Yritys X:n tieto- ja pilviturvallisuuden kehittäminen asiakkaiden vaatimusten mukaiseksi

Pekka Tyynelä

2022 Laurea

Laurea-ammattikorkeakoulu

Yritys X:n tieto- ja pilviturvallisuuden kehittäminen asiakkaiden vaatimusten mukaiseksi

Pekka Tyynelä

Turvallisuus ja riskienhallinta

Opinnäytetyö

Toukokuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuus ja riskienhallinta

Tradenomi (AMK)

Pekka Tyynelä

Yritys X:n tieto- ja pilviturvallisuuden kehittäminen asiakkaiden vaatimusten mukaiseksi

Vuosi 2022 Sivumäärä 39

Tämän tutkimuksellisen kehittämistyön tavoitteena oli tuottaa Yritys X:lle tietoturvallisuusdokumentti, joka kokoaa yhteen kaiken olennaisen Yrityksen X tieto- ja pilviturvallisuuden hallinnasta. Tietoturvallisuusdokumentin tarkoituksena oli helpottaa Yrityksen X myyntiyksiköiden työskentelyä tarjouspyyntöjen tietoturvallisuusvaatimuksien osalta. Asiakkaiden tietoturvallisuusvaatimukset kasvavat jatkuvasti, joten opinnäytetyölle nähtiin selkeä tarve tilaajaorganisaatiossa.

Opinnäytetyön muodoksi valikoitui tutkimuksellinen kehittämistyö, joten siinä yhdistyivät tutkimuksellisuus sekä käytännön työelämän kehittäminen. Opinnäytetyön tietoperusta pohjautui yleisesti tunnettuihin tieto- ja pilviturvallisuuden viitekehyksiin ja standardeihin. Tietoperustan tarkoituksena tässä opinnäytetyössä oli avata kehitettävää ilmiötä sekä yleisesti tukea opinnäytetyöprosessia kaikissa sen vaiheissa.

Käytettyjä tutkimusmenetelmiä tässä opinnäytetyössä olivat dokumenttianalyysi sekä asiantuntijahaastattelut. Dokumenttianalyysissa syvennyttiin asiakkailta tulleiden tarjouspyyntöjen tietoturvavaatimuksiin, joiden pohjalta syntyi Excel-taulukko, johon listattiin kaikki olennaisimmat tarjouspyynnöissä esiintyneet tietoturvavaatimukset. Asiantuntijahaastattelut suoritettiin Yrityksen X tietoturvallisuuspäälliköille ja niiden tarkoituksena oli saada tarkempaa tietoa Yrityksen X tieto- ja pilviturvallisuuden hallinnasta käytännössä.

Opinnäytetyön tuotoksena syntyi tietoturvallisuusdokumentti, joka avaa Yrityksen X tieto- ja pilviturvallisuuden pääpiirteet yleisellä tasolla. Tietoturvallisuusdokumentin sisältö pohjautui pääosin dokumenttianalyysista ja asiantuntijahaastatteluista kerättyyn aineistoon. Tietoturvallisuusdokumentti tehtiin mahdollisimman informatiiviseksi ja tiiviiksi, jotta sen käyttäminen olisi mahdollisimman tehokasta ja helppoa. Dokumenttia on jatkossa myös mahdollista muokata ja päivittää, mikäli tilaajaorganisaatio näkee sen tarpeelliseksi.

Asiasanat: pilviturvallisuus, tietoturvallisuus, tietoturvallisuuden hallintajärjestelmä

Laurea University of Applied Sciences **Abstract**

Safety, Security and Risk Management

Bachelor's Thesis

Pekka Tyynelä

Development of Company X's Information and Cloud Security to Meet Customer Requirements

Year 2022 Pages 39

The objective of this thesis is to create an information security document that brings together all the essentials of Company X's information and cloud security management. The purpose of the information security document is to facilitate the work of Company X's sales units regarding the information security requirements set by customers. Customers' information security requirements are constantly changing, so there was a clear need for the thesis in the commissioner organization.

Research development work was chosen as the form of the thesis, so the thesis combines research with the development of practical working life. The theoretical framework of the thesis is based on well-known information and cloud security frameworks and standards. The purpose of the theoretical framework in this thesis is to introduce the phenomenon and to generally back up the thesis process in all its stages.

The research methods used in this thesis are document analysis and expert interviews. The document analysis focuses on the information security requirements set by the customers. The result of the analysis is an Excel-chart that lists all the most relevant requirements set by the customers. The expert interviews were conducted with Company X's information security managers and their purpose is to provide more detailed information on Company X's information and cloud security management in practice.

The output of the thesis is an information security document, which opens up the main features of Company X's information and cloud security at a general level. The content of the information security document is mainly based on data collected from the document analysis and expert interviews. The document was made informative and concise, so it can be used efficiently. In the future, it will also be possible to edit and update the document if Company X deems it necessary.

Keywords: cloud security, information security, information security management system

Sisällys

1 Johdanto

Tietotekniikka on muuttanut elämäämme enemmän kuin mikään muu teknologia. Teknologisen kehityksen varjopuolena on kuitenkin siihen keskittynyt rikollisuus. Kyberrikolliset toimivat globaalisti ympäri maailmaa. Perinteinen rikollisuus on muuttunut digitaaliseksi, eli rikollinen toiminta tapahtuu sähköisissä toimintaympäristöissä ja tietoverkoissa. Digitaalinen rikollisuus kohdistuu käyttäjien päätelaitteisiin sekä erilaisiin palveluihin ja toimintoihin, joista he voivat saada taloudellista hyötyä. Jokainen omistaa nykypäivänä erilaisia laitteita, jotka ovat yhteydessä internettiin ja käyttää niitä kaikkialla päivittäin. Tämän takia tietoturvallisuudesta on tullut tärkeä turvallisuuden osa-alue, joka tulee ottaa huomioon kaikessa toiminnassa muun muassa työpaikalla. (Järvinen & Rousku 2017, luku 1.)

Tässä tutkimuksellisessa kehittämistyössä pyritään ratkaisemaan opinnäytetyön tilaajan havaitsema käytännön ongelma tutkimuksellisia kehittämismenetelmiä sekä monipuolisia tietoja pilviturvallisuuden tietolähteitä apuna käyttäen. Käytetyt menetelmät ja tietolähteet valikoituivat niiden luotettavuuden ja halutun lopputuotoksen kannalta. Tutkimuksellisen kehittämistyön lopputuotoksena syntyy tietoturvallisuusdokumentti, jonka opinnäytetyön tilaajayritys ottaa käyttöönsä.

Opinnäytetyön tilaajayritys on halunnut pysyä nimettömänä koko opinnäytetyöprosessin ajan, joten tässä opinnäytetyöraportissa sitä tullaan kutsumaan nimellä Yritys X. Yritys X on koko Suomen alueella toimiva suuri kiinteistöpalveluihin keskittynyt yritys, joka on osa suurempaa kansainvälistä konsernia. Yritys X:llä on asiakkaita sekä julkisella että yksityisellä sektorilla.

1.1 Opinnäytetyön taustaa

Tämä opinnäytetyö sai alkunsa Yrityksen X myyntiyksiköiden löytämästä tarpeesta. Yrityksen kasvavana haasteena on se, että yrityksen asiakkaiden tietoturvavaatimukset koventuvat jatkuvasti ja myyjien on yhä hankalampaa vastata asiakkaiden tarjouspyyntöjen yhteydessä esittämiin tietoturvallisuusvaatimuksiin. Erilaisia tietoturvallisuuspolitiikkoja ja ohjeistusta yrityksestä löytyy runsaasti, mutta myyntiyksiköillä on ollut vaikeuksia löytää näistä tarjouspyyntöihin tarvittavia tietoja. Tämän johdosta myyntiyksiköt kokevat tarvitsevansa tietoturvallisuusdokumentin, joka kokoaa yhteen kaiken tarjouspyyntöihin tarvittavan tiedon tietoturvallisuusasioiden hallinnasta yrityksessä.

Opinnäytetyö on yritykselle tärkeä, koska riskinä on, että tarjouskilpailuja saatetaan hävitä. Tämä johtuu osittain siitä, että tietoturvallisuusvaatimuksiin ei osata vastata tarpeeksi kattavasti, vaikka organisaatio täyttäisikin halutut vaatimukset. Opinnäytetyön pääasialliset hyötyjät ovat yrityksen myyntiyksiköt, mutta dokumentille voi löytyä tarvetta myös yrityksen laki-

ja vastuullisuusyksikön puolelta. Tietoturvallisuusdokumentti tulee olemaan kaikkien yrityksen työntekijöiden saatavilla yrityksen Intranetissä.

Opinnäytetyön muodoksi valikoitui tutkimuksellinen kehittämistyö. Tutkimuksellisessa kehittämistyössä päätarkoituksena on työelämän kehittäminen tutkivalla otteella. Tällöin yhdistyy tutkimuksellisien menetelmien soveltaminen yhdessä konkreettisen kehittämistoiminnan kanssa. (JAMK 2022.) Opinnäytetyössäni kehitän Yrityksen X tieto- ja pilviturvallisuutta tutkimuksellisia menetelmiä apuna käyttäen.

Tutkimuksellisen kehittämistyön luonteeseen kuuluu käytännöstä nousseiden ongelmien ratkaiseminen tai uusien käytäntöjen luominen. Usein myös luodaan uutta tietoa työelämän käytännöistä. Tutkimuksellisessa kehittämistyössä käytetään monipuolisesti erilaisia menetelmiä sekä kerätään kriittisesti arvioiden tietoa sekä teoriasta että käytännöstä kehittämisen tueksi. Tutkimuksellisessa kehittämistyössä myös tyypillisesti korostuu aktiivinen vuorovaikutus eri tahojen kanssa. (Ojasalo, Moilanen & Ritalahti 2015, 18.)

1.2 Opinnäytetyön tavoite, tutkimusongelma ja rajaukset

Opinnäytetyön taustalla on Yrityksen X tavoite helpottaa myyntiyksiköiden työskentelyä ja näin ollen lisätä myyntityön tehokkuutta. Opinnäytetyön tavoite on vastata Yrityksen X löytämään kehittämiskohteeseen tekemällä tietoturvallisuusdokumentti, joka vastaa Yrityksen X tarpeita. Opinnäytetyöstä löytyviä huomioita tullaan vertailemaan Yrityksen X nykyisiin käytäntöihin ja ottamaan myös käyttöön, mikäli tämä katsotaan tarpeelliseksi.

Tämän opinnäytetyön tutkimusongelma voidaan johtaa Yrityksen X haasteista tarjouspyyntöjen tietoturvallisuusvaatimuksien kanssa ja kysymysmuotoon aseteltuna se on ”Millainen tietoturvallisuusdokumentti helpottaisi myyntiyksiköitä tarjouspyyntöihin vastaamisessa?” Tähän ongelmaan pyritään löytämään ratkaisua tässä opinnäytetyössä erilaisia tutkimusmenetelmiä ja tietoperustaa apuna käyttäen.

Kun opinnäytetyön aihe on varmistunut, tulee sitä useimmiten rajata. Rajauksella tarkennetaan ajatusta siitä, mitä halutaan tietää tai osoittaa kerätyllä aineistolla (Hirsjärvi, Remes & Sajavaara 2009, 81). Opinnäytetyön rajausta alettiin alun perin pohtia tietoturvallisuusdokumenttiin tulevan sisällön perusteella. Dokumenttianalyysin ja Yrityksen X henkilöstön kanssa käytyjen keskustelujen ja palaverien pohjalta tietoturvallisuusdokumentin sisältö rajattiin hallinnolliseen ja tekniseen tietoturvallisuuteen sekä pilviturvallisuuteen. Pois päätettiin rajata kyberturvallisuus ja fyysinen tietoturvallisuus. Perusteita näiden pois rajaamiselle ovat opinnäytetyön tekoon käytettävän työmäärän kohtuullistaminen sekä tietoturvallisuusdokumentin sisällön pitäminen selkeänä ja rajattuna. Keskustelujen pohjalta ei myöskään herännyt suurta tarvetta keskittyä kyberturvallisuuden osa-alueeseen koska asiakkaiden vaatimukset eivät yleensä suoranaisesti käsittele tätä turvallisuuden osa-aluetta.

1.3 Aiemmat tutkimukset aihealueesta

Tietoturvallisuuden kehittämisestä eri organisaatioissa on tehty monia erilaisia tutkimuksia. Asiakasvaatimuksien pohjalta lähtöisin olevaa tietoturvallisuuden kehittämistyötä ei ole aikaisemmin tehty samalla tavalla kuin tässä opinnäytetyössä, joten suoraa vertailukohdetta oli hankala löytää. Alla kuitenkin muutama esimerkki opinnäytetöistä, joissa on onnistuneesti kehitetty jotain tietoturvallisuuden osa-aluetta organisaatiossa.

