Tietoturvakartoitus ja kehittämisehdotus teollisuusalan Pk-yritykselle

Panu Pietikäinen

Julkaisuvuosi Laurea

Laurea-ammattikorkeakoulu

Tietoturvakartoitus ja kehittämisehdotukset teollisuusalan Pk-yritykselle

Panu Pietikäinen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tietojenkäsittely (AMK)

Panu Pietikäinen

Tietoturvakartoitus ja kehittämisehdotukset teollisuusalan PK-yritykselle

Vuosi 2021 Sivumäärä 39

Tämän opinnäytetyön tavoitteina oli tehdä teollisuusalan Pk-yritykselle tieturvakartoitus, jonka pohjalta luoda kehitysehdotukset valittuihin tietoturvan osa-alueisiin. Opinnäytetyön toimeksiantajana toimi Suomessa toimiva teollisuusalan Pk-yritys, jonka liiketoiminta-alueena on kevyiden henkilönostimien myynti teollisuus- sekä toimistokiinteistöihin. Yritys työllistää Suomessa neljää henkilöä. Opinnäytetyö on tapaustutkimus, jonka tarkoituksena oli löytää yrityksen tietoturva-alueiden ongelmakohdat.

Opinnäytetyön teoriaosuudessa käsitellään yleisesti tietoturvaa käsitteenä sekä valittuja tietoturvan osa-alueita. Tietoperustana käytetään myös VAHTI-ohjeistusta, jota hyödyntäen perusteltiin toimeksiantajayritykselle räätälöidyt kehitysehdotukset ilmenneisiin ongelmakohtiin. Opinnäytetyön tutkimusosiossa aineistonkeruumenetelminä käytettiin teemahaastatteluita sekä havainnointia tukemaan haastatteluiden tuloksia. Teemahaastattelut suoritettiin yrityksen henkilöstön kanssa, jotta yrityksen tietoturvatilanteesta saatiin mahdollisimman tarkka kuvaus. Havainnointi toteutettiin seuraamalla yrityksen johtoa heidän päivittäisessä toiminnassaan. Haastatteluiden sekä havainnoinnin tulosten analysointimenetelmänä käytettiin teemoittelua. Tuloksissa ilmenneiden ongelmakohtien riskitason arvioinnissa hyödynnettiin riskimatriisia.

Tutkimustuloksina selvisi, että yrityksellä on suuria haasteita erityisesti tietoaineistoturvallisuuden osa-alueella. Lisäksi yrityksellä ilmeni ongelmakohtia myös muilla tietoturvan osa-alueilla, kuten tietolaitteisto- ja käyttöturvallisuuden osa-alueilla. Opinnäytetyön tuloksena luotiin yritykselle nykytilanteen kartoitusvaiheessa ilmenneille ongelmakohdille kehitysehdotuksia tietoturvan parantamiseksi. Kehitysehdotukset noudattavat VAHTI-ohjeistuksen vaatimuksia ja ovat perusteltu yrityksen tarpeita vastaavaksi.

Asiasanat: Tietoturvallisuus, tietoturvakartoitus, VAHTI-ohjeistus, tietoturvauhka

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Thesis

Panu Pietikäinen

Information security audit and development proposal for the industrial SME

Year 2021 Pages 39

The objective of this thesis project was to implement information security mapping at a client company. As result of this mapping development suggestions were offered concerning company's information security. The client this thesis project is a small business operating in Finland and its business area is to sell lifts and scaffolds to industries and office premises. The company employs four people. This thesis is a case study where the purpose is to find problem areas concerning the company's information security. The study was limited to investigate only the chosen areas of information security.

The theoretical framework discusses generally the meaning of information security and the chosen information security areas for this thesis. In addition, the VAHTI instruction is included and the modified development suggestions were justified for the client based on this instruction. Semi-structured interviews were used as a research method in the empirical section of the thesis project. Additionally, observation was used to support the results of the interviews. Semi-structured interviews were conducted with the personnel of the client company to get the most realistic and specific descriptions of the current state of information security. Observation was carried out by observing the management in their daily operations. The results of interviews and observation were analyzed by dividing the data into themes. A risk matrix was used to evaluate the level of risk of each problem area.

