LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvallisuuden kehittäminen tilitoimistossa

Hirvonen, Lauri

2017 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvallisuuden kehittäminen tilitoimistossa

Lauri Hirvonen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma

Lauri Hirvonen

Tietoturvallisuuden kehittäminen tilitoimistossa

Vuosi 2017 Sivumäärä 69

Tämän opinnäytetyön tarkoitus on ollut selvittää kohdeyrityksen tämän hetken tietoturvallisuustaso sekä puutteet, toimenpiteet halutun tietoturvallisuustason saamiseksi sekä miten toimenpiteet toteutetaan. Tarve opinnäytetyölle ilmaantui, kun tilitoimisto X (nimi muutettu) tunnisti tietoturvallisuuden kehittämistarpeensa. Kehityshankkeen tarkoituksena oli kehittää yrityksen yleistä toiminnan laatua, parantaa kilpailukykyä ja vastata asiakkaiden muuttuviin ja kehittyviin tietoturvallisuustarpeisiin. Hankkeessa tunnistettiin organisaation tietoturvallisuustavoitteet ja määriteltiin organisaation tietoturvapolitiikka. Siihen liittyy tietoturvallisuusprosessien luominen sekä niiden käyttö tietoturvallisuusriskien hallintaan.

Opinnäytetyön tutkimusmenetelminä käytettiin laadullisia menetelmiä kolmen eri tutkimusmenetelmän avulla: teemahaastattelulla, aivoriihellä sekä havainnoinnilla. Tutkimukset toteutettiin vuonna 2016.

Työn teoreettinen pohja saatiin selvittämällä ensin aiheeseen liittyvät termit ja käsitteet, tämän jälkeen selvitettiin tietoturvan osa-alueet. Lisäksi teoreettisessa pohjassa tutustuttiin lainsäädäntöön sekä taloushallintoliiton ohjeeseen hyvästä tilitoimistotavasta. Viitekehyksenä on käytetty VAHTI-ohjeistusta.

Tietoturvajärjestelyjen tarkoitus on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus ottaen huomioon niiden luottamuksellisuus, eheys ja saatavuus ja niihin liittyvät riskit.

Työssä tunnistettiin yrityksen tietoturvariskit ja analysoitiin ja arvioitiin riskien vaikutukset. Näiden perusteella yritykselle luotiin ja otettiin käyttöön tietoturvallisuuspolitiikka ja -ohje, joiden avulla saavutetaan roolit ja vastuut tietoturvariskien hallinnaksi.

Asiasanat: tietoturvallisuus, riskienhallinta, VAHTI, tietoturvan osa-alueet

Laurea University of Applied Sciences **Abstract**
Security Management

Lauri Hirvonen

Development of information security in Accounting Office X

Year 2017 Pages 69

The purpose of the thesis was to review the information security level of the target organization and resolve the measures to obtain the demanded level and the implementation of these measures. The need for the thesis came when accounting office X (name changed) recognized the need to the development of information security. The purpose of the development project was to develop the organization's overall business process quality, improve its competitiveness and respond to changing and evolving information security needs of its customers. The project identified the organization's information security intentions and defined the organization's information security policy. It involves the creation of information security processes and their use for the management of information security risks.

The qualitative methods used in the thesis were three different research methods: theme interviews, brainstorming and observation. The research was carried out in 2016.

The theoretical background of the thesis was obtained by first studying the related terms and concepts by literature research. After that the different areas of information security were researched. In addition, the theoretical background was introduced to legislation and to the Financial Management Association's guideline on good accounting practice. VAHTI guidelines have been used as reference frames.

The purpose of the information security arrangements is to ensure the proper protection of data material, information systems and services, taking into account their confidentiality, integrity and availability and related risks.

The thesis identified organization’s information security risks and they were analyzed and the effects of the risks were evaluated. Based on these, an information security policy and guidance were created and introduced to enable the organization to achieve roles and responsibilities for managing information security risks.

Keywords: information security, risk management, VAHTI, areas of information security

Sisällys

1 Johdanto

Tietoturvallisuus on muuttunut tärkeämmäksi oksaksi organisaatioiden turvallisuutta, jossa perinteisesti on merkityksenä organisaatioiden tietojen luottamuksellisuuden, käytettävyyden ja eheyden takaamisesta. Teknologia kehittyy nopeasti, joten mukana pysyminen vaatii selvästi menetelmien jatkuvaa seuraamista sekä toimenpiteiden kehittämistä. Tietoturvallisuudessa kannattaakin panostaa toiminnan jatkuvuuden varmistamiseen, sillä täydellistä turvallisuutta on mahdotonta saavuttaa. (Elinkeinoelämän keskusliitto 2017.)

Näin ollen teknologian kehittymisen myötä tarvintaan jatkuvaa seuraamista ja toimenpiteiden kehittämistä. Aihe on täten ajankohtainen ja koska tälle työlle oli tilaus, valitsin tämän aiheekseni. Tilanne oli opinnäytetyötä varten sopiva, koska yritys halusi panostaa tietoturvallisuuden kehittämiseen. Aiheesta keskusteltiin yrityksen toimitusjohtajan kanssa ja kiinnostus aiheeseen oli molemminpuolista, sovittiin työn tekemisestä. Tavoitteena oli tehdä tietoturvallisuuden nykytilan kartoitus, tunnistaa tietoturvariskejä sekä kehittämissuunnitelma ohjeistuksen muodossa. Ohjeistukseksi tehtiin tietoturvaohje sekä –politiikka, joka on tämän työn liitteenä (liite 3). Tietoturvaohje sisälsi yksityiskohtaisia salassa pidettäviä ohjeita ja se jätettiin kokonaan tämän opinnäytetyön ulkopuolelle. Ohjeistus tehtiin tunnistettujen riskien ja VAHTI-ohjeiden perusteella.

Opinnäytetyön tietoperustassa kerrotaan ensin kohdeyrityksestä ja sen jälkeen tietoturvallisuudesta ja sen merkityksestä liiketoiminnassa sekä erityisesti tilitoimistoissa. Sitten perehdytään tietoturvallisuuden suunnitteluun osa-alueittain sekä standardeihin ja VAHTI-ohjeisiin. Tämän jälkeen esitellään tutkimusmenetelmät ja tutkimuksen eteneminen. Tämän jälkeen tunnistetaan tietoturvallisuuden uhat osa-alueittain, josta siirrytään kartoituksen tuloksiin ja kehittämistarpeisiin. Lopussa tehdään johtopäätökset ja arvioidaan työn luotettavuutta.

Seuraavassa kerron tarkemmin kohdeyrityksestä, työn tavoitteesta ja lähtökohdista sekä tutkimuksen rajauksesta ja toteutuksesta.

2 Opinnäytetyön tavoite ja lähtökohdat

Opinnäytetyön lähtökohtana on tilitoimiston tietoturvallisuuden kehittäminen. Seuraavaksi kerron tarkemmin kohdeyrityksestä, tutkimuksen rajauksesta ja tutkimusmenetelmistä.

2.1 Kohdeyritys

Opinnäytetyön tutkimuksen kohdeyritys on tilitoimisto. Opinnäytetyössä käytetään vain nimitystä tilitoimisto X, sillä opinnäytetyön julkisuuden vuoksi nimeä ei ole haluttu kerrottavan. Tilitoimisto X on auktorisoitu ja Taloushallintoliiton jäsenyritys (Yrityksen toimitusjohtaja 2015). Yritys on perustettu vuonna 2007 ja sen liikevaihto oli vuonna 2016 lähes kaksi miljoona euroa (Asiakastieto 2017). Yritys työllistää 25 taloushallinnon ammattilaista ja sen toimipaikka on Helsingissä. Tilitoimisto on kasvanut voimakkaasti viime vuosina. Viimeisen 10 vuoden aikana sen liikevaihto on noin kymmenkertaistunut; yli puolet kasvusta on tapahtunut yritysostoin sekä fuusioitumalla. Opinnäytetyön teon aikana yritys on avannut toimipisteet Espoossa ja Turussa. Tilitoimisto on tiedostanut tietoturvallisuuden merkityksen liiketoiminnassaan. Tietoturvallisuus on todettu tärkeäksi elementiksi laadun, luotettavuuden, maineen ja toiminnan jatkuvuuden ylläpitämiseksi. Yritys on myös halukas edelleen laajentamaan toimintaansa, joten tietoturvallisuustietouden ja -politiikan luominen katsotaan merkittäväksi prosessiksi yritystoiminnan kehittämisen kannalta. Tilitoimisto on erikoistunut sähköiseen taloushallintoon ja käyttää mm. ProCountor -kirjanpito-ohjelmistoa, joka toimii pilvipalveluna niin tilitoimistossa kuin asiakkaillakin. (Yrityksen toimitusjohtaja 2015.)

2.2 Tutkimuksen rajaus ja toteutus

Opinnäytetyön tutkimukselle on siis tarve kohdeyrityksen tilitoimisto X:n tarpeista lähtökohdin. Koska opinnäytetyö on kuitenkin rajallinen tutkimus, on sitä rajattu seuraavanlaisesti. Opinnäytetyön tutkimusongelma on, mitkä ovat tarvittavat kehittämistoimenpiteet halutun turvallisuustason saamiseksi. Kyseessä on toimintatutkimus, jossa tavoitteena on ratkaista yhteistyössä käytännön ongelmia ja saamaan aikaan muutosta. Tutkimuksella etsitään ratkaisuja käytännön ongelmiin. (Ojasalo, Moilanen & Ritalahti 2010, 58.)

Opinnäytetyön tutkimusasetelma kohdistuu yrityksen tietoturvallisuuden kehittämiseen kokonaisuutena. Aluksi on tärkeää selvittää tietoturvallisuuden nykytila, jotta kehittäminen on ylipäänsä mahdollista. Tietoturvallisuuden kehittäminen on tilitoimisto X:ssä todettu tärkeäksi, koska yrityksessä on yritysostojen kautta erilaista työkulttuuria ja toimintatapoja, jotka pitää yhtenäistää myös tietoturvallisuuden osalta. Yritys kokee myös tietoturvallisuuden kehittämisen tärkeäksi menestystekijäksi erilaisissa tarjouskilpailuissa, joissa pyydetään esittämään tietoturvallisuuden prosessikuvauksia. Myös joissain tapauksissa tietoturvallisuussertifi-

oinnin puuttuminen saattaa olla poissulkeva tekijä kilpailutuksesta. (Yrityksen toimitusjohtaja 2015.)

Yksityiset yritykset sekä muut vastaavat toimijat eivät yleisesti ole ilman erillistä sopimusta velvoitettuja noudattamaan julkisuuslain hyvää tiedonhallintatapaa tai tietoturvallisuusasetuksen vaatimuksia. Nämä tietoturvavaatimukset on siis huomioitava sopimuksia tehdessä, jolloin se voidaan toteuttaa turvallisuussopimusmenettelyllä. Sopimusmenettelyn malleja on kuvattu VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohjeessa sekä VAHTI 2/2013 Toimitilojen tietoturvaohjeessa. ICT-varautumisen vaatimukset on huomioitava, mikäli ne liittyvät sopimuksen kohteeseen sekä tietenkin organisaation oma hankintoja koskeva ohjeistus on huomioitava. (Valtiovarainministeriö 2014, 34.)

Tietoturvavelvoitteiden noudattaminen voidaan todentaa joko viranomaisen harkinnan mukaan ulkoisella arvioinnilla tai sopijakumppanin itsearvioinnilla huomioiden salassa pidettävien tietojen määrä ja suojaustasoluokka. Mikäli tietoja käsitellään sähköisesti, voi todennukseen liittyä tietojärjestelmän auditointi. Viranomainen voi vaatia tarjouskilpailuun osallistujalta tai voittajaksi valitulta tarjoajalta todistusta yritysturvallisuusselvityksestä. (Valtiovarainministeriö 2014, 34.)

Myös Taloushallintoliitto asettaa vaatimuksia auktorisoidun tilitoimiston osaamiselle, järjestelmille ja toimintamalleille ja valvoo niitä. Palvelujen lähtökohtana pidetään luottamuksellisuutta asiakkaan ja taloushallinnon palveluyrityksen välillä. Taloushallintoliiton jäsenenä tilitoimisto joutuu takaamaan, että sen palvelu on jatkuvaa. Taloushallintoliitto valvoo myös, että tilitoimisto toimii hyvän tilitoimistotavan mukaisesti. Auktorisointi edellyttää muun muassa, että toiminta on lain mukaista ja tietosuojasta annettujen lakien vaatimukset ja suositukset on otettava toiminnassa huomioon. (Taloushallintoliitto 2015.)

Tutkimusongelmaa tukevat seuraavat kysymykset:

- Mikä on tämän hetken turvallisuustaso ja mitkä ovat turvallisuuspuutteet?
- Mihin toimenpiteisiin tulee ryhtyä, jotta haluttu taso saavutetaan?
- Miten nämä toimenpiteet toteutetaan?

Tutkimuskysymyksiä selvittämään on valittu tutkimusmenetelmiksi teemahaastattelu, havainnointi sekä aivoriihi. Teemahaastattelu toteutetaan lomake- ja avoimen haastattelun välimuotona. Lomakehaastattelussa kysymysten muoto ja esittämisjärjestys on täysin etukäteen määritelty, kun taas avoimessa haastattelussa haastateltavan ajatuksia, mielipiteitä ja käsityksiä sitä mukaan kuin ne tulevat esille keskustelussa. Tässä tutkimuksessa käytettävälle teemahaastattelulle on luonnollista, että teemat ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. (Hirsjärvi, Remes & Sajavaara 2010, 208 – 209.) Jotta haastatte-

lujen aikana kaikki mahdollinen informaatio tulee saaduksi, on tutkimuksessa päädytty teemahaastatteluun. Näin ollen haastattelun edetessä on mahdollista esittää tarkentavia lisäkysymyksiä.

Työn toiseksi tutkimusmenetelmäksi on valittu havainnointi. Havainnoinnin avulla saadaan tietoa, toimivatko ihmiset siten, miten sanovat toimivansa. Havainnoinnin suurin etu on se, että sen avulla saadaan tietoa esimerkiksi organisaatioiden toiminnasta ja käyttäytymisestä. (Hirsjärvi ym. 2010, 212 – 213.) Havainnot kohdistuvat toimintaan ja käyttäytymiseen, kuten esimerkiksi siihen, miten tutkittavaa asiaa käytetään tai miten ihmiset toimivat vuorovaikutustilanteissa, jotka liittyvät ilmiöön. Havainnointia voidaan tehdä sekä ihmisten puheesta ja käyttäytymisestä. Tutkijan on pystyttävä objektiivisesti erottamaan omat havaintonsa siitä, mitä muut ihmiset kertovat omista havainnoistaan. Havainnointia voidaan dokumentoida monella eri tavalla, esimerkiksi tekemällä muistiinpanoja, valokuvaamalla tai videoimalla. (Jyväskylän yliopisto 2015.)

Aivoriihi, jota käytettiin työn yhtenä tutkimusmenetelmänä, on luova ongelmaratkaisun standardimenetelmä, jolla on tarkoitus tuottaa ideoita ryhmässä. Ryhmä vetäjän johdolla pyrkii ideoimaan uusia lähestymistapoja tai luomaan ratkaisuja johonkin ongelmaan. Aivoriihi aloitetaan esivaiheella, jossa asetetaan sekä rajataan aivoriihen tavoitteet. Tämän jälkeen lämmittelyvaiheessa tavoite on vapautua ennakkoluuloista ja rajoittavista tekijöistä. Tässä vaiheessa ryhmän vetäjä kertaa toimintaperiaatteet. Ideointivaiheessa aloitetaan ideoimaan vapaasti. Ideoita ei perustella sekä niiden arvioiminen on kielletty. Vetäjä kirjaa tavoitteet näkyville ja niitä pyritään koko ajan yhdistelemään ja kehittämään. Valintavaiheessa syntyneitä ideoita tarkastellaan kriittisesti ja niitä arvioidaan vetäjän ohjeiden mukaan. (Ojasalo ym. 2010, 145 – 147.)

Valitsin aivoriihen tutkimusmenetelmäksi yhdessä ideoimisen vuoksi. Ryhmässämme oli jäsenenä neljä henkilöä. Aivoriihi toteutettiin 22.3.2016 tilitoimisto X:n tiloissa. Jäsenet valikoitiin henkilöstöosastolta, IT-osastolta sekä johdosta tilitoimiston toimitusjohtajan ja henkilöstöpäällikön arvion perusteella. Osallistujat valikoituivat sillä periaatteella, että tavoitteena oli saada kattavasti osallistumaan erilaisissa tehtävissä toimivia työntekijöitä kattamaan organisaation toimintaa. Näin ollen jäsenemme olivat erilaisissa tehtävissä toimivia ihmisiä. Osa henkilöistä oli henkilöä oli yrityksessä uudempia työntekijöitä ja kaksi vanhempaa, jotta esille tuotuihin asioihin ei vaikuttaisi pelkästään jo käytettävät toimintamallit.

Tilitoimisto X on auktorisoitu tilitoimisto, joten Taloushallintoliiton antamia ohjeita ja vaatimuksia tietoturvallisuudesta voidaan pitää pohjana ja alimpana vaatimustasona tietoturvallisuuden kehittämiseen. Sain pyynnöstä Taloushallintoliiton jäsenmateriaalia, johon kuului tietoturvallisuustason määrittelyä koskeva kaavake ja muuta materiaalia. En voi julkaista tätä

materiaalia tämän opinnäytetyön osana, mutta voin viitata näihin dokumentteihin. Kehittämisen osalta käytin VAHTI-ohjeita.

3 Tietoturvallisuuden määritelmä

Perinteisesti tiedon arvoon perustuvassa määritelmässä tietoturvallisuudessa on kolme osatekijää: luottamuksellisuus, käytettävyys ja eheys. Luottamuksellisuus tarkoittaa, että tietojärjestelmien tiedot ovat ainoastaan niihin oikeutettujen henkilöiden käytettävissä. Käytettävyydellä puolestaan tarkoitetaan, että tiedot ovat saatavissa järjestelmästä oikeassa muodossa riittävän nopeasti. Eheys merkitsee laajasti ymmärrettynä, että tietojärjestelmän sisältämät tiedot ovat paikkaansa pitäviä eivätkä sisällä tahallisia tai tahattomia virheitä. (Hakala, Vainio & Vuorinen 2006, 4.)

Tietoturvallisuus on osana organisaation toiminnan laatua. Tietoturvajärjestelyiden tarkoituksena on taata tietoaineistojen, -järjestelmien sekä palveluiden oikeanlainen suojaus niin, että luottamuksellisuuteen, saatavuuteen ja eheyteen liittyvät riskit huomioidaan. Käytännössä siis tämä tarkoittaa, että järjestelmät ja tiedot ovat vain henkilöt, jotka ovat käyttöön oikeutettuja ja hekin vain asianmukaisesti työtehtävissään. Tietojen, järjestelmien sekä palveluiden on myös oltava luotettavia, oikeita sekä ajantasaisia ja niiden on pysyttävä toiminnassa ja oltava saatavilla, kun niitä tarvitaan. Etenkin sähköisissä palveluissa palveluiden käyttö milloin ja missä vain on kasvanut, käyttötavat ovat muuttuneet. (Pietikäinen 2013.)

