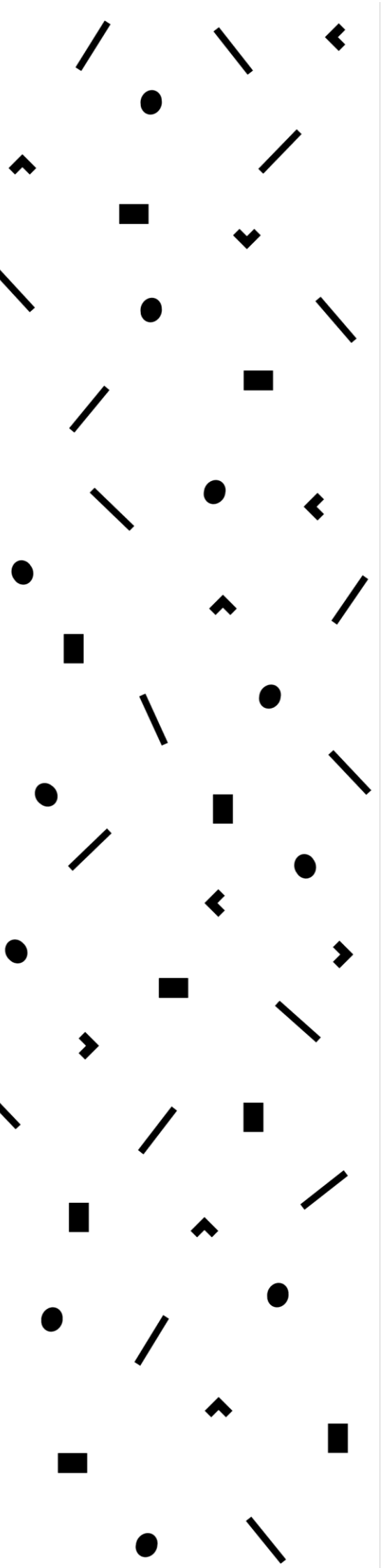


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Tietoturvaohjeistus

Case: LAMK

LAHDEN
AMMATTIKORKEAKOULU
Liiketalouden ala
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kevät 2017
Jere Karhunen

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

KARHUNEN, JERE:

Tietoturvaohjeistus
Case: LAMK

Tietojenkäsittelyn opinnäytetyö, 30 sivua, 3 liitesivua

Kevät 2017

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli tuottaa riskienhallintaa käsittelevä tietoturvaohjeistus Lahden ammattikorkeakoululle yleisten tietoturvaohjeiden tueksi sekä tutkia kuinka EU:n tietosuojauudistus vaikuttaa koulun toimintaan henkilötietojen suojauksen osalta. Ohjeistus toteutettiin tutustumalla olemassa oleviin ohjeisiin ja sääntöihin sekä kirjallisuuteen, jonka pohjalta se tehtiin.

Teoriaosassa käsiteltiin tietoturvallisuutta, siihen liittyvää riskienhallintaa ja EU:n tietosuojauudistusta yleisellä tasolla. Teoria toimi pohjana tietoturvaohjeistukselle. Teoriaosuus pohjautui aiheeseen liittyvään kirjallisuuteen sekä muuhun sähköiseen materiaaliin.

Tutkimusosuus toteutettiin haastattelemalla Lahden ammattikorkeakoulun henkilöstöä. Haastattelut toteutettiin teemahaastatteluina, joissa oli puolistrukturoituja kysymyksiä. Haastattelut tallennettiin ja litteroitiin referoiden. Haastateltavilla oli myös mahdollisuus lisätä tai muuttaa vastauksiaan jälkikäteen sähköpostin välityksellä. Tutkimuksella kartoitettiin henkilöstön ymmärrystä tietoturvallisuudesta ja uudesta tietosuoja-asetuksesta sekä siitä, miten muutoksiin on jo mahdollisesti varauduttu.

Tutkimuksessa selvisi, että henkilötietojen suojaus on hyvällä tasolla Lahden ammattikorkeakoulussa. Parantamisen varaa löytyi dokumentoinnista ja koulun on alettava tekemään tietosuoja-asetuksen vaatimia muutoksia. Suurin osa haastateltavista ymmärsi, millaisia muutoksia tietosuoja-asetus vaatii ja tiesi pääosin, miten näihin on varauduttu. Osa ei ollut kuullut koko tietosuojauudistuksesta.

Asiasanat: tietoturvallisuus, tietoturvaohjeistus, riskienhallinta

Lahti University of Applied Sciences
Degree Programme in Information Technology

KARHUNEN, JERE:

Information security guidance protocol
Case: LAMK

Bachelor's Thesis in Information Technology, 30 pages, 3 pages of appendices

Spring 2017

ABSTRACT

The purpose of the thesis was to produce an information security guidance protocol for risk management for Lahti University of Applied Sciences and to study how the EU data protection regulation affects the University's way to protect personal data. The security guidance protocol was based on existing instructions, rules and literature related to the topic.

The theoretical part of the thesis deals with information security, risk management and the EU data protection regulation on a general level. The theoretical part acts as a basis for the information security guidance and it based on literature and other online material.

The study was conducted by interviewing staff members of Lahti University of Applied Sciences. The interviews were theme based and they involved semi-structured questions. Interviews were recorded and the main points transcribed. Participants were given the opportunity to add or change their answers afterwards via email. The study surveyed the staff members' understanding of information security, the new data protection regulation and how the University has prepared for these changes.

The study finds that personal data protection is on a good level at Lahti University of Applied Sciences. Documentation needs to be improved and the University has to start making the changes the EU data protection regulation requires. Most of the participants understood what kind of changes the data protection regulation requires and knew for the most part how the University has prepared for them. Some participants, however, had not even heard about the regulation.

Keywords: information security, information security guidance, risk management

SISÄLLYS

1 JOHDANTO

Tietoturva on tänä päivänä läsnä kaikissa yrityksissä jollakin tavalla. Sen olemassaoloa ei aina tiedosteta eikä sille monesti anneta sen tarvitsemaa arvoa. Turvallisuuden tulisi olla aina lähtökohtana, kun lähdetään toteuttamaan yritystoimintaa. Hyvin toteutettu tietoturva minimoi jo itsessään riskejä ja antaa hyvän pohjan toiminnan laajentumiselle. Turvallisuus on elinehto yrityksille, ilman sitä yrityksen toiminta loppuu hyvin nopeasti. Jokaisella työntekijällä on kuitenkin omat työskentelytapansa mutta yhtenäiset tietoturvaohjeistukset takaavat sen, että työntekijöillä on tarvittavat tiedot siitä, miten tulisi toimia.

Tietoturvariskejä on monenlaisia. Riskit voivat olla fyysisiä, käyttäjästä tai ohjelmistosta riippuvaisia. Riskien eri tyypit on hyvä tiedostaa, jotta ne voidaan ottaa huomioon ja niihin voidaan puuttua. Tietoturvallisuus ja riskienhallinta ovat jatkuvia prosesseja, joita yrityksen tulee aika ajoin tarkastella. EU:n hyväksymän uuden tietosuoja-asetuksen johdosta yritykset joutuvat tulevaisuudessa kiinnittämään enemmän huomiota tietoturvallisuuteen ja mahdollisiin riskeihin, joita siihen liittyy.

Tämän opinnäytetyön aiheena on tietoturvaohjeistuksen luominen riskienhallinan osalta Lahden ammattikorkeakoululle sekä tutkia miten EU:n tietosuojauudistus tulee vaikuttamaan koulun toimintaan henkilötietojen suojauksen osalta. Aihe tuli toimeksiantajalta. Lahden ammattikorkeakoululle ei ollut tehty omaa tietoturvaohjeistusta sen jälkeen, kun se irtaantui Päijät-Hämeen koulutuskonsernista vuonna 2014 ja sen katsottiin olevan tarpeellinen. Yrityksellä oli olemassa erilaisia ohjeistuksia ja sääntöjä tietoturvaan liittyen useissa eri paikoissa mutta niitä ei ollut kasattu yhteen minnekään. Ohjeistus tulee toimimaan yleisohjeena riskienhallinnalle ja sitä voidaan käyttää muiden ammattikorkeakoulujen riskienhallinan kehittämisessä. Työn tarkoitus on kartoittaa yrityksen henkilötietosuojauksen nykytilaa ja pohtia kuinka tietosuojauudistus tulee siihen vaikuttamaan.

Opinnäytetyössä tullaan hyödyntämään aiheeseen liittyvää kirjallisuutta, sähköistä materiaalia, yrityksellä jo olemassa olevia tietoturvaohjeistuksia ja johdon määrittelemää tietoturvapolitiikkaa. Ohjeistuksen sekä teoriaosuuden pohjana käytetään pääsääntöisesti valtiohallinnon tekemiä VAHTI-tietoturvaohjeita.