Janne Jalava (2021) kehitti opinnäytetyössään erään suomalaisen konsultointiyrityksen tietoturvallisuutta luomalla tälle julkisen tietoturvallisuuspolitiikan. Käytetyt tutkimusmenetelmät työssä olivat kirjallisuuskatsaus, asiantuntijahaastattelu sekä benchmarking. Opinnäytetyön tuotoksena syntynyt julkinen tietoturvapolitiikka toimii julkisena esityksenä yrityksen tietoturvallisuuden tahtotilasta sekä osittain myös pohjana konsultointiyrityksen omalle jatkuvalle tietoturvan kehittämistyölleen. (Jalava 2021.)

Anthony Baxter (2021) kehitti opinnäytetyössään tietoturvallisuuden riskienhallintaa valtioneuvoston kansliassa. Baxterin käyttämät kehittämismenetelmät koostuivat dokumenttianalyysistä, kyselystä, teemahaastattelusta sekä kirjallisuuskatsauksesta. Opinnäytetyöprosessiin kuului kehittämismenetelmien lisäksi valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytilan kartoitus sekä perehtyminen asiaan liittyvään lainsäädäntöön. Näiden pohjalta Baxter pystyi luomaan kehittämisehdotuksia tietoturvallisuuden riskienhallinnan kokonaisvaltaiseen kehittämiseen valtioneuvoston kansliassa. (Baxter 2021.)

2 Tietoperusta

Tietoperusta muodostaa kehittämistyön perustan kokoamalla kehittämisen kannalta oleellisen tiedon yhteen. Tutkimuksellisen kehittämistyön tietoperustassa määritellään käsitteet ja niiden väliset suhteet. Käsitteet ja niiden määritelmät osoittavat tutkimuksen näkökulman, auttavat jäsentämään ilmiötä sekä toimivat viestinnän pohjana. Tietoperustan tehtävänä on auttaa tutkijaa tuntemaan kehitettävä aihealue, jotta tutkimuksellinen kehittämistyö voidaan suorittaa onnistuneesti. (Ojasalo ym. 2015, 34.)

Seuraavissa kappaleissa esitän ja avaan opinnäytetyöprosessin kannalta olennaisimpia tieto- ja pilviturvallisuuden käsitteitä ja aihealueita. Tämän opinnäytetyön tietoperusta pohjautuu yleisesti tunnettuihin tieto- ja pilviturvallisuuden viitekehyksiin ja standardeihin. Tietoperustan tarkoituksena tässä opinnäytetyössä on avata kehitettävää ilmiötä sekä yleisesti tukea opinnäytetyöprosessia kaikissa sen vaiheissa. Tietoperusta on erityisesti ollut apuna tietoturvallisuusdokumentin teossa sekä haastattelukysymysten laadinnassa.

Tietoturvallisuus voidaan käsittää ja jakaa monella eri tavalla riippuen organisaatiosta ja kontekstista. Perinteinen jakotyyli on hallinnolliseen, tekniseen ja fyysiseen tietoturvallisuuteen, jota tullaan käyttämään myös tässä opinnäytetyössä. Pääpaino opinnäytetyössä tulee olemaan hallinnollisessa tietoturvallisuudessa työn rajaukset huomioon ottaen. Nämä osa-alueet tukeutuvat kuitenkin vahvasti toisiinsa, joten myös muita osa-alueita tullaan käsittelemään joissain määrin, kun se on katsottu tarpeelliseksi.

2.1 Tietoturvallisuus

Tieto on suojattava kohde, jota voidaan säilyttää digitaalisessa, fyysisessä kuin työntekijöiden tiedoista muodostuvana aineettomanakin muotona. Tieto on erittäin tärkeää organisaation liiketoiminnalle, ja siksi sitä on suojattava asianmukaisesti. Tietoa voidaan välittää monin eri keinoin, kuten sähköisenä tai suullisina viesteinä sekä lähettien välityksellä. Välityskeinosta tai muodosta riippumatta tieto tulee kuitenkin aina suojata asianmukaisin keinoin. (SFS-ISO 27000:2017, 3.2.2.)

Tietojärjestelmällä tarkoitetaan nimensä mukaisesti järjestelmää, jossa käsitellään tietoja, kuten erilaiset sovellukset, palvelut tai muu tietotekniikkaomaisuus. Se on kokoelma erilaista tietoa, jota käytetään avuksi esimerkiksi liiketoiminnan tavoitteiden saavuttamiseen. Tietojärjestelmä käyttää erilaisia laitteistoja tiedon tehokkaan siirtämisen toteuttamiseksi. (SFS-ISO 27000:2017, 2.39; Indeed 2021.)

Tiedolla ja tietojärjestelmillä on luonnollinen elinkaari niiden syntymisestä tai perustamisesta niiden tuhoamiseen tai hävittämiseen. Suojattavien kohteiden arvo voi muuttua niiden elinkaarien aikana, mutta tietoturvallisuus on silti tärkeä osa elinkaarien jokaista vaihetta. (SFS-ISO 27002:2017, 0.5.)

Tietoturvalla eli tietoturvallisuudella tarkoitetaan erilaisia teknisiä ja hallinnollisia toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Tiedon luottamuksellisuus tarkoittaa sitä, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Eheys tarkoittaa sitä, että tietoja ei pääse muuttamaan muut kuin siihen oikeutetut. Käytettävyydellä tarkoitetaan sitä, että tietojärjestelmät ja tiedot ylipäänsä ovat niiden käyttöön oikeutettujen saatavilla ja hyödynnettävissä. (Traficom 2020.)

Tietoturvallisuus on yksi Elinkeinoelämän keskusliiton yritysturvallisuusmallin osa-alueista. Tietoturvallisuudesta tulee jatkuvasti yhä keskeisempi osa organisaatioiden turvallisuutta. Tietoturvallisuuden osa-alueita ovat esimerkiksi hallinnollinen tietoturvallisuus, tekninen tietoturvallisuus, tieto- ja yksityisyydensuoja, tietojen merkityksen arviointi, tietojen luokittelu ja käsittely sekä järjestelmien ja prosessien toiminnan jatkuvuuden varmistaminen. (Elinkeinoelämän keskusliitto 2021.)

Yrityksen tietoturvallisuudesta puhuttaessa täytyy kuitenkin muistaa, että yrityksen tarkoitus on tehdä voittoa omistajilleen. Tietoturvallisuuden perimmäisenä tarkoituksena on tukea yrityksen liiketoimintaa ja sen tulee tapahtua kustannustehokkaasti sekä riskiperusteisesti (Peltier 2014, xiii-xiv).

Hallinnollisen tietoturvallisuuden kontrolleja ovat esimerkiksi tietoturvallisuuspolitiikat ja -ohjeistukset. Ne luovat raamit yrityksen tietoturvallisuudelle, joiden tarkoituksena on johtaa ja ohjeistaa organisaation työntekijöitä toimimaan ja työskentelemään tietoturvallisella tavalla. Hallinnollinen tietoturvallisuus on erityisen tärkeää, koska myös teknisen ja fyysisen tietoturvallisuuden kontrollit määräytyvät sen pohjalta. (Vacca 2013, 386.)

Teknisen tietoturvallisuuden kontrollit ovat ohjelmistoja tai laitteita, jotka kontrolloivat pääsyä tietojärjestelmiin. Niiden tarkoituksena on auttaa pienentämään virheiden määrää ja turvallisuuspolitiikan rikkomuksia. Teknisiä kontrolleja ovat muun muassa salasanat, palomuurit, tiedonsalaus sekä pääsyoikeuksien hallintalistat. Tärkeää teknisen tietoturvallisuuden onnistumisen kannalta on vähimpien oikeuksien periaate (Principle of Least Privilege), joka tarkoittaa, ettei mikään järjestelmä, ohjelmisto tai henkilö saa enempää käyttöoikeuksia kuin on työn onnistuneen tekemisen kannalta tarpeellista. (Vacca 2013, 386.)

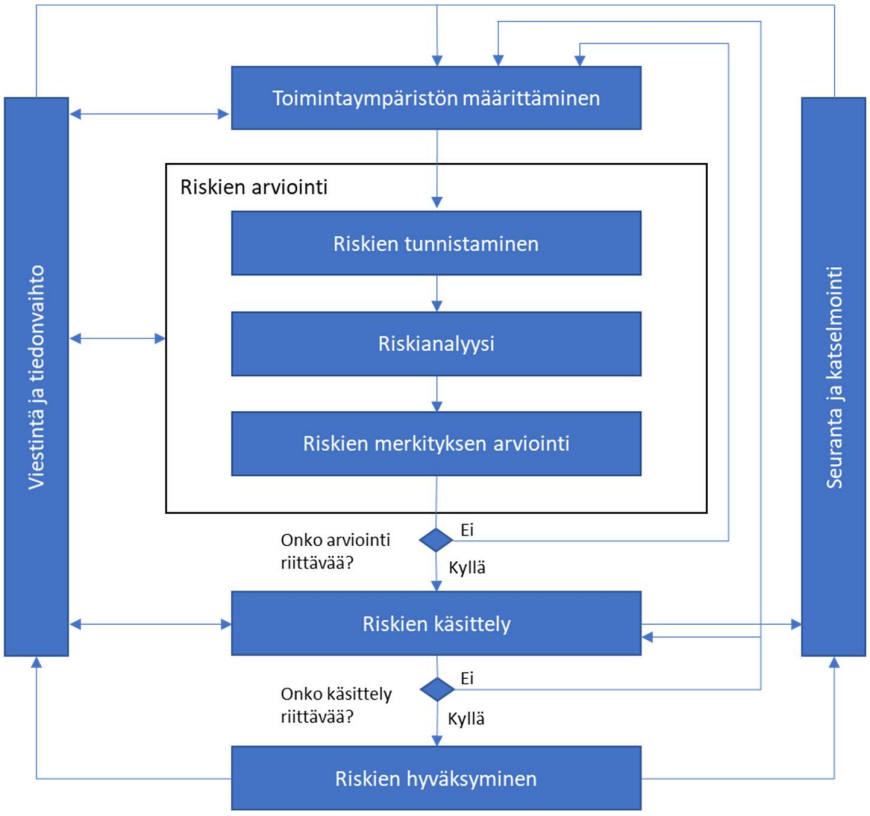
Fyysisen tietoturvallisuuden kontrollit valvovat ja suojaavat työpaikan fyysistä ympäristöä, kuten työskentely- ja ICT-tiloja. Niiden tehtävänä on myös kontrolloida pääsyä näihin tiloihin. Nämä tilat ovat tietoturvallisuuden kannalta myös hyvä erottaa toisistaan. Fyysisen tietoturvallisuuden kontrollit voidaan jakaa valvoviin ja estäviin. Valvovien kontrollien tehtävä on valvoa ja raportoida mahdollisista ei-toivotuista tapahtumista. Näitä ovat muun muassa varashälyttimet ja valvontakamerat. Estävien kontrollien tehtävä on fyysisesti estää luvaton pääsy valvottuihin tiloihin. Näitä ovat muun muassa lukot ja korkeat aidat. (Vacca 2013, 386; Andress 2014, 135.)

Kyberturvallisuuden sanaston (2018) mukaan: ”Tietoturvauhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen.” Uhkia tietojärjestelmille on monenlaisia. Jotkin niistä ovat tahallisia yrityksiä yrittää horjuttaa niitä. Toiset puolestaan odottamattomia ja ikäviä yllätyksiä. Uhkia ovat muun muassa vakoilu, tietojen kiristäminen tai tietojen tuhoaminen. Yleensä suurimman uhkan näille järjestelmille muodostaa kuitenkin ihmisten tekemät virheet tai luonto, kuten tulvat tai hurrikaanit. Yritykset saattavat pyrkiä ennakoimaan ja torjumaan kaikki mahdolliset uhat, mutta tämä ei yksinkertaisesti ole mahdollista. Uhkatekijät ovat uhkia vain silloin, jos niille annetaan mahdollisuus hyödyntää jotain haavoittuvuutta. Vaikka haavoittuvuus olisi olemassa, ei ole varmuutta, että sitä koskaan hyödynnettäisiin. Tämän vuoksi organisaatioiden on tärkeää pohtia mitkä uhkat ovat suurimpia omalle organisaatiolle ja keskittyä niiden torjumiseen. (Vacca 2014, 4–5.)

2.2 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä koostuu yleensä erilaisista ohjeista, menettelytavoista, toimintaperiaatteista sekä niihin liittyvistä toiminnoista ja resursseista, joita organisaatio hallinnoi kootusti suojatakseen kaikkea sille kuuluvaa tieto-omaisuutta. Se on järjestelmällinen lähestymistapa tietoturvallisuuden laatimiseen, toteuttamiseen, käyttöön, seurantaan, katselmointiin, ylläpitoon sekä parantamiseen organisaatiossa. Tietoturvallisuuden hallintajärjestelmä perustuu riskien arviointiin sekä organisaation määrittelemiin riskien hyväksyntätasoihin. Tietoturvallisuuden hallintajärjestelmä voidaan toteuttaa myös osana organisaation muita toiminnan seuranta- ja suunnittelumekanismeja kuten laatuohjelmaa. (SFS-ISO 27000:2017, 3.2.1; Johdon tietoturvaopas 2011, 14.)