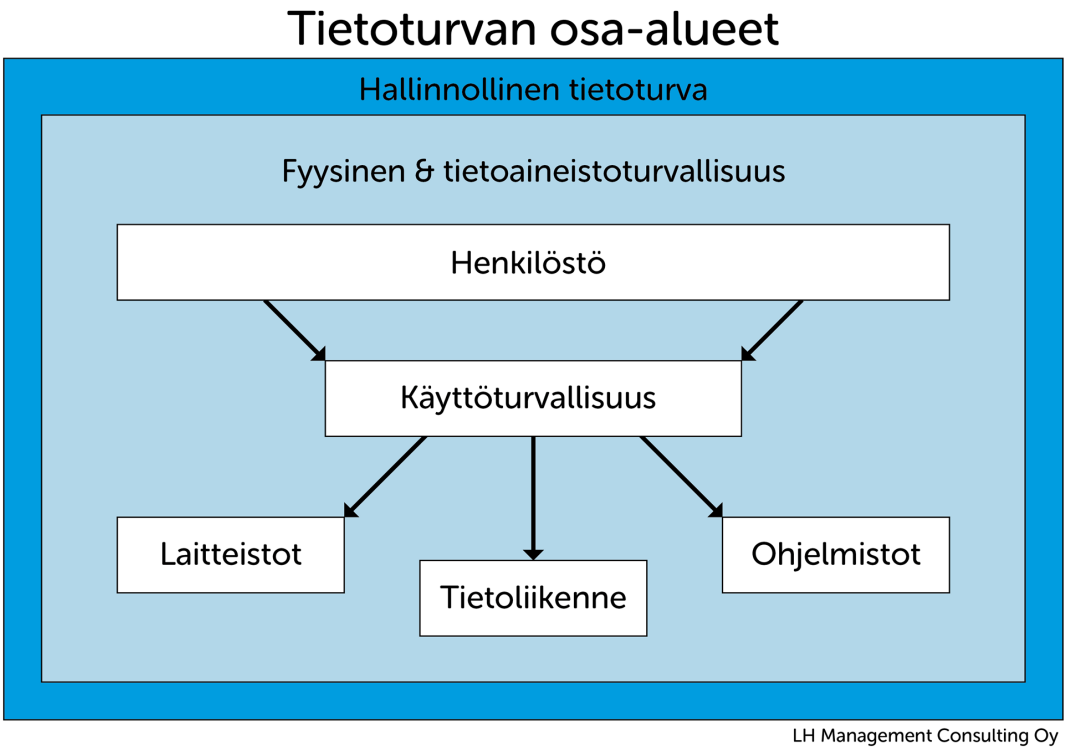
Tietoturvatoimenpiteillä turvataan yksilön ja yhteisön kuin yhteiskunnankin etuja. Tämän vuoksi tietoturvallisuus on yhteiskunnan palveluiden, toimintojen, sovellusten ja infrastruktuurin perusedellytys. Toimintaympäristöt ovat verkottuneet ja siksi harvat organisaatiot ovat vastuussa vain omasta tietoturvallisuudestaan. Jokaisen organisaatiossa työskentelevän velvollisuus on huolehti tietoturvallisuudesta. Yleensä kiire, huolimattomuus, osaamattomuus sekä muut tietojärjestelmien toteutus ja käytön laadulliset tekijät johtavat suurimpiin tietoturvallisuuden ongelmiin. (Pietikäinen 2013.)

3.1 Tietoturvallisuuden osa-alueet

Tietoturvallisuus on yleisesti jaettu kahdeksaan osa-alueeseen (Kuvio 1):

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus

- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus



Kuvio 1: Tietoturvan osa-alueet

Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden tavoitteena on varmistaa tietoturvan kehittäminen sekä johtaminen. Hallinnolliseen turvallisuuteen liittyvät myös yhteydenpito eri elimiin organisaation sisällä, jotka vastaavat turvallisuudesta sekä organisaation ulkopuolella toimiviin viranomaisiin. Erityisen tärkeää on arvioida lainsäädännön ja erilaisten yksityisoikeudellisten sopimusten vaikutusta organisaation tieturvakäytäntöihin. Hallinnollisen turvallisuuden ylläpito yleensä kuuluu organisaation tietohallinnon tehtäviin. (Hakala ym. 2006, 10 – 11.) Hallinnollisilla toimilla ja henkilöstön koulutuksella voidaan saada aikaan merkittäviä tuloksia tietoturvallisuuden kehittämisessä (Puhakainen 2006). Tietoturvatutkimuksen mukaan pk-yritykset keskittyivät tietojärjestelmänsä suojauksessa pääasiassa teknisiin keinoihin, vaikka työntekijöiden tahattomien virheiden ja tietämättömyyden koetaan monesti uhkaavan tietoturvallisuutta eniten. Tutkimuksen mukaan yritykset näkevät merkittävämpänä yksittäisenä tietoturvaongel-

mana työntekijät, joiden osaaminen ja taidot eivät vastaa työn vaatimuksia. (Tietotekniikan liitto ry 2007.)

Henkilöstöturvallisuus

Henkilöstöturvallisuus tarkoittaa henkilöstöstä johtuva riskien hallintaa. Henkilöstöturvallisuuden pohjana on sitoutunut sekä osaava henkilöstö, jolle tietoturvavastuut ja –tehtävät on selvästi kerrottu tehtävänkuvissa. Tärkeimpiä asioita ovat siis prosessit, jotka liittyvät työhönottoon, toimenkuvien merkittäviin muutoksiin sekä palvelusuhteen päättymiseen. Ja näistä prosesseista on oleellista olla kaikilla osallisilla käytössään sovittu toimintamalli. (Valtiovarainministeriö 2007, 57.)

Henkilöstöhallinnon prosessit sekä muut prosessit tarvitaan riittävällä tasoilla määriteltynä, jotta avainhenkilöriskien syntyminen vältetään. Avainhenkilöriskien hallinnassa tunnistetaan toiminnan kannalta avainhenkilöt ja varmistetaan heidän käytettävyytensä eri tilanteissa. Suunnitelmassa huomioidaan etukäteen lomat, poissaolot, työnkierrot sekä väliakaisjärjestelyt riittävän hyvin ja lisäksi valmistetaan henkilöstö poikkeustilanteisiin. Tietoturvallisuuden toteutumiseen myös henkilöstön riittävällä määrällä, työtyytyväisyydellä sekä motivaatiolla on selvä vaikutus. (Valtiovarainministeriö 2007, 57.) Henkilöturvallisuudesta yleensä vastaa henkilöstöhallinto tietohallinnon sekä muiden turvallisuuselinten kanssa (Hakala ym. 2006, 11).

Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on turvata organisaation häiriötön toiminta kaikissa tilanteissa huomioiden tilanteiden erityispiirteet ja riskit. Organisaatiot ovat itse vastuussa omasta fyysisestä suojauksestaan. Tähän tietoturvallisuuden osa-alueeseen kuuluvat esimerkiksi kulun-, kamera- sekä muu tekninen valvonta ja vartiointi sekä ilmastointi-, vesi-, palo-, sähkö- ja murtovahinkojen torjunta. Turvallisuustarpeiden perusteella määräytyvät vähimmäisvaatimukset tilaturvallisuutta lisääville toimille ja järjestelmille. (Valtiovarainministeriö 2007, 59.)

Yleensä toimitilojen hallinta ja turvajärjestelyiden toteutus on kiinteistöhallinnolla tai rakennuksen omistajalla. Kuitenkin käyttäjäorganisaation johto tietää parhaiten sen toiminnot ja niiden käyttämien tietotekniikan turvallisuustarpeet ja johto päättää turvallisuusratkaisuista. (Hakala ym. 2006, 11; Valtiovarainministeriö 2007, 59.)

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisuiden, esimerkiksi lähi- ja laajaverkkojen sekä muiden viestintäjärjestelmien turvallisuudesta. Toiminnasta vastuussa on organisaation tietohallinto. (Hakala ym. 2006, 12.)

Tietoliikennetoiminnot sekä niitä toteuttavat eri verkkojärjestelmät suunnitellaan ja rakennetaan organisaatiossa hyvän tiedonhallintatavan mukaisesti niin, että valittu arkkitehtuuri auttaa varautumista eri uhkia vastaan. Tietoliikenneturvallisuuteen kuuluvat esimerkiksi tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaaminen, käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, huomattavien tietoturvapoikkeamien tarkkailu, kirjaaminen ja selvittäminen sekä tietoliikenneohjelmien testaaminen ja hyväksyminen. (Valtiovarainministeriö 2007, 61.)

Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa laitteistojen suojaamista, asentamista, ylläpitoa sekä poistoa ja niihin liittyvää hallinnointia, jossa laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu määritellään. Yleisestikin laitteistoturvallisuudella turvataan laitteiston elinkaarta. Elinkaareen kuuluu asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja –sopimukset ja turvallinen poisto elinkaaren lopussa. (Valtiovarainministeriö 2007, 63.) Laitteiston turvallisuudesta yleensä vastaa tietohallinto (Hakala ym. 2006, 12).

Palvelusopimuksien palvelun tasoa määrittelevien rajojen ja vasteaikojen sopimisella voi olla suuria vaikutuksia, jotta tietoturvatason saa pidettyä yllä ja jotta tietoturvapoikkeamiin reagoidaan. Erityisesti tämä on tärkeää, jos joko koko palvelu on palvelun tarjoajalla tai osa organisaation laitteistosta sijaitsee siellä. Tilanteessa, jossa laitteisto on toisen osapuolen tiloissa, täytyy kiinnittää huomiota fyysisen turvallisuuden järjestämiseen niissä tiloissa. Laitteiston ylläpidossa huolehditaan, että kaikki tiedot laitteista voidaan palauttaa poikkeaman jälkeen joka käytännössä tarkoittaa, että laitteistojen käyttöjärjestelmistä, ohjelmistoista sekä niiden asetuksista on olemassa varmuuskopiot. Kaikkia järjestelmän laitteita on pystyttävä valvomaan koko ajan ohjelmien avulla sekä niiden käyttöasteiden seuraamista on kyettävä seuraamaan säännöllisesti. (Valtiovarainministeriö 2007, 63.)

Ohjelmistoturvallisuus

Ohjelmistoturvallisuus tarkoittaa käyttöjärjestelmien, varus- ja työkaluohjelmien sekä muiden ohjelmistojen ja sovellusten tunnistamis- ja suojausominaisuuksia, valvonta- ja lokime-

nettelyjä sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. Ohjelmistojen turvallisuuteen vaikuttavat ohjelmistokehityksessä käytetyt prosessit, ohjelmiston käytönaikaiset sekä ohjelmiston palvelualustan asetukset ja käyttäjien koulutus ja ohjeistus. (Valtiovarainministeriö 2007, 69.)

Ohjelmistoturvallisuuteen voi vaikuttaa myös esimerkiksi rajoittamalla käyttäjien ja muiden ohjelmien pääsyä ohjelmiston sisältämään tietoon tietoverkon eriyttämisellä ja parantamalla ohjelmistoympäristön turvallisuutta. Sitä voidaan parantaa esimerkiksi turvapäivityksiä sekä -ohjelmia asentamalla ja käyttämällä järjestelmien turvaominaisuuksia. (Valtiovarainministeriö 2007, 69.) Ohjelmistoturvallisuudesta vastaa yleensä organisaation tietohallinto (Hakala ym. 2006, 12).

Tietoaineistoturvallisuus

Tietoaineistoturvallisuus sisältää tietojen säilyttämiseen, varmistamiseen ja palauttamiseen sekä tuhoamiseen liittyvät toimet. Aineistoihin sisältyvät myös manuaalisen tietojenkäsittelyn asiakirjat ja automaattisen tietojenkäsittelyn tulosteet. Pääsääntöisesti tietoaineistoturvallisuudesta vastaa tietohallinto ja organisaation arkistoinnista vastuussa oleva yksikkö. (Hakala ym. 2006, 11.)

Käyttöturvallisuus

Yrityksen jokapäiväisten toimintojen ja rutiinien turvaamista kutsutaan yleensä käyttöturvallisuudeksi. Käyttöturvallisuuden osa-alue sisältää kaikki manuaalisen sekä automaattisen tietojenkäsittelyn suojatoimenpiteet, esimerkiksi salasanojen hallinnoinnin ja järjestelmien valvonnan ja sen luonteen vuoksi sitä pidetään joskus ylimääräisenä tietoturvan osa-alueena. Yritys itse päättää, haluaako se esimerkiksi dokumentoida salasanakäytännöt useampaan kertaan. Ne voidaan kirjata ohjelmisto- ja käyttöturvallisuuteen tai ainoastaan vain toiseen osa-alueeseen. (Miettinen 2002, 158 – 159; Hakala ym. 2006, 12.)

3.2 Tietoturvallisuuden lainsäädäntö

Tietoyhteiskuntakaari (7.11.2014/917) tuli voimaan 1.1.2015. Lailla kumottiin muun muassa sähköisen viestinnän tietosuojalaki (16.6.2004/516) ja viestintämarkkinalaki (23.5.2004/393) ja siihen on koottu keskeiset sähköistä viestintää koskevat säädökset. Tietoyhteiskuntakaari poistaa siinä olleita päällekkäisyyksiä sekä selkeyttää sääntelyä.

Lain tarkoituksena on edistää sähköisen viestinnän palvelujen tarjontaa sekä käyttöä ja varmistaa, että viestintäverkkoja ja viestintäpalveluja on jokaisen saatavilla maanlaajuisesti

kohtuullisin ehdoin. Tavoitteena on myös lisäksi turvata radiotaajuuksien häiriötön ja tehokas käyttö sekä edistää kilpailua. Niin ikään tarkoitus on varmistaa, että viestintäverkot ja -palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja, turvallisia sekä hinnaltaan edullisia. Lain tavoitteena on sähköisen viestinnän luottamuksellisuuden turvaaminen sekä yksityisyyden suojan toteutuminen. (7.11.2014/917.)

4 Tietoturvan ja –suojan merkitys liiketoiminnassa

Tietoturva ja –suoja ovat Suomen lainsäädännön mukaisesti osa yrityksen päivittäistä toimintaa ja koskee organisaatioiden koko toimintaa sekä henkilöstöä. Yhteiskunta ja yritysmaailma ovat nykyään entistä riippuvaisempia tietojärjestelmistä ja niiden varmuudesta. Tietoturvan tärkeyttä lisäävät esimerkiksi tietojärjestelmien etäkäyttö ja mobiililaitteiden käytön huomattava lisääntyminen sekä pilvipalvelut, joita käytettäessä tietojen sijainti ei välttämättä ole käyttäjän tiedossa. Nyky-yhteiskunnassa tietojen käsittely tapahtuu verkottuneessa ympäristössä ja yritykset ovatkin vastuussa myös itsensä lisäksi muiden tietoturvallisuudesta. Tietoturvallisuus on osa organisaation riskienhallintaa. (Andreasson, Koivisto & Ylipartanen 2013a, 30 – 32.)

Tiedot ja täten tietoturvallisuus ovat nykyään ehdottomia edellytyksiä yrityksen toiminnalle. Tietojen tulee olla oikeita ja luotettavia sekä saatavilla tarvittaessa. Asianmukaisella tietoturvallisuudella turvataan yrityksen toimintaa, yhteiskuntaa sekä asiakkaiden ja sopimuskumppaneiden tietoja. Yrityksen tulee omaan toimintaansa liittyvien tietojen lisäksi huolehtia myös sidosryhmiensä ja asiakkaidensa tiedoista. (Valtiovarainministeriö 2011, 13.)

Tietoturvallisuuden ensisijaisena tarkoituksena on yrityksen vastuulla olevien palveluiden jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietojen, järjestelmien ja palveluiden on pysyttävä toiminnassa sekä niiden on oltava saatavilla kun niitä tarvitaan. (Andreasson ym. 2013a, 32 – 33.)

Hyvin toteutettuna tietoturvallisuus rakennetaan osaksi yrityskulttuuria, jolloin koko henkilöstö ymmärtää tietoturvan merkityksen ja työskentelee sen saavuttamiseksi ja ylläpitämiseksi. Tietoturvallisuus pitää sisällään teknisiä ja hallinnollisia toimenpiteitä, jotka tulee suunnitella huolella lainsäädännön vaatimukset huomioon ottaen ja joiden vaikutuksia tulee seurata toiminnan kehittämiseksi. Hyvän tietoturvallisuustason saavuttaminen ja ylläpitäminen vaatii yritykseltä määrätietoista toimintaa ja johtamista. Tietoturvaa ei tulisi nähdä välttämättömänä pahana, jolla kiusataan työntekijöitä vaan se pitäisi nähdä yrityksen kilpailuetuna. Tämä tietenkin edellyttää että tietoturva on hoidettu asianmukaisesti liiketoiminnan vaatimusten edellyttämällä tavalla. (Laaksonen ym. 2006, 17 – 18.)

Tarpeet tietosuojan huomioimiseen ovat lisääntyneet, koska yrityksissä käsitellään entistä enemmän henkilötietoja. Tietojärjestelmien kehittyessä, yritykset ovat ottaneet käyttöön uusia järjestelmiä. Tietotekniikka tuo yrityksille jatkuvasti uusia mahdollisuuksia, mutta samalla tietojenkäsittelyn sekä yksityisyyden suojaamisen riskit ovat kasvaneet. (Salminen 2009, 18 – 19.)

Liiketoiminnan sähköistyessä pelisäännöt kehittyvät ja monipuolistuvat lainsäädännön kehittymiseen verrattuna. Tietosuojaan liittyvän lainsäädännön vaikutus yrityksissä kasvaa jatkuvasti sitä mukaan, kun uutta sähköistä liiketoimintaa otetaan käyttöön sekä entistä tärkeämmäksi muodostuu asiakastietojen käsittely. (Salminen 2009, 20.)

Sähköisen viestinnän tietosuojalakiin tuli uudistuksia 1.6.2009. Lakimuutos antoi työnantajille oikeuden muun muassa tutkia tiettyjen edellytysten täyttyessä sähköpostiliikenteen tunnistamistietoja. (Andreasson & Koivisto 2013b, 142.) Media reagoi nykyään todella herkästi yritysten aiheuttamiin yksityisyyden loukkauksiin. Yritykselle tällainen negatiivinen julkisuus voi olla hyvinkin haitallista. Yrityksen imagon kolhu voi vaikeuttaa tuotteiden myyntiä sekä aiheuttaa asiakaskunnassa että muissa sidosryhmissä negatiivisia reaktioita liiketoimintaan. (Salminen 2009, 20.)

Menestyvän sähköisen liiketoiminnan edellytyksenä on, että asiakkaat luottavat yritykseen ja uskaltavat antaa omat tietonsa yritykselle. Hyvän liiketoiminnan edellytyksenä on asiakkaiden luottamus. Yrityksen imagosta on tällöin hyötyä. Yrityksen pystyessä osoittamaan asiakkailleen, että se toimii yksityisyyden suojaamisessa vastuullisesti ja luotettavasti, voi saada siitä itselleen merkittävän kilpailuedun suhteessa niihin, jotka eivät ole tätä asiaa huomioineet. (Salminen 2009, 21.)

Asiakasrekisterin arvo on monesti merkittävä osa yrityksen arvoa. Asiakastietojen arvoa voidaan hahmotella esimerkiksi miettimällä, kuinka paljon maksaisi hankkia asiakkuudet uudelleen, jos nykyisiä asiakastietoja ei olisi enää saatavilla. (Salminen 2009, 22 - 23.)

4.1 Kirjanpitolaki

Kirjanpito ja tilinpäätökset täytyy säilyttää 10 vuotta. Myös näiden aineistoa on arkistoitava, tositteet kuuden vuoden ajan. Aiemmin tasekirja piti säilyttää paperisena, mutta uuden kirjanpitolain myötä kaikki aineisto voidaan säilyttää myös sähköisenä. (Taloushallintoliitto 2017.) Muutoksen myötä tasekirja-nimikkeestä luovuttiin ja uudessa laissa siitä käytetään nimeä ”luettelo kirjanpitoaineistosta ja tilinpäätös” (ProCountor 2017). Paperinen kirjanpito pitää yhä arkistoida Suomessa. Sähköinen arkistointi sen sijaan vapautui luvanvaraisuudesta,

mutta aineiston on oltava saatavissa ja tarkasteltavissa Suomesta viipymättä. Aineiston hävittämistavalle ei ole asetettu vaatimuksia. (30.12.2015/1620.)

4.2 Hyvä tilitoimistotapa

Tilitoimistopalveluiden lähtökohtana pidetään luottamuksellisuutta asiakkaan ja taloushallinnon palveluyrityksen välillä. Lisäksi asiakkaan aineisto, liikesalaisuudet ja muut luottamukselliset tiedot, sekä niiden perusteella tilitoimiston tuottama tieto, on turvattava. Tiedon turvaamisella tarkoitetaan teknisiä, fyysisiä ja henkilöiden toimia koskevia menettelyjä. (Taloushallintoliitto 2015.)

Jatkuvasta asiakastiedostojen varmistuksesta pitää huolehtia. Yksittäisten asiakkaiden perus- ja muita tietoja, sekä aineistoa on säilytettävä järjestelmällisellä tavalla asiakaspalvelun sujuvuuden turvaamiseksi. Taloushallintoliitto ohjeistaakin tietojen säilyttämistä kahdella tapaa, sähköinen tallennus sekä pysyväisarkisto ulkoiselle medialle, kuten DVD:lle. Tiedot tallennetaan sähköisesti yhtenäisellä tavalla jatkuvuuden turvaamiseksi. Jokainen asiakkuus tallennetaan omaan kansioonsa, johon luodaan alikansioita. (Taloushallintoliitto 2015.)