2 TIETOTURVAOHJEISTUS

Tietoturvaohjeistus on yrityksen tai organisaation kokoama ohjeistus, joka kertoo miten työssä tulisi toimia, mitä pitäisi ottaa huomioon ja mikä on kiellettyä. Tietoturvaohjeistuksen tulisi olla kaikkien yrityksessä tai organisaatiossa toimivien henkilöiden saatavilla ja tiedossa. Tietoturvaohjeistuksen tulee noudattaa Suomen lakeja sekä johdon määrittelemää tietoturvapolitiikkaa. Ohjeistus ei voi olla ristiriidassa tietoturvapolitiikan kanssa. Työssä tuotettu tietoturvaohjeistus sisältää organisatorisia toimenpiteitä, jotka tekevät riskienhallinnasta helpompaa ja tehokkaampaa. Ohjeistus lyötyy työn lopusta liitteenä 2.

2.1 Työn taustat ja rajaus

Lahden ammattikorkeakoulu irtaantui Päijät-Hämeen koulutuskonsernista vuonna 2014, jolloin se jäi ilman omia tietoturvaohjeistuksia. Irtaantuessaan yritykselle jäi vanhoja tietoturvasääntöjä sekä erinäköisiä ohjeistuksia mutta niitä ei ikinä kasattu yhtenäiseksi kokonaisuudeksi. Tietoturvaohjeistuksen kokoaminen on hyvin laaja ja aikaa vievä projekti. Tämän takia toimeksiantajan kanssa sovittiin, että tietoturvaohjeistus toteutetaan vain riskienhallinnan osalta tässä opinnäytetyössä.

Tutkimuksen kohteena on uusi tietosuojauudistus, jonka Euroopan parlamentti ja neuvosto hyväksyi keväällä 2016 ja jota aletaan soveltaa toukokuussa 2018. Aihe on ajankohtainen, koska tietosuoja-asetuksen asettamat velvoitteet ja muutokset ovat pakollisia kaikille rekisterienpitäjille. Uusi asetus yhtenäistää jäsenmaiden tietosuojalakeja, tuo rekisteröidyille lisää oikeuksia ja rekisterinpitäjille lisää velvotteita.

2.2 Työn tavoitteet

Opinnäytetyön tavoitteena on tehdä tietoturvaohjeistus riskienhallinasta Lahden ammattikorkeakoululle. Lisäksi työssä tutkitaan, miten EU:n tietosuojauudistus tulee vaikuttamaan koulun toimintaan henkilötietojen suojauksen osalta ja kuinka siihen tulisi varautua. Työssä tarjotaan,

analysoinnin lisäksi, konkreettisia toimia ja muutoksia nykyisiin toimintatapoihin, jotta tulevan tietosuojauudistuksen vaatimukset täyttyisivät. Työtä voidaan myös hyödyntää muissa yrityksissä, joita uusi tietosuojauudistus ja sen tuomat muutokset sekä velvoitteet koskevat.

Työn tutkimusogelmana on, kuinka EU:n tietosuojauudistus tulee vaikuttamaan Lahden ammattikorkeakoulun henkilötietojen suojaukseen. Ongelmaa lähdetään selvittämään laadullisena tutkimuksena henkilöhaastatteluiden avulla.

2.3 Opinnäytetyön rakenne

Opinnäytetyön kolmannessa kappaleessa käsitellään tietoturvallisuutta yleisellä tasolla. Työssä avataan yksityiskohtaisemmin sen eri osa-alueita sekä EU:n tietosuojauudistusta, jotta lukija saa tarvittavan pohjatiedon aiheesta. Neljännessä osiossa käsitellään riskienhallintaa ja siihen liittyviä menetelmiä ja periaatteita. Tämän jälkeen käydään läpi työn tutkimusosa. Tutkimusosassa käsitellään tutkimuksen kulku, tutkimustulokset, -menetelmät sekä niistä tehdyt johtopäätelmät ja muutosehdotukset. Viimeisessä kappaleessa on työn pohdinta, jossa mietitään opinnäytetyön hyödynnettävyyttä ja luotettavuutta sekä mahdollisia jatkotutkimusaiheita. Liitteinä löytyvät haastattelukysymykset sekä Lahden ammattikorkeakoululle tehty tietoturvaohjeistus riskienhallinasta.

3 TIETOTURVALLISUUS

Tietoturvallisuus on osa organisaation toimintaa, sillä tarkoitetaan järjestelyitä, joilla pyritään varmistamaan tietojärjestelmien, datan ja palveluiden luottamuksellisuus, eheys ja saatavuus. Tämä tarkoittaa, että tietoja saa käsitellä vain ne henkilöt, joille niihin on myönnetty lupa. Nämäkin henkilöt saavat käsitellä tietoja vain työlle asetetulla ja työn vaatimalla tavalla. Tietojen, järjestelmien ja palveluiden on pysyttyvä muuttumattomana ja oikeina eivätkä ne saa tuhoutua minkään tapahtuman tai häiriön vuoksi. Lisäksi tietojen tulee olla aina saatavilla, kun niitä tarvitaan. (Pietikäinen 2013.)

KUVA 1, tietoturvallisuuden kolmikanta (Opentext 2017)

3.1 Tietoturvallisuuden osa-alueet

Tietoturvallisuus pitää sisällään hyvin paljon asioita, jonka takia se yleensä jaotellaan eri osa-alueisiin. Jaottelu auttaa hahmottamaan käsitteen laajuutta ja sen avulla osa-alueisiin pystytään paneutua tarkemmin. Kun aihetta osataan tarkastella kaikista näkökulmista, saadaan organisaatiolle luotua eheämpi tietoturvakokonaisuus. Seuraavissa kappaleissa käsitellään tietoturvallisuuden yleisimmät osa-alueet sekä tietoturvallisuuteen liittyvä riskienhallinta yksityiskohtaisemmin.

3.1.1 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus tarkoittaa tietoturvallisuuden johtamista, joka on yrityksen tai organisaation perusta tietoturvallisuudelle. Se koostuu johdon hyväksymästä tietoturvapolitiikasta ja periaatteista, vastuunjaosta, tietoturvallisuudelle varatuista varoista sekä riskienhallinasta. (Väistö 2005. 4.)

Ilman asianmukaisia tietoturvallisuusperiaatteita, johtamista ja suunnittelua, turvallisuustoimenpiteet voivat sisältää puutteita tai ne voivat keskittyä epäolennaisiin asioihin. Hallinnolliset toimenpiteet pohjautuvat ohjeisiin, jotka ovat muodostettu johdon määrittelemien periaatteiden ja tietoturvapolitiikan pohjalta. (Väistö 2005. 4.)

On tärkeää, että käyttäjät ymmärtävät minkä pohjalle organisaation tietoturvallisuus perustuu. Henkilökunnan on tärkeä ymmärtää johdon määrittelemä tietoturvapoliitikka sekä sen pohjalta tehdyt ohjeistukset ja säännöt. Käyttäjän tulee olla myös tietoinen ohjekokonaisuudesta ja varsinkin niistä ohjeista, jotka vaikuttavat hänen työhönsä. Organisaation tietoturvallisuuteen liittyvät vastuut tulevat olla myös selkeästi määriteltynä ja dokumentoituna. Käyttäjien vastuut tulee heille ohjeistaa ja kouluttaa, jotta jokainen käyttäjä tietää omat vastuunsa ja pystyy toimimaan niiden edellyttämällä tavalla. (Väistö 2005. 4.)

Hallinnollinen tietoturvallisuus on kaikkien muiden tietoturvallisuuden osa-alueiden perusta. Hallinnolliset toimenpiteet määrittelevät linjauksen organisaation tietoturvatoiminnalle ja sitä parantaville toimenpiteille. Hallinnollinen tietoturvallisuus voidaan jaotella osa-alueisiin, joihin kuuluu muun muassa tietoturvapolitiikan luominen, resurssien suunnittelu, vastuunjako ja toimenpiteiden organisointi, riskien tunnistaminen, suojausten määrittely, henkilökunnan kouluttaminen sekä valvonta ja seuranta. (Väistö 2005. 4.)

3.1.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöstöstä aiheutuvan riskien hallintaa. Tietoturvallisuuden näkökulmasta tähän liittyy niin salassapito- kuin käytettävyysriskejä erilaisia tietojärjestelmiä käytettäessä. (Valtiovarainministeriö 2009b.) Henkilöstöturvallisuudella on iso merkitys tietojen suojaamisessa, koska niitä käsittelee ihminen. Henkilöstön virheellinen toiminta voi johtaa tietoturvan kannalta kriittisiin tilanteisiin (Laaksonen, Nevasalo & Tomula 2006, 143.). On siis tärkeää ennaltaehkäistä sekä minimoida henkilöstöstä aiheutuvia riskejä.

Tiedonhallinta on nykyään organisaatioiden keskeinen haaste tietoturvallisuudessa. Tietoa säilytetään useissa paikoissa, jolloin riski tietojen vuotamisesta ulkopuolisille on huomattavasti suurempi. Henkilöstöllä on oltava tarvittavat työvälineet riskienhallintaan - riskitietoisuus ja osaaminen luovat sille pohjan (Valtiovarainministeriö 2003.). Riskinä on myös, että tärkeää tietoa on vain yhden ihmisen varassa. Tiedon jakamisen ja viestinnän täytyy olla tarvittavalla tasolla organisaatiossa, ettei tällaista pääse tapahtumaan.