Tietoturvallisuusriskien hallintaprosessi (Kuvio 1) eroaa hieman tavallisesta riskienhallintaprosessista. Tietoturvariskien hallintaprosessissa riskien arviointi ja käsittelyprosessit voivat toistua useampaan otteeseen, jotta voidaan varmistua etenkin suurten riskien asianmukaisesta arvioinnista ja hallintakeinojen oikeanlaisesta määrittämisestä. (SFS-ISO 27005:2018, 6.)



Kuvio 1: Tietoturvariskien hallintaprosessi (SFS-ISO 27005:2018, 6)

Tietoturvallisuusriskien hallintaprosessi lähtee toimintaympäristön määrittämisestä. Sisäisen ja ulkoisen toimintaympäristön määrittämiseen sisältyy tietoturvariskien hallintaan

tarvittavien peruskriteerien asettaminen, rajojen ja laajuuden määrittely sekä tietoturvariskien hallinnan organisointi. (SFS-ISO 27005:2018, 6, 7.1.)

Toimintaympäristön määrittämisen jälkeen siirrytään tietoturvariskien arviointiin. Se pitää sisältää riskien tunnistamisen, riskianalyysin sekä riskien merkityksen arvioinnin. Riskien arvioinnissa ensin määritetään suojattavien tietokohteiden arvo ja määritetään niihin kohdistuvat tai jo olemassa olevat uhkat ja haavoittuvuudet. Tämän jälkeen määritetään käytössä olevat hallintakeinot sekä niiden vaikutukset tunnistettuihin riskeihin. Seuraavaksi määritetään näiden seuraukset. Lopuksi asetetaan riskit tärkeysjärjestykseen jo aikaisemmin toimintaympäristön määrittämisen yhteydessä asetettujen riskien merkityksen arviointikriteerien mukaisesti. (SFS-ISO 27005:2018, 8.1.)

Riskien arvioinnin jälkeen on vuorossa riskien käsittely. Riskien käsittelyyn on neljä vaihtoehtoa: riskin muokkaaminen, jakaminen, säilyttäminen tai välttäminen. Sopivat käsittelyvaihtoehdot eri riskeille valitaan riskien arvioinnin tulosten ja niistä aiheutuvien kustannus/hyötysuhteen perusteella. Riskien käsittelylle täytyy myös tehdä riskinkäsittelysuunnitelma, jossa yksilöidään käsittelytoimenpiteiden tärkeysjärjestys ja aikataulu. (SFS-ISO 27005:2018, 9.1.)

Riskien käsittelyn jälkeen päästään tietoturvariskien hyväksymiseen. Riskinkäsittelysuunnitelmassa tulee kuvata, kuinka arvioidut riskit käsitellään, että ne täyttävät riskienhyväksymiskriteerit, jotka on jo aikaisemmin toimintaympäristön kanssa määritelty. Tietoturvariskien hyväksymisen päätökset ja vastuut tulee kirjata muodollisesti. Organisaation tulee luoda luettelo hyväksytyistä riskeistä ja perustella ne riskit, jotka eivät ole normaalien hyväksymiskriteerien mukaisia. (SFS-ISO 27005:2018, 10.)

Viestintä ja tiedonvaihto on tärkeä osa tietoturvariskien hallintaprosessia ja sitä tulee toteuttaa jatkuvasti koko prosessin ajan. Tietoa tulee jakaa päätöksentekijöiden ja muiden riskienhallintaprosessissa mukana olevien sidosryhmien kesken. Riskeistä puhumisen ja viestinnän tavoitteena on saavuttaa kaikkien sidosryhmien ja päätöksentekijöiden välille yksimielisyys siitä, miten riskienhallinta toteutetaan. (SFS-ISO 27005:2018, 11.)

Riskien seuranta ja katselmointi on oleellinen ja jatkuva osa tietoturvariskien hallintaprosessia. Riskien seuranta on tärkeää, jotta saadaan aikaisessa vaiheessa tietoa toimintaympäristön muutoksista ja saataisiin pidettyä yllä yleiskuvaa riskeistä. Organisaation tulee jatkuvasti seurata muun muassa uusia suojattavia kohteita, uusia uhkia, tarvetta muuttaa suojattavien kohteiden arvoja, tunnistettuja haavoittuvuuksia sekä tietoturvahäiriöitä. (SFS-ISO 27005:2018, 12.1.)

2.3 Tietoturvallisuuspolitiikka

Yrityksen X tietoturvallisuuspolitiikat ovat olennainen osa tätä opinnäytetyötä. Ne ovat olleet suurimmassa roolissa tähän opinnäytetyöhön kuuluvan tietoturvallisuusdokumentin teossa. Ne ovat ainoa lähde asiantuntijahaastattelujen lisäksi, joista saa tietoa, kuinka Yritys X hoitaa tietoturvallisuuden hallintaansa. Yritys X:llä on käytössään Yrityksen X emoyhtiön tietoturvallisuuspolitiikka sekä oma tietoturvallisuuspolitiikkansa, jonka tarkoitus on tarkentaa ja osittain myös tiukentaa emoyhtiön tietoturvapolitiikassa esitettyjä tietoturvallisuuden hallintakeinoja.

Politiikka on korkean tason lausunto yrityksen tavoitteista, päämääristä sekä yleisistä keinoista niiden saavuttamiseksi tietyllä osa-alueella. Tietoturvallisuuspolitiikka on koko organisaation laajuinen dokumentti, jossa käsitellään tietojen käsittelyyn ja suojaamiseen liittyviä päätöksiä. Tietoturvallisuuspolitiikka on tehokkaan tietoturvallisuuden hallintajärjestelmän kulmakivi ja se toimii pohjana kaikille muille yrityksen tietoturvaohjeistuksille, -standardeille sekä -prosesseille. Tämän vuoksi on tärkeää tehdä siitä asianmukainen ja kattava. (Peltier 2014, xxi–2.)

Tietoturvallisuuspolitiikalla on kaksi roolia: sisäinen ja ulkoinen. Sisäisen tietoturvallisuuspolitiikan rooli on kertoa työntekijöille mitä heiltä odotetaan ja kuinka heidän tekemisensä arvioidaan. Ulkoisen tietoturvallisuuspolitiikan rooli on kertoa yrityksen ulkopuolisille tahoille, kuinka yritys näkee omat vastuunsa ja kuinka se suojaa muun muassa tietojaan. (Peltier 2014, 2.)

ISO 27001 (5.2) mukaan tietoturvallisuuspolitiikan tulee soveltua organisaation toiminta-ajatukseen, kertoa tietoturvatavoitteet tai muodostaa perusta niiden asettamiselle sekä sisältää sitoutumisen tietoturvallisuusvaatimuksien täyttämiseen ja tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen. Tietoturvallisuuspolitiikan tulee olla koko organisaation tiedossa ja tarvittaessa myös sidosryhmien saatavilla sekä sen tulee olla dokumentoidussa muodossa. (ISO/IEC 27001:2017, 5.2.)

2.4 Pilviturvallisuus

Pilvipalveluilla tarkoitetaan tietojenkäsittelykapasiteettia tai -palvelua, joka on verkon yli saavutettavissa. Pilvipalveluiden tuottamisessa hyödynnetään skaalautuvien, joustavien ja jaettujen resurssien mallia, joka on osittain automatisoitu itsepalveluperiaatteella tuotettavaksi. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 10.)

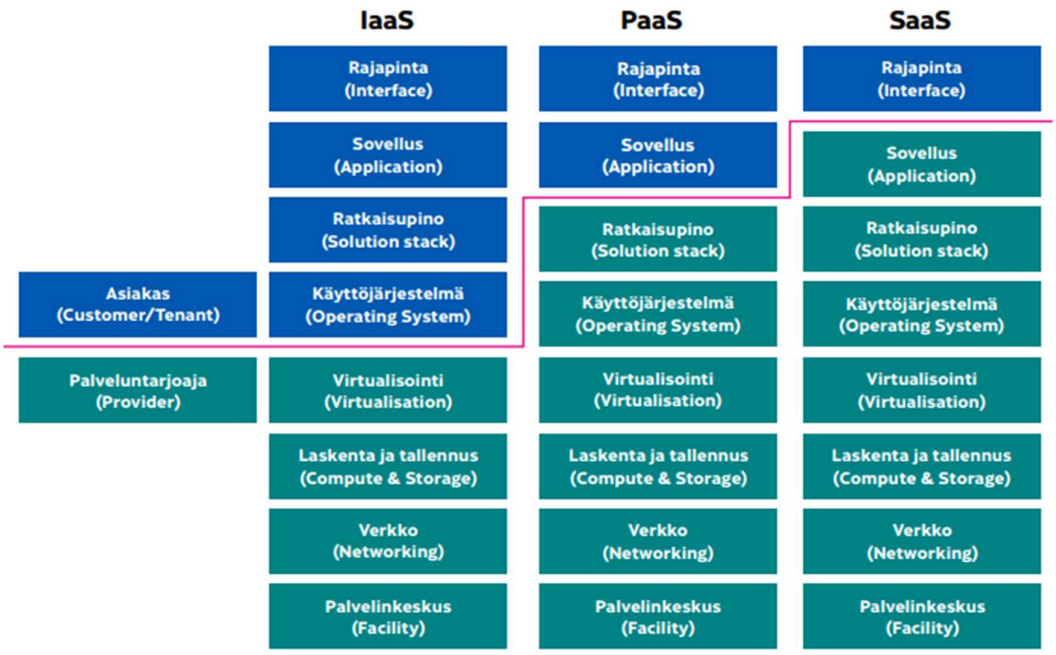
Pilvipalvelut ovat viime vuosina kasvattaneet suosiotaan huomattavasti niin yritysten kuin yksityishenkilöidenkin keskuudessa. Pilvipalveluiden kustannustehokkuus, monipuolisuus ja helppokäyttöisyys tukevat monien eri tahojen tarpeita. Vuoden 2021 viimeisellä

vuosineljänneksellä pilvi-infrastruktuurin palveluna ostamiseen käytettiin yli 50 miljardia dollaria. Suurimmat pilvipalveluiden tarjoajat ovat Amazon Web Services, Microsoft Azure sekä Google Cloud. (Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille 2019, 3; Korhonen 2022.)

Pilviturvallisuudella tarkoitetaan pilvipalveluihin tallennetun tiedon suojaamista varkaudelta, vuotamiselta ja poistamiselta. Keinoja pilviturvallisuuden varmistamiseen ovat muun muassa erilaiset palomuurit, penetraatiotestaukset, virtuaaliset erillisverkot (VPN) sekä julkisten verkkojen välttäminen. (Frankenfield 2021.)

Pilvipalveluiden turvallisuudessa on tärkeää tuntea pilvipalveluiden palvelu- ja toteutusmallit. Pilvipalveluiden yleisimpiä palvelumalleja on kolme: infrastruktuuri palveluna (Infrastructure as a Service, IaaS), ohjelmistoalusta palveluna (Platform as a Service, PaaS) sekä ohjelmisto palveluna (Software as a Service, SaaS). (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 10.)

Infrastruktuuri palveluna (IaaS) tarkoittaa, että kaikki palveluntuottamiseen tarvittava infrastruktuuri tulee palveluntarjoajalta. Ohjelmistoalusta palveluna (PaaS) tarkoittaa, että palvelut tuotetaan valmiin ohjelmistoalustan avulla. Ohjelmisto palveluna (SaaS) puolestaan tarkoittaa että, palveluntarjoaja tuottaa kaikki pilvipalveluihin liittyvät palvelut kokonaisuudessaan. Pilviturvallisuuteen liittyvät vastuut riippuvat valitusta palvelumallista ja sen toteutukseen liittyvistä yksityiskohdista, mutta ne jakautuvat kuitenkin aina palveluntarjoajan ja asiakkaan välille. Vastuujako toteutuu tyypillisesti (Kuvio 1) mukaisesti. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 10.)



Kuvio 2: Tyypillinen turvallisuuden vastuujakomalli asiakkaan ja palveluntarjoajan välillä (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 10)

Pilvipalveluiden yleisimpiä toteutusmalleja on kolme: yksityinen pilvi (private cloud), julkinen pilvi (public cloud) sekä yhdistelmäpilvi (hybrid cloud). Yksityinen pilvi on palvelu, joka tuotetaan vain palvelun tilanneelle organisaatiolle joko tilaajaorganisaation ja/tai palveluntarjoajan konesaleista. Yksityisellä pilvellä pystytään tyypillisesti tuottamaan turvallisempaa palvelua kuin muilla toteutusmalleilla. Julkinen pilvi on julkisesti tarjolla oleva palvelu, jonka kuka tahansa voi hankkia ja se tuotetaan lähes aina palveluntarjoajan konesaleissa. Julkinen pilvi on yksityistä alttiimpi hyökkäyksille sen laajemman hyökkäyspinta-alan vuoksi. Yhdistelmäpilvi on julkisen ja yksityisen toteutusmallin yhdistelmä. Yhdistelmäpilvessä voidaan tyypillisesti täydentää yksityistä pilveä julkisen pilven palveluilla. Turvallisuustaso yhdistelmäpilvessä riippuu siitä, kuinka turvallisuus on järjestetty toteutusten rajapinnoissa ja siitä mitä tietoja on ylipäänsä mahdollista siirtää yksityisestä pilvestä julkiseen pilveen. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 11.)