Säilytettävää tietoa on ainakin asiakkaan sähköinen aineisto, jota tallennetaan jatkuvasti sähköiseen arkistoon. Viralliset dokumentit tulee tallentaa .pdf –muodossa ja kirje- ja lomakepohjat word- tai excel-muodossa. Tiedostot tulee nimetä yhtenäisesti. Lisäksi sähköpostikirjeenvaihto tulee tallentaa määräajoin sähköisesti omiin kansioihinsa. Lain mukaan säilytettävä aineisto voidaan tallentaa myös sähköisesti ja siirtää sieltä pysyväisarkistoon esimerkiksi DVD:lle. (Taloushallintoliitto 2015.)

Taloushallintoliitto suosittaa kirjallisen salassapitosopimuksen laatimista, joka pätee myös sopimussuhteen päätyttyä ja se on suositeltavaa solmia kaikkien työ- tai sopimussuhteessa olevien kanssa (Taloushallintoliitto 2015).

5 Yrityksen tietoturvan suunnittelu

Tietoturvallisuuden kehittäminen monesti nähdään erillisenä tietohallinnon kehittämiskohteena, jolloin tietoturvallisuus on tietohallinnon tehtävä. Tietohallinnon toteuttaessa tehtävän ilman muiden tahojen sitoutumista, on yrityksen tietoturvallisuussuunnitelma toteutettu pelkästään tietohallinnon toimesta ja näkökulmasta. Tietohallinnolla ei useinkaan ole tarvittavaa kokonaisuuden hallintaa yrityksen toiminnasta. Tietoturvallisuus tulee suunnitella riittävän laajasta näkökulmasta, jotta organisaatioon syntyy vain yksi turvallisuuskulttuuri eikä päällekkäisiä, jopa toimintaa haittaavia prosesseja ja tietoturvajärjestelmiä. On myös mah-

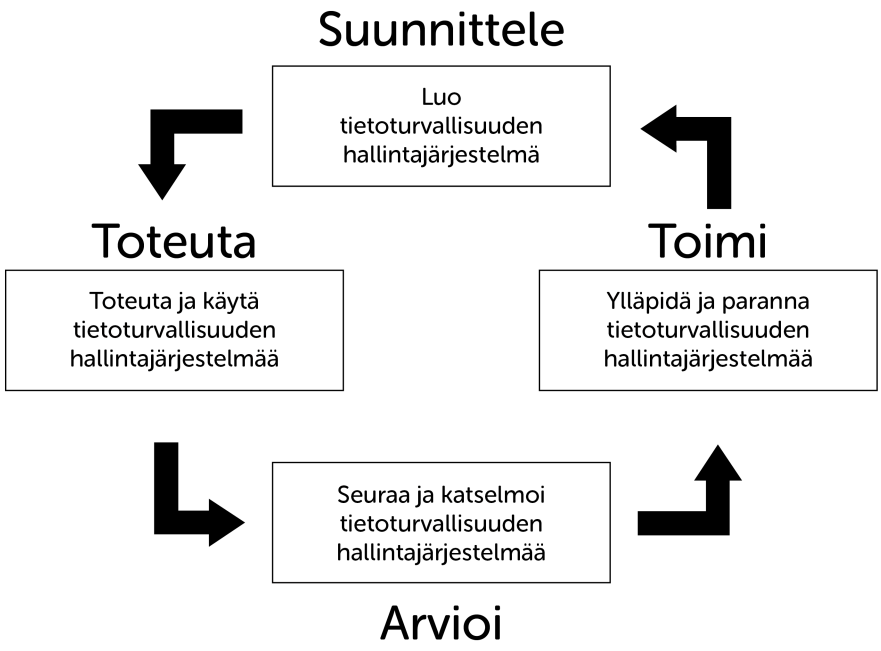
dollista, että suunnitteluvaiheessa prosessit ovat ristiriidassa keskenään. (Hakala ym. 2006, 14, 18).

Tietoturvallisuuden suunnittelu olisi hyvä toteuttaa tiimityönä, jonka jäsenillä on yhdessä riittävä kokonaisnäkemys yrityksen toiminnasta ja sen prosesseista. Usein edes prosessinomistajina toimivat esimiehet eivät ole riittävän tietoisia prosessien yksityiskohdista ja työmenetelmistä. Työntekijöiden ottaminen mukaan suunnitteluprosessiin voi olla hyödyksi paitsi eri näkökulmien huomioimisessa myös tietoturvatietoisuuden leviämisessä yrityksessä. (Hakala ym. 2006, 14, 18).

5.1 Tietoturvallisuuden hallintajärjestelmä

Yritysjohdon tietoturvatyön organisoimiseksi ja helpottamiseksi on kannattavaa luoda erillinen tietoturvan johtamis- ja hallintajärjestelmä. Järjestelmän tulisi kattaa kaikki tietoturvan hallinnoimisessa, johtamisessa sekä valvonnassa tarvittavat menettelyt ja toimenpiteet. Hallintajärjestelmä ei ole pelkästään yksittäinen dokumentti, vaan jatkuvasti kehitettävä prosessi. Yrityksen toimialasta ja koosta riippuen, tärkeimmät hallintajärjestelmän osat ovat riskianalyysi, tietoturvapolitiikka, tietoturva-, jatkuvuus- ja toipumissuunnitelmat. (Valtiovarainministeriö 2003.)

Tietoturvan johtamis- ja hallintajärjestelmän kehittämisessä suositellaan käytettävän PDCA -mallia (Plan-Do-Check-Act). Suomenkielinen vastine on: suunnittele – toteuta – arvioi – toimi. Kuviossa 2 on esiteltynä PDCA-malli. Suunnitteluvaiheessa määritellään suojattavat kohteet, millainen tietoturvan taso yritykselle halutaan ja luodaan tietoturvan hallintajärjestelmä. Toteuttamisen jälkeen arvioidaan ja kehitetään työtä oikeaan suuntaan. Tilanteen muuttuessa toimenpiteet aloitetaan alusta. Näin prosessi on jatkuvaa, joka mahdollistaa kehittymisen. (Hakala ym. 2006, 106.)



Kuvio 2: Tietoturvan hallintajärjestelmän kehittäminen PDCA-mallia soveltaen

5.1.1 Suojattavien kohteiden määrittely

Tietoturvallisuuden hallintajärjestelmän suunnittelu ja käyttöönotto kannattaa aloittaa tavoitteiden määrittelyllä. Ne voivat olla esimerkiksi järjestelmiä tai fyysisiä dokumentteja. Määrittelyn tavoitteena on yrityksen toiminnan kannalta tärkeimpien turvattavien kohteiden suojaaminen. Suojattavien kohteiden dokumentoinnin jälkeen pitää kohteet vielä luokitella kriittisyyden mukaan. Liiketoiminnan kannalta oleellisimmat kohteet on turvattava ensin, joten ne muodostavat tärkeysjärjestyksen kärkipään. Vastaavasti muut laitteet, kuten henkilöstön tietokoneet, sijoittuvat luokittelussa alempiin kategorioihin. (Harju 2010, 23.)

5.1.2 Riskienhallinta

Suojattavien kohteiden määrittelyn jälkeen pohditaan tärkeitä tietoja uhkaavia tekijöitä. Riskienhallinnaksi kutsutaan kaikkia toimenpiteitä, joilla näihin uhkiin pyritään vaikuttamaan. Tässä tutkimuksessa käsitellään kuitenkin vain tietoturvan kannalta oleellisia riskejä. Toisaalta myös vesiputken rikkoutuminen tai tulipalo on riski, varsinkin IT-laitetiloissa. Yrityksen kannattaa luokitella kaikki erilaiset uhat sekä niiden toteutumismahdollisuudet. Tietojen perusteella voidaan tehdä riskianalyysi, jonka tarkoituksena on kartoittaa uhkaavia tietoturvaongelmia. (Suomen Riskienhallintayhdistys ry 2017.)

5.1.3 Tietoturvapolitiikka

Riskianalyysistä paljastuvien asioiden korjaaminen aloitetaan tekemällä tietoturvapolitiikka. Se on yritysjohdon laatima sekä allekirjoittama dokumentti, joka sisältää yleisellä tasolla tietoturvatavoitteet ja -linjaukset. Asiakirja ei sisällä mitään teknisiä ohjeistuksia tai tarkkoja toimenpiteitä, vaan ne sijoitetaan erilliseen dokumenttiin, tietoturvasuunnitelmaan. Politiikan tarkoituksena on henkilöstön motivointi ja rohkaiseminen tietoturvallisempiin toimintatapoihin ja osoittaa, että yritysjohto on mukana prosessissa. (Laaksonen ym. 2006, 146.)

Tietoturvapolitiikka on juuri omalle yritykselle räätälöity dokumentti. Laatimalla oman tietoturvapolitiikan yritys varmistaa juuri itselleen tärkeimpien asioiden huomioimisen ja kirjaamisen. Tietoturvapolitiikkaan dokumentoitavia asioita ovat esimerkiksi yleiset linjaukset, vastuut, koulutukset, tietojen suojaamisen sekä laiminlyöntitapaukset (Laaksonen ym. 2006, 147).

Politiikka on pysyvä tahtotila ja sitä päivitetään, mikäli sille on tarvetta. Politiikkaa tulisi tarkastella säännöllisesti sekä pohtia sen sisältöä. Mikäli muutokselle huomataan tarvetta, johto laatii päivitetyn tietoturvapolitiikan. (Laaksonen ym. 2006, 146.)

Tietoturvapolitiikan avulla johto määrittelee tietoturvatoiminnan toimintalinjat, vastuut sekä tavoitteet. Jokaiselle työntekijälle tietoturvallisuuden merkityksen ja tietoturvatyön periaatteiden määrittely, dokumentointi sekä viestintä on välttämätön perusta tietoturvakulttuurin luomiselle. Tietoturvapolitiikka on perusta, joka toimii pohjana erilaisille tietoturvasuunnitelmille ja –ohjeistuksille. (Valtiovarainministeriö 2007, 25.)

Organisaation toiminnan tarkoitus ja strategia, riskianalyysi, lait sekä määräykset ohjaavat tietoturvapolitiikan luomista. Ylin johto hyväksyy organisaatiokohtaisen tietoturvapolitiikan vahvistaen noudatettavat turva- ja varautumisperiaatteet ja määrittelee vastuut sekä sisäisen toimintaorganisaation. Yksiköiden esimiehet vastaavat turvallisuus- ja varautumisperiaatteiden toteutumisesta tulosohjauksen periaatteiden mukaisesti. (Valtiovarainministeriö 2007, 25.)

Tietoturvapolitiikan valmistelu ja ylläpito on yleensä annettu vastuuksi tietoturvallisuudesta vastaavalle henkilölle. Johto varmistaa, että tietoturvapolitiikkaa tarkistetaan ja päivitetään säännöllisesti kolmen vuoden välein ja toiminnan sekä organisaation muuttuessa. (Valtiovarainministeriö 2007, 25.)

5.1.4 Tietoturvasuunnitelma

Tietoturvasuunnitelma sisältää organisaation tietoturvallisuuden hallinnon järjestelyt, tietojen käsittely- ja käytön valvontamenettelyt, laitteistojen sekä järjestelmien hankintojen tietoturvallisuuden näkökohdat, toiminnan jatkuvuuden varmistamisen ja tietoturvasuunnitelman ylläpidon. Tietoturvasuunnitelmassa organisaatio määrittää tiedon käsittelytavat ja luottamuksellisuusluokat ja siihen tulisi sisällyttää kuvaus henkilöstön koulutuksesta. (Sosiaali- ja terveysministeriö 2007, 17.)

5.1.5 Jatkuvuus- ja toipumissuunnitelma

Poikkeustilanteiden varalle kannattaa laatia jatkuvuus- ja toipumissuunnitelmat. Nämä dokumentit sisältävät kirjalliset ohjeet niistä toimenpiteistä, joilla yritys selviytyy erilaisista ongelmatilanteista. (Laaksonen ym. 2006, 227.)

Poikkeustilanteisiin varautuminen ja niiden hoitamisen keinot määritellään jatkuvuussuunnitelmassa. Riskien tiedostaminen sekä hallinta ja tärkeiden liiketoimintaprosessien palauttaminen normaaliin on myös tärkeä osa suunnitelmaa. Jatkuvuussuunnittelu on kokonainen prosessi, joka vaatii kehitystä sekä ylläpitoa. Mahdollisimman kattavan suunnitelman tekemiseen on yritysjohdon lisäksi myös tietohallinnon ja muiden osastojen syytä osallistua. (Raggad 2010, 217.)

Jatkuvuussuunnitelmien lisäksi olisi hyvä tehdä toipumissuunnitelmia. Yleensä kyseisellä termillä tarkoitetaan niitä toimenpiteitä, joilla palautetaan yksittäisiä osia prosesseista. Esimerkkinä voidaan pitää palvelinympäristöjä. Jokaista asennettua järjestelmää varten olisi hyvä olla oma toipumissuunnitelma, joka sisältää keinot toimintaan palauttamiseksi. Toipumissuunnitelmat tulee myös testata ja varmistaa, että ne toimivat oikein myös käytännössä. (Raggad 2010, 217 – 218.)

5.2 Tietoturvallisuusriskien arviointi

Riskien arviointi on todella tärkeä osa organisaation riskien hallintaa. Se on lisäksi keskeinen osa jatkuvaa tietoturvatyötä. Riskien arvioinnilla käsitetään niitä suunnitelmallisia toimenpiteitä, joilla yritetään tunnistaa uhkat ja haavoittuvuudet sekä arvioida mahdollisien uhkien seuraukset. (Valtiovarainministeriö 2003.)

5.3 VAHTI-ohjeet

VAHTI on asetettu toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä valtiovarainministeriön taholta. Valtiovarainministeriö kehittää sekä vahvistaa VAHTIn toimintaa ja tuloksellisuutta, jotta digitaalisen ympäristön tuleviin uusiin haasteisiin pystytään vastaamaan paremmin. (Valtiovarainministeriö 2017a.)

VAHTIn päämääränä on tietoturvallisuutta kehittämällä parantaa valtiohallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTIn toiminnalla on huomattavasti parannettu tietoturvallisuutta valtion lisäksi myös yrityksissä sekä kansainvälisesti. (Valtiovarainministeriö 2017b.) VAHTI-ohjeita on monia erilaisia ja ne sisältävät kattavasti erilaisia ohjeistuksia.

5.4 Standardit

Halutessaan yritys voi hakea todistusta tietoturvallisista toimintatavoistaan, tällöin kyse on tietoturvallisuuden hallintajärjestelmän sertifioinnista. ISO (International Organization for Standardization) on organisaatio, joka on määritellyt sertifioinnissa vaadittavat kriteerit. Tietoturvallisuuden hallintajärjestelmän vaatimukset ovat kuvattuna ISO/IEC 27001 -standardissa. Sertifiointivaiheessa yritykseltä vaaditaan laajaa dokumentaatiota tietoturvan hallintajärjestelmästä. (Laaksonen ym. 2006, 106.)

Virallisten ISO-standardien hankkiminen on maksullista, mutta silti kannattavaa. Internetistä on saatavilla hyviä ilmaisia teoksia, kuten esimerkiksi suomen kielellä laadukasta materiaalia tarjoaa valtiohallinnon VAHTI –työryhmä, jota käytetään tämänkin opinnäytetyön pohjana. He ovat julkaisseet lukuisia tietoturvallisuuteen liittyviä ohjeistuksia ja suosituksia, jotka ovat vapaasti luettavissa. (Valtiovarainministeriö 2017a.) Vaikka virallinen sertifikaatti ei olisikaan tavoitteena, kannattaa yrityksen silti tutustua mahdollisimman moneen aiheeseen liittyvään dokumenttiin ja ohjeistukseen.

6 Työn tutkimusmenetelmät ja tutkimuksen eteneminen

Tapaustutkimuksen lähtökohdat ovat tieteellisen tutkimuksen strategiassa ja se on tyypillinen tutkimusstrategia esimerkiksi liiketaloustieteissä. Tapaustutkimus soveltuu kehittämistyön lähestymistavaksi, kun tavoitteena on tuottaa kehittämisideoita ja –ehdotuksia. Tutkimuksen kohteena eli tapauksena voi olla yritys tai osa siitä, prosessi, palvelu, toiminta tai tuote. Ta-

paustutkimus tuottaa tietoa ilmiöstä nykyajassa sen todellisessa toimintaympäristössä ja tilanteessa. (Ojasalo ym. 2010, 52.)

Tapaustutkimuksen tavoitteena on tuottaa yksityiskohtaista ja syvällistä tietoa tutkittavasta tapauksesta. Tapaustutkimuksessa on oleellisempaa saada selville tarkemmasta asiasta paljon kuin laajasta vähän. Tutkimuksessa on tarkoitus selvittää kuinka jokin tapahtuu ja on mahdollista eikä sitä, kuinka yleistä jokin on. Tapaustutkimus vastaa kysymyksiin ”miksi?” ja ”miten?”. Tapaustutkimuksella ei pyritä tilastolliseen yleistämiseen eikä se ole otos joukosta. Tutkimuksessa huomioidaan siis ajalliset ja paikalliset, sosiaaliset tilanteet ja yhteydet. (Ojasalo ym. 2010, 52 – 53.)

Tapaustutkimus voi auttaa ymmärtämään työntekijöiden välisiä suhteita ja toimintaa yrityksessä. Se sopii myös hyvin epävirallisen käyttäytymisen ja prosessien tutkimiseen. Tutkimuksen kohteita on vähän, monesti vain yksi, kuten esimerkiksi organisaatio, tapahtuma, toiminto tai prosessi. (Ojasalo ym. 2010, 53.)

Tapaustutkimukselle ominaisia piirteitä on, että monia menetelmiä käyttämällä saadaan monipuolinen, kokonaisvaltainen ja syvällinen kuva tapauksesta. Tapaustutkimus toteutetaan usein laadullisena tutkimuksena ja menetelmänä. Tutkimusaineistot kerätään usein esimerkiksi havainnoimalla ja analysoimalla kirjallisia aineistoja. Havainnointia voidaan käyttää myös todellisiin tilanteisiin, jolloin tilanteisiin johtaneita syitä voidaan analysoida. Haastatteluja käytetään myös yhtenä tiedonhakumenetelmänä, koska tapaustutkimus liittyy usein ihmisen toiminnan tutkimiseen erilaissa tilanteissa. (Ojasalo ym. 2010, 53.)

Tutkimus aloitettiin tekemällä laaja kirjallisuustutkimus tietoturvallisuudesta ja sen perusteista. Tilitoimisto oli tietoturvallisuuden kehittämisessä alussa, joten kirjallisuustutkimuksen jälkeen aloitettiin tutkimus sekä havainnoimalla suojeltavia kohteita sekä haastattelemalla tilitoimiston riskeistä tilaajayrityksen henkilöitä. Tässä tavoitteena oli nimenomaan kartoittaa suojeltavat kohteet ja riskienhallinta ja löytää ongelmille uudet toimintamallit, jonka pohjalta saatiin rakennettua uusi tietoturvallisuuspolitiikka sekä –ohje.

6.1 Havainnointi tilitoimisto X:ssä

Tutkimus aloitettiin sopimalla yhteinen aika tilitoimisto X:n kanssa. Havainnoinnin aikana kävimme tilitoimiston X:n tilaajan kanssa yhdessä läpi nykyisen tilanteen valtiohallinnon ohjeen VAHTI 7/2003 mukaan.

Havainnointiin oli sovittu aika tilitoimiston toimipaikkaan. Tutkimuksesta oli tiedotettu henkilöstölle sekä kerrottu, miksi tutkimus tulee ja mitä siinä tehdään. Tavoite oli havainnoida ih-

misten käyttäytymistä sekä tarvittaessa kysyä tarkentavia kysymyksiä henkilöstöltä. Vaikka havainnointi koskikin käyttäytymistä ja ihmisten vastauksia, huomio kiinnittyi kuitenkin lisäksi muutamiin fyysisen turvallisuuden osiin, joita nostettiin sitten myöhemmin esille haastatteluissa tarkentavia kysymyksiä ja myös toimenpide-ehdotuksia varten.