Henkilöstöturvallisuudessa käytettävät toimenpiteet ovat lähinnä ennaltaehkäiseviä mutta niitä harvoin huomioidaan tarpeeksi. Henkilöstöturvallisuuteen vaikuttaa vahvasti työilmapiiri ja esimiestoiminta. Tyytyväinen työntekijä on yleensä myös turvallisempi. Uusien työntekijöiden taustoista olisi hyvä olla selvillä työnkuvasta riippumatta.

3.1.3 Fyysinen tietoturva

Fyysisen turvallisuuden tarkoitus on taata organisaation häiriötön toiminta ja turvallinen toimintaympäristö jokaisessa tilanteessa huomioon ottaen myös riskit (Laaksonen ym. 2006, 125). Fyysiseen tietoturvallisuuteen kuuluu muun muassa valvonnan eri muodot, erilaisten vahinkojen torjuminen sekä vartiointi. Tiedon on säilyttävä eheänä, luottamuksellisena ja saatavana jokaisessa tilanteessa. Fyysisessä turvallisuudessa on otettava huomioon teknisten laitteiden ja palvelimien sijanti, palo-, vesi- ja

murtoturvallisuus, jotta tietoturvallisuus on taattu. (Valtiovarainministeriö 2009a.)

Fyysisten turvallisuusjärjestelyiden toteutus jää usein kiinteistön omistajalle (Valtiovarainministeriö 2009a.). Fyysistä tietoturvallisuutta toteutettaessa on tärkeä muistaa, että kaikki organisaation tilat eivät ole samanarvoisia vaan esimerkiksi tilat, joissa on teknisiä laitteita, ovat korkeampaa suojausta vaativia tiloja (Laaksonen ym. 2006, 125). Organisaation hallitus tietää kuitenkin parhaiten omat turvallisuustarpeensa ja loppu kädessä päättää turvallisuuteen liittyvistä järjestelyistä (Valtiovarainministeriö 2009a.).

Helppoja ratkaisuja fyysisen turvallisuuden parantamiseksi ovat esimerkiksi henkilökortit ja sähköavaimet, joilla saadaan vähennettyä luvatonta liikkumista organisaation tiloissa. Toimitiloihin liittyvät turvallisuuden kehittämistarpeet tulee ottaa huomioon johdon tekemissä vuosisuunnitelmissa. Fyysinen tietoturva muodostaa pohjan tietoturvalle, jota ilman hallinnolliset ja tekniset ratkaisut ovat hyödyttömiä. (Valtiovarainministeriö 2009a.)

3.1.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan toimia, jotka pyrkivät takaamaan tietoliikenteen turvallisuuden. Tällaisia toimia ovat muun muassa verkkojen ja laitteiston ylläpito, verkon hallinta ja valvonta, viestinnän salaus, ohjelmien testaus sekä ongelmatilanteiden dokumentaatio ja selvittäminen. Tietoliikenteen turvallisuus tulisi ottaa huomioon jo suunnitteluvaiheessa. Jälkikäteen tehtävät muutokset ovat yleensä enemmänkin paikkauksia eikä pysyviä ratkaisuja. Myöhemmin tehtävät muutokset ovat myös huomattavasti kalliimpia kuin alussa toteutetut järjestelyt. (Valtiovarainministeriö 2009g.)

Suunnitteluvaiheessa on tärkeää tehdä tarkka selvitys turvallisuustavoitteista. Sen pohjalta suunnitellaan tilaratkaisut, turvakomponenttien asettelu, verkon siirtokapasiteetin mitoitus sekä

mahdolliset erikoistarpeet. Yhteyksien ei tulisi olla missään vaiheessa riippuvaisia yksittäisestä komponentista. Tietoliikenneyhteyksien testaus on sekä tilaajan että toimittajan velvollisuus. (Valtiovarainministeriö 2009g.)

Tärkeä osa tietoliikenneturvallisuutta ovat palomuurit. Palomuurien tehtävä on pitää kaksi tai useampi verkkosegmentti erillään toisistaan kuin myös hallita niiden välistä liikennettä asetettujen sääntöjen mukaisesti. Palomuuri on joko sovellus, tai erillinen laite johon kuuluu alusta, käyttöjärjestelmä ja palomuurisovellus. Palomuurin sääntökannat tulee luoda ja testata. Sääntökannan hallintaa varten täytyy luoda prosessi, jonka tarkoitus on kuvata vastuut ja tehtävät erilaisille muutospyynnöille. Prosessin tulee myös varmistaa dokumentaation ajantasaisuus. (Valtiovarainministeriö 2009g.)

Tietoliikenneturvallisuuteen kuuluu myös verkon operointi ja valvonta. Organisaation tulisi laatia tietoverkolle tietoliikennepolitiikka. Politiikan pitäisi käsittää tietoliikenneyhteyksiin, niiden käyttöön, valvontaan ja käyttäjäryhmiin liittyvät asiat. Verkon valvontaan kuuluu fyysinen ja liikenteen valvonta. Henkilöstöön liittyvässä valvonnassa tulee ottaa huomioon, (759/2004) laki yksityisyyden suojasta työelämässä, mitä ja miten saadaan valvoa. (Valtiovarainministeriö 2009g.)

Langattomissa tietoliikenneyhteyksissä on omat ongelmansa ja siksi keskeisten tietojärjestelmien yhteydet olisi hyvä olla langallisia tiedonsiirtokanavia. Jos organisaatiolla on olemassa kriittinen langaton yhteys, tulisi sillä olla varayhteys, joka ei ole langaton. Langattomien yhteyksien todennusmekanismit sekä salausvaatimukset tulee olla tarvittalla tasolla verkon luottamuksellisuuden varmistamiseksi. Nämä määritellään riskianalyysin perusteella. (Valtiovarainministeriö 2009g.)

> *”Langattomassa verkossa myös muut käyttäjät voivat ottaa yhteyttä laitteeseen, ellei sitä ole estetty tukiasemassa (ns. langaton verkon erotus). Jos käyttäjien tunnistautuminen verkkoon on toteutettu ja säädetty huonosti, myös pahantahtoisten tahojen on mahdollista kytkeytyä siihen ja lähettää muille käyttäjille tai verkon*

> *laitteille haitallista liikennettä. Siksi on hyvä huolehtia myös päätelaitteiden turvallisuudesta." (Viestintävirasto 2017, 4.)*

Tietoliikenneturvallisuuteen liittyy myös ulkopuoliset yhteydet. Organisaation ulkopuolelta tulevat yhteydet ovat aina tietoturvariski, minkä takia niiden tulee aina noudattaa tietoverkolle määriteltyä käyttö- ja turvallisuuspolitiikkaa. Yhteydet tulee olla suojattu palomuurilla, jotka seuraavat turvallisuus- ja käyttöpolitiikan mukaisia säännöksiä. (Valtiovarainministeriö 2009g.)

Ulkopuolisten yhteyksien tietoturvallisuusratkaisut toteutetaan riskianalyysien pohjalta. Etähuoltoyhteydet voidaan toteuttaa siten, että kun laite on havainnut vian, se lähettää vikailmoituksen huollosta vastaavalle yritykselle ja järjestelmävastaava voi sitten sallia ja avata etäyhteyden. Etähuollosta vastaava taho on todennettava tietoturvapolitiikan määrittelemällä tasolla. Kriittisten järjestelmien etäkäyttöä tulisi välttää, ja jos etäkäyttö on välttämätöntä, voidaan käyttö kohdistaa rajatulle, ei kriittiselle, osalle. Kaikki muu käyttö on tarpeetonta ja se tulee estää. (Valtiovarainministeriö 2009g.)

3.1.5 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan datan suojaamista. Tietoaineistoa voidaan turvata esimerkiksi niiden luokittelulla, ohjeistetulla hallinnalla, säilyttämisellä, käsittelyllä ja tuhoamisella (Valtiovarainministeriö 2009f.). Tietojen käsittelyyn liittyy erilaisia määräyksiä ja lakeja kuten henkilötietolaki (523/1999), jonka tarkoitus on tuoda yksityisyyden suojaa turvaavia perusoikeuksia. Näiden lisäksi on myös kansainvälisiä sopimuksia, joissa on määrätty ulkomaisten asiakirjojen salassapidosta (Valtiovarainministeriö 2009f.).

Kaikella datalla tulisi olla omistaja. Datan omistaja päättää sen käytöstä ja luokituksista. Käyttäjillä tulisi olla vain tarvittavat käyttöoikeudet töidensä toteuttamiseen. Työtehtävien vaihtuessa tulee oikeudet muuttaa työtehtäville sopiviksi. (Valtiovarainministeriö 2009f.) Tietoaineistoihin

liittyvistä tiukoista määräyksistä ja säädöksistä huolimatta, vuoden 2011 liikenne- ja viestintäministeriön julkisen tietoaineisto saatavuuden periaatepäätöksessä todetaan, että tietoaineiston tulee olla avoimesti saatavilla selkein ja tasapuolisin ehdoin (Liikenne- ja viestintäministeriö 2011.).