According to the research results the company has major issues especially in the area of data security. In addition, potential problems were identifid in other information security areas. The results of this thesis were the development suggestions provided for the employer in order to strengthen the information security of the company. The development suggestions follow the requirements of the VAHTI instructions and are intended to correspond the needs of the employer.

Keywords: Information security, information security mapping, VAHTI- instruction, information security threat

Sisällys

1 Johdanto

Lähes kaikki yritykset käyttävät tietotekniikan mahdollistamia työkaluja liiketoiminnassaan. Vaikka uudet teknologiat tarjoavat nopeampia ja parempia ratkaisuja yrityksille liiketoiminnansuorittamiseksi, tuo se aina mukanaan myös tietoturvauhat. Mikäli yritys ei varaudu tietoturvan aiheuttamiin uhkiin, voivat seuraukset olla kriittisiä yrityksen liiketoiminnalle. Tämän takia on tärkeää tehdä yritykselle tietoturvanauditointeja säännöllisin väliajoin, jotta yrityksen liiketoiminnan jatkuvuus voidaan varmistaa.

Tämä opinnäytetyö on tapaustutkimus. Tässä työssä suoritettiin tietoturvakartoitus toimeksiantajayritykselle. Kartoituksen tulosten perusteella yritykselle muodostettiin kehittämissuunnitelma tietoturvan parantamiseksi. Yritystä käsitellään opinnäytetyössä nimettömästi, koska tietoturvaan liittyvät asiat ovat yrityksen sisäistä tietoa ja yritys ei halua näin arkaluontoista aiheitta käsitellä julkisesti.

Työ etenee toimeksiantajayrityksen esittelyllä, jonka jälkeen esitetään opinnäytetyön keskeisimmät tavoitteet. Seuraavaksi luvussa kaksi käsitellään opinnäytetyön tietoperustaa. Tietoperusta käsittelee tietoturvaa opinnäytetyölle rajattujen tietoturvaosa-alueiden osalta sekä esittelee lyhyesti yleisimpiä tietoturvatyökaluja ja -ohjeistuksia. Opinnäytetyön tutkimusmenetelmät ovat esitetty luvussa kolme, minkä jälkeen tutkimuksen toteutus on kuvattu. Tutkimuksen toteutuksen jälkeen luku viisi esittelee opinnäytetyön tuloksena esitetyt kehitysehdotukset ja etenee johtopäätöksiin.

1.1 Toimeksiantajayritys

Toimeksiantajayritys on vuonna 2015 perustettu Pk-yritys. Yritys on teollisuusalan pienyritys, joka tuottaa sekä kehittää kevyitä henkilönostimia. Yrityksellä ei ole omaa henkilönostimien tuotantoa, vaan tuotanto on ulkoistettu kokonaan toiselle yritykselle. Tuotannosta vastaavat henkilöt ovat kuitenkin ulkoisia toimijoita, eikä heillä ole pääsyä yrityksen verkkoon. Yrityksen toimistorakennus sijaitsee Nummelassa. Yritys työllistää tällä hetkellä neljä henkilöä Suomessa sekä yrityksellä on kaksi ulkoistettua myyntiedustajaa muualla Euroopassa.

Yrityksen verkko perustuu Microsoftin O365 -palvelun ympärille. Yritys hyödyntää myös runsaasti O365 -palvelun ohjelmia ja erilaisia pilvipalveluita työssään. Yritystä perustaessa tietoturva on otettu hyvin huomioon, sillä yksi perustajajäsenistä on itse IT-taustainen henkilö ja ymmärrys tietoturvaa kohtaan on ollut varsin hyvällä tasolla. Kuitenkin IT-taustainen perustajajäsen on lähtenyt yrityksestä pois, eikä osallistu enää yrityksen operatiiviseen toimintaan.

Yrityksen liiketoiminta on kasvanut nopeaa vauhtia perustamisen jälkeen, eikä perustamisvaiheessa ole ollut resursseja tietoturvan ylläpitämiseksi. Yritys on kuitenkin tiedostanut, että tietoturvaan tulee käyttää resursseja, sekä investointeja tietoturvan parantamiseksi on tehtävä. Yrityksen ongelmana kuitenkin on ollut ymmärtämättömyys tietoturvasta. Yritys on itse toivonut opinnäytetyön tarjoavan heille tiedon siitä, mitä asioita yrityksen tulee korjata, jotta tietoturva paranisi yrityksessä.