Pilviturvallisuuden kannalta on tärkeää myös tuntea palveluntarjoaja sekä palveluiden ja tietojen fyysinen sijainti. Palvelun tilaajan on varmistuttava palveluntarjoajan kyvykkyydestä tuottaa luotettavaa ja turvallista palvelua. Muun muassa kotimaisten palveluntarjoajien luotettavuutta voidaan arvioida ja selvittää kansallisen yritysturvallisuusselvityksen avulla. Pilvipalveluissa käsiteltävien tietojen säilytys sekä käsittely voi tapahtua eri sijainneissa kuin esimerkiksi pilvipalvelun tuottamiseen liittyvät hallinnointi- ja ylläpitotoimet. Tämä tuo omat riskinsä tietojen turvallisuuden takaamiseksi. PiTuKrin mukaan esimerkiksi pilvipalveluissa olevien henkilötietojen tulee fyysisesti sijaita tietosuojasääntelyn mahdollistamalla alueella

(EU/ETA) ja muun salassa pidettävän tiedon tulee sijaita fyysisesti Suomessa. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 12–16.)

Pilviturvallisuus ei juurikaan eroa muiden tietojenkäsittely-ympäristöjen turvallisuudesta, mutta erilaisista toteutusmalleista johtuen siihen liittyvät riskit vaihtelevat. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) jakaa pilviturvallisuuden riskit neljään eri luokkaan (Taulukko 1).

Politiikka ja organisaatioriskit	Tietojen ylläpito-oikeuden menettäminen, vastuullisuushaasteet, pilvipalveluntarjoajan konkurssi tai toimitusketjun epäonnistuminen.
Tekniset riskit	Resurssien riittämättömyys, tietovuodot, palvelunestohyökkäykset tai salausavainten häviäminen.
Oikeudelliset riskit	Eri maiden lainsäädäntöjen erilaisuus, lisensointi tai viranomaisten haasteet.
Yleiset riskit	Tietoverkon häiriöt, käyttäjän manipulointi (social engineering), varmuuskopioiden häviäminen tai luonnonkatastrofit. (Vacca 2013, 98–102.)

Taulukko 1: Pilviturvallisuuden riskit

2.5 Aiheeseen liittyvää lainsäädäntöä

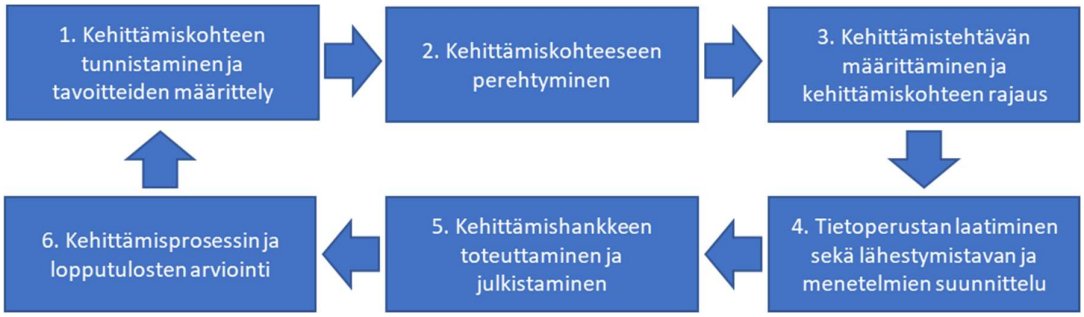
Yrityksen tietoturvallisuusjohtamisen keskeinen osa on lainsäädännön asettamien vaatimusten seuraaminen. Keskeisin lainsäädäntö mikä tietoturvallisuuden osalta tulee huomioida, keskittyy tietosuojaan ja sen vaatimuksiin. Tietosuojalla tarkoitetaan jokaisen henkilön perusoikeutta, joka turvaa henkilön oikeuksien sekä vapauksien toteuttamista henkilötietojen käsittelyssä. Tietosuoja ja tietoturva linkittyvät toisiinsa siten että tietoturvallisuus on yksi tietosuojan toteuttamisen keinoista. Tietoturvallisuuden tarkoituksena on suojata esimerkiksi tietoaineistoa ja tietojärjestelmiä. (Tietosuojavaltuutetun toimisto 2022a.)

Vuonna 2016 voimaan tullut EU:n yleinen tietosuoja-asetus asettaa organisaatioille ja yrityksille tarkat vaatimukset henkilötietojen keräämiselle, säilytykselle sekä hallinnoinnille. Pääkohtia asetuksessa ovat muun muassa se, että tietojenkäsittelyn tulee aina perustua henkilön suostumukseen, tietojenkäsittelyn tiedotuksen avoimuus, oikeus päästä käsiksi omiin tietoihinsa, oikeus korjata tietojaan tai vastustaa niiden käsittelyä sekä oikeus tulla unohdetuksi. (Euroopan unioni 2021.)

Tietosuojalaki 1050/2018 täydentää ja tarkentaa EU:n yleistä tietosuoja-asetusta. Tietosuojalaki avaa enemmän yleisen tietosuoja-asetuksen kansallista soveltamista Suomessa ja siinä säädetään esimerkiksi tietosuoja-asioita valvovien viranomaisten nimittämisestä, toimivaltuuksista sekä organisaatioista. Muut tarkennukset liittyvät esimerkiksi erityisten henkilötietoryhmien käsittelyyn, henkilötunnusten käsittelyyn sekä rajoituksista rekisteröidyn oikeuksiin. (Tietosuojalaki 2015/2018; Tietosuojavaltuutetun toimisto 2022b.)

3 Tutkimuksellisen kehittämistyön toteutus

Tässä kappaleessa keskitytään kuvailemaan tämän opinnäytetyöprosessin vaiheet teoriaa apuna käyttäen. Opinnäytetyöprosessi eteni Ojasalon ym. (2015, 24) esittämän tutkimuksellisen kehittämistyön prosessin (Kuvio 1) mukaisesti.



Kuvio 3: Tutkimuksellisen kehittämistyön prosessi (mukaillen Ojasalo ym. 2015, 24)

Ensimmäinen vaihe opinnäytetyöprosessissa on kehittämiskohteen tunnistaminen ja tavoitteiden määrittely. Kehittämistyö voi olla joko ongelmaperustainen tai uudistamisperustainen. Ongelmaperustaisessa kehittämisessä pyritään löytämään ratkaisua käytännössä havaittuun haasteeseen tai ongelmaan. Uudistamisperustaisessa kehittämisessä puolestaan etsitään uutta erilaisia rajapintoja kohtaamalla. (Ojasalo ym. 2015, 26.) Kehittämiskohde tunnistettiin Yrityksessä X, jo ennen tämän opinnäytetyön varsinaista aloittamista, koska se oli jo jonkin aikaa tuonut haasteita Yrityksen X myyntiyksiköiden työskentelylle. Kehittämiskohteeksi tunnistettiin tietoturvallisuusdokumentaation hajanaisuus ja tästä johtuvat vaikeudet tarjouspyyntöjen tietoturvallisuusvaatimuksiin vastaamisessa. Tässä opinnäytetyössä kehittämistyö on siis ongelmaperustainen.

Jäljelle ensimmäisestä vaiheesta jäi siis tavoitteiden määrittely. Tavoitteeksi voitiin kehittämiskohteen löytämisen perusteella määritellä myyntiyksiköiden työn helpottaminen tarjouspyyntöjen vastaamisen osalta, jonka pohjalta syntyi idea tietoturvallisuusdokumentista, joka kasaisi kaiken oleellisen yhteen tietoturvallisuusasioiden hallinnasta Yrityksessä X. Näin ollen

myyjät pystyisivät saamaan tarjouspyyntöihin tarvittavat tiedot yhdestä dokumentista sen sijaan että etsisivät sitä lukuisista eri tietoturvallisuusohjeista ja -politiikoista.

Toinen vaihe opinnäytetyöprosessissa on kehittämiskohteeseen perehtyminen. Tässä vaiheessa on tärkeää opetella tuntemaan kehittämisen kohde perusteellisesti. Tarkemmin tämä tarkoittaa taustatiedon hankkimista kohteesta, kuten esimerkiksi yrityksen taustatiedot, strategiat, arvot, toimiala sekä toimintaympäristö. Tähän vaiheeseen sisältyy myös tutkimuskirjallisuuden hankkiminen ja tutustuminen. (Ojasalo ym. 2015, 28–30.)

Kehittämiseen kohteeseen perehtyminen on tämän opinnäytetyön tapauksessa suoritettu työharjoittelun aikana, jolloin tutuiksi tulivat niin toimintaympäristö kuin yrityksen strategia. Tutkimuskirjallisuus tähän opinnäytetyöhön valikoitui tietoturvallisuusdokumentin tarpeiden mukaisesti, joten tietoperusta keskittyy tässä tapauksessa luotettuihin lähteisiin tieto- ja pilviturvallisuuden osa-alueilla sekä Yrityksen X omaan tietoturvallisuusdokumentaatioon.

Kolmas vaihe opinnäytetyöprosessissa on kehittämistehtävän määrittäminen ja rajaus. Kehittämistehtävässä syntyy usein jokin konkreettinen tuotos, toimintatapa tai kehittämisidean luominen. Tässä vaiheessa tulee pohtia huolellisesti mihin kehittämisellä pyritään ja se tulee tarkasti määritellä. (Ojasalo ym. 2015, 32–33.)

Kehittämistehtävä määriteltiin yhdessä Yrityksen X kanssa, jotta voitiin varmistaa oikeanlainen lopputulos. Kehittämistehtävälle oli huomattu selkeä tarve, joten määrittelyyn ei kulunut kauaa aikaa, koska haluttu lopputulos oli alusta asti selvillä. Tässä opinnäytetyössä kehittämistehtävällä pyrittiin helpottamaan myyntiyksiköiden työskentelyä helposti luettavan tietoturvallisuusdokumentin avulla. Kehittämistehtävän rajaus toteutettiin tässä tapauksessa dokumenttianalyysin sekä Yrityksen X tarpeiden mukaan.

Neljäs vaihe opinnäytetyöprosessissa on tietoperustan laatiminen sekä lähestymistavan ja menetelmien suunnittelu. Tietoperustan tehtävä on muodostaa kehittämistehtävän perusta kokoamalla yhteen kehittämisen kannalta oleellista tietoa. Tietoperustassa määritellään sekä käsitteet että niiden väliset suhteet, joista muodostuu kehittämistehtävän käsitejärjestelmä. (Ojasalo ym. 2015, 34.)

Tietoperusta tässä opinnäytetyössä muodostuu pääosin tietoturvallisuuden, tietoturvallisuuden hallintajärjestelmän, sekä pilviturvallisuuden eri käsitteiden määritelmistä ja yhteyksistä. Tietoperustan teoria pohjautuu laajasti tunnettuihin tieto- ja pilviturvallisuuden standardeihin ja viitekehyksiin sekä kansainvälisesti tunnettujen tieto- ja pilviturvallisuuskirjailijoiden teoksiin.

Lähestymistapa määritellään kehittämistehtävän perusteella. Erilaisten lähestymistapojen tunteminen helpottaa kehittämistehtävän suunnittelua ja niiden avulla on helpompi yhdistää

tutkimuksellisuus kehittämisen osaksi. Erilaisia lähestymistapoja tutkimukselliselle kehittämistyölle ovat muun muassa tapaustutkimus, toimintatutkimus sekä konstruktiivinen tutkimus. Kehittämishankkeessa voi olla piirteitä myös monesta eri lähestymistavasta. (Ojasalo ym. 2015, 36.)

Tässä opinnäytetyössä käytetty lähestymistapa on konstruktiivinen tutkimus, koska kehittämistehtävän lopputuotoksena syntyi konkreettinen tuotos tietoturvallisuusdokumentin muodossa. Konstruktiivisen tutkimuksen tavoitteena on ratkoa jokin käytännön ongelma luomalla jokin konkreettinen tuotos. Konstruktiivisessa tutkimuksessa muutetaan jotain konkreettista kohdetta, ei niinkään ihmisten toimintatapoja. (Ojasalo ym. 2015, 37–38.)

Kehittämismenetelmät jaetaan yleensä määrällisiin (kvantitatiivisiin) ja laadullisiin (kvalitatiivisiin) menetelmiin. Kehittämistyölle tärkeää on näiden menetelmien moninaisuus ja tärkeää on pohtia mitä tietoa tarvitaan ja mihin tarkoitukseen sitä käytetään. Eri menetelmiä käyttämällä saadaan monia näkökulmia ja erilaista tietoa kehittämistehtävää varten. (Ojasalo ym. 2015, 40.)

Kehittämismenetelmät tässä opinnäytetyössä valikoituivat kehittämistehtävän ja Yrityksen X tarpeiden perusteella. Käytetyt menetelmät tässä opinnäytetyössä olivat dokumenttianalyysi sekä haastattelu. Näiden menetelmien tarkoituksena oli saada opinnäytetyön tuotoksesta Yrityksen X näköinen ja sen standardien mukainen. Käytettyjä kehittämismenetelmiä käydään tarkemmin läpi tämän opinnäytetyön neljännessä luvussa.