3.1.6 Käyttöturvallisuus

Käyttöturvallisuus tarkoittaa tietojärjestelmien käyttämiseen, tietojenkäsittelyyn sekä niihin liittyvien aputoimintojen parantamiseen käytettäviä keinoja (Valtiovarainministeriö 2009c.). Käyttöturvallisuudessa tulee ottaa huomioon palveluiden ulkoistaminen, etäkäyttöön liittyvät asiat, prosessien ja muutosten hallinta sekä poikkeusoloihin varautuminen. Jos palveluita ulkoistetaan pitää ymmärtää oma toimintaympäristö sekä toiminto, joka ulkoistetaan, jotta palveluntarjoajalle osataan esittää tarvittavat vaatimukset (Valtiovarainministeriö 2009c.). Ulkoistetun toiminnon tietämys ja osaaminen tulee kuitenkin pitää riittävänä, jotta tietoturvallisuus ei vaarannu muilta osin sekä toiminto voidaan tarvittaessa ottaa takaisin organisaatiolle (Valtiovarainministeriö 2009c.).

Etäyhteyksien ja mobiililaitteiden kanssa on toimittava tarvittavien salaus- ja todennusmekanismien mukaisesti. Prosessien hallinnan kannalta on tärkeää, että kaikilla tietojärjestelmien operointi- ja hallintatoimilla on olemassa ohjeistukset. Hankalissa poikkeustilanteissa ei välttämättä voida toimia normaalien toimintapojen mukaan mutta näihin tilanteisiin on varauduttava, jotta silloin osataan toimia hallitusti. Poikkeusoloihin voidaan varatua laatimalla valmiussuunnitelma, jonka toimivuutta tulisi testata säännöllisesti. (Valtiovarainministeriö 2009c.)

3.1.7 Laitteistoturvallisuus

Valtiohallinnon VAHTI-ohjeiden mukaan laitteistoturvallisuuteen kuuluu laitteistojen suojaus, asennukset, ylläpito sekä niihin liittyvä hallinnointi. Organisaatiossa on yleensä sovittu laitteiston elinkaariin liittyvät asiat palvelusopimuksissa. Elinkaaren määrittelyllä voi olla iso vaikutus

tarvittavan tietoturvallisuustason ylläpidettävyyteen sekä nopeuteen, jolla poikkeuksiin reagoidaan. (Valtiovarainministeriö 2009d.) Organisaation kannattaakin miettiä olisiko tarpeen pitää kriittisiä laitteita myös omassa varastossa, jotta ongelman tullessa ei oltaisiin riippuvaisia palveluntarjoajan nopeudesta toimittaa niitä (Andreasson & Koivisto 2013, 65.).

Laitteistoja ylläpidettäessä on huolehdittava, että kaikki tarvittavat tiedot pystytään milloin tahansa palauttamaan, kun poikkeustilanne on ohi. Tämä koskee myös henkilöstön mobiililaitteita ja muistitikkuja. Tiedoista on oltava tarpeeksi tuoreet varmuuskopiot. Järjestelmien laitteita on pystyttävä valvomaan ja käyttöasteiden kehittymistä seuraamaan jatkuvasti. Tietoturvapäivitykset tulee tehdä säännöllisesti ja ne pitää testata ennen niiden asentamista järjestelmiin. (Valtiovarainministeriö 2009d.) Laitteiden omia tietoturvaominaisuuksia kannattaa myös hyödyntää. Matkapuhelimiin saa esimerkiksi PIN-koodin lisäksi erillisiä turvakoodeja sovellusten avaamiseen (Andreasson & Koivisto 2013, 65.).

3.1.8 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan toimia, jotka kohdistuvat ohjelmistoihin ja käyttöjärjestelmiin. Näitä ovat esimerksi tunnistamis-, todentamis-, valvonta- ja varmistusmenettelyt sekä ohjelmistojen päivityksiin ja ylläpitoon liittyvät asiat. Käyttöjärjestelmät sekä tietoliikenneohjelmistot tulee valita käyttötarkoituksen ja sopivuuden perusteella. Organisaatiossa tulee myös mielellään olla aikasempaa osaamista näistä järjestelmistä ja ohjelmistoista. Ohjelmistot tulee myös testata huolellisesti ja niiden täytyy tukea vahvaa salausta sekä käyttäjätodennusta. (Valtiovarainministeriö 2009e.) Sovellusten, olivat ne sitten valmissovelluksia, räätälöityjä tai itse tehtyjä, tulee olla linjassa organisaation tietoturvapoliitikan ja standardien kanssa.

Organisaatiolla pitää olla erikseen testi- ja tuotantoympäristö. Kaikki uudet sovellukset ja sovellusmuutokset tulee viedä tuontantoon testiympäristön kautta. Testiympäristön tulee olla identtinen tuotantoympäristön kanssa.

Ohelmistoasennuksissa tulee huomioida komponenttien tietoturvakovennukset ja asennukset tulee suunnitella huolellisesti. Jos asennuksissa huomataan jotain poikkeavaa, tulee ne dokumentoida. (Valtiovarainministeriö 2009e.)

3.2 EU:n tietosuojauudistus

Euroopan unionin tietosuojauudistus sai lopullisen päätöksen, kun Euroopan parlamentti ja neuvosto hyväksyi uuden tietosuoja-asetuksen huhtikuussa 2016. Tietosuojauudistukseen kuuluu yleisesti sovelletteva tietosuoja-asetus sekä direktiivi, joka koskee lainvalvonta-, ja oikeusviranomaisien toimintaa. Uudistuksella yhdenmukaistetaan ja vahvistetaan jäsenmaiden nykyistä henkilötietolainsäädäntöä. Säädöksiä aletaan soveltaa 25.toukokuuta 2018 mutta rekisterinpitäjien tulee tehdä erilaisia selvityksiä, toimintatapoihinsa liittyen, jo siirtymäajan aikana. (Tietosuojavaltuutetun toimisto 2015.)

3.2.1 Tietosuojauudistuksen tausta

EU katsoi tarpeelliseksi uudistaa ja nykyaikaistaa henkilötietoja koskevaa lainsäädäntöä, koska teknlogian kehittyminen ja globalisoituminen olivat lisänneet henkilötietojen keräystä. Lisäksi jäsenmaiden lainsäädäntöä haluttiin yhtenäistää, koska yhtenäinen ja parempi henkilötietolainsaadäntö parantaa henkilöiden luottamusta sähköisiin palveluihin ja kehittää digitaalisia sisämarkkinoita. Tietosuoja-asetuksella haluttiin vahvistaa rekisteröityjen asemaa ja tuoda rekisterienpitäjille enemmän velvollisuuksia, koska jäsenmaiden omat henkilötietolainsäädännöt eivät olleet ajantasaisia. (Tietosuojavaltuutetun toimisto 2015.)

3.2.2 Vaikutukset

Uusi tietosuoja-asetus vastaa monilta osin jo nykysääntelyä mutta tuo myös uusia velvotteita ja oikeuksia. Asetuksella haluttiin parantaa

rekisteröidyn oikeuksia samalla kun rekisterinpitäjien velvollisuuksia lisättiin. Uudistuksen myötä rekisteröity voi saada itseään koskevat tiedot sähköisesti ja tietoja voi jatkossa siirtää helpommin järjestelmästä toiseen, esimerkiksi jos henkilö vaihtaa pankkia, voidaan henkilötiedot siirtää sähköisesti uuteen pankkiin. Asetuksella rajoitetaan lapsia koskevaa henkilötietojen käsittelyä, jos siihen ei ole vanhempien suostumusta. (Tietosuojavaltuutetun toimisto 2015.)

Jo siirtymäaikana, rekisterinpitäjien tulee tehdä selvitys henkilötietojen käsittelyn nykytilasta ja selvittää vastaako se tämänhetkisiä säädöksiä ja tulevaa tietosuoja-asetusta vaaditulla tavalla. Rekisterinpitäjä voi tehdä nykytilan kartoituksen esimerkiksi tietotilinpäätöksellä, joka on raportti organisaation tietojen käsittelystä ja siihen liittyvistä asioista. Selvityksen lisäksi rekisterinpitäjän tulee varmistaa riittävä tietoturva ja varautua poikkeustilanteisiin sekä kriisiviestintään. (Opitietosuojaa.fi 2017.)

Tietosuoja-asetus tuo myös uusia velvollisuuksia rekisterienpitäjille. Uusia velvollisuuksia ovat muun muassa tietosuojavastaavan nimittäminen sekä tietoturvaluokkauksista ilmoittaminen. Nämä eivät aikaisemmin olleet pakollisia, pois lukien tietosuojavastaavan nimittäminen terveydenhuoltoalan yrityksissä. Jatkossa rekisterinpitäjä on myös osoitusvelvollinen näyttämään, että tietosuojasäännöksiä oikeasti noudatetaan, kun aiemmin on riittänyt vain suostumus niiden noudattamiseen. Tietosuojavaltuutetun toimisto valvoo Suomessa asetuksen soveltamista ja voi esimerkiksi antaa sanktioita rekisterinpitäjälle sakkojen tai huomautuksen muodossa. (Tietosuojavaltuutetun toimisto 2015.)

