saatavissa: http://matkailu.luc.fi/Tuotekehitys/Tyokaluja-/Ideointiin/Vuosikello. Viitattu: 12.7.2017.

Mehan, J. 2014. CyberWar, CyberTerror, CyberCrime and CyberActivism – An in-depth guide to the role of standards in the cybersecurity environment. United Kingdom: IT Governance Publishing.

Miettinen, E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Oikeusministeriö. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Viitattu 9.6.2017.

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Aalto yliopisto.

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton:CRC Press

Rauhala Yhtiöt Oy. Vakuuta liiketoimintasi – Tietojen varmistus toiminnan jatkuvuuden tukena. Saatavissa: http://www.rauhala.fi/hubfs/Rauhala_Docs/Vakuuta_liiketoimintasi_Rauhala.pdf?t=1497960114023. Viitattu 5.7.2017.

Rousku, K. 2014. Kyberturvaopas – tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

SFS-EN ISO 27001. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. 2017. Helsinki: Suomen Standardisoimisliitto.

SFS-EN ISO 27002. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-EN ISO 27005. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. 2013. Helsinki: Suomen Standardisoimisliitto SFS.

Suomen Riskienhallintayhdistys. PK-RH Riskienhallinta. Saatavissa: http://www.pk-rh.fi/. Viitattu 2.8.2017.

Suomen standardisoimisliitto SFS ry. Julkaisut ja palvelut. Tuotteet valokeilassa. ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. Saatavissa: https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta. Viitattu 20.7.2017.

Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/6JEcJrDjj/Laadi_tietotilinpaatos.pdf. Viitattu: 1.8.2017.

VAHTI 2/2011. Johdon tietoturvaopas. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=6068ca18-6214-4244-8ce6-dffe952e3e8e&groupId=10229. Viitattu 8.8.2017.

VAHTI 3/2007 Tietoturvallisuudella tuloksia. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229. Viitattu 1.6.2017.

VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10229. Viitattu 25.8.2017.

VAHTI 4/2013. Henkilöstön tietoturvaohje. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229.

VAHTI 5/2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=35e1f7af-9ecd-4787-8cbf-a685213cd4f8&groupId=10229. Viitattu 1.6.2017.

Valtiovarainministeriö. VAHTI-toiminta. Saatavissa: http://vm.fi/vahti. Viitattu 21.7.2017.

Viestintävirasto. Kyberturvallisuuskeskus. 2014a. Pilvipalveluiden turvallisuus – Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf. Viitattu 15.6.2017.

Viestintävirasto. Kyberturvallisuuskeskus. 2014b. Salasanat haltuun – Neuvoja salasanojen käyttöön ja hallintaan. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Salasanat_haltuun.pdf. Viitattu 12.6.2017.

Viestintävirasto. Kyberturvallisuuskeskus. 2015a. Laita etätyön tietoturva kuntoon. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/10/ttn201510071118.html. Viitattu 6.7.2017

Viestintävirasto. Kyberturvallisuuskeskus. 2015b. Sähköpostin tietoturva. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/palveluidenturvallinenkaytto/sahkoposti.html. Viitattu 15.6.2017.

Viitala, R. & Jylhä, E. 2007. Liiketoimintaosaaminen – Menestyvän yritystoiminnan perusta. Helsinki: Edita.

Vuori, M., VTT Automaatio & Halmevuo, J. 2004. PK-yrityksen riskienhallinnan työvälinesarja – Tietoriskien hallinta. Saatavissa: http://www.pk-rh.fi/uploads/riskikartat/tietoriskikartta.pdf. Viitattu 2.8.2017.

Sisällys

Sisällys