Viides vaihe sisältää kehittämishankkeen toteuttamisen ja julkistamisen. Kehittämistehtävässä on tärkeää raportoida etenemisestä koko kehittämisprosessin ajan. Tekstin jatkuva kirjoittaminen edistää kehittämistyön etenemistä ja se voi myös jäsentää omia ajatuksia paremmin, jonka johdosta syntyy helpommin uusia ajatuksia prosessin eteenpäin viemiseksi. Kehittämistyön loppuraportin pääpaino keskittyy yleensä kehittämisprosessin, tietoperustan ja kehittämistehtävän tarkkaan kuvaamiseen. Näiden lisäksi on tärkeää tuoda esille myös kehittämistehtävän aikaansaannokset sekä arviointi. (Ojasalo ym. 2015, 46–47.)

Tämä kehittämishanke toteutettiin ikään kuin vuoropuheluna opinnäytetyöraportin ja varsinaisen tietoturvallisuusdokumentin välillä. Tietoturvallisuusdokumenttiin tuli sisältöä samaan tahtiin kuin varsinaiseen opinnäytetyöraporttiin, jotta kumpikaan ei jäisi laahaaman jälkeen ja ajatukset säilyisivät selkeinä molempien osalta. Tämän toimintatavan avulla pystyttiin varmistamaan molempien sekä opinnäytetyöraportin että tietoturvallisuusdokumentin kannalta haluttu lopputulos.

Viimeinen eli kuudes vaihe opinnäytetyöprosessissa on kehittämisprosessin ja lopputuloksen arviointi. Arviointia kuitenkin tapahtuu koko opinnäytetyöprosessin ajan, koska sen avulla voidaan suunnata kehittämistyötä haluttuun suuntaan. Lopullisen arvioinnin tarkoituksena on

näyttää, miten kehittämistyö onnistui. Kehittämistyön arviointi keskittyy yleensä kehittämistyön panoksiin, prosessiin sekä lopputuotoksiin ja näiden kaikkien välisiin suhteisiin. (Ojasalo ym. 2015, 47.)

Suuri osa tätä opinnäytetyöprosessia on ollut jatkuva pohdiskelutyö käytettyjen lähteiden ja menetelmien luotettavuudesta ja riittävyydestä. Opinnäytetyöprosessin ja siitä saatavan lopputuotoksen jatkuva arviointi auttoi tässä tapauksessa saamaan parempia tuloksia ja työnjälkeä. Tätä opinnäytetyötä on jatkuvasti arvioitu opinnäytetyön tilaajan, koulun kuin itse kirjoittajankin toimesta, jotta pystyttiin varmistamaan kaikkien kannalta haluttu lopputulos.

4 Menetelmät

Tutkimusmenetelmät kehittämistyössä on perinteisesti jaettu määrällisiin (kvantitatiivisiin) ja laadullisiin (kvalitatiivisiin) menetelmiin. Määrällinen menetelmä on perinteisesti joko strukturoitu lomakehaastattelu tai lomakekysely. Näissä menetelmissä kysytään suurelta joukolta vastaajia samoja asioita. Tyypillisiä laadullisia menetelmiä taas ovat erilaiset teema-, ryhmä- ja avoimet haastattelut. Laadullisissa menetelmissä tutkittavia on yleensä paljon vähemmän kuin määrällisessä, mutta analysoitavaa aineistoa tulee yleensä enemmän. (Ojasalo ym. 2015, 104–105.)

Tutkimuksellisessa kehittämistyössä laadullisten ja määrällisten menetelmien raja kuitenkin yleensä hämärtyy ja niissä menetelmät ovat enemmänkin välinearvon roolissa. Tutkimuksellisessa kehittämistyössä menetelmien tarkoituksena on auttaa parhaisiin mahdollisiin uusiin käytäntöihin. (Ojasalo ym. 2015, 105.) Tässä opinnäytetyössä tämä uusi käytäntö, tai pikemminkin tuotos, tulee olemaan uusi tietoturvallisuusdokumentti erityisesti Yrityksen X myyntiyksiköiden käyttöön.

Opinnäytetyössä käytettiin tutkimusmenetelminä kahta erilaista metodia. Oikeiden menetelmien valinta opinnäytetyössä on erityisen tärkeää, jotta prosessi olisi sujuva ja tuottaisi oikeita tuloksia. Käytetyt menetelmät tässä opinnäytetyössä ovat dokumenttianalyysi sekä haastattelu. Näiden menetelmien tarkoituksena oli helpottaa työskentelyä tietoturvallisuusdokumentin parissa, jotta siitä saatiin Yrityksen X näköinen ja standardien mukainen.

4.1 Dokumenttianalyysi

Pääasiallinen tiedonkeruumenetelmä opinnäytetyössäni oli dokumenttianalyysi. Dokumenttianalyysillä pyritään yleensä tekemään päätelmiä kirjalliseen muotoon saatetusta aineistosta. Aineistoa dokumenttianalyysissä voivat olla esimerkiksi tekstiksi muutetut haastattelut, artikkelit, muistiot, raportit tai ylipäänsä mikä tahansa tutkittavasti ilmiöstä kirjoitettu, kuvattu tai puhuttu materiaali. (Ojasalo ym. 2015, 136.)

Dokumenttianalyysin tavoitteena on suorittaa dokumenttien analysointi järjestelmällisesti ja tämän avulla luoda selkeä ja sanallinen kuvaus kehitettävästä ja tutkittavasta asiasta. Sisällönanalyysissä pyritään aineisto järjestämään tiiviiksi ja selkeäksi. Analyysin perimmäinen tarkoitus on informaatioarvon lisääminen. Tämän avulla saadaan aineistoon selkeyttä, jotta pystytään tekemään luotettavia ja ymmärrettäviä johtopäätöksiä. (Ojasalo ym. 2015, 136.)

Yhtenä dokumenttianalyysin vahvuutena on sen herkkyys asiayhteydellä ja se, että sitä voidaan käyttää myös sellaisen aineiston kanssa, jota ei alun perin ole edes tarkoitettu tutkimusta varten (Ojasalo ym. 2015, 136). Opinnäytetyössäni käytin aineistona Yrityksen X asiakkailta tulleita tarjouspyyntöjä ja selkeää on, ettei näitä ole alun perin tarkoitettu tutkimukseen, vaan niiden tarkoituksena on ollut toimia ainoastaan tarjouskilpailutuksen välineenä. Tarjouspyynnöissä kiinnitin huomiota ainoastaan niiden liitteisiin, joiden sisältö muodostui erilaisista tietoturvavaatimuksista ja näiden selvityspyynnöistä Yritykselle X. Tämän on myös yksi syy siihen, että kiinnitin dokumenttianalyysissä huomiota ainoastaan aineiston sisältöön, enkä niiden käyttötarkoitukseen tai siihen kuinka niiden sisältö on muodostunut.

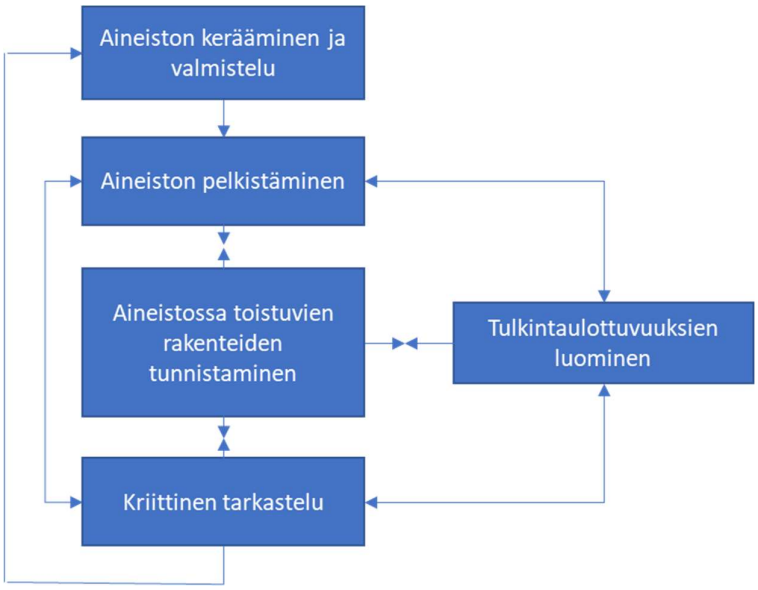
Dokumenttianalyysin aineisto koostui viidestä eri tarjouspyynnöstä, jotka sisälsivät tietoturvallisuusvaatimuksia Yritykselle X. Näistä vain neljä oli opinnäytetyön kannalta käyttökelpoisia dokumenttianalyysiin, koska yhdessä niistä ei ollut opinnäytetyön kannalta relevanttia sisältöä, joten se jätettiin dokumenttianalyysin ulkopuolelle. Neljästä analyysissä käytettävästä tarjouspyynnöstä kolme sisälsi suoria tietoturvallisuusvaatimuksia Yritykselle X ja yhdessä tarjouspyynnössä pyydettiin selvityksiä tietyistä tietoturvallisuuden alueista. Tarjouspyynnöistä kolme ovat kunnalliselta puolelta ja yksi yksityiseltä puolelta.

Kaikki analysoidut tarjouspyynnöt liittyivät suoraan erilaisiin teknisiin järjestelmiin, joten suurin osa niiden sisällöstä on suoria teknisiä vaatimuksia kyseiselle järjestelmälle tai sen ylläpidolle. Teknisiin järjestelmiin liittyvät vaatimukset rajasin pois tästä opinnäytetyöstä, koska tarkoitus oli keskittyä ainoastaan Yrityksen X yleiseen toimintaan liittyviin hallinnollisiin ja teknisiin tietoturvallisuusvaatimuksiin. Suoraan teknisiin järjestelmiin liittyviä vaatimuksia ei sisällytetty tietoturvallisuusdokumenttiin, koska muuten dokumentista tulisi liian spesifi tiettyä järjestelmää kohtaan.

Alun perin dokumenttianalyysissä oli tarkoituksena keskittyä myös pilviturvallisuuteen, mutta saamissani tarjouspyynnöissä ei siihen liittyviä vaatimuksia ollut. Tästä johtuen dokumenttianalyysissä ei käsitellä pilviturvallisuutta, mutta sitä käsitellään silti haastattelussa, koska yhtenä vaatimuksena tietoturvallisuusdokumentille oli, että siinä olisi oma osio pilviturvallisuusasioihin liittyen.

Ojasalon ym. (2015, 137) mukaan dokumenttianalyysissä on kaksi erilaista analyysitapaa: sisällön erittely ja sisällön analyysi. Sisällön analyysissä pyritään kuvaamaan analysoitavien dokumenttien sisältöä sanallisesti ja siinä tavoitteena on tunnistaa ja etsiä tekstin merkityksiä.

Sisällön erittely puolestaan tarkoittaa dokumenttien analyysiä, jossa kuvataan määrällisesti, muun muassa numeroilla, tekstin sisältöä. Nämä analyysitavat eivät myöskään ole toisiaan pois sulkevia. Analyysitapa, jota opinnäytetyössäni käytän, on sisällön analyysi, mutta siinä on myös hieman sisällön erittelyä. Laadullisen tutkimuksen yleisessä mallissa (Kuvio 4) esitetyt vaiheet kuvaavat hyvin myös dokumenttianalyysin vaiheita (Ojasalo ym. 2015, 138).



Kuvio 4: Laadullisen tutkimuksen yleinen malli (Ojasalo ym. 2015, 138)

Dokumenttianalyysissä käytettävä aineisto minulla oli jo valmiiksi saatavilla, joten aineiston keräämiseen ei kulunut aikaa. Jokainen tarjouspyyntö liitteineen oli omassa Excel-tiedostossaan. Aluksi luin jokaisen tiedoston muutamaan otteeseen läpi, jotta sain jo alustavan yleiskuvan tiedostojen sisällöistä. Valmistelun aloitin järjestämällä aineistot yhteen kansioon ja numeroimalla ne, jotta niihin olisi helpompi viitata myöhemmin. Aineiston valmistelun tarkoituksena on saada aineisto selkeään ja sisällöltään valmiiseen muotoon analysointia varten (Ojasalo ym. 2015, 138).

Tämän jälkeen aloitin aineiston pelkistämisen poistamalla aineistosta kaiken ylimääräisen, joka ei suoraan liittynyt Yrityksen X hallinnolliseen tai tekniseen tietoturvallisuuteen. Tämän johdosta aineiston tekstimäärä supistui huomattavasti. Aineiston pelkistämisen tarkoituksena on tiivistää sekä selkeyttää aineistoa, eli pyritään tunnistamaan ja rajaamaan aineistosta pieni määrä näkökulmia (Ojasalo ym. 2015, 139).