Uudistus vähentää useissa EU-valtioissa toimivien yritysten kustannuksia, kun heidän tarvitsee jatkossa toimia vain yhden tietosuojaviranomaisen kanssa. EU perusti Euroopan tietosuojaneuvoston varmistamaan tietosuojasääntelyn soveltamisesta. Uusi tietosuoja-asetus kumoaa nykyisen EU:n henkilötietodirektiivin ja sitä sovelletaan sellaisenaan Suomessa. (Tietosuojavaltuutetun toimisto 2015.)

4 RISKIENHALLINTA

Riski on ei-toivotun tapahtuman mahdollisuus, joka voi olla haitallista organisaatiolle. Näitä ovat esimerkiksi tietojen vuoto tai korruptoituminen. (Raggad 2010, 23.) Riskienhallinta on tietoturvallisuuden tärkein osa-alue. Yrityksen tulee tunnistaa, ymmärtää ja hallita riskit, jotka ovat kriittisiä yrityksen toiminnan kannalta (Lark 2015, 12.). Miten voi hallita riskejä, joiden olemassaoloa ei tiedetä?

Riskienhallinta lähtee termien määrittelyistä ja dokumentaatiosta. Termit on hyvä määritellä, koska ihmiset ymmärtävät asioita eri tavalla. Monet esimerkiksi sekoittavat riskin riskitekijöihin tai riskivaikutuksiin. Tärkein riskeihin vaikuttava tekijä on reagointi tunnistettuihin riskeihin. Ilman toimia riskit harvemmin pienenevät. Hyvin toteutettu riskienhallinta on järjestelmällistä ja kustannustehokasta. (Andreasson & Koivisto 2013, 41.)

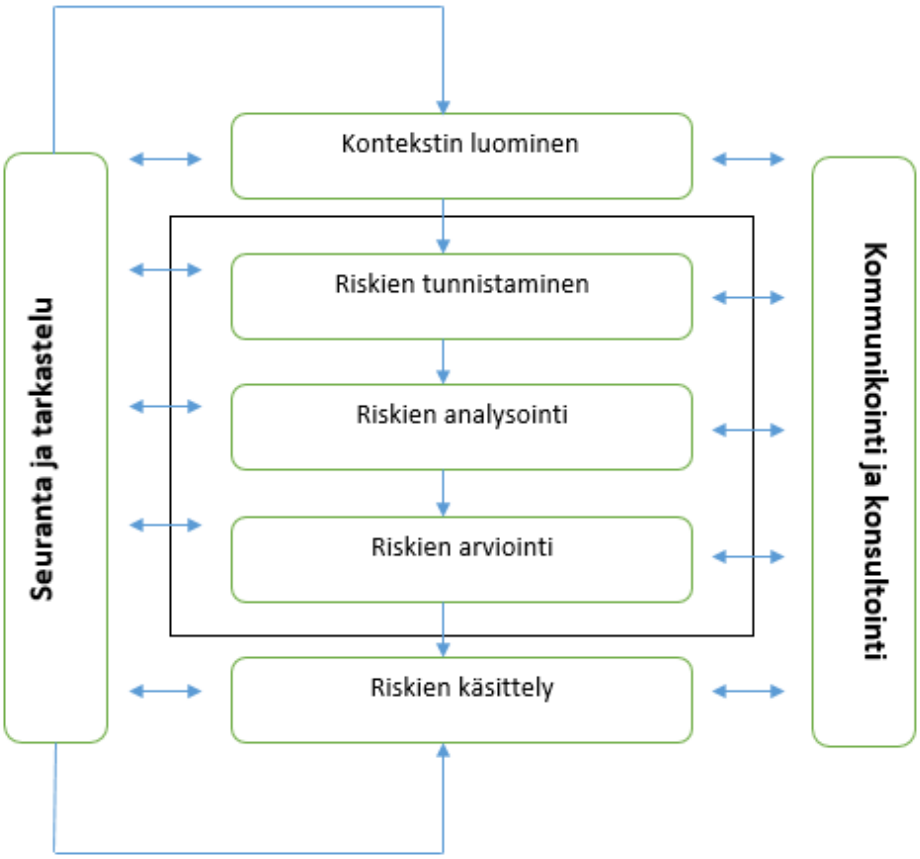
Riskejä voi hallita kahdella eri tapaa. Ne voidaan, joko hyväksyä, jos ne eivät ole kriittisiä yrityksen toiminnan kannalta tai ne voidaan minimoida hyväksyttävälle tasolle, jonka organisaation johto on määritellyt. Riskienhallintaa varten on olemassa erilaisia stardardeja, periaatteita ja protokollia kuten myöhemmin esitelty PDCA-malli.

4.1 Riskien tunnistaminen ja arviointi

Riskienhallintaprosessissa on selkeät vaiheet. Ensimmäiseksi uhat on tunnistettava, analysoitava ja arvioitava. Tämän jälkeen suunnitellaan toimenpiteet riskien minimoimiseksi. Viimeiseksi suunnitellaan, miten toimitaan vahingon sattuessa ja miten siitä päästään eteenpäin. Mahdollisesti toteutuneesta riskistä otetaan opiksi, ettei se tulevaisuudessa toistuisi. (Valtiovarainministeriö 2003, 16.)

Riskien arviointi on suunniteltuja toimenpiteitä, joilla pyritään tunnistamaan organisaation tietoturvallisuuteen liittyviä uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisten tapahtumien seurauksia. Riskejä arvioidessa määritellään niiden suuruus, todennäköisyys ja seurakset. Jos riski

todetaan merkittäväksi, niin sille valitaan tarvittavat toimenpiteet ja toteutustapa. (Valtiovarainministeriö 2003, 16.)



KUVIO 1, ISO 31000:200 mukainen riskienhallintaprosessi (Lark 2015, 15)

Uhkien tunnistamisessa ja riskien arvioimisessa kriittinen asenne on hyvä lähtökohta. Uhkien tunnistaminen voidaan aloittaa suuremmasta mittakaavasta eli kartoitusmenetelmillä. Luodaan kokonaiskuva tilanteesta, että löydetään ongelmakohdat, joita sitten tutkitaan yksityskohtaisemmin. Uhkien tunnistaminen etenee siis kokonaiskuvasta yksittäiseen uhkaan tai riskiin. Kokonaiskuvaa kannattaa arvioida uudestaan tietyin väliajoin, esimerkiksi tietoturvapoliitikan päivittämisen yhteydessä, jotta se pysyy ajan tasalla. (Valtiovarainministeriö 2003, 17.)

Riskien arviointi kannattaa suunnitella huollisesti ja pitää mahdollisimman yksinkertaisena. Arviointi voidaan tehdä esimerkiksi työryhmässä, johon osallistuu organisaation toiminnan tuntevia henkilöitä. Työryhmässä päätetään riskianalyysin laajuus ja sen rajaus, tehdään

toteutussuunnitelma, aikataulu sekä mietitään mahdolliset jatkotoimenpiteet. Ensimmäisenä on tunnistettava organisaation toiminnan jatkuvuuden kannalta kriittiset kohteet, joita tulee suojata. Organisaatiossa on hyvä ymmärtää, että riskien arvinointi kuin myös koko tietoturvallisuus on jatkuvaa ja säännöllistä työtä. (Valtiovarainministeriö 2003, 18-19.) Se mielletään useasti kertaluontoiseksi asiaksi mikä voi johtaa haavoittuvuuksiin tulevaisuudessa.

4.2 Riskienhallinnan kolme periaatetta

IT risk–kirjan mukaan riskienhallinta kannattaa rakentaa kolmen ydinperiaatteen ympärille. Nämä periaatteet ovat tietotekniikalle osoitettujen varojen hyvin suunniteltu käyttö, johon kuuluvat laitteistot, sovellukset sekä toimintatavat, jotka ovat hyvin ymmärretty ja johdettu eivätkä ole yhtään tarvittavaa monimutkaisempia. Hyvin suunniteltu ja toteutettu riskienhallintaprosessi, joka huomioi kaikki riskit organisaation näkökulmasta, jotta niitä voidaan priorisoida ja tehdä investoinnit tarpeen mukaan. Sekä riskitietoisen kulttuurin luominen, jossa jokainen organisaation henkilö on perillä mahdollisista riskeistä keskustelun aikaansaamiseksi. (Westerman & Hunter 2007, 36–37.)

Hyvä perusta minimoi riskejä jo itsessään. Kun perusta on hyvin rakennettu, ovat riskit epätodennäköisempiä. Kun ongelmia tulee, niihin tartutaan nopeammin kiinni ja ne saadaan helpommin hoidettua. Näin riskejä on helpompi arvioida, koska muuttujia on vähemmän. Organisaation on myös helpompi mukautua ja uudistua. (Westerman & Hunter 2007, 38–43.)