6.2 Haastattelut

Havainnoinnin jälkeen haastattelin tilitoimisto X:n henkilöstöä yrityksen tavoitteista sekä mahdollisista uhkista. Haastattelut toteutettiin maaliskuussa 2016.

6.3 Aivoriihi

Aivoriihi pidettiin kaksi kertaa, joissa molemmilla kerroilla osallistujina lisäkseni oli tietohallintojohtaja sekä henkilöstöpäällikkö. Toisella kerralla mukana oli myös toimitusjohtaja. Hyvänä lisänä aivoriiheen olisi ollut vielä lakiosaston johtaja, mutta hän ei valitettavasti päässyt kummallakaan kerralla osallistumaan. Aivoriihinä olivat skenaariomenetelmä, tarkistuslista, potentiaalisten ongelmien analyysi sekä haavoittuvuusanalyysi.

6.3.1 Skenaariomenetelmä

Skenaarioanalyysissä käydään läpi erilaisia tilanteita, joiden avulla pyritään mahdollisten uhkien tunnistamiseen. Analyysissä aloitus tapahtuu skenaarioiden luomisella. Tähän vaiheeseen on suositeltavaa ottaa mukaan henkilöstöä eri yksiköistä ja tehtävistä sekä eri alueiden erityisosaajia. Skenaarioiden laadinnassa on hyvä hyödyntää tietoja läheltä piti -tilanteista sekä aiemmin mahdollisesti sattuneista tietoturvavahingoista. Apuna voidaan käyttää myös tietoturvaan liittyvää yleistä aineistoa. Analyysin seuraavassa vaiheessa laadittujen tapausten pohjalta pyritään saamaan kuva suojausten nykytilasta sekä mahdollisista tietoturvapuutteista. (Valtiovarainministeriö 2003, 27.)

Ensimmäisessä tapaamisessamme, jossa läsnä oli henkilöstöpäällikkö sekä tietohallintojohtaja, aloitettiin uhkien kartoittaminen. Ensin keskusteltiin vapaasti tietoturvallisuusasioista. Tästä johdatin keskustelun skenaarioihin, joissa käytiin läpi tilitoimisto X:ssä tapahtuneita lähellä piti –tilanteita sekä sattuneita vahinkoja. Aluksi keskustelu ei edennyt halutulla tavalla, mutta kerrottuani heille esimerkinomaisesti muutamia tapauksia muun muassa kannettavan tietokoneen katoamisesta aiheutuvista toimenpiteistä ja siihen liittyvistä riskeistä keskustelu vapautui ja kaikki keskustelijat ymmärsivät nopeasti, mistä oli kysymys.

Tietohallintojohtaja osasikin nopeasti kertoa heille tapahtuneesta tapauksesta, jossa tietokone piti viedä huoltoon, koska se ei enää käynnistynyt. Tähän liittyi huoli tiedoista, joita koneella oli ja niiden joutumisesta mahdollisesti organisaation ulkopuolelle.

Henkilöstöpäällikkö kertoi riskistä, jota heillä liittyi oman henkilöstön vuokraamiseen asiakasyrityksille ja tähän liittyvästä mahdollisesta aivovuodosta ja liiketoiminnan tappiosta, mikäli työntekijä rekrytoitaisiin suoraan asiakasyrityksen palvelukseen. Tutkija nosti myös esille havainnon liittyen neuvotteluhuoneiden läpinäkyvyyteen sekä asiakkaiden pääsyn työtiloihin.

6.3.2 Tarkistuslistat

Tarkistuslistojen avulla voidaan uhka kerrallaan tarkastella, liittyykö uhka tarkasteltavan organisaation toimintaan. Tarkistuslista on hyvä väline karkeaan ongelmakohtien paikallistamiseen sekä uhkien tunnistamiseen. Tarkistuslistoja voidaan myös käyttää muistilistoina, kun mietitään uhkien vaikutusta organisaatiossa. Tarkistuslistat eivät ole täydellisiä, joten käytettäessä niitä on syytä miettiä, kattavatko ne organisaation liittyvät keskeiset uhat. Useissa VAHTI-ohjeissa on julkaistu tarkistuslistoja, joita voidaan käyttää apuna uhkien tunnistamisessa. (Valtiovarainministeriö 2003, 29.) Tämän opinnäytetyön teossa käytettiin VAHTI 2003:n liitteen 2 mukaista tarkistuslistaa (liite 1).

Ensimmäisen tapaamisen alussa pyysin molempia keskusteluun osallistuneita henkilöitä täyttämään VAHTI 2003:n liitteen 2 mukaisen tarkistuslistan ja lähettämään sen minulle täytettynä. Tästä sain pohjaa hahmottaakseni, mitä asioita organisaatio kokee tarpeelliseksi tietoturvallisuuden osalta ja mitkä asiat eivät koske organisaatiota.

Tarkistuslistat osoittivat, että ohjelmistoturvallisuus oli hyvillä kantimilla, koska käytettävät ohjelmat toimivat selainpohjaisesti, ulkopuolisen palveluntarjoajan tarjoamina palveluina. Suurimmaksi heikkoudeksi osoittautui hallinnollinen tietoturvallisuus.

6.3.3 Potentiaalisten ongelmien analyysi

Potentiaalisten ongelmien analyysi on uhkien tunnistamiseen tarkoitettu tehokas menetelmä. Uhkien tunnistamiseen edellytetään avointa mieltä ja erilaisten kokemusten ja näkemysten yhdistämistä. Tarkistuslistojen käyttö tai tavallinen keskustelu ei täytä näitä vaatimuksia. Potentiaalisten ongelmien analyysi (POA) on tehokas menetelmä riskien luovaan ideointiin ja käsittelyyn ryhmässä. (Valtiovarainministeriö 2003, 26.)

Potentiaalisten ongelmien analyysissa on useita eri vaiheita. Analyysi laaditaan ryhmätyönä POA:n vetäjän johdolla. Kohteen koosta tai asiasisällöstä riippuen joudutaan pitämään mah-

dollisesti useita kokouksia. Analyysin toteutuksen edellytyksenä on, että organisaation johto antaa tukensa analyysin laadintaan sekä mahdollistaa siihen tarvittavat resurssit. POA aloitetaan valitsemalla tarkasteltava kohde. Valintaperusteet ja rajaukset esitellään loppuraportissa. (Valtiovarainministeriö 2003, 26.)

Toisessa tapaamisessa oli läsnä tietohallintojohtaja, henkilöstöpäällikkö sekä toimitusjohtaja. Kerroin etukäteen, että tapaamisen tarkoitus oli tehdä potentiaalisten ongelmien analyysi ja avasin analyysin tekotavan. Lisäksi pyysin henkilöitä käymään läpi täyttämänsä tarkistuslistan, jotta orientoituminen tilaisuuteen käynnistyisi varhaisessa vaiheessa.

Toimin tilaisuuden vetäjänä ja osallistui itsekin analyysin aivoriiheen. Aluksi kerrottiin, mitä tulemme tekemään ja mitkä ovat seuraavat vaiheet. Useaan otteeseen mainitsin, että tarkoitus on vain saada mahdollisimman paljon erilaisia uhkia, joiden todennäköisyyksiä voidaan sitten arvioida myöhemmin. Kaikille henkilöille jaettiin eri värisiä post-it lappuja ja ohjeistettiin jokaiselle lapulle kirjattavan yhden uhkan tai riskin. Työskentely aloitettiin yksilötyönä, ja aikaa annettiin noin viisi minuuttia lappujen kirjoittamiseen. Tilanteessa meni hiukan pidempään, koska en halunnut keskeyttää ajatustyöt. Halusin aloittaa yksilötyönä, jotta kukin osasto (HR, IT ja johto) voisi tuoda omaan yksikköönsä tai itselleen mieleen tulevia asioita ilmi eikä ajatus siirtyisi toisen esittämään uhkaan.

Kun laput saatiin täytettyä, kirjattiin ne exceliin ja luettiin samalla ääneen. Ohjeistin, että jos tässä vaiheessa tulee mieleen vielä jotain, kirjaa sen lapulle eteensä. Osa lapuissa olevista uhkista oli samoja, joten niitä ehdottaneiden määrä kirjattiin myös exceliin. Tämän jälkeen käytiin vielä samalla menetelmällä läpi uudet lapuille kirjatut uhkat.

Erilaisia uhkia kartoitettiin yhteensä noin 50 kappaletta. Tämän jälkeen vielä keskusteltiin havaituista uhkista yhteisesti. Osallistujat, minut pois lukien, olivatkin todella innokkaita löytämistämme uhkista ja alkoivatkin jo suunnitella omatoimisesti jatkotoimia ja huomasin, kuinka tutkimuksen jo tässä vaiheessa tietoturvallisuuden kehittäminen organisaatiossa oli ajatustasolla alkanut.

Tulosten kirjausten jälkeen mietittiin, mistä riski johtuu ja mitä riski toteutuessaan aiheuttaa sekä kuinka todennäköinen riski on. Tunnistettujen riskien osalta luotiin mitta-asteikko. Mitta-asteikossa oli kaksi tasoa: taloudellinen vaikutus ja todennäköisyys. Jokaiselle riskille saatiin näin määriteltyä numeraalinen vastine kuvaamaan todennäköisyyttä sekä taloudellista vaikutusta. Todennäköisyyttä sekä taloudellista vaikutusta saatava mitta-asteikko haarukoitiin kartoittamiemme riskien perusteella viisiportaiseksi (taulukko 1). Kertomalla luvut keskenään, saatiin jokaisen riskin suuruutta kuvaavan riskiluvun. Työn tilaajan toiveesta painotettiin taulukossa taloudellista vaikutusta kertomalla ensin sitä kuvaavan suhdeluvun itsellään ja vasta

tämän jälkeen todennäköisyydellä. Riskilukujen jälkeen järjestettiin taulukko niin, että riskit tulivat allekkain alkaen suurimman riskiluvun saaneesta riskistä, riskiluvun pienentyen alaspäin.

Todennäköisyys	Suhdeluku	Taloudellinen vaikutus*
kerran viidessä vuodessa	1	0 - 300 €
< kerran vuodessa	2	301 - 2 000 €
kaksi kertaa vuodessa	3	2001 - 8 000 €
kuukausittain	4	8001 - 50 000 €
viikoittain	5	50 001 - 1 000 000 €

Taulukko 1: POA:n mitta-asteikko

Riskien lajittelun jälkeen toimitusjohtajan johdolla päätettiin kunkin tunnistetun riskin kohdalla vastuuhenkilö ja –taho, joka vastaa vastuulleen tulevan riskin hallinnasta. Tässä yhteydessä käytiin läpi myös riskienhallintakeinoja yleisellä tasolla. Potentiaalisten ongelmien riskitaulukko on tämän opinnäytetyön liitteenä (liite 2).

Jaotteluiden yhteydessä tehtiin vielä haavoittuvuusanalyysin yrityksen toimintaan liittyen. Lisää tästä vaiheesta seuraavassa kappaleessa.

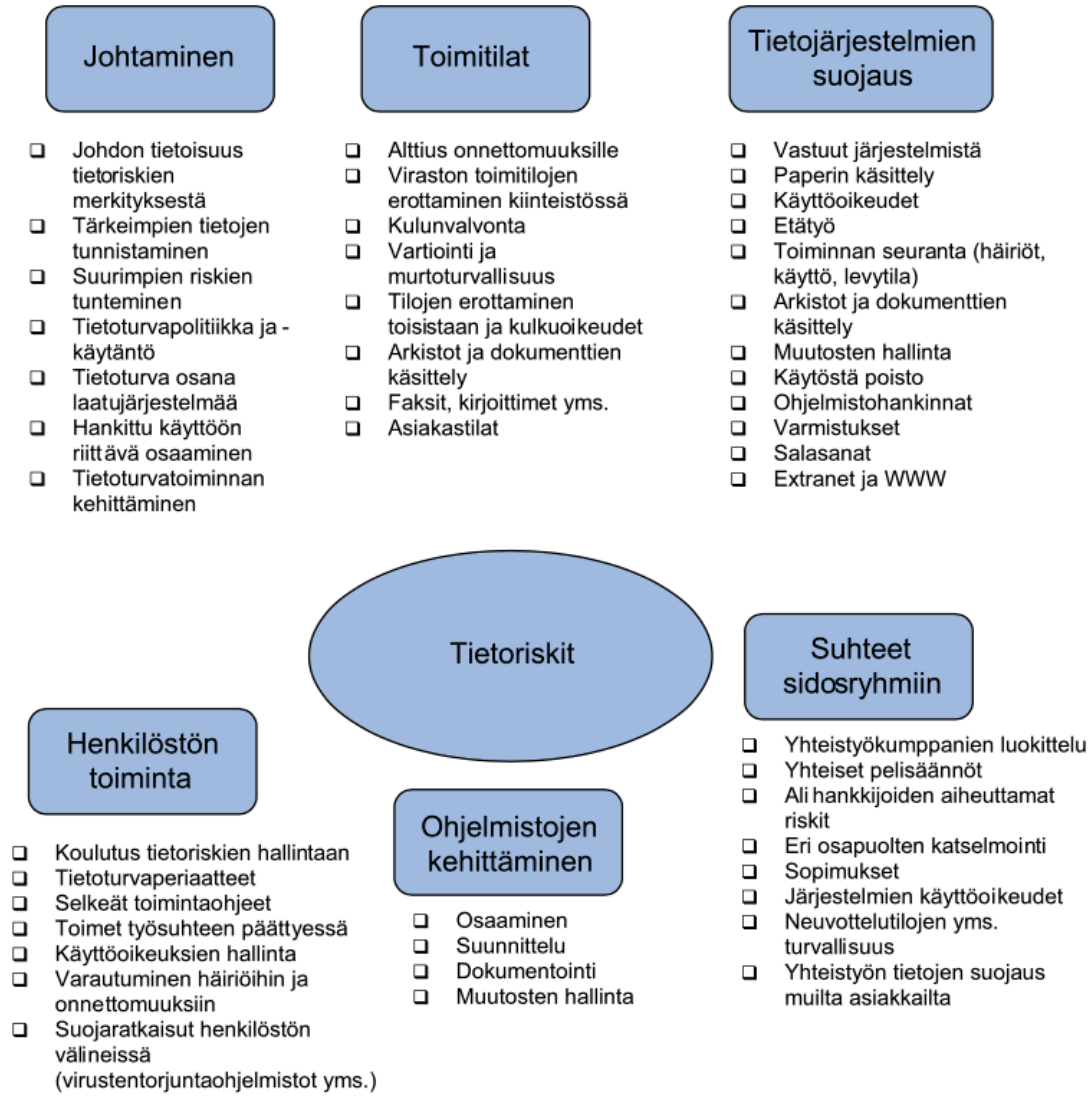
6.3.4 Haavoittuvuusanalyysi

Haavoittuvuusanalyysillä kartoitetaan riskien hallintaan liittyvää epävarmuutta, joka uhkaa organisaation toimintaa. Haavoittuvuusanalyysin näkökulma on tulevaisuudessa ja siinä pyritään tarkastelemaan, miten jatkossa tullaan selviämään. Myös kokemuksista ja tapahtuneista kannattaa ottaa opiksi. Tarkastelemalla myös muille tapahtuneita vahinkoja ja tilanteita saadaan vihjeitä omista vahvuuksista ja heikkouksista. Haavoittuvuusanalyysissä voidaan tarkastella kokonaisuuksien toimintaa, jolloin siihen voi esimerkiksi sisältyä toiminnan organisointi, toimintaedellytykset, sidosryhmät, henkilöt, omaisuus ja talous. (Valtiovarainministeriö 2003, 27.)

Haavoittuvuusanalyysillä tunnistetaan osa-alueet, joihin liittyvät kaikista suurimmat riskit ja siten selvittää riskejä tarkemmin sekä toteuttaa riskejä vähentäviä toimenpiteitä. Tietoturvallisuutta koskevassa haavoittuvuusanalyysissä voidaan käyttää apuna tietoriskikarttaa (kuvio 3). Riskikartan avulla tarkastellaan tietoturvallisuuden osa-alueita ja mietitään mahdollisia uhkia. (Valtiovarainministeriö 2003, 28.)

Haavoittuvuusanalyysissä käytettiin VAHTI 2003 –ohjeessa olevaa tietoriskikarttaa. Karttaa läpikäydessä emme kartoittaneet enää uusia riskejä, joita emme olisi jo POA:ssa löytäneet.

Tietoriskikartta kuitenkin helpotti vastuiden jaon suunnittelua, koska siinä on valmiiksi jaoteltu tietoriskit omiin kategorioihinsa. Osasimme tämän perusteella luontevasti jakaa vastuut omille osastoilleen.



Kuvio 3: Tietoriskikartta (Valtiovarainministeriö 2003, 28)

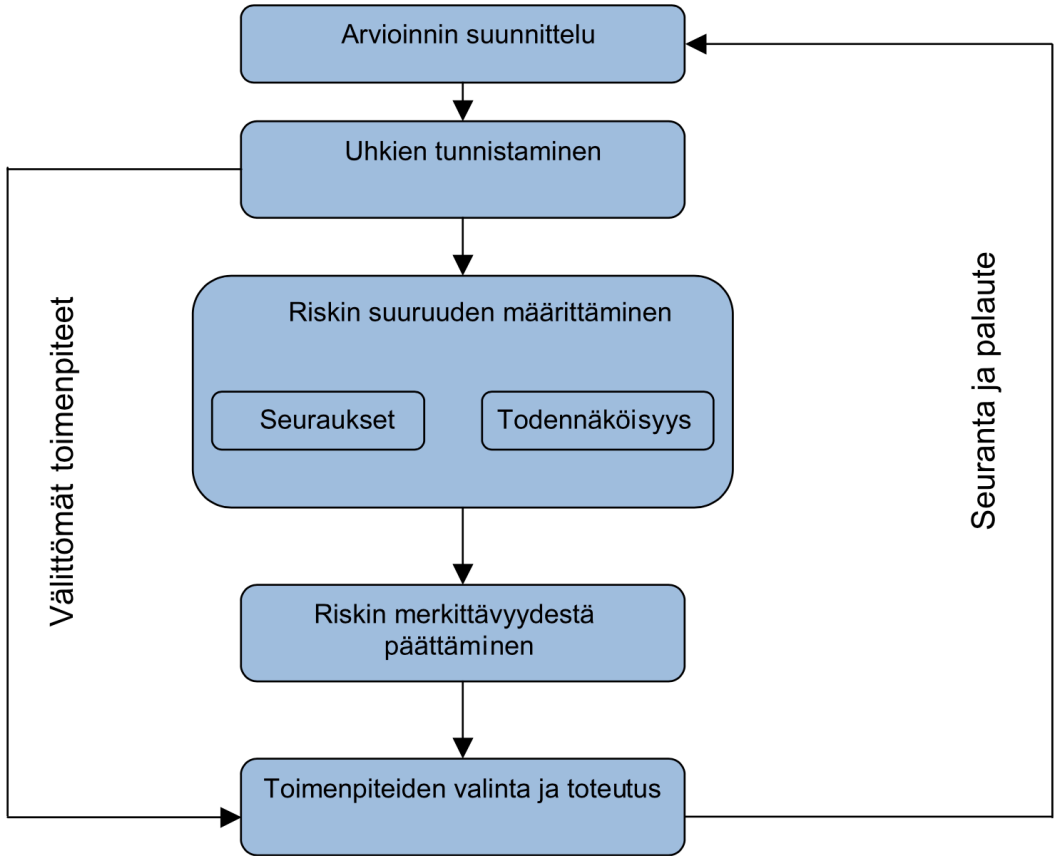
6.4 Toimenpiteet

Havainnoinnin sekä haastattelujen jälkeen kartoitin tilanteen olemassa olevan kirjallisuuden ja tutkimusten perusteella ja toteutin tilaajan tavoitteiden mukaisen tietoturvapolitiikan sekä tietoturvasuunnitelman ja -ohjeen. Tein työn tilaajalle ehdotelman, kuinka yritys voi myöhemmin itsenäisesti tarkastella ja tarkistaa näiden toteutumista sekä jatkuvuutta tietoturvallisuuden hallintajärjestelmän mukaisesti.

Seuraavassa kappaleessa esitellään tietoturvallisuuden uhkien tunnistaminen osa-alueittain, tietopohjaan pohjautuen. Tämän jälkeen esitellään kartoituksen perusteena tehty tietoturvapolitiikka sekä –ohje.