Aineiston pelkistämisen jälkeen tein Excel-taulukon (Liite 1), johon lisäsin kaikki tietoturvallisuusdokumentin kannalta oleellisimmat tietoturvallisuusvaatimukset ja selvityspyynnöt, joita asiakkaiden tarjouspyynnöt sisälsivät. Tämän Excel-taulukon tarkoitus oli auttaa aineistossa toistuvien rakenteiden tunnistamisessa ja tulkinnassa. Taulukon avulla pystyin löytämään

yhtäläisyyksiä eri asiakkaiden esittämissä vaatimuksissa, joka auttoi pohtimaan tietoturvallisuusdokumenttiin tulevaa sisältöä.

Kriittinen tarkastelu on osa jokaista dokumenttianalyysin vaihetta ja sillä pyritään parantamaan tulosten luotettavuutta ja laatua. Sen tavoitteena on muun muassa tunnistaa ja korjata eri vaiheissa mahdollisesti esiintyviä virheitä tai vääristymiä. (Ojasalo ym. 2015, 138.) Kriittinen tarkastelu näkyi dokumenttianalyysissä siten, että pyrin analyysin aikana jatkuvasti tarkastamaan, ettei tarjouspyyntöihin jäänyt mitään olennaista tietoa, jota olisi voinut käyttää analyysin myöhemmissä vaiheissa.

4.2 Haastattelu

Toinen tiedonkeruumenetelmä tässä opinnäytetyössä on haastattelu. Haastattelu on yksi käytetyimmistä tiedonkeruumenetelmistä sekä kehittämis- että tutkimustöissä. Haastatteluilla saadaan nopeasti kerättyä syvällistä tietoa kehittämistehtävän kohteesta. Yksi haastattelun tehtävistä on asioiden syventäminen ja selventäminen. (Ojasalo ym. 2015, 106.)

Haastattelu on menetelmänä joustava, koska siinä tutkija voi tehdä haastattelun aikana uusia kysymyksiä ja opastaa vastaajaa. Haastattelua käytetään yleensä silloin, kun ilmiötä ei tunneta tarpeeksi hyvin, jotta voitaisiin esittää tästä yksityiskohtaisia kysymyksiä. Haastateltavat valitaan yleensä sillä perusteella, että haastattelun aiheena oleva ilmiö koskettaa heitä. (Kananen 2015, 143–145.) Haastattelu on sopiva menetelmä tähän opinnäytetyöhön, koska haastattelujen aihealueet koskevat Yrityksen X tieto- ja pilviturvallisuuden osa-alueita, josta opinnäytetyön tekijällä itsellään on vain vähän kokemusta. Haastateltavat ovat puolestaan omien aihealueidensa asiantuntijoita ja johtajia.

Käytetty haastattelumuoto tässä opinnäytetyössä on puolistrukturoitu asiantuntijahaastattelu. Puolistrukturoitu haastattelu on nimensä mukaisesti strukturoidun ja strukturoimattoman haastattelun välimuoto. Strukturoidussa haastattelussa tutkija esittää joukon avoimia kysymyksiä, jotka esitetään jokaiselle haastateltavalle samassa järjestyksessä. Strukturoidussa haastattelussa haastattelijan vaikutus pyritään jättämään minimiin. Strukturoimaton haastattelu on muodoltaan yleensä avoin- tai teemahaastattelu. Teemahaastattelussa keskustellaan tietyistä ennakkoon valituista teemoista vapaamuotoisesti, kun taas avoimessa haastattelussa keskustellaan aiheesta yleisesti ilman mitään rajoittavia tekijöitä. (Kananen 2015, 145.)

Asiantuntijahaastattelussa voidaan soveltaa haastattelutyyppejä sen mukaan mitä tutkitaan ja useimmiten asiantuntijahaastattelu on puolistrukturoidun haastattelun muunnelma. Asiantuntijaksi voidaan kutsua henkilöä, jolla on jotain sellaista tietoa tietystä aihealueesta, jota maallikolla ei ole. Asiantuntijuus ei ole pysyvä ominaisuus tai kyky, vaan se voi määrittyä muun muassa vuorovaikutuksessa tai toiminnassa esimerkiksi ammatillisten tehtävien kautta.

Asiantuntijoita haastatellaan yleensä sen vuoksi että heillä oletetaan olevan tietoa tutkittavasta aiheesta. (Hyvärinen, Nikander & Ruusuvuori 2017, luku 9.)

Asiantuntijahaastattelu on sopiva menetelmä opinnäytetyöhön, koska haastattelujen tarkoituksena oli saada sisältöä tietoturvallisuusdokumenttiin tieto- ja pilviturvallisuuden hallinnasta Yrityksessä X. Haastateltavat vastaavat näistä aihealueista Yrityksessä X, joten he ovat omien alojensa asiantuntijoita. Kukaan muu Yrityksen X sisältä ei tunne näitä aihealueita paremmin kuin haastateltavat, joten haastatteluista saadun tiedon luotettavuus ja oikeellisuus on varmaa. Asiantuntijahaastatteluja tässä opinnäytetyössä suoritettiin vain kaksi kappaletta, jotta haastattelujen luotettavuus ja merkityksellisyys säilyisi mahdollisimman korkealla. Mikäli haastateltavia olisi valittu enemmän, niin niistä saatua tietoa ei olisi voinut varmuudella todeta oikeaksi. Tietoturvallisuuspäälliköt ovat Yrityksen X sisällä ne henkilöt, jotka vastaavat ja ovat perillä tieto- ja pilviturvallisuusasioiden hallinnasta yrityksessä.

Ensimmäinen haastattelu suoritettiin Yrityksen X tietoturvallisuuspäällikölle ja haastattelun aiheena oli hallinnollinen tietoturvallisuus Yrityksessä X. Haastattelu suoritettiin Teams-sovelluksen välityksellä. Haastattelukysymykset lähetettiin haastateltavalle etukäteen, jotta haastateltava ehti perehtyä niihin ennen haastattelua. Tällä tavoin haastattelu sujui jouhevasti ja kysymyksiin saatiin kattavat ja valmiiksi pohditut vastaukset. Alustavat haastatteluvastaukset kirjattiin ylös muistiinpanoina jo haastattelun aikana. Haastattelun jälkeen muistiinpanot kirjattiin puhtaaksi ja lähetettiin haastateltavalle vielä tarkistettavaksi, jotta vastaukset saatiin varmasti oikein ja väärinymmärryksiltä vältyttäisiin. Haastattelun tuloksia käytettiin apuna tietoturvallisuusdokumentin hallinnollisen tietoturvallisuuden osuuden kirjoittamisessa.

Toinen haastattelu suoritettiin Yrityksen X emoyhtiön tietoturvallisuuspäällikölle ja haastattelun aiheena oli tekninen tietoturvallisuus ja pilviturvallisuus Yrityksessä X. Haastattelu suoritettiin Teams-sovelluksen välityksellä. Toinen haastattelu toteutettiin samalla tavalla kuin ensimmäinenkin, ainoastaan kysymysten sisältö ja haastateltava vaihtuivat. Toisen haastattelun tuloksia käytettiin apuna tietoturvallisuusdokumentin teknisen tietoturvallisuuden ja pilviturvallisuuden osuuksien kirjoittamisessa.

5 Tulokset

Tämän luvun tarkoituksena on esittää dokumenttianalyysistä sekä haastatteluista saatuja tuloksia. Haastattelujen osalta tuloksien esitys perustuu haastattelukysymyksien havainnollistamiseen, koska haastatteluiden vastaukset ovat Yrityksen X salassa pidettävää tietoa.

Olennainen osa tutkimuksellista kehittämistyötä on kehittää jotain työelämässä esiintyvää osa-aluetta. Tässä opinnäytetyössä kehityksen painopisteenä on tieto- ja pilviturvallisuus. Opinnäytetyön tuloksena syntyi haastattelujen ja dokumenttianalyysin lisäksi konkreettinen

tietoturvallisuusdokumentti, jonka tarkoitus on vastata Yrityksen X tarpeisiin ja helpottaa myyntiyksiköiden työskentelyä tarjouspyyntöjen vastausprosesseissa.

5.1 Dokumenttianalyysi

Dokumenttianalyysin tuloksena syntyi Excel-taulukko (Liite 1), johon on kirjattu kaikki oleellisimmat asiakkaiden tarjouspyynnöissä esiintyneet tietoturvallisuusvaatimukset sekä selvityspyynnöt. Taulukosta voidaan huomata, että noin 89 prosenttia (24 kpl) vaatimuksista/selvityspyynnöistä liittyvät hallinnolliseen tietoturvallisuuteen ja noin 11 prosenttia (3 kpl) liittyvät tekniseen tietoturvallisuuteen.

Yhteensä tietoturvallisuusvaatimuksia/selvityspyyntöjä sisällytettiin taulukkoon 27 kappaletta. Tekniseen tietoturvallisuuteen liittyvät on merkitty punaisella ja hallinnolliseen tietoturvallisuuteen liittyvät mustalla tekstillä. Huomioon otettavaa on, ettei kaikkiin vaatimuksiin vastata suoraan tietoturvallisuusdokumentissa, koska tietoturvallisuusdokumentin sisältö pidetään yleisellä tasolla menemättä liikaa tietoturvallisuuden hallinnan yksityiskohtiin.

Taulukosta voidaan nopeasti päätellä, että varsinkin kunnalliset asiakkaat vaativat palveluntuottajaa toimimaan jonkin yleisesti tunnetun tietoturvallisuuden hallintajärjestelmän periaatteiden mukaisesti. Dokumenttianalyysistä käy ilmi myös se, että asiakkaat odottavat palveluntarjoajalta säännöllistä raportointia tietoturvallisuuden tasosta ja tilasta sekä henkilöstön ja johtajien vastuiden oikeanlaista määrittelyä tietoturvallisuusasioiden hoidossa.

Tärkein asia, jonka taulukko ikään kuin kiteyttää, on se, että jokainen asiakas vaatii palveluntoimittajaltaan kattavaa tietoturvallisuusdokumentaatiota. Tämä johtaa juurensa suoraan tämän opinnäytetyön tarpeeseen, koska opinnäytetyön tarkoituksena on nimenomaan helpottaa tämän vaatimuksen toteuttamista.

Dokumenttianalyysin aineistomäärä jäi suunniteltua niukemmaksi, mutta tämä ei varsinaisesti vaikuta opinnäytetyön lopputuotokseen. Niukasta aineistomäärästä huolimatta voidaan silti vahvistaa käsitys siitä, että Yritys X:llä on todellinen tarve tietoturvallisuusdokumentille, joka avaa asiakkaille sen mitä tietoturvallisuuden hallinta Yrityksessä X sisältää.

5.2 Haastattelut

Haastatteluja tässä opinnäytetyössä suoritettiin kaksi kappaletta, joista molemmat olivat yksilöhaastatteluja. Haastateltavat valittiin Yrityksen X sisältä ja haastatteluiden sisältö on suunniteltu heidän asemansa ja tietojensa pohjalta. Haastattelujen tuloksia ei tässä raportissa sanatarkasti esitetä, koska niiden sisältö on salassa pidettävää tietoa. Haastattelupohjat (Liitteet 2 & 3) löytyvät raportin lopusta.

Yrityksen X tietoturvallisuuspäällikön haastattelun (Liite 2) kysymyksillä pyrittiin muun muassa selvittämään Yrityksen X ja Yrityksen X emoyhtiön roolien ja vastuunjaon kuvaus hallinnollisen tietoturvallisuuden hoitamisessa. Muut kysymykset koskivat hallinnollisen tietoturvallisuuden kontrolleja, tietoturvallisuusasioiden koulutusta henkilöstölle, tietoturvallisuuden auditointiprosesseja sekä tietoturvallisuuden hallintajärjestelmän jatkuvaa parantamista.

Haastattelusta saatujen vastauksien avulla sain muotoiltua tietoturvallisuusdokumenttiin selkeän kuvauksen Yrityksen X tietoturvallisuuden hallinnasta hallinnollisen tietoturvallisuuden osalta. Haastattelusta dokumenttiin päätyneitä tietoja olivat myös muun muassa hallinnollisen tietoturvallisuuden kontrollien kuvaus, tietoturvallisuusasioiden koulutus henkilöstölle, tietoturvallisuuden hallinnointijärjestelmien auditoinnit sekä tietoturvallisuuden jatkuvan parantamisen periaatteet.

Yrityksen X emoyhtiön tietoturvallisuuspäällikön haastattelun (Liite 3) kysymyksillä pyrittiin selvittämään Yrityksen X teknisen tietoturvallisuuden sekä pilviturvallisuuden hallinnan yleispiirteitä. Teknisen tietoturvallisuuden kysymykset koskivat muun muassa Yrityksen X ja sen emoyhtiön välistä vastuunjakoa, teknisen tietoturvallisuuden kontrolleja sekä tietoturvapoikkeamia ja niihin reagoimista. Pilviturvallisuuden kysymysosio puolestaan keskittyi pilviturvallisuudesta huolehtivien osapuolien vastuualueisiin, pilviturvallisuuden riskienhallintaan, pilvipalveluiden turvakäytäntöjen arviointiin sekä tietosuojaan.