Riskienhallintaprosessi kuvaa, sirpaleiset ja yhdestä näkökulmasta kuvatut, riskit kokonaisuuksina. Prosessi mahdollistaa organisaation tarkastella ja arvioida riskiä sekä toimia sen vaatimalla tavalla. Jos riskejä ei osata arvioida oikein, voi tärkeimmät riskit jäädä huomaamatta, mikä altistaa organisaation haavoittuvuuksille. Jos riskit ovat arvioitu väärin, on niihin varatut resurssit myös arvioitu väärin. Yleensä resursseja varataan

vielä liian vähän, keskimääräisesti 100–200 prosenttia. (Westerman & Hunter 2007, 44–47.)

KUVIO 2, Organisaation rakenne riskienhallintaprosessissa (Westerman & Hunter 2007, 110)

Riskitietoisessa kulttuurissa on tietoturvallisuusriskeihin liittyvää vahvaa osaamista, yleistä tietoisuutta siitä miten riskikäyttäytyminen vaikuttaa ja miten välttää sitä. Tällaisessa ympäristössä rohkaistaan kaikkia kaikilta organisaation tasoilta puhumaan riskeistä avoimesti ja ottamaan henkilökohtaista vastuuta niiden hallinnasta. (Westerman & Hunter 2007, 48–51.) Riskitietoisen kulttuurin luominen lähtee organisaation johdosta ja heidän luomistaan visioista.

4.3 PDCA malli

Riskienhallinnassa käytetään paljon myös PDCA mallia, joka tulee sanoista plan, do, check, act. Vapaasti suomennettuna suunnittele, toteuta, arvioi ja toimi. PDCA mallia käytetään monissa ISO–standardeissa, joita organisaatiot voivat hyödyntää riskienhallintaa toteuttaessaan.

Suunnittele-vaihe on hallinnollisia toimenpiteitä. Tähän kuuluvat esimerksi tietoturvapolitiikka, -tavoitteet, -prosessit sekä riskienhallinnalle ja tietoturvallisuuden kehittämisellä oleelliset menettelytavat. Toteuta-vaihe on sanansa mukaisesti suunnittele-vaiheen toteuttamista. Arvioi-vaihe on tuloksien seuraamista ja mittaamista siltä osin kuin se on mahdollista. Viimeisessä eli toimi-vaiheessa korjataan ja parannetaan jo olemassa olevaa prosessia, jotta saadaan aikaan tietoturvallisuuden jatkuva parantuminen. (Andreasson & Koivisto 2013, 42–43.)

Tietoturvallisuuden toimivuutta ja tehokkuutta tulee tarkastella säännöllisesti - vähintään kerran vuodessa. Tämä sisältää tietoturvapoliitikan, tavoitteiden ja menetelmien tarkastelua sekä mahdollisia muutostarpeita. Säännöllisen tarkastelun tarkoitus on varmistaa organisaation tieturvallisuuden jatkuva soveltuvuus ja oleellisuus. (Andreasson & Koivisto 2013, 43.)

4.4 Riskianalyysi

Riskianalyysin tarkoituksena on selvittää organisaation mahdolliset uhat, kuinka todennäköisiä ne ovat ja millaista vahinkoa niistä voi aiheutua. Riskianalyysit eivät yleensä ole kovin tarkkoja, koska ne monesti perustuvat olettamuksiin eikä faktoihin. Analyysien pohjalta on kuitenkin helpompi tehdä hallinnollisia päätöksiä, koska ne auttavat hahmottamaan tarvittavat ja taloudellisesti kannattavat suojautumiskeinot uhkia vastaan. (Tiihonen 2014.) Riskianalyysien tekoon on monia valmiita malleja kuten perinteinen riskianalyysi, joka ei noudata mitään valmiiksi nimettyä tai yksityiskohtaisesti kuvattua menetelmää.

Perinteisessä riskianalyysissä lähdetään liikkeelle suojeltavasta asiasta. Suojeltavan asian selvittyä mietitään mikä sitä voisi uhata ja mitä voisi tapahtua. Tämän jälkeen arviodaan uhan toteutumisen vaikutuksia kuten kustannuksia tai maineen menetystä. Kun uhan vaikutukset ovat selvillä, lähdetään arvioimaan tämän todennäköisyyttä. Lopuksi selvitetään sopivan suojausmenetelmän hinta ja, jos mahdollista, sen tehokkuus. Näiden avulla voidaan laskea kuinka paljon toteutunut uhka tulisi

maksamaan ja kuinka paljon suojautuminen sitä vastaan maksaisi sekä kuinka tehokas suojautumismenetelmä olisi. (Tiihonen 2014.)

Toinen tapa toteuttaa riskianalyysi on tehdä vikapuuanalyysi. Toisin kuin perinteinen riskianalyysi, vikapuuanalyysin pohdinta lähtee lopputulemista eli uhista joita esimerkiksi järjestelmien toiminnassa voisi tapahtua. Kun uhat ovat tunnistettu, lähdetään etenemään syy-seurausketjua takaperin, kunnes löydetään uhan mahdollisesti aiheuttaneita syitä. Analyysin hahmottamisen apuna käytetään yleensä puuta ja sen eri osia. Uhkien tunnistamiseen tämä menetelmä ei varsinaisesti tarjoa mitään nimettyjä keinoja mutta jos analysoitavalle kohteelle on aiemmin jo tunnistettu uhat, voidaan niitä hyödyntää tässä menetelmässä. (Meriläinen 2003. 9-10.)

5 TUTKIMUS EU:N TIETOSUOJAUUDISTUKSEN VAIKUTUKSISTA LAHDEN AMMATTIKORKEAKOULUN TOIMINTAAN

Tutkimuksen lähtökohtana oli selvittää kuinka uusi tietosuojauudistus vaikuttaa nykyisiin toimintatapoihin Lahden ammattikorkeakoulussa. Tutkimuksessa keskityttiin tarkastelemaan henkilötietojen suojaukseen ja turvaamiseen liittyviä asioita. Tutkimuksessa käytettiin induktiivista lähestymistapaa.

Tutkimus toteutettiin henkilöhaastatteluina. Haastattelut olivat vapaamuotoisia ja niissä käytettiin kolmea eri teemaa: aiempi osaaminen ja perehdytys työhön, nykyiset toimintamallit ja EU:n tietosuojauudistus. Haastateltavat saivat tutustua kysymyksiin ennen haastattelua. Kustakin teemasta kysyttiin muutama puolistrukturoitu kysymys ja mahdollisesti tarkentavia kysymyksiä. Kaikki haastattelut tallennettiin, minkä jälkeen ne litteroitiin referoiden. Litteroinnit lähetettiin haastateltaville tarkasteltavaksi ja he saivat tehdä vastauksiinsa muutoksia tai täydennyksiä jälkikäteen sähköpostin välityksellä.

Tutkimukseen osallistui kuusi Lahden ammattikorkeakoulussa työskentelevää henkilöä. Kyseisillä henkilöillä oli hyvä ymmärrys koulun henkilötietojen käsittelystä ja siihen liittyvistä toimintatavoista, koska he työskentelevät niiden parissa tai niihin liittyvissä toiminnoissa päivittäin. Haastateltavien työnkuvat vaihtelivat opintokoordinaattorista henkilöstöpäällikköön asti. Lähes kaikkien haastateltavien mielestä, heillä oli tarpeeksi hyvä ymmärrys tietoturvallisuudesta. Monilla oli, henkilötietojen suojauksen kannalta, työnkuvaan sopiva koulutus ja useilla vielä pitkä työhistoria samankaltaisista työtehtävistä.

Useimmat heistä eivät saaneet nykyiseen työhönsä perehdytystä vaan oppi tuli ikään kuin työn kautta. Osa heistä oli siirtynyt samankaltaisista työtehtävistä nykyiseen, jolloin on saatettu katsoa perehdytys tarpeettomaksi. Kaikkien mielestä tietoturvaportaali tai samantyylinen paikka, jossa olisi kerättynä kaikki tietoturvallisuuteen liittyvät ohjeistukset ja säännöt, olisi tarpeellinen. Erimielisyyksiä tuli siitä, olisiko tämä portaali

Lahden ammattikorkeakoulun oma vaiko esimerkiksi yhteinen Lappeenrannan teknillisen yliopiston kanssa, koska koulujen yhdistyminen on tapahtumassa lähitulevaisuudessa.

5.1 Henkilötietojen suojaus ja sen muuttuminen LAMKissa

Tutkimuksessa selvisi, että henkilötiedot ovat suojattu hyvin Lahden ammattikorkeakoulun henkilörekistereissä. Henkilötietoihin pääsy on rajattu, eri käyttäjien mukaan, kaikissa haastateltavien käyttämissä henkilörekistereissä. Henkilöstöllä ja opiskelijoilla ovat eri käyttöoikeudet järjestelmiin ja henkilöstöllä ne ovat vielä rajattu työtehtävien mukaan. Lisäksi järjestelmissä käytetään suojattuja yhteyksiä ja Föhrin (2017) mukaan esimerkiksi kirjastojärjestelmässä käyttöä on rajattu vain tietyille ip-osoitteille.