7 Tietoturvallisuuden osa-alueiden uhkien tunnistaminen

VAHTI 7/2003 mukaisesti riskien arviointi ja uhkien tunnistaminen toteutettiin kuvion 4 mukaan haastattelemalla organisaation ICT-vastaavaa (tietohallintojohto) sekä henkilöstöpäällikköä (ylin johto). Uhkien tunnistamiseen käytettiin tarkistuslistaa, skenaariomenetelmää, haavoittuvuusanalyysiä sekä potentiaalisten ongelmien analyysiä. Tulosten perusteella tehtiin riskitaulukko, jossa painotettiin riskin toteutumista kertomalla toteutumisen riskiluku itsellään.



Kuvio 4: Riskien arvioinnin ja hallinnan vaiheet (Valtiovarainministeriö 2003, 16)

7.1 Hallinnollinen tietoturvallisuus

Vahti 6/2006 –ohjeistuksen mukaisesti tietoturvallisuuden kehitystyö on jaettu kypsyysvaiheisiin (taulukko 2) (Valtiovarainministeriö 2006, 33). Organisaatio on kypsyysvaiheessa ”aloitta-

va". Aluksi organisaatiolle tehtiin uhka- ja riskianalyysi. Riskien tunnistamiseen käytettiin havainnointia, haastatteluja sekä tarkkailua ja aivoriihiä. Riskien analysoitiin käytettiin muun muassa työkaluna potentiaalisten ongelmien analyysiä.

Tietoturvallisuuden kehitystyön kypsyysvaihe ja niihin soveltuvat arviointimenetelmät				
1. Aloittava	2. Toistettava	3. Määritelty	4. Hallittu	5. Optimoituva
Riskienhallinta COSO-ERM malli[3] (ks liite, lähde 11) Ohje riskien arvioinnista tietoturvallisuuden kehittämiseksi valtionhallinnossa. VAHTI 7/2003.	Arvioinnit tietoturvallisuuden osa-alueittain, esim. Valtion keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.	Hallintajärjestelmä dokumentoitu. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. VAHTI 3/2003.	Toiminalle on asetettu tulosmittarit ja tietoturvastandardeja sovelletaan vakiintuneesti.	Toiminnanjatkuva sisäinen ja ulkoinen arviointi ja mittaaminen. Benchmarking.
Ohje tietoturvallisuuden arvioinnista valtionhallinnossa. VAHTI ohje, 2006.				
Muutos ja tietoturvallisuus. VAHTI -ohje, 2006.				

Taulukko 2: Tietoturvallisuuden arviointi eri kypsyysvaiheissa.

7.2 Fyysinen turvallisuus

Havainnointi- sekä haastattelututkimuksen tuloksena havaittiin, että tiloihin pääseminen oli helppoa, sekä asiakkaat pääsivät työtiloihin, joissa tietoaineistoa käsiteltiin. Lisäksi neuvotteluhuoneet olivat lasiseinistä johtuen liian avoimet ja paljastivat niissä olevat henkilöt. Tässä ajateltiin mahdollisten asiakkaiden suhtautumista kilpailijoihinsa sekä heidän anonymiteettiään. Tiloissa toimi myös toinen yritys ilman fyysistä rajaa. Vartioinnin laatu sekä hälytysjärjestelmän ja kameravalvonnan puuttuminen myös havaittiin. Myöskään onnettomuuksien tai ilkivallan varalle ei ollut jatkuvuussuunnitelmaa.

7.3 Henkilöturvallisuus

Aivoriihen ja riskien tunnistamismenetelmien perusteella havaittiin, että työntekijöillä ei ole salassapitositoumuksia eikä kilpailukieltosopimuksia. Tämä on iso riski, mikäli joku työntekijöistä perustaisi kilpailevan liiketoimen tai siirtyisi kilpailijalle töihin. Myös kiire ja osaamattomuus nousivat riskienhallinnan kohteiksi.

7.4 Tietoaineistoturvallisuus

Tilitoimistossa käsitellään yritysten tietojen lisäksi myös henkilötietoja muun muassa palkanmaksun ja sen oheistoimien yhteydessä. Palkka- ja henkilötietoja pääsivät käsittelemään kaikki tilitoimiston kirjanpitoa tekevät henkilöt. Osa ohjelmistoista ja lisensseistä on hankittu

Euroopan talousalueen ulkopuolisilta toimijoilta, joka asettaa vaatimuksensa henkilötietojen käsittelylle (Henkilötietolaki 523/1999 22 §). Tilitoimistolla oli myös toisessa sijainnissa vanha paperiarkisto, jonka tietoja ei ollut missään muualla saatavissa.

7.5 Ohjelmistoturvallisuus

Ohjelmistot sekä lisenssit on ostettu ulkopuolisilta toimijoilta, joista osa toimii Euroopan talousalueen ulkopuolella. Näiden toimintojen auditointi on osittain rajattu tämän opinnäytetyön ulkopuolelle. Ohjelmistot toimittavat tahot vastaavat omalta osaltaan tietoturvallisuudesta sekä niiden toiminta on heidän omasta puolestaan tarkastettu. Tämä osuus jätettiin opinnäytetyön ulkopuolelle. Kaikilla käyttäjillä oli ohjelmistoihin pääkäyttäjäoikeudet, eikä niitä oltu mitenkään rajattu. Kaikki työntekijät näkivät siis esimerkiksi kaikkien asiakkaiden tiedot.

7.6 Laitteistoturvallisuus

Tilitoimistossa on käytössä kannettavat tietokoneet sekä kaikilla työntekijöillä on yrityksen puolesta hankittu matkapuhelin. Tietokoneet olivat PC-tietokoneita, joissa oli Windows 7 asennettuna. Matkapuhelimina oli joko Android- tai iOS- käyttöjärjestelmää käyttäviä laitteita eri valmistajilta. Yrityksellä ei ole omaa palvelinta, vaan se on vuokrattu suomalaiselta palveluntarjoajalta, joka omalta osaltaan vastaa laitteen tietoturvallisuudesta. Palvelimen tietoturvallisuus on rajattu tämän työn ulkopuolelle.

Tilitoimistossa ei ollut käytössä yhtenäistä linjaa laitteiden salaukselle tai suojaukselle salasanalla tai muulla biometrisellä tunnisteella. Laitteita ei voitu myöskään sulkea tai tyhjentää etäkäytöllä. Käytössä ei ollut myöskään ohjattua varmuuskopiointia tai haittaohjelmien torjuntaohjelmia.

7.7 Tietoliikenneturvallisuus

Tietoliikenne perustui toimistossa WLAN-tekniikkaan, joka oli salaamatonta sekä samoilla tukiasemilla oli myös vierailijaliikennettä. Henkilöstö teki myös etätöitä, eikä käytössä ollut tällöinkään salattua yhteyttä.

8 Kartoituksen tulokset ja kehittämistarpeet

Havaittiin, että kehitettävää oli kaikilla tietoturvallisuuden osa-alueilla. Näistä kriittisimmät olivat potentiaalisten ongelmien analyysin mukaan kannettavan tietokoneen katoaminen, neuvotteluhuoneiden avoin näkyvyys, asiakkaiden pääsy työntekijöiden tilaan sekä työnteki-

jöiden salassapidon rikkominen. Kaiken kaikkiaan tehdyssä uhkien kartoituksessa noin 50 erilaista uhkaa tai riskiä, joista riskienhallintatoimenpiteitä kohdistetaan noin 40:een. Suurin osa riskeistä keskittyi henkilöstön toimintaan sekä laitteiden turvallisuuteen.

Hallinnollisessa tietoturvallisuudessa havaittiin eniten puutteita, johon keskittymällä saataisiin henkilöstöä ohjeistamalla ja kouluttamalla henkilöihin liittyviä riskejä pienennettyä.

Työn tuloksena organisaatiolle luotiin tietoturvallisuuspolitiikka sekä ohjeistus. Organisaation pyynnöstä ohjeistus jätetään kokonaan julkaisematta. Tietoturvallisuuspolitiikka on tämän opinnäytetyön liitteenä (liite 3)

Kehittämistarpeet

Hallinnollinen tietoturvallisuus

Suurimmat kehityskohteet liittyivät hallinnolliseen tietoturvallisuuteen. Tietohallinto ei ollut omatoimisesti alkanut kehittämään tietoturvallisuutta, vaan pääpaino oli liiketoimintaprosessien hallinnassa. HR- ja lakiosaston tulisi toimia tiiviimmin yhteistyössä uusien henkilöiden palkkauksessa, erityisesti avainhenkilöiden kohdalla tapahtuviin rekrytointiprosesseihin. Näissä pitäisi huomioida sopimussakot sekä erilaiset kilpailukieltoasiat. Yhtenä ajatuksena oli tilitoimiston kanssa projektiluontoisen turvallisuuspäällikön palkkaaminen, joka loisi prosessikuvaukset ja tarvittavat dokumentit yhdessä eri osastojen kanssa. Turvallisuuspäällikkö voisi myös tehdä tietoturvallisuuden kannalta tarvittavien toimintojen hankintaesitykset, hankintojen kilpailutuksen sekä valvoa niiden toimeenpanon. Lisäksi turvallisuuspäällikkö voisi tehdä jatkuvia auditointeja liiketoiminnan eri osa-alueille ja osastoille ja huolehtia kehitystyön ohjautumisesta yhdenmukaisesti koko organisaation tasolla.

Fyysinen tietoturvallisuus

Toinen, samat tilat jakanut yritys muutti toisiin tiloihin, jolloin tilitoimiston kanssa ei ollut enää yhteisiä tiloja. Neuvotteluhuoneiden lasiseinät teipattiin valoa läpäisevällä kalvolla, joka kuitenkin esti henkilöiden tunnistettavuuden. Molemmat toimenpiteet suoritettiin saatujen tulosten perusteella opinnäytetyön teon aikana. Tilojen kamera- sekä hälytysvalvonnan hankinnan suunnittelua aloitettiin. Vartioinnin todettiin olevan riittävällä tasolla. Kulunvalvontajärjestelmän käyttöönotto parantaisi vielä tietoturvallisuutta kulkujen rekisteröitymisen kautta ja mahdollisia väärinkäytöksiä olisi helpompi selvittää myöhemmin. Kameratallenteiden säilyvyys on kuitenkin rajallista päälle tallennuksen takia.

Henkilöturvallisuus

Henkilöstölle pitäisi järjestää koulutusta työhönoton yhteydessä sekä säännöllisesti esimerkiksi vuosittain. Koulutuksen tulisi sisältää ainakin tilitoimiston käytänteet tietoaineiston turvallisesta käsittelystä, tilojen käytöstä sekä salassapitoasioista. Koulutusten lisäksi tulisi järjestää tietoiskuja tietoturvallisuudesta esimerkiksi tietoturvallisuuskysely, joka on järjestetty selainpohjaisesti ja se pitäisi uusia kunnes kaikki vastaukset ovat oikein. Lisäksi avainhenkilöt pitäisi sitouttaa yhtiöön kilpailukieltosopimuksin ja salassapitositoumuksin. Avainhenkilöille voisi vielä lisäksi asettaa karenssin, jonka puitteissa he eivät voisi aloittaa kilpailevaa liiketoimintaa tai siirtyä kilpailijalle. Avainhenkilöillä tulisi lisäksi olla avoin osakkeiden omistamispolitiikka, eli heidän tulisi ilmoittaa kaikki omistuksensa ja muut sivutyöt työnantajalleen.

Tietoaineistoturvallisuus

Tietoaineistojen käsittelyä ja oikeuksia rajattiin sekä uusia ohjelmia otettiin käyttöön ja paperisen arkiston skannausprojekti otettiin suunnittelun alle jo tämän opinnäytetyön teon aikana. Yleisestikään tietoaineistoa ei oltu luokiteltu eikä aineiston käsittelystä oltu tehty prosesseja, joten se on yksi tietoaineistoturvallisuuden pääteemoista. Pysyväisarkistosta olisi helpointa hankkiutua eroon skannaamalla dokumentit sähköiseen muotoon, jolloin riskit aineiston säilyvyyden suhteen poistuisivat.

Ohjelmistoturvallisuus

Ohjelmistojen osalta ei nähty tarpeelliseksi aloittaa kehitystöitä, koska tilitoimistolla ei ole omia ohjelmia.

Laitteistoturvallisuus

Tietokoneiden ja matkapuhelimien käyttöön liittyen olisi tarpeellista saada niihin käyttöön salaus, kryptaus sekä tunnistautumiseen tarvittava koodi tai biometrinen tunniste. Myös laitteiden varmuuskopiointi ja etätyhjennys ja paikantaminen toisivat lisäturvallisuutta.

Tietoliikenneturvallisuus

WLAN-verkosta ei haluttu luopua sen helppouden takia, mutta yrityksen verkko ja vierailijaverkko tulisi eriyttää omilla tukiasemillaan. Lisäksi työasemiin sekä matkapuhelimiin pitäisi asentaa haittaohjelmien torjunta- ja suojausohjelmisto sekä liikenteen salaava VPN-yhteys. Myös tietoliikenteen toimivuuden varmistamiseksi tulisi hankkia varayhteys esimerkiksi mobiiliverkkoa hyödyntäen ja tuplavarmistuksena kahdelta eri operaattorilta.

9 Johtopäätökset

Tietoturvallisuuden kehittäminen tilitoimisto X:ssä oli kokonaisvaltainen katsaus ja kehittämistyö tilitoimiston tietoturvallisuuteen. Kokonaisuudessaan kohdeyrityksen tietoturvallisuus nojasi pitkälti teknisiin järjestelyihin, mutta niissäkin oli rutkasti kehittämisen varaa. Tutkimuksessa tuli myös ilmi useita hallinnollisia ongelmia sekä prosessien ja niiden kuvausten puutteita. Voimakkaan kasvun ja konsolidaatioiden myötä yhtenäisen yrityskulttuurin rakentamiseen oli panostettu, mutta prosessit ja tietoturvallisuus olivat jääneet pienen yrityksen tasolle. Kasvun myötä ja henkilöstön uudelleen organisoinnin seurauksena nyt oli mahdollista tehdä jokaiselle tietoturvallisuuden osa-alueelle ohjeistus ja vastuuhenkilöt sekä toimintaa yleisesti ohjaava tietoturvallisuuspolitiikka. Myös tietoturvallisuuden hallintajärjestelmän laadinta aloitettiin opinnäytetyön tulosten ja havaintojen pohjalta. Liitteenä tässä työssä on yritykselle laatimani tietoturvallisuuspolitiikka (liite 3), jonka johto on hyväksynyt. Laaditut tietoturvallisuusohjeet salataan kokonaan oppilaitokselta ja julkaisulta, koska yritys ei antanut lupaa niiden käyttöön opinnäytetyön osana.

Kehittyminen

Opinnäytetyön aiheena oli tietoturvallisuuden kehittäminen ja tavoitteena alkukeskusteluissa oli saada tietoturvallisuuden tasoa nostettua. Muutamia konkreettisia toimintoja saatiinkin tehtyä jo opinnäytetyön teon aikana, mutta monet prosessit, kuten henkilöstön koulutus ja tietoiskut jäävät organisaation harteille. Lähdeaineistoon perehtyminen ja katsaus sitä kautta johdon osallistuminen tietoturvallisuuteen strategian osana oli mielestäni merkittävimpiä aikaansaannoksia, vaikka niiden tulokset ovatkin seuraavassa vaiheessa tämän opinnäytetyön valmistumisen jälkeen. Vastuiden jako ja tietoturvallisuuden nykytilanne avasi ylimmän johdon silmät tietoturvallisuuden johtamiselle ja tätä kautta johtamisjärjestelmän kehittämiselle tietoturvallisuuspolitiikan pohjalta. Opinnäytetyö nostikin hyvin esille puutteita ja kehitettäviä asioita.

Yrityksen tietojärjestelmät ja palvelimet oli ostettu lisensseinä tai leasing-sopimuksina vastuullisilta toimittajilta, joka pienensi ohjelmistoihin ja täten muun muassa asiakkaiden tietoihin liittyviä riskejä omalta osaltaan.

Opinnäytetyön tärkeimpinä tuloksina tietoturvallisuuden osalta olivat hallinnolliseen tietoturvallisuuteen liittyvät kehitystarpeet. Tietoturvallisuuden taso yrityksessä oli kypsyystason mukaisella asteikolla kohdassa aloittava.

9.1 Tutkimuksen arviointi ja luotettavuus

Haastatteluihin ja aivoriiheen osallistuneet henkilöt olivat hyvin valittu työn tavoitteisiin nähden. Vaikka kaksi osallistujaa olivatkin olleet työsuhteessa yritykseen alle kaksi vuotta, oli heillä vankkaa osaamista eri organisaatioista työkokemuksensa puolesta. Alussa tietoturvallisuus koettiin pelkästään tekniseksi tietoturvallisuudeksi, joka pienensi osallistujien intoa, mutta projektin käynnistyessä he hahmottivat millaisesta kokonaisuudesta on kyse. Mielestäni tutkimuksen tavoitteisiin päästiin hyvin ja tietoturvallisuuden nykytilanne sekä turvallisuuspuutteet tulivat kattavasti arvioitua. Tarvittavat kehitystoimet ovat laaja-alaisia eikä organisaatiolla ole välttämättä mahdollisuutta toteuttaa niitä kaikkia, liittyen esimerkiksi tilaratkaisuihin ja sopimusasioihin. Tilat ovat vuokratiloja ja niihin tarvittavien muutosten tekeminen voi olla jopa mahdotonta vuokranantajan ne kieltäessä. Myöskään henkilöstön ei jo työsuhteessa ollessa tarvitse allekirjoittaa heitä rajoittavia sopimuksia niin tahtoessaan. Jo yhden työntekijän kieltäytyessä koko prosessi voi vesittyä. Johto oli kuitenkin sitoutunut tietoturvallisuuden kehittämiseen ja uskonkin yrityksen saavan tietoturvallisuustasonsa nostettua hallintajärjestelmän, tietoturvapolitiikan sekä –ohjeistuksen avulla.

9.2 Kehitysehdotukset ja mahdolliset jatkotutkimukset

Organisaation tietoturvallisuuden kehittyessä, olisi hyvä tehdä uusia kartoitustutkimuksia ja verrata jo saatujen riskienhallintatyökalujen käyttöä ja aikaan saatuja muutoksia esimerkiksi puolen vuoden välein. Kun jo havaitut riskit on saatu hallintaan, voisi tietoturvallisuutta auditoida esimerkiksi Katakrin tai sertifikaatin mukaisesti ja näin löytää uusia kehityskohteita. Tilitoimiston kanssa olikin jo puhetta, että tällaisia jatkotutkimuksia voisi tulevaisuudessa tehdä. Tietoturvallisuuden saavuttaessa esimerkiksi Katakrin ”elinkeinoelämän suositus” –tason tai IV-tason, voisi olla ajankohtaista nostaa tietoturvallisuutta tasoa ylöspäin. Jokainen näistä vaiheista, varsinkin auditointivaiheissa, olisi hyvä tutkimuksen kohde. Lisäksi vuosittain voisi järjestää henkilöstökyselyn ja tiedustella, miten he ovat kokeneet tietoturvallisuuden uudistukset. Myös yksiköiden esimiehiltä pitäisi saada jatkuvaa palautetta, kuinka he kokevat muutokset ja miten ne tulisi toteuttaa ilman, että yrityksen ydinprosessit hidastuvat tai hankaloituvat. Lisäksi prosesseja voisi testata järjestämällä skenaarioharjoituksia ja saada henkilökunta tajuamaan tilanne. Benchmarkkaamalla jokin muu yritys tai useita yrityksiä voitaisiin saada selville hyviä käytänteitä liittyen muun muassa hallinnolliseen ja henkilöturvallisuuteen. Valitettavasti en saanut alan isommista toimijoista ketään osallistumaan benchmarkkaukseen.

Lähteet

Asiakastieto. 2017. Viitattu 15.4.2017. https://www.asiakastieto.fi/web/fi/

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013a. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma Oy.

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

Elinkeinoelämän keskusliitto. 2017. Tietoturvallisuus. Viitattu 18.4.2017. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/tietoturvallisuus/

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

Harju, E. 2010. Tietoturvasta huolehtiminen on elinehto. Varsinais-Suomen Yrittäjä 3/2010.

Henkilötietolaki 523/1999

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010 (15. – 16. painos). Tutki ja kirjoita. Hämeenlinna: Kariston Kirjapaino Oy.