Haastatteluvastauksien avulla pystyin avaamaan tietoturvallisuusdokumenttiin tarkemmin Yrityksen X teknisen tietoturvallisuuden ja pilviturvallisuuden pääpiirteitä. Kaikkia haastattelun vastauksia ei käytetty sellaisenaan tietoturvallisuusdokumentin kirjoittamiseen, vaan niitä muokattiin sellaiseen muotoon, jonka voi esittää potentiaalisille asiakkaille, eikä sisältäisi teknisiä yksityiskohtia Yrityksen X tieto- ja pilviturvallisuuden hallinnointiin liittyen. Tärkeimmät asiat, jotka haastattelusta päätyivät tietoturvallisuusdokumenttiin, olivat pilviturvallisuuden vastuunjaon kuvaus, teknisen tietoturvallisuuden sekä pilviturvallisuuden kontrollit sekä näiden molempien osa-alueiden auditoinnin kuvaukset.

6 Johtopäätökset

Tämän opinnäytetyön tutkimusongelma määritettiin kysymykseksi: ”Millainen tietoturvallisuusdokumentti helpottaisi myyntiyksiköitä tarjouspyyntöihin vastaamisessa?” Tämän opinnäytetyön tarkoitus oli vastata tähän ongelmaan tietoturvallisuusdokumentilla, joka sisältää yleiskuvauksen Yrityksen X tieto- ja pilviturvallisuuden hallinnasta aina työntekijän rekrytoinnista hallintajärjestelmien jatkuvaan parantamiseen. Itse kysymykseen ei suoraan saada vastausta lyhyen opinnäytetyöprosessin aikana, mutta tietoturvallisuusdokumentti on tehty tämä kysymys mielessä pitäen. Yrityksen X kanssa käytyjen keskustelujen perusteella voidaan tosin

todeta, että dokumentille on todellinen käyttötarve, ja se tulee varmasti olemaan hyödyllinen työkalu tulevaisuudessa.

Tietoturvallisuusdokumentin sisältö on dokumenttianalyysin, asiantuntijahaastatteluiden, tietoperustan sekä Yrityksen X kanssa käytyjen keskustelujen lopputulos. Nämä kaikki ovat omalta osaltaan muovanneet dokumentin sisällön lopulliseen muotoonsa. Tietoturvallisuusdokumentin sisältö on syntynyt kriittisesti analysoimalla näitä kaikkia tiedonlähteitä ja valitsemalla niiden pohjalta kaikki merkityksellisimmiksi koetut aihealueet lopulliseen dokumenttiin.

Tietoturvallisuusdokumentin tarkoituksena ei ollut syventyä Yrityksen X tieto- ja pilviturvallisuuden hallintaan yksityiskohtaisesti, vaan tarkoituksena on alusta alkaen ollut tehdä dokumentti, joka avaa Yrityksen X tieto- ja pilviturvallisuuden pääpiirteet yleisellä tasolla. Mikäli mahdollinen asiakas vaatii tarkempaa informaatiota tieto- ja pilviturvallisuuden yksityiskohdista Yrityksessä X, tullaan tämä avaamaan asiakaskohtaisesti tarjouspyynnöissä erikseen.

Yrityksen X tahtotila oli, että tietoturvallisuusdokumentti olisi mahdollisimman informatiivinen mutta ei tekstiosuudeltaan liian pitkä. Tietoturvallisuusdokumentin ensimmäisten versioiden tarkastelun jälkeen, tekstiä poistettiin runsaasti, jotta dokumentin sisältö olisi mahdollisimman suoraviivainen, eikä sisältäisi mitään ylimääräistä. Dokumenttia tullaan käyttämään jatkossa tarjouspyyntöihin vastaamisen apuna ja sitä on jatkossa myös helppo muokata ja päivittää tarpeiden mukaan. Tietoturvallisuusdokumentin sisältö on jaettu kahdeksaan kappaleeseen, joiden sisältöä kuvataan alla olevassa taulukossa (Taulukko 2).

Johdanto	Johdannossa kuvaillaan dokumentin tarkoitusta ja siinä kuvaillaan ja avataan mihin Yrityksen X toiminta tietoturvallisuuden osalta perustuu sekä mitä sen tietoturvallisuuden hallintajärjestelmä pääpiirteissään sisältää.
Tietoturvallisuuden hallinta	Tietoturvallisuuden hallintakappaleessa käydään tarkemmin läpi muun muassa mihin tietoturvallisuuden hallinta perustuu, tieto- ja pilviturvallisuuden vastuunjakoa yritysten välillä, tietoturvallisuuden vastuuhenkilöitä, tietoturvariskien arviointiprosessia sekä tiedon luokittelua Yrityksessä X.

Arvioinnit	Arviointikappaleessa käydään läpi tietoturvallisuuden auditointiprosessia ja avataan tarkemmin sisäisen ja ulkoisen arvioinnin tarkoitusta.
Perehdyttäminen ja koulutus	Perehdyttäminen ja koulutuskappaleessa syvennytään Yrityksen X perehdytysprosessiin yleisesti sekä tietoturvallisuuskoulutuksen osalta.
Säädösten seuraaminen	Säädösten seuraaminen nimisessä kappaleessa käydään läpi, kuinka Yritys X seuraa muuttuvaa lainsäädäntöä sekä tämän mukana tulevia vaatimuksia yrityksen tietoturvallisuudelle
Jatkuva parantaminen	Jatkuvan parantamisen kappaleessa käydään läpi Yrityksen X toimia tietoturvallisuuden hallintajärjestelmän jatkuvan parantamisen varmistamiseksi.
Organisaatiot	Organisaatiokappaleessa on listattuna Yrityksen X ja sen emoyhtiön vastuuhenkilöitä tietoturvallisuuden osalta.
Liitteet	Liitekappaleessa on lista sertifikaateista ja muista tietoturvallisuuteen liittyvistä luvista/todistuksista, joita Yrityksellä X on käytössään.

Taulukko 2: Tietoturvallisuusdokumentin sisältö

Tietoturvallisuusdokumentin sisältö on tarkastettu lopuksi Yrityksen X tietoturvallisuuspäällikön kanssa ja häneltä saadun palautteen perusteella voidaan todeta, että tutkimusongelma on saatu ainakin tietoturvallisuusdokumentaation osalta ratkaistua. Tarjouskilpailuissa on toki aina oikeanlaisen dokumentaation lisäksi olemassa paljon muitakin kokonaisuuksia, jotka vaikuttavat niiden lopputulokseen. Opinnäytetyön tuloksena syntynyt tietoturvallisuusdokumentti tulee kuitenkin omalta osaltaan helpottamaan tarjouskilpailuissa menestymistä.

6.1 Pohdinta

Opinnäytetyöprosessia ja etenkin opinnäytetyöraportin kirjoittamista hieman hankaloitti Yrityksen X tahtotila pysyä nimettömänä koko opinnäytetyöprosessin ajan, jonka vuoksi lopullisen opinnäytetyöraportin sisältö jäi haluttua niukemmaksi. Tämä ei kuitenkaan vaikuttanut opinnäytetyöprosessista syntyneen tietoturvallisuusdokumentin tekoon, joten opinnäytetyölle asetetut tavoitteet niin opinnäytetyöntekijän kuin Yrityksen X näkökulmasta pystyttiin saavuttamaan halutulla tasolla.

Opinnäytetyön toteutus onnistui siihen määritellyssä aikataulussa ja opinnäytetyöprosessi sujui lähes ongelmitta. Yhteistyö opinnäytetyön tilaajan kanssa oli sujuvaa, vaikkakin haastattelujen lisäksi varsinaisen raportin kirjoittamisprosessin aikana varsin niukkaa. Tämä ei silti haitannut opinnäytetyöprosessin etenemistä, koska opinnäytetyölle oli saatu asetettua selkeät raamit ja tavoitteet jo ennen opinnäytetyöraportin varsinaista kirjoittamista. Myös tietoturvallisuusdokumenttiin haluttu sisältö saatiin suhteellisen tarkasti määriteltyä jo ennen sen varsinaista kirjoittamista, joka teki opinnäytetyöprosessin etenemisestä sujuvaa ja vaivatonta molemmille osapuolille.

Oma osaaminen ja tietämys erityisesti tieto- ja pilviturvallisuuden osa-alueilla kasvoi opinnäytetyöprosessin aikana huomattavasti ja uskon, että tästä on hyötyä myös tulevaisuuden työpaikkoja silmällä pitäen. Myös haastatteluiden järjestäminen niiden suunnittelusta aina analyysiin asti osoittautui yllättävän opettavaiseksi kokemukseksi ja uskon tästä olevan hyötyä myös tulevaisuudessa.

Mahdollisia jatkotutkimuksen ja -työn aiheita voisi olla tietoturvallisuusdokumentin jatkaminen esimerkiksi teknisen tietoturvallisuuden ja mahdollisesti tulevaisuudessa kyberturvallisuudenkin osalta. Etenkin teknisen tietoturvallisuuden puolelta dokumenttia olisi suositeltavaa jatkaa, koska dokumenttianalyysistä pois jätetyissä asiakasvaatimuksissa nousi jatkuvasti esille tekniset turvallisuusvaatimukset tarjouspyynnöissä olevien järjestelmien osalta.

Tämän opinnäytetyöprosessin loppuunsaattaminen on tapahtunut yhteistyössä työn tilaajan sekä opinnäytetyön tekijän kanssa. Molemmat tahot ovat saavutettuun lopputulokseen tyytyväisiä ja vakuuttuneita siitä, että opinnäytetyö oli tarpeellinen sekä hyödyllinen kokemus molemmille osapuolille.

6.2 Luotettavuus ja eettisyys

Kaikenlaisissa tutkimuksissa on tarkoituksena pyrkiä välttämään virheitä, mutta on silti mahdollista, että tulosten pätevyys ja luotettavuus vaihtelevat. Tämän takia jokaisessa tutkimuksessa on tärkeää arvioida tehdyn tutkimuksen luotettavuutta. Tutkimuksen arviointiin on vahvasti liitoksissa kaksi eri käsitettä: reliaabelius ja validius. Reliaabeliuksella tarkoitetaan

tutkimuksen toistettavuutta ja validiuksella puolestaan tutkimusmenetelmän tai mittarin kykyä mitata sitä, mitä oli tarkoituskin mitata. (Hirsjärvi ym. 2009, 231.)

Opinnäytetyöprosessi kokonaisuudessaan on toteutettu yleisten eettisten tutkimusperiaatteiden mukaisesti. Tämä tarkoittaa, että tutkimuksen kaikissa vaiheissa on pyritty tarkkuuteen, rehellisyyteen sekä huolellisuuteen. Opinnäytetyön aikana on myös varmistettu se, ettei opinnäytetyöprosessista koidu riskejä tai haittaa yhdellekään tämän opinnäytetyöprosessin osapuolille.

Asiantuntijahaastatteluista saatavan tiedon luotettavuus pyrittiin tässä opinnäytetyössä varmistamaan valitsemalla oikeat henkilöt haastattelun kohteeksi, jotta haastatteluista saatava tieto tulisi mahdollisimman läheltä tämän tutkimuksellisen kehittämistyön aihepiiriä ja että se palvelisi tämän opinnäytetyön tarkoitusta parhaimmalla mahdollisella tavalla. Haastattelut suoritettiin nimettömästi eikä haastateltavista kerätty mitään ylimääräistä tietoa, jonka pohjalta haastateltavat olisivat tunnistettavissa haastatteluiden perusteella. Myöskään Yrityksen X omaa dokumentaatiota ei tässä opinnäytetyössä esitellä tarkemmin, jotta voidaan varmistaa opinnäytetyön tilaajan anonyymisyys.

Haastateltavien määrä tässä opinnäytetyössä jäi hyvin pieneksi ja tämä johtui yksinomaan siitä, ettei haastattelujen aihepiirien kysymyksiin olisi yksinkertaisesti ollut muita henkilöitä, joilta olisi löytynyt samankaltaista tietoa ja kokemusta Yrityksen X tieto- ja pilviturvallisuudesta. Mikäli haastatteluja olisi suoritettu Yrityksen X muulle henkilöstölle, ei niistä mahdollisesti saatava tieto olisi ollut tämän tutkimuksellisen kehittämistyön kannalta tarpeeksi luotettavaa.

Dokumenttianalyysin luotettavuus tutkimusmenetelmänä on vähäisempi kuin asiantuntijahaastatteluiden. Koskivat dokumentit mitä tahansa aihetta, niin ne on lähes aina tehty johonkin muuhun tarkoitukseen kuin tutkimusta varten, jonka vuoksi niiden syntykontekstiin tulee kiinnittää erityistä huomiota (Alastalo & Vuori 2022).

Tässä opinnäytetyössä käytetyt dokumentit olivat Yrityksen X asiakkailta tulleita tarjouspyyntöjä ja niihin liittyviä tietoturvavaatimuksia. Tässä opinnäytetyössä dokumentteihin suhtauduttiin ainoastaan vaatimuksina Yrityksen X tietoturvallisuudelle ja niiden analyysissä keskityttiin tämän vuoksi ainoastaan niiden sisältöön, eikä niinkään niiden syntyperään. Dokumenttien käyttöön tässä opinnäytetyössä on saatu lupa, ja niistä syntyneestä Excel-taulukosta ei pysty erittelemään mistä yrityksestä tai organisaatiosta ne ovat peräisin, jotta pystytään varmistamaan myös Yrityksen X asiakkaiden anonyymisyys.