Kaikista paitsi Winha-järjestelmästä löytyy ajantasainen rekisteriseloste ja tietojärjestelmäkuvaus (Ahonen 2017). Osa syynä tähän on järjestelmän poistuminen ja korvautuminen toisella järjestelmällä lähitulevaisuudessa. Tietoturvaloukkasten varalle ei ole vielä toimintasuunnitelmaa tai jos on niin haastateltavat eivät olleet siitä tietoisia. Toimintasuunnitelmaa ollaan kyllä tekemässä tällaisten tilanteiden varalle (Ryhänen 2017).

Henkilötietojen suojaus ei tule muuttumaan Lahden ammattikorkeakoulussa tietojärjestelmien suojauksien tai henkilöstön tietojenkäsittelytapojen osalta. Nykyiset suojausmenetelmät tulevat olemaan täysin riittäviä uudelle tietosuoja-asetukselle. Sen sijaan dokumentointi tulee olemaan kaiken ydin tulevassa, tietosuoja-asetukseen littyvässä, osoitusvelvollisuudessa. Järjestelmät ja prosessit tulee olla tarkasti kuvattuna, jotta pystytään osoittamaan yrityksen tietoturvallisuuden ja henkilötietojen suojauksen toteutuminen tarvittavalla tasolla. Koulun tulee päivittää kaikki rekisteriselosteet sekä tietojärjestelmäkuvaukset sekä kartoittaa henkilötietojen käsittelyn nykytila esimerkiksi tietotilinpäätöksellä.

Koulun tulee myös varatua tietoturvaloukkauksiin ja niiden käsittelemiseen, koska jatkossa tietoturvaloukkauksista tulee ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa tapahtumasta. Tähän voidaan varautua tekemällä toimintasuunnitelma loukkausten varalle, jos sellaista ei vielä ole. Tutkimukseen osallistuneet eivät tällaisesta toimintasuunnitelmasta olleet tietoisia.

5.2 Muut velvoitteet

Dokumentoinnin parantamisen lisäksi yrityksen tulee varautua myös uudistuksessa tuleviin tietojen siirtoon ja poistamiseen liittyviin asetuksiin. Lahden ammattikorkeakoulun henkilörekistereistä on mahdollista poistaa tai anonymisoida tietoa vain sellaisista rekistereistä, joissa ei ole viranomaisvelvoitetta.

Lahden ammattikorkeakoulu tekee muiden ammattikorkeakoulujen kanssa jo yhteistyötä näiden uudistuksien osalta (Golnick 2017). Koulut haluavat tehdä yhteisiä linjauksia tietojen siirron ja poistamisen osalta, koska asiasta ei ole vielä ennakkotapauksia tai konkreettisia esimerkkejä. Tietosuoja-asetus on osittain ristiriidassa kouluja koskevan viranomaisvelvoitteen kanssa, jonka takia päätösten kanssa edetään varovaisesti. Näiden henkilörekisterien lisäksi ongelmia tulee olemaan myös HAKA -kirjautumisen kanssa, jossa käyttäjätunnusten tulisi olla koko eliniän kestäviä (Ryhänen 2017).

Lahden ammattikorkeakoulun tulee myös nimittää tietosuojavastaava. Tietosuojavastaavaa ei ole vielä nimitetty, koska koulu on yhdistymässä Lappeenrannan teknillisen yliopiston kanssa mahdollisesti jo vuoden vaihteessa. On järkevämpää odottaa yhdistymisen toteutumista ja sen jälkeen nimittää konsernille yhteinen tietosuojavastaava. Tietosuojavastaava voisi mahdollisesti toimia myös riskienhallintaprosessin omistajana, kuten liitteessä 2 on esitetty.

5.3 Johtopäätelmät

Eu:n tietosuojauudistus muuttaa henkilötietojen käsittelyn kertaheitolla nykyaikaan. Tässä vaiheessa kannattaa viimeistään aloittaa muutoksien valmistelut ja selvitykset. Siirtymävaihe on jo puolessa välissä ja vuosi menee nopeasti muutoksia tehdessä. Tietosuoja-asetus on niin rekisteröidyn kuin rekisterinpitäjän kannalta hyvä asia. Suomen henkilötietolaki on jo kymmeniä vuosia vanha eikä se enää tietyiltä osin vastannut nykymaailman tarpeita. Rekisterinpitäjille se tuo kuluja mutta myös pakottaa heidät tarkastelemaan omia käytäntöjään ja tietoturvansa nykytilaa.

Lahden ammattikorkeakoulussa on tiedostettu tulevat muutokset ja niistä on hiljattain alettu keskustelemaan. Tietosuojauudistusta varten on perustettu oma työryhmä, joka alkaa selvittämään mitä muutoksia koulun toimintaan tulee tehdä. (Iivonen 2017; Golnick 2017) Koulun henkilötietojen suojaus on lähtökohtaisesti hyvällä tasolla. Tekniset suojauskäytännöt ovat niin henkilötietolain kuin uuden tietosuoja-asetuksen vaatimalla tasolla. Muutos henkilötietojen käsittelemisessä tulee näkymään lähinnä ajatusmalleissa ja työskentelytavoissa. Riskiperusteinen lähestymistapa ja vaikutusten arvioiminen pakottavat muuttamaan nykyisiä toimintatapoja, joissa on alettu vasta vahingon tapahtuessa miettimään, että mitä pitäisi tehdä.

Muutosten tapahtuminen vie aikaa, jonka takia ne on aloitettava heti. Muutos riskiperusteiseen lähestymistapaan saadaan käynnistettyä omaksumalla ja toteuttamalla liitteenä 2 olevan tietoturvaohjeistuksen organisatoriset toimenpiteet. Vaikeuksia voi tulla vastaan riskitietoisuuden lisäämisessä, koska isohkoissa organisaatioissa, kuten Lahden ammattikorkeakoulussa, sisäinen viestintä ei tavoita välttämättä koko henkilöstöä.

Nähtäväksi jää miten tarkkaa ja laajaa selvitystä henkilötietojen käsittelystä tulee tehdä osoittaakseen tietosuojaviranomaisille hyvien tietosuojaperiaatteiden noudattamisen. Moni asia tietosuojauudistuksesta

on vielä epäselvää mutta EU:n tietosuojatyöryhmä tulee antamaan ohjeita ja linjauksia näihin vielä siirtymäajan kuluessa. Viimeistään ennakkotapauksien ja muutamien sanktioiden jälkeen nähdään, ne todelliset, tietosuojauudistuksen tuomat haasteet ja vaikutukset.

6 POHDINTA

Opinnäytetyön aihe oli todella ajankohtainen, koska tietosuojauudistuksen siirtymävaihe on nyt puolivälissä. Tietosuoja-asetuksen tuomista muutoksista on noussut paljon keskustelua varsinkin ammattikorkeakouluissa, koska asetus on osittain ristiriidassa viranomaisvelvoitteen kanssa. Rekisteröidyllä tulisi olla oikeus tulla unohdetuksi tai poistaa häntä koskevia tietoja mutta ne tulisi kuitenkin säilyttää viranomaisia varten. Jos EU:n tietosuojatyöryhmä ei selvennä näitä ristiriitoja, tiettyjen rekisterinpitäjien osalta, ennen kuin asetusta aletaan soveltaa, tullaan niiden todelliset vaikutukset näkemään vasta ennakkotapausten kautta. Näiden muutoksien osalta koulujen kannattaa löytää yhteisiä linjauksia ja muutenkin tehdä enemmän yhteistyötä.

Aluksi työhön oli vaikea päästä kiinni ja olisin sen osalta toivonut toimeksiantajalta ja ohjaavalta opettajalta enemmän ohjausta. Kun aiheeseen pääsi sisälle, alkoi lähteitä löytää enemmän ja enemmän. Myös kaksi aihetta teki opinnäytetyöstä hieman työläämpää. Aiheiden yhdistäminen oli toimeksiantajan toive, koska ne sopivat hyvin yhteen. Tietosuojauudistuksesta löytyi vain tuoreita ja lähinnä elektronisia lähteitä, kun taas tietoturvallisuudesta ja riskienhallinasta löytyi paljon myös painettua materiaalia. Materiaalia löytyi paljon myös englanniksi.

Työn tutkimusosuus jäi hieman suppeaksi haastatteluiden vähäisestä määrästä johtuen. Olisi ollut hyvä saada myös haastateltua henkilö kenellä olisi ollut enemmän faktapohjaista tietoa tietosuoja-asetuksen tuomista muutoksista. Esimerkiksi toimihenkilö tietosuojavaltuutetun toimistosta. Haastattelukysymykset olisi pitänyt suunnitella paremmin, koska haastateltavat eivät ymmärtäneet kaikkia kysymyksiä, jonka takia he eivät pystyneet harkita vastauksiaan kunnolla etukäteen. Heille annettiin kuitenkin mahdollisuus muuttaa tai lisätä vastauksiaan jälkikäteen, joka lisää tutkimuksen luotettavuutta.