Jyväskylän yliopisto. 2015. Havainnointi eli observointi. Viitattu 15.4.2017. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/havainnointi-eli-observointi-osallistuminen-ja-kenttaetyoe

Kirjanpitolaki. 1620/2015.

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

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2010 (1. – 2. painos). Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro Oy.

Pietikäinen, S. 2013. Tietoturvallisuus - mitä se on? Viitattu 18.4.2017. https://www.vahtiohje.fi/web/guest/691

Procountor. 2017. Kirjanpitolaki uudistui. Viitattu 12.5.2017. http://blog.procountor.com/kirjanpitolaki-uudistui

Puhakainen, P. 2006. A design theory for information security awareness. Väitöskirja. Oulun Yliopisto. Viitattu 20.4.2017. http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf

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

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Talentum Media Oy.

Sosiaali- ja terveysministeriö. 2007. Julkaisu 2007:19. Tietoturvallisuussuunnitelman laatiminen. Opas sosiaali- ja terveydenhuollon toimintayksiköille. Helsinki: Yliopistopaino.

Suomen Riskienhallintayhdistys ry. 2017. Mistä riskienhallinnassa on kysymys. Viitattu 12.3.2017. http://pk-rh.fi/index.php?page=riskienhallinta

Taloushallintoliitto. 2015. Hyvä tilitoimistotapa. Viitattu: 5.3.2015. https://taloushallintoliitto.fi/laatu-tyokalut/hyva-tilitoimistotapa

Tietotekniikan liitto ry. 2007. Pk-tietoturvatutkimus. Viitattu: 10.4.2015. http://www.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/PK-tietoturvatutkimus/pk-yritysten%20tietoturvakysely%202007.5.21_SZ.pdf

Tietoyhteiskuntakaari. 917/2014.

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003. Helsinki: Edita Prima Oy.

Valtiovarainministeriö. 2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. VAHTI 6/2006. Helsinki: Edita Prima Oy.

Valtiovarainministeriö. 2007. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI 3/2007. Helsinki: Painopaikka Edita Prima Oy.

Valtiovarainministeriö. 2011. Johdon tietoturvaopas. VAHTI 2/2011. Juvenes Print - Tampereen Yliopistopaino Oy.

Valtiovarainministeriö. 2014. Tietoturvallisuuden arviointiohje. VAHTI 2/2014. Juvenes Print - Suomen Yliopistopaino Oy.

Valtiovarainministeriö. 2017a. VAHTI-toiminta. Viitattu 20.4.2017. http://vm.fi/vahti

Valtiovarainministeriö. 2017b. VM, VAHTI ja tietoturvallisuus. Viitattu 20.4.2017. https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus;jsessionid=1FF667302E838561FB138C12D58F2DE1058D472E52303EF0FDA010071542878CBF43F9F680BB02BBB37B95

Yrityksen toimitusjohtaja. Haastattelu 4.1.2015. Helsinki.

Kuviot

Taulukot

Liitteet

Liite 1: Tarkistuslista

TIETOTURVAUHKIEN TUNNISTAMISEN TARKISTUSLISTOJA

Tässä liitteessä on esitetty esimerkkejä tietoturvallisuusuhkien tunnistamisen tarkistuslistoista. Seuraavat tarkistuslistat on sovellettu valtionhallintoon Pk-yrityksen riskienhallinta -työvälinesarjassa julkaistuista tarkistuslistoista:

1. Tietoriskien hallinnan johtaminen ja organisointi
2. Tietoriskit suhteissa asiakkaisiin ja sidosryhmiin
3. Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa
4. Toimintaympäristön, työ- ja palvelutilojen tietoturvallisuus
5. Tietojärjestelmien suojaus

Tarkistuslistojen soveltamisessa tulee muistaa, että tarkistuslistat eivät koskaan ole täydellisiä, joten niitä käytettäessä on syytä miettiä kattavatko ne organisaation toimintaan liittyvät keskeiset uhkat ja tehdä tarvittavat täydennykset.

LIITE 2

1. Tietoriskien hallinnan johtaminen ja organisointi

Tarkistuslista tietoriskien hallinnan johtamiseen liittyvistä asioista ja johdon toimiin liittyvien riskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

1.1 Hallinnollinen tietoturvallisuus

1.1.1 Johdon tietoisuus tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko organisaation johto tietoinen tietoriskien vaikutuksista liiketoimintaan?	☐	☐	☐
Onko tunnistettu ne organisaation tiedot, jotka ovat toiminnalle elintärkeitä?	☐	☐	☐

1.1.2 Oireita tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko toimitilojen rikosturvallisuudesta huolehdittu?	☐	☐	☐
Ovatko työntekijät sitoutuneet työhönsä ja työnantajaansa eivätkä ole esim. siirtymässä kilpailijalle?	☐	☐	☐
Voiko luottaa siihen, että organisaation palveluksesta lähteneet tai irtisanotut henkilöt eivät levitä tietoja organisaatiosta?	☐	☐	☐
Onko laitteistojen tai toimitilojen paloturvallisuudesta huolehdittu?	☐	☐	☐
Toimiiko koko henkilöstö huolellisesti ja rehellisesti?	☐	☐	☐
Seurataanko edellä mainittuja erilaisia häiriötilanteita?	☐	☐	☐

1.1.3 Tietoriskien hallinnan johtaminen

	Kyllä	Ei	Ei koske meitä
Onko toiminnan turvallisuudesta huolehtiminen vastuutettu nimetylle henkilölle organisaation johdossa?	☐	☐	☐
Onko organisaation omaisuuden ja tietojen suojaamistahto konkretisoitu tietoturvapolitiikaksi ja käytännöiksi?	☐	☐	☐
Arvioidaanko tietojen käsittelytapoja ja turvajärjestelyjä laatujärjestelmän auditointien yhteydessä?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Onko johdolla valmius vakuuttaa sidosryhmille tietojen ja tietämyksen säilyvyys organisaatiossa?	☐	☐	☐
Onko laadittu tietoturvasuunnitelma?	☐	☐	☐
Raportoidaanko tietoturvasta suoraan ylimmälle johdolle?	☐	☐	☐

1.1.4 Tietoriskien tunteminen

	Kyllä	Ei	Ei koske meitä
Onko tunnistettu tilanteet, jotka saattavat lamauttaa toiminnan?	☐	☐	☐
Onko tunnistettu tilanteet, jotka häiritsevät ja haittaavat toiminnassa tarvittavien tietojen saantia?	☐	☐	☐
Onko tunnistettu tilanteet, jotka voivat aiheuttaa tietojen häviämisen tai muuttumisen?	☐	☐	☐
Onko arvioitu em. tilanteiden menetyksiä tai vahinkoja?	☐	☐	☐
Onko turvakäytäntöjen kehittämiskustannukset suhteutettu toiminnan keskeytymisestä aiheutuviin menetyksiin?	☐	☐	☐

1.1.5 Tietoriskien hallintamenettelyt

	Kyllä	Ei	Ei koske meitä
Onko turvaamisen tavoitteet määritelty?	☐	☐	☐
Onko turvatyön mittarit määritelty?	☐	☐	☐
Onko organisaatiolla toiminnan turvaamisen strategia osana toimintastrategiaa?	☐	☐	☐
Onko organisaatiolla käytettävissä laaja-alaista turva-asioiden osaamista?	☐	☐	☐
Onko olemassa toimintamalli tietokonevirusten hallitsemiseksi?	☐	☐	☐
Onko olemassa toipumissuunnitelma ja toimintaohjeet, jotka ohjaavat vastuuhenkilöitä ja muuta henkilöstöä varajärjestelyjen käyttöönotossa ja toiminnassa häiriötilanteissa?	☐	☐	☐
Onko peruskäyttäjille laadittu ja tiedotettu tietoturvaohjeet?	☐	☐	☐
Seurataanko järjestelmien käyttöä esimerkiksi etäkäyttöä epämääräisinä kellonaikoina, tärkeiden tietojen kopiointia tai lähettämistä?	☐	☐	☐
Onko olemassa tiedottamismenettely, jolla kerrotaan organisaatiossa tapahtuneesta häiriötilanteesta tarvittaville osapuolille?	☐	☐	☐
Vastaako joku turvakäytäntöjen kehittämisestä?	☐	☐	☐
Onko organisaatiossa tietoturvaryhmä?	☐	☐	☐
Onko poikkeusolojen tietojenkäsittelyn valmiussuunnitelma?	☐	☐	☐
Onko laadittu ennakkosuunnitelmat häiriötilanteisiin ja tietoturva-hyökkäysten/haittaohjelmien varalle?	☐	☐	☐

LIITE 2

2. Tietoriskit suhteissa asiakkaisiin ja sidosryhmiin

Tarkistuslista organisaation ja sen asiakkaiden ja sidosryhmien välisen yhteistyön tietoriskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

2.1 Hallinnollinen tietoturvallisuus

2.1.1 Asiakas ja sidosryhmäsuhteiden suunnittelu

	Kyllä	Ei	Ei koske meitä
Onko yhteistyökumppanit luokiteltu toiminnan jatkuvuuden kannalta elintärkeisiin, tärkeisiin ja tarpeellisiin?	☐	☐	☐
Onko eri osapuolten valinnassa otettu myös tietoriskit huomioon? (Tahojen luotettavuus, kyky hallita heille luovutettuja tietoja jne.)	☐	☐	☐
Onko kaikilla osapuolilla sama käsitys yhteistyösuhteiden luonteesta?	☐	☐	☐

2.1.2 Toiminnan tietoriskien tunnistaminen

	Kyllä	Ei	Ei koske meitä
Onko arvioitu kumppaneilla tapahtuvat tilanteet, jotka aiheuttavat haittaa organisaation toiminnalle?	☐	☐	☐
Onko kumppaneilla kirjallinen tietoturvapolitiikka ja toimintamallit tietojen käsittelyyn?	☐	☐	☐
Onko omassa organisaatiossa tietoturvapolitiikka dokumentoitu siten, että dokumentti voidaan luovuttaa kumppaneille ja kumppanit saavat sen perusteella kuvan toiminnan luotettavuudesta?	☐	☐	☐
Onko kaikkien kumppanien tietoturvallisuustoiminta katselmoitu yhteistyössä?	☐	☐	☐

2.1.3 Verkosto- ja alihankintasuhteiden käynnistys

	Kyllä	Ei	Ei koske meitä
Onko yhteistyöhön luotu yhteiset tietoturvaperiaatteet?	☐	☐	☐
Onko yhteistyökumppanien välisiin sopimuksiin liitetty organisaation tietoturvavaatimukset sekä tietojen siirron ja käsittelyn menettelyohjeet?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Sovitaanko erilliskäytäntöjä luottamuksellisten, kuten tuote-kehityksen, tietojen käytöstä, siirto- ja suojaustavoista?	☐	☐	☐
Onko kaikki osapuolet koulutettu yhteisiin tietojärjestelmiin?	☐	☐	☐
Onko yhteistyössä edellytettävät tietoturvaperiaatteet, menettely-tavat ja järjestelmät koulutettu alihankkijoille?	☐	☐	☐
Onko suunniteltu, miten hallitaan yhteistyösuhteen päättyminen?	☐	☐	☐

2.2 Fyysinen turvallisuus

2.2.1 Asiakkaiden ja yhteistyökumppanien käynnit toimitiloissa

	Kyllä	Ei	Ei koske meitä
Syntyykö asiakaskäynneillä tai yhteistyökontakteissa kuva oman organisaation luotettavuudesta ja luottamuksellisuudesta?	☐	☐	☐
Pidetäänkö muiden asiakkaiden, yhteistyötahojen ja projektien tiedot suojassa? (Ei neuvotteluhuoneissa, ei asiakaspalvelutiloissa)	☐	☐	☐
Onko neuvottelutilat ääni- ja näköeristetty?	☐	☐	☐
Selvitetäänkö uusien vierailijoiden taustat riittävän huolellisesti? (Koskee sekä kotimaisia että ulkomaisia vierailijoita).	☐	☐	☐

2.3 Käyttöturvallisuus

2.3.1 Tietoturvaratkaisut

	Kyllä	Ei	Ei koske meitä
Onko olemassa käytäntö, jolla käsitellään kumppanin henkilöstön tarve päästä organisaation tietoliikenneverkkoon ja järjestelmiin?	☐	☐	☐
Onko sovittu osapuolten toimenpiteet eri häiriötilanteiden hoitamiseksi?	☐	☐	☐
Arvioidaanko kumppanien turvakäytäntöjä?	☐	☐	☐

LIITE 2

3. Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa

Tarkistuslista arkipäivän tietojenkäsittelytapojen riskien tunnistamiseksi.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

3.1 Henkilöstöturvallisuus

3.1.1 Henkilöstön tietoisuus tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko henkilöstölle koulutettu toiminnan luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?	☐	☐	☐
Tunteeko henkilöstö organisaation vastuut tietojen luotta-muksellisuuden ja muun tietoturvallisuuden suhteen?	☐	☐	☐
Onko kaikille selvää, millaiset tiedot ovat kaikkein tärkeimpiä ja joiden suojaaminen on erityisen tärkeää?	☐	☐	☐
Onko kaikille selvää, mitä organisaation toiminnasta saa kertoa ulkopuolisille?	☐	☐	☐
Onko organisaatiolle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?	☐	☐	☐
Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?	☐	☐	☐
Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan turvakäytäntöjä?	☐	☐	☐
Onko olemassa menettely tietoturva-asioiden käsittelyä varten?	☐	☐	☐
Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?	☐	☐	☐
Onko tietojen luokittelu ja ohjeet osa arkipäivän käytäntöä?	☐	☐	☐
Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturva-rikkeistä tai käytäntöjen puutteista?	☐	☐	☐

3.1.2 Uudet työntekijät ja työsuhteen päättyminen

	Kyllä	Ei	Ei koske meitä
Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista?	☐	☐	☐
Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä?	☐	☐	☐
Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys?	☐	☐	☐
Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen?	☐	☐	☐

3.1.3 Työsuhteen päättyminen

	Kyllä	Ei	Ei koske meitä
Onko henkilön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo tulee poistaa?	☐	☐	☐
Onko suunniteltu muut toimet tietoturvallisuuden varmistamiseksi työsuhteiden päättyessä?	☐	☐	☐

3.1.4 Henkilöstön toimintatavat

	Kyllä	Ei	Ei koske meitä
Käsittelevätkö työntekijät luottamuksellisia tietoja vain työnsä kannalta tarkoituksenmukaisella tavalla?	☐	☐	☐
Onko organisaation keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet?	☐	☐	☐
Onko minimoitu mahdollisuus myydä tai luovuttaa ulos organisaatiosta sille keskeisiä tietoja ja dokumentteja?	☐	☐	☐
Ovatko organisaation sisäiset valvontajärjestelmät kunnossa (työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)?	☐	☐	☐
Onko työntekijöiden omin töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	☐	☐	☐
Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukollisia tiloja?	☐	☐	☐
Hoidetaanko jätepaperin keräys ja käsittely hallitusti?	☐	☐	☐
Ovatko puhelinkäyttäytymisen ohjeet olemassa?	☐	☐	☐
Onko tulipalon varalle toiminta ohjeistettu ja harjoiteltu?	☐	☐	☐
Onko tehtävien varahenkilöjärjestelyistä huolehdittu?	☐	☐	☐

LIITE 2

3.1.5 Tietojärjestelmien ja tietokoneiden käyttö

	Kyllä	Ei	Ei koske meitä
Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön?	☐	☐	☐
Käyttääkö jokainen työntekijä työssään vain omaa käyttäjä-tunnustaan?	☐	☐	☐
Onko ohjeistettu turvallisen salasanan muodostaminen?	☐	☐	☐
Pystyvätkö muut työntekijät lukemaan tai muuttamaan käyttäjän tietoja käyttäjän huomaamatta?	☐	☐	☐
Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet?	☐	☐	☐
Valvotaanko varmuuskopioiden ottamista?	☐	☐	☐
Onko Internetin käyttö ohjeistettu?	☐	☐	☐
Onko sähköpostin käyttö ohjeistettu?	☐	☐	☐
Onko virusten torjuntamenettelyt ohjeistettu niin työkoneiden kuin kotikoneiden osalta?	☐	☐	☐
Onko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?	☐	☐	☐
Salakirjoitetaanko kannettavilla tietokoneilla olevat luottamukselliset tiedot?	☐	☐	☐
Onko käyttäjiä kielletty asentamasta organisaation verkkoon ulkopuolisia ohjelmistoja tai modeemeja?	☐	☐	☐

4. Toimintaympäristön, työ- ja palvelutilojen tietoturvallisuus

Tarkistuslista toimintaympäristöön ja toimitiloihin liittyvien tietoriskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

4.1 Fyysinen turvallisuus

4.1.1 Kiinteistön turvallisuus

	Kyllä	Ei	Ei koske meitä
Onko kiinteistö altis onnettomuuksille? Sijaitseeko se lähellä rautatietä tai isoa valtatietä?	☐	☐	☐
Onko sähkönsyötön häiriöihin varauduttu?	☐	☐	☐
Onko kiinteistöllä suojelupäällikkö ja turvasuunnitelma?	☐	☐	☐
Onko kiinteistössä organisaatioita, joissa liikkuu paljon vieraita henkilöitä?	☐	☐	☐
Onko rakenteellinen suojaus palon, murron, vesivahingon ja sabotaasin varalta hoidettu?	☐	☐	☐
Onko kiinteistössä kulunvalvonta?	☐	☐	☐
Onko kiinteistössä vartiointi?	☐	☐	☐
Onko organisaation tiloihin pääsy suojattu kulunvalvonnalla?	☐	☐	☐
Onko kiinteistön yleisiin tiloihin, kuten puhelinkeskukseen, piha-alueelle, kellariin, katolle, asiaton pääsy estetty ja valvottu?	☐	☐	☐
Onko toimitiloissa kulunvalvonta ja vartiointi?	☐	☐	☐
Onko toimitiloissa hälytysjärjestelmää?	☐	☐	☐
Ovatko takaovet ja -ikkunat lukittu?	☐	☐	☐
Säilytetäänkö avaimia huolella?	☐	☐	☐

LIITE 2

4.1.2 Toimitilojen turvajärjestelyt

	Kyllä	Ei	Ei koske meitä
Onko kulkuoikeuksien myöntäminen nimetty vastuuhenkilölle?	☐	☐	☐
Onko kulkeminen tiloissa rajattua ja valvottua?	☐	☐	☐
Onko muilla kuin työntekijöillä kulkuavaimet tiloihin?	☐	☐	☐
Onko työntekijöiden omin töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	☐	☐	☐
Onko vierailusäännöt ja -käytännöt olemassa?	☐	☐	☐
Onko tärkeät laitteet, kuten työasemat ja palvelimet, sijoiteltu valvottuihin tiloihin?	☐	☐	☐
Onko tärkeät tilat sijoiteltu pois viemärien ja putkistojen lähistöltä?	☐	☐	☐
Ovatko laitetilat alttiita lämpötilan vaihteluille?	☐	☐	☐
Onko alkusammutuskaluston käyttöä harjoiteltu?	☐	☐	☐
Onko tulipalon varalle harjoiteltu tiloista poistumista?	☐	☐	☐

4.2 Tietoaineistoturvallisuus

4.2.1 Asiakaspalvelutilat

	Kyllä	Ei	Ei koske meitä
Pidetäänkö luottamukselliset tiedot poissa asiakaspalvelutiloista?	☐	☐	☐
Pidetäänkö tietokonepäätteet, kirjoittimet, faksit yms. poissa kulkuväyliltä?	☐	☐	☐
Onko asiakastilat sijoitettu siten, että asiakkaiden liikkumista voidaan valvoa?	☐	☐	☐
Ovatko neuvottelutilat ääni- ja näköeristettyjä?	☐	☐	☐
Huolehditaanko neuvottelutilojen siivouksesta siten, että vanhojen palaverien asiakirjat, fläpit ja piirtoheitinkalvot eivät jää tilaan?	☐	☐	☐
Onko asiakkaita varten suunniteltu esimerkiksi puhelin sellaiseen paikkaan, että sen käyttö ei aiheuta riskiä? (Ei esimerkiksi työhuoneeseen)	☐	☐	☐

4.3 Käyttöturvallisuus

4.3.1 Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuu-henkilölle?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilö-kohtainen salasana?	☐	☐	☐