Opinnäytetyössä käytetyt lähteet on valittu niiden luotettavuuden ja asiaankuuluvuuden perusteella. Opinnäytetyössä on pyritty käyttämään niin tuoreita lähteitä, kuin on ollut olosuhteiden kannalta mahdollista. Lähes kaikki tässä opinnäytetyössä käytetyt tieto- ja

pilviturvallisuusasioihin liittyvät lähteet ovat organisaatioilta tai henkilöiltä, jotka ovat laajasti tunnettuja ja arvostettuja näiden aihealueiden osalta. Tuoreen tutkimuskirjallisuuden löytäminen oli hieman haasteellista, mutta tämän osalta tiedon ajankohtaisuus ei ole niin merkittävä asia kuin esimerkiksi tietoturvallisuuden, jonka teoriapohja muuttuu jatkuvasti maailmanlaajuisen tietoteknisen kehittymisen johdosta.

Lähteet

Painetut

Hirsjärvi, S. Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. painos. Helsinki: Tammi

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu

Peltier, T. 2014. Information security fundamentals. 2. painos. Boko Raton, Florida: CRC Press

SFS-EN ISO/IEC 27000:2017. Yleiskuvaus ja sanasto. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017.

SFS-EN ISO/IEC 27001:2017. Vaatimukset. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017.

SFS-EN ISO/IEC 27002:2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Aihealueet: Informaatioteknologia, turvallisuus. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017.

SFS-ISO/IEC 27005:2018. Tietoturvariskien hallinta. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.12.2018.

Sähköiset

Alastalo, M & Vuori, J. 2022. Dokumentit. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 27.3.2022. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/dokumentit/

Andress, J. 2014. The basics of information security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2. painos. E-kirja. Waltham, Massachusetts: Syngress. Viitattu 8.2.2022. https://books.google.fi/books?id=9NI0AwAAQBAJ&printsec=frontcover&hl=fi#v=onepage&q&f=false

Baxter, A. 2021. Tietoturvallisuuden riskienhallinnan kehittäminen valtioneuvoston kansliassa Opinnäytetyö. Laurea-ammattikorkeakoulu. Viitattu 11.3.2022. https://www.theseus.fi/handle/10024/498767

Elinkeinoelämän keskusliitto (EK) 2021. Yritysturvallisuus. Viitattu 28.11.2021. https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/

Euroopan unioni 2021. Yleinen tietosuoja-asetus. Viitattu 11.3.2022. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Frankenfield, J. 2021. Cloud Security. Investopedia. Viitattu 28.1.2021. https://www.investopedia.com/terms/c/cloud-security.asp

Hyvärinen, M. Nikander, P. & Ruusuvuori, J. 2017. Tutkimushaastattelun käsikirja. E-kirja. Tampere: Vastapaino. Viitattu 2.2.2022.

Indeed 2021. What Is an Information System? Definition and Uses. Viitattu 8.2.2022. https://www.indeed.com/career-advice/career-development/what-is-information-system

Jalava, J. 2021. Tietoturvapolitiikan kehittäminen Sulavalle Opinnäytetyö. Laurea-ammattikorkeakoulu. Viitattu 11.3.2022. https://www.theseus.fi/handle/10024/500032

JAMK 2022. Opinnäytetyön ohjaajan käsikirja. Viitattu 24.1.2022. https://oppimateriaalit.jamk.fi/yamk-kasikirja/tyoelaman-tutkiva-kehittamistoiminta/

Johdon tietoturvaopas 2011. Vahti-ohje. Valtiovarainministeriö. Viitattu 8.2.2022. https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_2_2011_etusivu_ohjepdf_2.pdf

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. E-kirja. Helsinki: Alma Talent Oy. Viitattu 4.2.2022.

Korhonen, S. 2022. Pilvipalvelut menevät kaupaksi ennätystahtiin – katso suurimmat toimittajat. Kauppalehti. Viitattu 9.2.2022. https://www.kauppalehti.fi/uutiset/pilvipalvelut-menevat-kaupaksi-ennatystahtiin-katso-suurimmat-toimittajat/40b94f7e-232a-45ca-8623-216dff1bc0c1

Kyberturvallisuuden sanasto 2018. Turvallisuuskomitea. Viitattu 8.2.2022. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille 2019. Traficom. Viitattu 9.2.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät – uudenlaista osaamista liiketoimintaan. 3–4 painos. E-kirja. Helsinki: Sanoma Pro Oy. Viitattu 20.1.2022.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) 2020. Traficom. Viitattu 9.2.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Tietosuojalaki 1050/2018. Viitattu 11.3.2022. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050#L3

Tietosuojavaltuutetun toimisto 2022a. Tietosuoja. Viitattu 11.3.2022. https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto 2022b. Tietosuojalaki. Viitattu 11.3.2022. https://tietosuoja.fi/tietosuojalaki

Traficom 2020. Tietoturva. Viitattu 28.1.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Vacca, J. 2013. Computer and Information Security Handbook. 2. painos. E-kirja. Waltham, Massachusetts: Morgan Kaufmann Publishers. Viitattu 4.2.2022.

Vacca, J. 2014. Managing Information Security. 2. painos. E-kirja. Waltham, Massachusetts: Syngress. Viitattu 4.2.2022.

Julkaisemattomat

Tietoturvapäällikkö, 2022. Haastattelu 23.2.2022. Yritys X. Teams.

Tietoturvapäällikkö, 2022. Haastattelu 3.3.2022. Yrityksen X emoyhtiö. Teams.

Kuviot

Taulukot

Liitteet

Liite 1: Dokumenttianalyysi

Asiakas 1 (Kunta) **Pyydetyt selvitykset**	**Asiakas 2 (Kunta)** **Tietoturvallisuusvaatimukset**	**Asiakas 3 (Yritys)** **Tietoturvallisuusvaatimukset**	**Asiakas 4 (Kunta)** **Tietoturvallisuusvaatimukset**
Selvitys organisaation tietoturvallisuuden hallintajärjestelmästä ja turvallisuuspolitiikasta	Palveluntuottaja (Yritys X) sitoutuu noudattamaan tilaajan tietoturva- ja suojapolitiikkaa	Toimittaja (Yritys X) on määritellyt tietoturvallisuuden ja jatkuvuudenhallinnan johtamisen roolit ja vastuut ja ne sisältyvät henkilöiden tehtäväkuvauksiin	Palveluntuottaja (Yritys X) sitoutuu noudattamaan tilaajan tietoturvapolitiikkaa
Selvitys asiakkaan palvelun kattavista riippumattomista sertifikaateista	Palveluntuottajan tulee toimia ISO 27001 tai vastaavan tietoturvanhallintajärjestelmän periaatteiden mukaisesti	Toimittaja on määrittänyt henkilöstön roolit ja vastuut tiedon turvaamisen ja jatkuvuuden hallinnan suunnittelussa ja toteuttamisessa myös häiriötilanteet huomioiden	Palveluntuottajan tulee toimia ISO 27001 tai vastaavan tietoturvanhallintajärjestelmän periaatteiden mukaisesti
Selvitys käyttämienne välineiden turvakäytänteistä ja kovennuksista	Palveluntuottajalla tulee olla dokumentoituna tietoturvallisuuden hallinta, joka varmistaa, että organisaation omaisuuden, informaation, tiedon ja IT-palvelujen luottamuksellisuus, eheys ja saatavuus vastaavat sovittuja tarpeita	Häiriötilanteiden asettamat vaatimukset on otettu huomioon henkilösuunnittelussa, tehtävänkuvauksissa ja koulutuksessa	Palveluntuottajan tulee raportoida tilaajalle tietoturvallisuudesta puolivuosittain tai useammin, mikäli asiasta on sovittu erikseen
Selvitys käyttämienne välineiden tietoturvapäivitysten seuranta- ja asennusprosessista	Palveluntuottaja raportoi tilaajalle tietoturvallisuudesta vuosittain	Toimittajalla tulee olla kirjallinen tietoturvallisuuspolitiikka, jossa määritellään tietoturvallisuuden keskeiset tavoitteet, vastuut ja periaatteet.	
Selvitys tilaajan dataan pääsevien henkilöiden identiteetinhallinnan ja pääsynhallinnan käytänteistä	Palveluntuottaja ylläpitää ja päivittää ajantasaisia ympäristö- ja järjestelmäkuvauksia	Tietoturvallisuuspolitiikan tulee olla organisaation johdon hyväksymä	
Selvitys verkkohyökkäyksien torjunnasta	Palveluntuottaja vastaa toipumissuunnitelman kehityksestä sekä vuosittaisesta päivityksestä ja testauksesta	Tietoturvallisuuspolitiikkaa voidaan käyttää pohjana tietoturvallisuusstrategian määrittelylle	
Kuvaus Riskienhallintaprosessista (GDPR)		Tietoturvallisuusdokumentaation päivittäminen ja katselmointi on organisoitu ja vastuutettu	
Selvitys turvallisuuspoikkeamiin reagoinnin ja raportoinnin prosessista		Toimittajan tietoturvallisuudenhallintaan liittyviä politiikkoja, ohjeita ja muuta dokumentaatiota katselmoidaan ja tarvittaessa päivitetään säännöllisesti	
Selvitys tietoturvallisuuden auditointiprosesseista ja niiden tuloksista		Tietoturvallisuusdokumentaation katselmoinnille ja päivittämiselle on olemassa prosessi ja vastuuhenkilöt	
Teknisiä tietoturvallisuusvaatimuksia/selvityspyyntöjä 3 kpl (11%) **Hallinnollisia tietoturvallisuusvaatimuksia/selvityspyyntöjä 24 kpl (89%)** **Yhteensä 27 kpl**			

Liite 2: Yritys X tietoturvallisuuspäällikön haastattelupohja

Teema: Hallinnollinen tietoturvallisuus

- Mitkä ovat Yrityksen X ja Yrityksen X emoyhtiön roolit hallinnollisen tietoturvallisuuden hoitamisessa?
    - Millainen on yritysten välinen vastuunjako?
- Onko tietoturvallisuuden vastuut määritelty ja jaettu selkeästi organisaation sisällä? Miten?
- Millaisia hallinnollisen tietoturvallisuuden kontrolleja Yrityksessä X on käytössä?
    - Onko tietoturvapolitiikka jalkautettu kaikille yrityksen työntekijöille ja tarvittaville sidosryhmille?
- Miten tietoturvallisuusasiat on koulutettu henkilöstölle?
    - Miten varmistetaan henkilöstön tietoturvalliset työtavat?
    - Miten tietoturvallisuusasioista viestitään henkilöstön ja sidosryhmien kesken?
    - Miten tietoturvahäiriöistä ja poikkeamista ilmoitetaan?
- Kuinka usein tietoturvallisuuden hallintajärjestelmää auditoidaan ulkoisten tai sisäisten tahojen toimesta?
    - Millaisia tuloksia auditoinneista on saatu?
- Miten tietoturvallisuuden toteutumista seurataan/arvioidaan organisaation sisällä?
- Millä tavoin tietoturvallisuuden hallintajärjestelmän jatkuvan parantamisen periaate toteutuu hallinnollisen tietoturvallisuuden osalta?

Liite 3: Yritys X:n emoyhtiön tietoturvallisuuspäällikön haastattelupohja

Teema 1: Tekninen tietoturvallisuus

- Mitkä ovat Yrityksen X ja Yrityksen X emoyhtiön roolit teknisen tietoturvallisuuden hoidossa?
    - Millainen on yritysten välinen vastuunjako?
- Millaisia teknisen tietoturvallisuuden kontrolleja Yrityksessä X on käytössä?
- Arvioidaanko teknisen tietoturvallisuuden tasoa säännöllisesti?
- Millä tavoin tietoturvapoikkeamiin reagoidaan Yrityksessä X?
- Millä tavoin tietoturvallisuuden hallintajärjestelmän jatkuvan parantamisen periaate toteutuu teknisen tietoturvallisuuden osalta?

Teema 2: Pilviturvallisuus

- Miten pilviturvallisuuden vastuut on jaettu palveluntarjoajan ja Yritys X:n välillä?
    - Onko vastuut dokumentoitu?
- Miten riskienhallinta pilviturvallisuuden osalta toteutetaan?
    - Onko riskienhallinta säännöllistä?
- Mitkä ovat Yrityksen X ja Yrityksen X emoyhtiön roolit pilviturvallisuusasioiden hoitamisessa?
    - Millainen on yritysten välinen vastuunjako?
- Miten varmistetaan pilvipalveluissa käsiteltävien tietojen tietosuoja?
- Tarkastellaanko pilvipalveluiden turvakäytäntöjen toimintaa ulkoisten/sisäisten osapuolten toimesta?
- Millaisin keinoin pilvipalveluiden turvallisuus varmistetaan?