Tutkimusta voidaan kuitenkin hyödyntää muissa yrityksissä, kun haetaan ideoita riskienhallintaan liittyvissä asioissa. Myös muut

ammattikorkeakoulut voivat työn kautta miettiä omaa henkilötietojen suojauksen nykytilaa ja sitä onko se tarpeeksi kattava tietosuoja-asetuksen kannalta.

Jatkotutkimuksia aiheesta voisi tehdä esimerkiksi kesällä 2018 kun uutta tietosuoja-asetusta aletaan soveltaa. Kuinka paljon ja mitkä asiat muuttuivat? Opinnäytetyön pystyisi myös tehdä kappaleessa 5.1 esitetystä tietotilinpäätöksestä, jolla Lahden ammattikorkeakoulun kannattaisi arvioida henkilötietojen käsittelyn nykytila.

LÄHTEET

Ahonen, A. 2017. Opintohallintojärjestelmän pääkäyttäjä. Lahden ammattikorkeakoulu. Haastattelu 18.04.2017.

Andreasson, A & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Föhr, P. 2017. Tieto- ja kirjastopalvelujärjestelmien pääkäyttäjä. Lahden ammattikorkeakoulu. Haastattelu 19.04.2017.

Golnick, T. 2017. Henkilöstöpäällikkö. Lahden ammattikorkeakoulu. Haastattelu 03.05.2017.

Henkilötietolaki 523/1999. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Iivonen, U. 2017. HR-asiantuntija. Lahden ammattikorkeakoulu. Haastattelu 25.04.2017.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Laki yksityisyyden suojasta työelämässä 759/2004. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Lark, J. 2015. ISO 31000 Risk management [Viitattu 10.03.2017]. Saatavissa: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_31000_for_smes.pdf

Liikenne- ja viestintäministeriö. 2011. Julkisen tietoaineiston saatavuudesta periaatepäätös [Viitattu 10.03.2017]. Saatavissa: https://www.lvm.fi/-/julkisen-tietoaineiston-saatavuudesta-periaatepaatos-784401

Meriläinen, J. 2003. Helsingin yliopisto. Seminaariesitelmä [Viitattu 5.4.2017]. Saatavissa: https://www.cs.helsinki.fi/group/turvasem/papers/merilainen.pdf

OpenText. 2017. Information Security and Privacy [Viitattu 09.03.2017]. Saatavissa: http://www.opentext.com/what-we-do/business-needs/information-governance/ensure-compliance/information-security-and-privacy

Opitietosuojaa.fi. 2017. Blogi [Viitattu 05.04.2017]. Saatavissa: https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Pietikäinen, S. 2013. Tietoturvallisuus - Mitä se on? Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/691

Raggad, B. 2010. Information Security Management. Boca Raton: CRC press.

Ryhänen, J. 2017. ICT-suunnittelija. Lahden ammattikorkeakoulu. Haastattelu 27.4.2017.

Tietosuojavaltuutetun toimisto, 2015. EU:n tietosuojauudistus [Viitattu 09.03.2017]. Saatavissa: http://tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tiihonen, P. 2014. Riskianalyysi. Lahden ammattikorkeakoulu. Oppimateriaali [Viitattu 5.4.2017]. Saatavissa: https://wiki.lamk.fi/display/opewiki/1+Riskianalyysi

Valtiovarainministeriö. 2003. Ohje riskien arvinoinnista tietoturvallisuuden edistämikseksi valtionhallinnossa. Ohje [Viitattu 10.03.2017]. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128

Valtiovarainministeriö. 2009a. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

Valtiovarainministeriö. 2009b. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus

Valtiovarainministeriö. 2009c. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/kayttoturvallisuus1

Valtiovarainministeriö. 2009d. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus

Valtiovarainministeriö. 2009e. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/ohjelmistoturvallisuus

Valtiovarainministeriö. 2009f Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus

Valtiovarainministeriö. 2009g. Vahti-ohjeet [Viitattu 09.03.2017]. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus

Westerman, G & Hunter, R. 2007. IT risk. Harvard Business School Press Series. Boston: Harvard Business School Press.

Viestintävirasto. 2017. Langattomasti, mutta turvallisesti. Raportti [Viitattu 10.03.2017]. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Väistö, H. 2005. Hallinnollinen tietoturvallisuus. Oppimateriaali. DIGMA [Viitattu 09.03.2017]. Saatavissa: http://www2.amk.fi/digma.fi/www.amk.fi/material/attachments/vanhaamk/etuotanto/041005/5h2DTrXIx/Hallinnollinen_tietoturva.pdf

LIITTEET

LIITE 1 Haastattelukysymykset

- Millainen on sinun tietoturvaosaamisesi nykyisessä työtehtävässäsi LAMKissa?
- Olivatko perehdytys ja ohjeistukset nykyiseen työhösi tietoturvan ja tietosuojan kannalta tarpeeksi kattavat?
- Miten LAMK huolehtii henkilöstön tietoturvaosaamisesta? Esimerkiksi onko sinulle tarjottu tietoturvallisuuteen liittyviä kouluttautumismahdollisuuksia tai oletko perehtynyt itsenäisesti tietoturvallisuuteen liittyviin materiaaleihin?
- Olisiko tarvetta LAMK:n omalle tietoturvaportaalille?
- Millaisia henkilörekistereitä vastuualueellasi / edustamassasi toiminnossa käytetään?
    - käyttötarkoitus?
    - mitä henkilötietoja ne sisältävät?
    - mitä henkilötietoja eri toimijat pääsevät katsomaan tai käsittelemään?
    - kuka tai ketkä ovat vastuussa ko. henkilörekistereihin liittyvästä tietoturvasta?
- Miten henkilötietojen suojaus huomioidaan?
- Onko ollut tietoturvaloukkauksia ja jos on, kuinka niitä on käsitelty? Jos ei ole ollut, onko suunnitelmaa, kuinka niitä käsiteltäisiin?
- Onko henkilötiedot mahdollista poistaa rekistereistä sen jälkeen, kun niitä ei enää tarvita?
- Onko nykyisistä henkilörekistereistä tehty ajantasainen rekisteriseloste ja tietojärjestelmäkuvaus?
- Oletko tutustunut uudistukseen, tiedätkö mitkä asiat muuttuvat?
- Miten muutoksiin on varauduttu ja onko niitä alettu jo toteuttamaan?
- Mihin sinun mielestäsi tulisi kiinnittää eniten huomiota? Missä asioissa tulee olemaan haasteita?

LIITE 2 Tietoturvaohjeistus riskienhallinnasta

1. Prosessin omistajan nimittäminen

Yksi henkilö, joka vastaa riskienhallintaprosessista. Tunnistaa, priorisoi, hallitsee ja seuraa riskejä. Kun yksi henkilö on vastuussa prosessista niin yrityksellä selkeämpi fokus riskienhallintaan ja henkilö joka jatkuvasti kehittää prosessia. Prosessin omistajaksi voisi harkita esimerkiksi tietosuojavastaavaa.

2. Riskikategorioiden määritteleminen

Selvästi määritellyt riskit ja riskikategoriat kehittävät riskienhallintaprosessia kahdella eri tapaa. Kategoriat ja niiden määritelmät toimivat tarkistuslistana riskien tunnistamiseen sekä arvioimiseen. Toiseksi ne auttavat organisaation johdon priorisoida ja seurata riskejä ryhmittämällä samanlaisia riskejä organisaation eri alueilla.

3. Riskirekisterin perustaminen

Riskirekisteri dokumentoi ja seuraa kaikkia riskejä. Rekisteristä tulisi löytyä ainakin riskin nimi, kuvaus, riskikategoria, omistaja, vaikutus ja sen todennäköisyys. Rekisteri pitää kirjaa myös mahdollisista toimenpiteistä riskin läpikäymiseen ja niiden edistymiseen. Tärkeintä on riskien seuraaminen niiden vaatimalla tavalla ja riskien vertaileminen.

4. Riskien arvioimisen jatkuva kehittäminen

Jatkuva riskien vaikutusten ja todennäköisyyksien arvioiminen parantaa yrityksen mahdollisuutta vertailla ja priorisoida riskejä laajemmalla skaalalla. Jatkuva lähestyminen laajasti mutta selkeästi määritetyillä kriteereillä on hyvä tapa selvittää riskit, joilla on eniten merkitystä.

5. Käyttäkää hyväksi todettuja käytänteitä

Suositellut ohjelmistokonfiguraatiot, virustorjunnan pitäminen ajan tasalla ja sisäinen valvonta takaavat riskeistä vastaaville henkilöille ”tarpeeksi

hyvän” perussuojauksen, jonka jälkeen nämä henkilöt voivat keskittyä enemmän poikkeustilanteisiin ja niihin varautumiseen.

6. Riskitietoisuuden lisääminen

Riskitietoisuuden luominen lähtee liikkeelle johdon visioista. Tämän tarkoituksena ei ole pelotella henkilöstöä vaan tuoda ilmi millaisia tilanteita voi työssä kohdata ja miten ne tulisi käsitellä. Voidaan toteuttaa esimerkiksi säännöllisillä tiedotteilla intran välityksellä. Pidetään henkilöstö niin sanotusti ajan tasalla.