LIITE 2

	Kyllä	Ei	Ei koske meitä
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	☐	☐	☐
Ovatko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

LIITE 2

5. Tietojärjestelmien suojaus

Tarkistuslista tietojen ja järjestelmien teknisten suojakeinojen kehittämiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

5.1 Tietoliikenneturvallisuus

	Kyllä	Ei	Ei koske meitä
Toimivatko modeemiyhteydet takaisinsoittoperiaatteella?	☐	☐	☐
Onko asiaton pääsy ja muu asiaton verkkoliikenne organisaation verkkoon estetty?	☐	☐	☐
Ovatko paikallisverkko, extranet- ja WWW-palvelimet eristetty toisistaan riittävästi?	☐	☐	☐
Tarkistetaanko sähköpostiliitteiden asianmukaisuus ja virukset ennen pääsyä organisaation verkkoon?	☐	☐	☐
Tarkistetaanko lähtevät sähköpostiliitteet?	☐	☐	☐
Suojataanko kannettavat tietokoneet kattavasti? (niin että varkaat eivät pääse tietoihin käsiksi)	☐	☐	☐

5.2 Ohjelmistoturvallisuus

5.2.1 Ohjelmistot

	Kyllä	Ei	Ei koske meitä
Hankitaanko ohjelmistot, laitteet ja muu tuki osaavilta toimittajilta?	☐	☐	☐
Onko käytössä vain lisensoidut lailliset ohjelmistoversiot?	☐	☐	☐
Onko laadittu järjestelmäkehityksen tietoturvasuunnitelma?	☐	☐	☐
Otetaanko hankintojen yhteydessä huomioon ohjelmistojen turvallisuus ja luotettavuus? (Tietojen hankinta luotettavuudesta, oma testaus)	☐	☐	☐
Ovatko tietojen varmistuskäytännöt vastuutettu ja suunniteltu?	☐	☐	☐
Onko harjoiteltu varmistusten palautusten onnistumista?	☐	☐	☐
Onko paloturvakaappi tietojen varmistuksille?	☐	☐	☐
Onko kaikissa työasemissa virustorjunta?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Onko virustentorjuntaohjelmiston ajantasaisuudesta huolehtiminen vastuutettu?	☐	☐	☐
Tapahtuuko työasemien virustentorjuntaohjelmistojen ja vastaavien päivitys automaattisesti?	☐	☐	☐

5.3 Tietoaineistoturvallisuus

5.3.1 Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuuhenkilölle?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	☐	☐	☐
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	☐	☐	☐
Onko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

5.4 Käyttöturvallisuus

5.4.1 Teknisen ympäristön hallinta ja valvonta

	Kyllä	Ei	Ei koske meitä
Onko tietotekniset turvatehtävät vastuutettu?	☐	☐	☐
Vastaavatko teknisen ympäristön ylläpidosta henkilöt, joilla on siihen riittävä tekninen osaaminen?	☐	☐	☐
Onko sähköpostipalvelimien asennus ohjeistettu?	☐	☐	☐
Onko järjestelmien ylläpidosta vastaavat koulutettu tietoriskien hallintaan ja järjestelmien suojaamiseen?	☐	☐	☐
Ovatko varahenkilöt tietoisia nykykäytännöistä?	☐	☐	☐
Onko tietojärjestelmäsuunnittelijoilla valmius ennakoida järjestelmää uhkaavat tilanteet ja suunnitella ja arvioida tarpeellisia suojaustapoja?	☐	☐	☐
Seurataanko järjestelmän virheitä ja levytilojen täyttymistä?	☐	☐	☐
Seurataanko järjestelmän käyttöä ja puututaanko siihen tarvittaessa?	☐	☐	☐

LIITE 2

5.4.2 Teknisen järjestelmä hankinta, huolto, muutokset ja poisto käytöstä

	Kyllä	Ei	Ei koske meitä
Otetaanko tietoturvaasiat huomioon laitehankinnoissa?	☐	☐	☐
Onko varauduttu teknisten järjestelmien rikkoutumiseen (varaosien saatavuus, kahdennus, varajärjestelmät, korvaavat toimintatavat)?	☐	☐	☐
Käytetäänkö luotettavia huoltoyrityksiä, joiden kautta tiedot eivät ole vaarassa joutua kolmansille osapuolille?	☐	☐	☐
Onko tekninen ympäristö ja sen muutokset dokumentoitu?	☐	☐	☐
Onko tietojen hävitysmenettely olemassa, jos laitteita myydään työntekijöille tai ulkopuolisille?	☐	☐	☐

5.4.3 Tekniset suojaamiskeinot

	Kyllä	Ei	Ei koske meitä
Onko suojaamiskeinojen kattavuus tarkistettu / auditoitu?	☐	☐	☐
Onko järjestelmien käyttö ilman käyttäjän luotettavaa yksilöintiä estetty?	☐	☐	☐
Ovatko tietojen varmistukset automaattiset ja aukottomat?	☐	☐	☐
Onko UPS-laitteita varasähkön varmistamiseksi?	☐	☐	☐
Salakirjoitetaanko työasemilla ja palvelimilla olevat tiedot ja sähköpostiliikenne?	☐	☐	☐
Vaatiiko käyttöä valvova ohjelmisto salasanalle tietyn määrä-muotoisuuden ja salasanan ennalta ajoitetun vaihtamisen?	☐	☐	☐
Tarkistetaanko työntekijöiden salasanojen muoto ja turvallisuus ajoittain?	☐	☐	☐
Jääkö järjestelmän lokitiedostoihin merkintä järjestelmän käyttäjistä?	☐	☐	☐
Rajataanko ulkopuolisilta pääsy organisaation verkkoon?	☐	☐	☐

Liite 2: Riskitaulukko

RISKIENHALLINTASUUNNITELMA
Potentiaalisten ongelmien analyysi TILITOIMISTO X

RISKILUOKKA	Tunnistettu riski	Riskin syy	Todennäköisyys	Vaikutus	Riskin vaikutus	Riskienhallintakeinot	Vastaa	Muuta
50	kannettavan tietokoneen katoaminen	Salasanojen geneerisyys & kryptauksen puute	2	5	Asiakkuuksien menetys, maine	Kryptausohjelmat ja salasanapolitiikka	IT-osasto	
45	neuvotteluhuoneiden läpinäkyvyys	Asiakkaiden tietojen paljastuminen	5	3	Asiakkuuksien menetys, maine	neukkareiden kalvotus	HR-osasto	Hoidettu
45	asiakas työtiloissa	Asiakkaat voivat nähdä muiden tietoja	5	3	Asiakkuuksien menetys, maine	ohjeistus, väliovi	HR-osasto	
36	työntekijä kertoo salassapidettäviä asioita	Ei salassapitositoumuksia	4	3	Asiakkuuksien menetys, maine	Ohjeistus	HR-osasto	
36	ulkopuolinen näkee näytöltä tietoja	Asiakkaiden tietojen paljastuminen	4	3	Asiakkuuksien menetys, maine	näytön suojakalvot, ohjeistus	IT-osasto	
32	haittaohjelma	Ei haittaohjelmien torjuntaohjelmistoa	2	4	tiedot leviävät	virusohjelma	IT-osasto	
32	työntekijän irtisanoutuminen	Ei salassapitositoumuksia, korvaavan henkilön löytyminen	2	4	asiakkaiden henkilön perässä	työntekijöistä huolehtiminen, olosuhteet	Lakiosasto	
32	työntekijän siirtyminen kilpailijalle	Ei salassapitositoumuksia	2	4	Asiakkuuksien menetys, maine	Salassapitositoumukset	Lakiosasto	
32	käyttäjä asentaa haittaohjelman	Käyttjäoikeuksia ei ole rajoitettu	2	4	Asiakkuuksien menetys, maine	käyttäoikeuksien määrittely	IT-osasto	
27	osaamattomuus	Puutteellinen perehdytys ja prosessit	3	3	asiakkaiden tiedot sekoittuvat	Ohjeistus, perehdyttäminen	IT ja HR	
27	kiire ja huolimattomuus	Puutteellinen perehdytys ja prosessit	3	3	Asiakkuuksien menetys, maine	työtehtävien mitoittaminen	JOHTO	
25	tahallinen tietojen levittäminen	Käyttjäoikeuksia ei ole rajoitettu, ei salassapitositoumuksia	1	5	Asiakkuuksien menetys, maine	tietoihin pääsyn rajoittaminen	JOHTO	
25	kannettavan tietokoneen varastaminen	Salasanojen geneerisyys & kryptauksen puute	1	5	Asiakkuuksien menetys, maine	Kryptausohjelmat ja salasanapolitiikka	IT-osasto	
25	avainhenkilön siirtyminen kilpailijalle	Ei salassapitositoumuksia	1	5	Asiakkuuksien menetys, maine	Kilpailukieltosopparit	Lakiosasto	
25	avainhenkilön irtisanoutuminen	Ei salassapitositoumuksia	1	5	Asiakkuuksien menetys, maine	Salassapito- ja kilpailukieltosopimukset	Lakiosasto	
25	työntekijän irtisanominen	Ei salassapitositoumuksia	1	5	Asiakkuuksien menetys, maine	Ohjeistus työsuhdeasioista	HR + johto	
20	tietoturva-aineiston käsittely	Ei tietoaineston luokittelua eikä prosessia	5	2	Asiakkuuksien menetys, maine	Silppuaminen	JOHTO	
18	ilkivalta	Ei kamera- tai hälytysvalvontaa	2	3	Menetetty työaika + työvälineet	Näkyvä valvonta ja vartiointi sekä kamera- ja hälytysvalvonta	JOHTO	

18	puhelimen katoaminen	Pääsy tietoihin, ei pakollista salasanaa tai salausta tai etäkäyttöä	2	3	Asiakkuuksien menetys, maine	ohjeistus, mahd. Politiikan muutos	IT ja HR	
18	salakuuntelu	Asiakkaat sekä toisen yrityksen henkilöstö pääsee liikkumaan henkilökunnan tiloihin	2	3	Asiakkuuksien menetys, maine	ohejeistus	HR-osasto	
18	puhelimen rikkoutuminen	Pääsy tietoihin, ei pakollista salasanaa tai salausta tai etäkäyttöä	2	3	Asiakkuuksien menetys, maine	ohejeistus, puhelimen sammuttaminen	HR-osasto	
18	salasanat liian helppoja	Ei salasanoihin liittyviä käytänteitä	2	3	Asiakkuuksien menetys, maine	complexity käyttöön	IT-osasto	
16	tietomurto	Ei haittaohjelmien torjuntaohjelmistoa eikä tietoliikenteen salausta tai palomuuria	1	4	huomioitava vuokrattu työvoima	Jatkuvuussuunnitelma	IT-osasto	
16	murto	Ei kamera- tai hälytys-, tai kulunvalvontaa	1	4	Menetetty työaika + työvälineet ja tieto	vartiointi, suojau, kamera, kv, ohjeistus	HR-osasto	
16	toisen kirjautumistunnuksien käyttö	Yhteisiä salasanoja käytön helpottamiseksi	4	2	vahingossa maksetaan jokin lasku tai toimitaan väärin tahattomasti	ohjeistus	IT-osasto	
16	pysyväisarkiston tuhoutuminen	Paperinen pysyväisarkisto	1	4	Asiakkuuksien menetys, maine	arkiston skannaus?	JOHTO	
12	tietojen kopiointi ulkoiselle medialle	Käyttjäoikeuksia ei ole rajoitettu, ei salassapitositoumuksia eikä prosessikuvausta tietojen kopioinnista	3	2	Tietoja katoaa	ohjeistus ja kryptaus	IT-osasto	
9	tulipalo	Ei harjoiteltua pelastautumista ja toimintaa poistuttaessa työpisteiltä eikä jatkuvuussuunnitelmaa toiminnan siirrosta väliaikaiseen toimitilaan	1	3	Menetetty työaika + työvälineet	varautuminen ohjeilla, vakuutukset	JOHTO	
9	vesivahinko	Ei jatkuvuussuunnitelmaa toiminnan siirrosta väliaikaiseen toimitilaan	1	3	Menetetty työaika + työvälineet		JOHTO	
9	alihankkijan tietomurto	Sopimuksissa ei ole määritelty korvausvelvollisuutta	1	3	alihankkijat erillisinä	sopimukset alihankkijoiden kanssa	Lakiosasto	
9	tekninen salakuuntelu	Asiakkaat sekä toisen yrityksen henkilöstö pääsee liikkumaan henkilökunnan tiloihin eikä tilojen käyttöä ole valvottu teknisesti	1	3	Asiakkuuksien menetys, maine	Ohjeistus asiakkaiden kanssa toimimisesta	HR-osasto	
9	tietoliikenteen salakuuntelu	Ei tietoliikenteen salausta eikä palomuureja	1	3	Asiakkuuksien menetys, maine	Salausohjelmisto, palomuuri ja verkkojen eriyttäminen	IT-osasto	Freedome
9	salakatselu	Ikkunoissa ei ole verhoja tai suojakalvoja	1	3		kalvot, valoverhot	HR-osasto	

8	sähkökatkos	Ei jatkuvuussuunnitelmaa toiminnan siirrosta väliaikaiseen toimitilaan	2	2	Menetetty työaika	varavoima / ups	Ei tarvetta, koska läppärit	
8	tietojen katoaminen	Ei varmuuskopiointia	2	2	selvitystyö ja tietojen palautus	Ohjeistus, käyttöoikeudet	IT-osasto	
8	tietokoneen rikkoutuminen	Ei salausta tai varmuuskopiointia	2	2		tietokone pitää tyhjentää	IT-osasto	
8	tietoliikennekatkos	Ei varayhteyttä	2	2	Menetetty työaika	varayhteys	IT-osasto	
4	palvelunestohyökkäys	Vain yksi yhteysverkko	1	2	Menetetty työaika	ip-osoitteen vaihto / toinen verkko	IT-osasto	
4	palohälytys	Ei harjoiteltua pelastautumista ja toimintaa poistuttaessa työpisteiltä eikä jatkuvuussuunnitelmaa toiminnan siirrosta väliaikaiseen toimitilaan	1	2	Menetetty työaika	Paloharjoitus	JOHTO	
0	varaston vesivahinko	Fyysisen tietoaineiston tuhoutuminen	0	0	Asiakkuuksien menetys, maine	Pysyväisarkiston skannaus	ETP	
0	varmuuskopioinnin puuttuminen	Tietoja ei saada palautettua työasemilta	0	0	Asiakkuuksien menetys, maine	Varmuuskopiointi pilvipalveluun	ETP	

Todennäköisyys	**Suhdeluku**	**Taloudellinen vaikutus***
kerran viidessä vuodessa	**1**	0 - 300 €
< kerran vuodessa	**2**	301 - 2 000 €
kaksi kertaa vuodessa	**3**	2001 - 8 000 €
kuukausittain	**4**	8001 - 50 000 €
viikoittain	**5**	50 001 - 1 000 000 €

*Painotus kaava x*x

Liite 3: Tietoturvapolitiikka

TILITOIMISTO X:N TIETOTURVAPOLITIIKKA

1.11.2016

Sisällysluettelo

1 Yleistä

Tietotekniikan (IT) järjestelmien tarkoitus on mahdollistaa ja tukea liiketoimintaprosesseja. IT-tietoturvan avulla IT-järjestelmiä voidaan käyttää kattavasti ja turvallisesti, joten se on arvokas, liiketoimintaa mahdollistava tekijä. Tieto ja tietojärjestelmät ovat osatekijöitä, jotka ovat muiden liiketoiminnan osatekijöiden tapaan arvokkaita organisaation kannalta. Siksi ne on suojattava asianmukaisella tavalla. IT-tietoturva suojaa tietoja ja tietojärjestelmiä useilta erilaisilta uhilta liiketoiminnan jatkuvuuden varmistamiseksi, tappioiden minimoimiseksi ja sijoitetun pääoman tuoton maksimoimiseksi sekä turvatakseen liiketoimintamahdollisuudet. IT-tietoturvallisuuden avulla tietoja, sovelluksia, verkkoja ja tietokonejärjestelmiä suojataan luvattomalta tunkeutumiselta, muutoksilta ja tuhoutumiselta.

1.1 Soveltamisala

Tätä käytäntöä sovelletaan työntekijöihin, sopijapuoliin, kolmansien osapuolien käyttäjiin ja sellaisiin IT-järjestelmiin, joista on pääsy Tilitoimisto X:n tietojärjestelmiin.

1.2 Roolit ja vastuut

Käyttäjien on tunnettava Tilitoimisto X:n IT-tietoturvallisuussäännöt ja noudatettava niitä. Heidän on myös ilmoitettava huomaamansa turvallisuutta vaarantavat tapahtumat ja uhat. Tilitoimisto X:n ICT-osasto omistaa tämän asiakirjan ja on vastuussa sen määrittämisestä ja päivittämisestä.

1.3 Luottamuksellisuus

Tämä IT-tietoturvapolitiikkaa täydentävä asiakirja voidaan jakaa työntekijöille, sopijapuolille ja kolmansien osapuolien käyttäjille, joilla on pääsy Tilitoimisto X:n tietojärjestelmiin. Asiakirjaa tai sen osia ei saa kopioida tai muuttaa ilman asiakirjan omistajan lupaa. Asiakirjaa ei myöskään saa antaa henkilöille, jotka eivät työskentele Tilitoimisto X:n palveluksessa.

1.4 Oikeudenloukkaukset ja seuraamukset

Keneen tahansa tämän käytännön vastaisesti toimineeseen työntekijään, mukaan lukien sopijapuolet ja kolmansien osapuolten käyttäjät, voidaan soveltaa kurinpito- ja mahdollisia oikeustoimia. Tuottamuksellinen ohjeiden vastainen toiminta voi myös saattaa tekijän korvausvelvolliseksi aiheuttamistaan vahingoista. Merkittävä tuottamuksellinen tietojärjestelmän väärinkäyttö voi johtaa työntekijän työsopimuksen purkamiseen sekä korvausvastuuseen.

2 Yleiset säännöt

- Tilitoimisto X:n ICT-järjestelmien käyttäjille myönnetään käyttäjätili, joka tunnistetaan henkilökohtaisen käyttäjätunnuksen avulla.

- Käyttäjät saavat käyttää ainoastaan niitä IT-palveluita, joihin heille on myönnetty oikeudet.
- Käyttäjälle voidaan myöntää pääsy useisiin IT-palveluihin, ja hänen on käytettävä näitä palveluita eettisellä, laillisella ja tehokkaalla tavalla.
- Jos pääsy IT-järjestelmään suojataan jollakin tunnistusmenetelmällä, käyttäjä ei saa paljastaa tätä menetelmää kenellekään muulle henkilölle.
- Käyttäjä ei saa käyttää toiselle käyttäjälle tarkoitettua käyttäjätunnusta tai yrittää saada selville toisen käyttäjän tai sellaisen palvelun tunnistusmenetelmiä, jota hänellä ei ole lupa käyttää.
- Käyttäjät eivät toiminnallaan pyri haittaamaan IT-resurssien toimintaa.
- Käyttäjien on kunnioitettava immateriaalioikeuksia sekä tietojen ja ohjelmistojen omistusoikeuksia.

2.1 Käyttäjien vastuu

Kukin käyttäjä on käyttäjätunnustaan käyttäessään vastuussa:

- kaikista hänen tunnukseltaan lähtöisin olevista toimista
- kaikista hänen tunnuksensa kautta lähetetyistä, tarkoituksella pyydetyistä, tavoitelluista tai tarkastelluista tiedoista
- hänen tunnuksensa kautta tietokoneelle laitetuista, julkisesti saatavista tiedoista.

2.2 Yleisesti kielletyt toimet

Alla oleva luettelo ei ole kaiken kattava, mutta sen avulla pyritään muotoilemaan puitteet toimille, joiden katsotaan olevan luvatonta käyttöä.

- Tilitoimisto X:n työntekijöillä ei ole missään tilanteessa käyttäessään Tilitoimisto X:n ICT-palveluita lupaa ryhtyä mihinkään sellaisiin toimiin, jotka ovat laittomia yhtiön sääntöjen tai suomen lakien ja asetusten mukaan
- Käyttäjillä ei ole oikeutta koettaa heikentää minkään Tilitoimisto X:n ICT-palvelun turvallisuutta.
- Käyttäjillä ei ole lupaa yrittää luoda, suorittaa tai asentaa mitään vahingollista ohjelmistoa, joka saattaa vaikuttaa tietokone- tai verkkolaitteistoon, ohjelmistoon tai tietoihin.
- Käyttäjillä ei ole lupaa yrittää asentaa yhtiön omistamalle tietokoneelle mitään ohjelmistoja ellei sitä ole hyväksytty ICT-yksikön toimesta
- Käyttäjillä ei ole lupaa yrittää häiritä minkään Tilitoimisto X:n ICT-palvelun toimintaa.
- Käyttäjillä ei ole lupaa yrittää heikentää minkään Tilitoimisto X:n ICT-palvelun rajoitusta tai tunnusvalvontatoimia.
- Käyttäjillä ei ole lupaa yrittää päästä luvattomasti mihinkään Tilitoimisto X:n ICT-palveluun.

2.3 Käyttäjän toimet

Käyttäjien on huomioitava, että heidän käyttäessään IT-järjestelmiä monet toimet saattavat näkyä järjestelmänvalvojille. Valvojille mahdollisesti näkyvät tiedot sisältävät tapahtuman aloitus- ja lopetusajat, tapahtuman alkuperän sekä annetut komennot ja niiden argumentit. Käyttäjien on huomioitava myös, että käyttäjien toimista kertovat järjestelmälokit säilytetään vianetsintää ja jäljitysketjuja varten. Nämä lokit saattavat sisältää tietoja postien lähetys- ja vastaanottoajoista, sähköpostiosoitteista, verkkosivuista, joilla käyttäjä on käynyt, ladattujen sivujen

koosta ja tyypistä, luetuista tai kirjoitetuista tiedostoista tai koneista, joilla käyttäjä on käyttänyt jotakin verkkopalvelua.

2.4 Tiedot

Käyttäjällä ei ole lupaa tarkastella, paljastaa, kopioida, nimetä uudelleen, poistaa tai muuntaa hänelle kuulumattomia tietoja ilman suoraa tai epäsuoraa lupaa. Edellä mainittu koskee myös tallennuslaitteissa olevia tietoja ja verkon kautta siirrettävänä olevia tietoja. Käyttäjän on noudatettava Tilitoimisto X:n ICT-järjestelmissä tallennettuna olevien ja laitteistoihin lähetettyjen tietojen yksityisyyttä ja luottamuksellisuutta.

Tilitoimisto X:n ICT:llä on laillinen oikeus ottaa haltuunsa ja tarkastaa kaikki tiedot, jotka on tallennettu tai lähetetty Tilitoimisto X:n ICT-laitteistoilla, kun Tilitoimisto X:n ICT tutkii järjestelmän ongelmia tai mahdollisia turvallisuusrikkomuksia, pitää yllä järjestelmän turvallisuutta ja eheyttä tai estää, havaitsee tai minimoi luvatonta toimintaa tätä laitteistoa käytettäessä.

2.5 Siirrettävä tallennusratkaisu

Käyttäjän vastuulla on varmistaa tietosuoja sellaisten arkojen tai luottamuksellisten tietojen osalta, jotka hän on tallentanut siirrettävään tallennuslaitteeseen. Käyttäjän on suojattava siirrettävässä tallennuslaitteessa olevat tiedot tiedostojen salauksella tai muulla vastaavalla menetelmällä. Tilitoimisto X:n ICT-vastaava luovuttaa käyttöön siirrettävät tallennuslaitteet. Omia tallennuslaitteita ei saa käyttää ilman ICT-vastaavan kirjallista lupaa.

2.6 Laitteisto

- Käyttäjien on oltava huolellisia käyttäessään IT-laitteistoja ja varmistettava kohtuullisin toimin, ettei niille aiheudu vahinkoa.
- Käyttäjien on ilmoitettava Tilitoimisto X:n ICT:lle kaikki IT-laitteiston vahingot, tappiot ja väärinkäytöt.
- Käyttäjillä ei ole lupaa muuttaa tai siirtää asennettuja IT-laitteistoja ilman asianmukaista lupaa.

2.7 Tietosuoja

Tilitoimisto X:n ICT pyrkii noudattamaan tietosuojavaatimuksia ja luottamuksellisuutta aina toimittaessaan IT-palveluja, mutta tietosuojaa ja luottamuksellisuutta ei voida taata. Käyttäjien on ymmärrettävä, ettei tietojen ja verkostojen suoja ole rikkomaton. Vaikka suurin osa ihmisistä kunnioittaa tietosuojaa ja yksityisyyttä, eräät henkilöt saattavat rikkoa niitä. Käyttäjien on myös ymmärrettävä, että verkkoa ja järjestelmiä ylläpitävien henkilöiden on työtehtäviä hoitaessaan tarkkailtava tiettyjen tietojen sisältöä, olivatpa tiedot sitten tallennuslaitteissa tai siirrettävänä, jotta Tilitoimisto X:n ICT-palveluiden oikeanlainen toiminta voidaan varmistaa.

3 Tietokoneet

3.1 Yleiset asiat

- Yhtiön lähiverkkoon saa liittää vain Tilitoimisto X:n ICT:n hyväksymiä tietokoneita.
- Tilitoimisto X:n ICT hallinnoi tietokoneiden ohjelmistojen asennusta ja suorittaa asennukset. Kaikkiin poikkeuksiin tarvitaan erillinen kirjallinen lupa.
- Yhtiön tietokonetta tai verkkoresursseja ei saa käyttää työhön liittymättömien ohjelmistojen, videoiden, kuvien musiikin tai muun samantapaisen materiaalin suorittamiseen tai tallentamiseen. Yhtiön tietokone ja verkkoresurssit on tarkoitettu käytettäväksi ainoastaan liiketoimintatarkoituksiin.
- Käyttäjällä ei ole tietokoneen järjestelmänvalvojan oikeuksia, ellei Tilitoimisto X:n ICT ole myöntänyt niitä hänelle.
- Tilitoimisto X:n ICT huolehtii tietokoneiden korjauksista, käyttäjän etätuesta ja tietokoneiden huollosta. Kaikki poikkeukset on hyväksytettävä Tilitoimisto X:n ICT:llä.
- Tilitoimisto X:n ICT suorittaa ajoittain rutiininomaiset tietokoneiden tietoturvahaavoittuvuuksia ja ohjelmistoja koskevat tarkistukset ja asennukset.
- Ainoastaan valtuutetut käyttäjät saavat käyttää yhtiön henkilökohtaisia ja yhteiskäyttöön tarkoitettuja tietokoneita. Esimerkiksi henkilökohtaisen tietokoneen luovuttaminen perheenjäsenen käyttöön on kiellettyä.
- Yhtiön henkilökohtaisia ja yhteiskäyttöön tarkoitettuja tietokoneita ei saa luovuttaa muiden käyttöön ilman Tilitoimisto X:n ICT:n lupaa.
- Tilitoimisto X:n ICT:lle on ilmoitettava välittömästi, jos tietokone häviää tai varastetaan tai jos sen väärinkäyttöä epäillään.

3.2 Tietokoneen turvallisuus, kun käyttäjä ei ole paikalla

Jos käyttäjä ei ole fyysisesti sen tietokoneen lähettyvillä, johon hänellä on valtuudet, tietokonejärjestelmä on lukittava, etteivät muut pääse käyttämään sitä.

3.3 Yhtiön tilojen ulkopuolella olevat yhtiön tietokoneet

- Yhtiön tilojen ulkopuolella olevia tietokoneita ei saa jättää valvomatta turvattomaan paikkaan.
- Tietokoneet on otettava matkustettaessa käsimatkatavaroihin ja mahdollisuuksien mukaan peitettävä.
- Tietokoneet on laitettava pois näkyvistä ja peitettävä, kun ne jätetään väliaikaisesti kulkuneuvoon tai muuhun samantapaiseen paikkaan.
- Tietokoneen näytöllä näkyvien tietojen tietosuojasta on huolehdittava erityisen tarkasti.

3.4 IT-laitteistojen palauttaminen

- Käyttäjien on palautettava kaikki hallussaan olevat ja Tilitoimisto X:n ICT:n omistamat laitteistot, kun heidän työsuhteensa tai -sopimuksensa päättyy.
- Myös kaikki muu yhtiön omaisuus, kuten kannettavat tietoliikennelaitteet, pääsykortit, ohjelmistot, manuaalit ja sähköiseen mediaan tallennetut tiedot, on palautettava.

3.5 Tietokoneen varmuuskopioiminen

Kaikki tietokoneella käsitellyt tiedot on tallennettava Tilitoimisto X:n ICT:n osoittamiin verkkoasemissa sijaitseviin kansioihin. Verkkokansioista otetaan päivittäin

varmuuskopiot. Käyttäjän vastuulla on varmistaa, että kaikki tiedot, joista on otettava varmuuskopiot, sijoitetaan verkkokansioihin.

4 Verkko

4.1 Yleiset asiat

- Käyttäjät eivät saa tarkoituksella häiritä tai yrittää häiritä verkon toimintaa.
- Käyttäjät eivät saa käyttää laitteistoja tai ohjelmistoja, jotka on tarkoitettu verkkoyhteyksien salakuunteluun tai analysointiin.
- Jos havaitaan viruksella tai muulla tavoin saastunut tietoliikennelaite, sen yhteys verkkoon voidaan katkaista, jotta virus ei pääsisi leviämään. Käyttäjät ovat velvollisia katkaisemaan laitteidensa verkkoyhteyden heti, jos Tilitoimisto X:n ICT pyytää sitä heiltä.
- Käyttäjät eivät saa ilman Tilitoimisto X:n ICT:n lupaa liittää uudestaan verkkoon sellaista tietoliikennelaitetta, jonka yhteys on katkaistu, jotta virusten uhalta vältytään.
- Kaikki verkkoon liitetyt tietokoneet, joita ei käytetä pitkään aikaan, on sammutettava.
- Ainoastaan Tilitoimisto X:n ICT:n hyväksymiä laitteita saa liittää yhtiön LAN-verkkoon langallisen tai langattoman verkkoyhteyden kautta.
- Käyttäjät eivät saa muodostaa yhtä aikaa yhteyttä sekä yhtiön langalliseen LAN-verkkoon että johonkin luvattomaan tai epäluotettavaan langattomaan verkkoon.
- Tilitoimisto X:n ICT:lle on ilmoitettava heti, jos jokin IT-laite häviää tai varastetaan tai jos sen väärinkäyttöä epäillään.

4.2 Vierailijoiden verkkoyhteydet

- Vierailevien henkilöiden, jotka eivät kuulu Tilitoimisto X:n henkilökuntaan, on käytettävä vierailukäyttöön tarkoitettuja langallisia tai langattomia verkkoyhteyksiä. On nimenomaisesti kiellettyä antaa vierailijoiden yhdistää tietoliikennelaitteitansa Tilitoimisto X:n sisäiseen verkkoon.
- Vierailijaa isännöivän X:laisen henkilön tehtävänä on varmistaa, että vierailija noudattaa verkkoyhteyksiin liittyviä sääntöjä.

5 Internet

5.1 Pääsy Internetiin

Käyttäjien, joiden on päästävä Internet-palveluihin Tilitoimisto X:n sisäisestä verkosta, on käytettävä Tilitoimisto X:n ICT:n hyväksymiä laitteistoja ja ohjelmistoja.

5.2 Internetissä julkaistujen materiaalien lataaminen, siirtäminen, jakaminen, kopioiminen tai suorittaminen

Suuri osa Internetissä olevasta materiaalista on suojattu esimerkiksi käyttöoikeussopimuksella. Kaikkien Internetistä saatujen aineistojen immateriaali- ja teollisoikeudet on tarkistettava, ennen kuin näitä aineistoja käytetään mihinkään tarkoitukseen.

Työhön liittymättömien ohjelmistojen, videoiden, kuvien ja musiikin, kuten pelien, työaseman apuohjelmien, näytönsäästäjien ja teemojen, IRC-kanavien, yhteisöpalveluiden, elokuvien ja valokuvien käyttäminen on kielletty.

Internet-sivustojen, joilla on, tai voidaan olettaa olevan, Suomen laissa kiellettyä, tietoturvaa vaarantavaa tai muuten epäsopivaa materiaalia käyttäminen on kielletty ellei työtehtävän suorittaminen sitä edellytä.

Vertaisverkon (P2P) asiakasohjelmistojen ja/tai P2P-verkkojen ja muiden vastaavien resurssien asentaminen on kielletty tiedostojen lataamista, siirtämistä tai jakamista varten.

Käyttäjän on aina otettava yhteys Tilitoimisto X:n ICT:hen, mikäli hänen on ladattava ja asennettava Internetistä ohjelmistoja, joita Tilitoimisto X:n ICT ei ole hyväksynyt

5.3 Yksityiset ja arkaluonteiset tiedot

On otettava huomioon, ettei Internet-yhteyksiä ole automaattisesti suojattu kolmansien osapuolien tarkastelulta. Käyttäjät eivät saa siirtää tietoja Internetin välityksellä ilman salausta, jos he katsovat siirrettävien tietojen olevan yksityisiä tai arkaluonteisia.

Käyttäjät eivät saa rekisteröityä yksityistä käyttöä varten Internet-sivuille tai -foorumeille Tilitoimisto X:n sähköpostitiedoilla.

Tilitoimisto X:n ICT voi käyttää teknisiä apuvälineitä rajoittamaan Internetin käyttöä näiden sääntöjen mukaisesti sekä valvomaan sääntöjen noudattamista.

6 Sähköposti

6.1 Sähköpostin kielletty käyttö

- työhön liittymättömien ohjelmistojen, kuvien, videoiden, musiikin jne. luominen tai jakaminen
- roskapostin, ketjukirjeiden tai vitsisähköpostien luominen tai jakaminen

- Tilitoimisto X:n sähköpostijärjestelmästä tai asiakasohjelmistosta tulleiden sähköpostien automaattinen lähettäminen eteenpäin muihin kuin Tilitoimisto X:n sähköpostiosoitteisiin, ellei Tilitoimisto X:n ICT ole antanut tähän lupaa.

6.2 Sähköpostin yksityinen käyttö

- Tilitoimisto X:n sähköpostijärjestelmän käyttö yksityisiin sähköpostitarkoituksiin on hyväksyttävää, mutta ei suositeltavaa. Käyttäjän vastuulla on varmistaa, ettei hän aiheuta pitkittynyttä kuormitusta verkko- tai sähköpostijärjestelmälle.
- Tilitoimisto X:n ICT:llä on lupa ryhtyä tarvittaviin toimiin, jos käyttäjän yksityinen sähköpostin käyttö haittaa Tilitoimisto X:n liiketoimintaa.
- Tilitoimisto X:n ICT ei ole vastuussa yksityisten sähköpostien varmuuskopioinnista tai palauttamisesta.
- Käyttäjät eivät saa muodostaa minkään Tilitoimisto X:n tietokoneen sähköpostiasiakasohjelmiston kautta yhteyttä ulkoiseen sähköpostijärjestelmään.

6.3 Ei-toivotut viestit ja teknisesti sopimattomat sähköpostit

Sähköposti- tai roskapostisuodatinjärjestelmät estävät ja poistavat automaattisesti muun muassa seuraavanlaiset sähköpostit:

- kaikki roskapostiviestit ja roskapostiksi tunnistettavat, viruksen luomat sähköpostiviestit poistetaan automaattisesti
- sähköpostit, joissa on käytetty sähköpostijärjestelmässä toimimatonta teknologiaa tai jotka aiheuttaisivat käsittelyongelmia
- Suoritettavaa tai muunlaista, mahdollisesti vaarallista koodia sisältävät sähköpostit.
- ylisuuret sähköpostiviestit.

Älykkäät, automaattiset ja itsestään oppivat sähköpostisuodatinmekanismit varmistavat, että kaikki vastaanottajat saavat kaikki heille osoitetut tarkoituksenmukaiset sähköpostinsa ja minimoivat samalla sellaisten ei-toivottujen sähköpostien määrän, jotka tulevat heidän postilaatikkoonsa. Roskapostien käsittelyyn liittyvien ongelmien vuoksi ei voida kuitenkaan täysin varmistaa, että roskapostien poistoon tarkoitettu suodatinjärjestelmä poistaisi ainoastaan roskaposteja. Joissakin tilanteissa järjestelmä saattaa käsitellä normaalia sähköpostia roskapostina ja poistaa sen automaattisesti.

6.4 Luottamuksellisia liiketoimintatietoja sisältävien sähköpostien salaaminen

Luottamuksellisia liiketoimintatietoja sisältävät sähköpostit, jotka lähetetään Tilitoimisto X:n sähköpostijärjestelmän ulkopuolelle, on aina salattava.

6.5 Liiketoiminnan kannalta oleelliset sähköpostit

Internet-sähköposti ei ole täysin luotettava viestintäkanava. Molempien osapuolten on aina varmistettava liiketoiminnan kannalta oleellisten tai muutoin tärkeiden sähköpostien lähettäminen ja vastaanottaminen.

6.6 Postilaatikon kokorajoitukset

Sanomavälitysjärjestelmä (sähköposti) ei ole tietojen arkistointijärjestelmä vaan viestintäväline. Äärimmäisen suuren, viesteistä koostuvan tietokannan palauttamiseen menee hätätilanteessa hyvin paljon aikaa. Jotta järjestelmän mahdollisia keskeytysaikoja olisi mahdollisimman vähän ja jotta niiden vaikutus liiketoimiin olisi mahdollisimman pieni, on postilaatikolle määritetty kohtuulliset kokorajoitukset.

7 Salasanat

7.1 Säännöt

- Käyttäjä on henkilökohtaisesti vastuussa omien salasanojensa salassapidosta.
- Salasanaa ei saa paljastaa toiselle käyttäjälle.
- Älä säilytä mitään salasanatietoja paperilla, ellet pysty säilyttämään tietoja turvallisessa paikassa.
- Valitse hyviä salasanoja, jotka sisältävät vähintään kahdeksan merkkiä, isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
- Käyttäjien ei tule luoda salasanoja, jotka ovat täysin samanlaisia tai huomattavan samantapaisia kuin käyttäjän aiemmin luomat salasanat.
- Käyttäjätunnuksien salasanat on muutettava säännöllisesti, vaikka järjestelmä ei vaatisi salasanan vaihtamista.
- Salasanat on aina salattava, kun niitä säilytetään tiedostojen tallennusmedialla.
- Saman salasanan käyttäminen sekä Tilitoimisto X:n käyttäjätunnuksissa että muissa tunnuksissa on kielletty.
- Salasana on vaihdettava välittömästi, jos joku saattaa tietää salasanan tai jos salasanan väärinkäyttöä epäillään tai sellainen on huomattu

7.2 Suositukset

Huonoja tai heikkoja salasanoja ovat muun muassa:

- Salasanassa on vähemmän kuin kahdeksan merkkiä.
- Salasana on sanakirjasta löytyvä sana (äidinkielinen tai vieraskielinen).
- Salasana on yleisessä kielenkäytössä käytetty sana, kuten perheenjäsenen, lemmikin, kaverin, työkaverin, kuvitteellisen hahmon tms. nimi.
- Tietokonetermit ja -nimet, komennot, sivustot, yhtiöt, laitteistot, ohjelmistot.
- Syntymäpäivät ja muut henkilökohtaiset tiedot, kuten osoitteet ja puhelinnumerot.
- Kirjain- tai numerosarjat, kuten aaabbb, qwerty, 12345 jne.
- Mikä tahansa yllä olevista takaperin kirjoitettuna.

8 Sisäinen tutkinta

Tietotekniikan väärinkäytöksistä suoritetaan aina sisäinen tutkinta. ICT:n havaitessa väärinkäytös tai tietoturvallisuutta vaarantava toiminta, raportoidaan havainnosta välittömästi turvallisuuspäällikölle.

Henkilöstöpäällikkö käynnistää asiasta sisäisen tutkinnan, joka suoritetaan yhdessä ICT-osaston tai ulkopuolisten asiantuntijoiden kanssa. Sisäisessä tutkinnassa

selvitetään yhtiön IT rekistereiden avulla tietoturvallisuuden vaarantanut käyttäjä, sekä selvitetään toiminnan järjestelmälle aiheuttaneet vahingot.

Henkilöstöpäällikkö tekee sisäisen tutkinnan perusteella raportin, joka toimitetaan toimenpide suosituksin toimitusjohtajalle. Toimitusjohtaja ryhtyy raportin pohjalta toimenpiteisiin, jotka kohdistuvat tietojärjestelmän väärinkäyttäjään.