1.2 Tavoitteet

Kehittämistyön tavoitteena on tehdä kohdeyritykselle tietoturvakartoitus. Kartoituksen tuloksista yritykselle muodostetaan kehittämisohjeistus, jolla yritys voi parantaa tietoturvaa. Kehittämistyössä on otettava huomioon se, että yrityksessä työskentelee ulkoisesti myös työntekijöitä muissa Euroopan maissa, joilla on pääsy yrityksen verkkoon. Ohjeistusten ja kehitysedotusten tarkoituksena on luoda toimintatapoja ja -ohjeistusta toimeksiantajayritykselle, jotta yritys pystyy parantamaan yrityksen tietoturvaa.

2 Tietoturvallisuus

Tietoturvallisuus on pieniä tekoja yrityksen jokapäiväisessä toiminnassa. Parhaimmillaan tietoturva on osa yrityksen kulttuuria ja perusarvoja, jolloin jokainen yrityksen työntekijä tietää ja ymmärtää tietoturvan tärkeyden. (Laaksonen, Nevasalo & Tomula 2006, 17.) Hyvän tietoturvallisuustason saavuttaminen ja ylläpitäminen vaatii yritykseltä määrätietoista toimintaa. Konkreettisesti se tarjoaa yritykselle erilaisia keinoja sekä toimintamalleja yrityksen liiketoiminta kriittisten sekä henkilötietojen suojaamiksesi. Vaikka tietotuvallisuus tuo mukanaan paljon rajoittavia tekijöitä, ei sitä saisi nähdä yrityksessä rajoittavana ja työtä hankaloittavana tekijänä vaan pikemminkin kilpailuetuna. (Laaksonen ym. 2006, 17–18.)

Tässä luvussa käsitellään toimeksiantajayrityksen näkökulmasta tärkeää valtiollista ohjeistusta sekä minkälaisia vaatimuksia ohjeet antavat yritykselle tietoturvallisuuden parantamiseksi. Ohjeet tarjoavat kehitystyölle tietoperustan, jonka pohjalta tutkimukseen voidaan tarjota kehittämisehdotuksia.

VAHTI on valtionvarainministeriön hallinnoima valtion tietoturvallisuudenryhmä, jonka tehtävänä on tuottaa ohjeistuksia tietoturvan jokaiselle osa-alueelle (Valtionvarainministeriö 2021). Hyvin toteutettu tieto- ja kybertuvallisuus ovat yhteiskunnan sekä yritysten toiminnan kulmakiviä. VAHTI-toiminnan tarkoituksena on parantaa valtion tieto- ja kybertuvallisuutta.

VAHTI-ryhmän työn tulos on konkreettisesti nähtävissä oleva yleinen kattava tietoturvaohjeistus. Tätä ohjeistusta käytetään julkishallinnon ohella myös yksityisyrityksissä sekä kansainvälisesti. (Valtiovarainministeriö 2016, Johdanto.)

VAHTI-ryhmä on jaettu sisäisesti vielä pienempiin työryhmiin, joissa jokaisella ryhmällä on omat vastuualueensa. Nämä vastuualueet ovat: Riskienhallinnan kehittäminen, toiminnan jatkuvuuden ja varautumisen kehittäminen, ICT-palveluiden digitaalisen tulevaisuuden kehittäminen, tietosuojankehittäminen sekä digiturvaosaamisen kehittäminen. (Digi- ja väestötietovirasto 2021.)

2.1 Tietoturvan osa-alueet

Tyypillisesti tietoturvan kokonaisuus voidaan jakaa useampaan eri osa-alueeseen, jotta osa-alueita olisi helpompi käsitellä. Pääsääntöisesti tietoturvan osa-alueita ovat hallinnollinen tietoturva, fyysinen turvallisuus, henkilöstöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus, käyttöturvallisuus sekä tietoliikenneturvallisuus. (Hakala, Vainio & Vuorinen 2006, 10.)

Tietoturvallisuus käsitteenä ei koske ainoastaan fyysisiä laitteita, vaan siinä on myös yhtenä osa-alueena ihmisen toiminta. Tietoturvan kaikki osa-alueet näkyvät ja vaikuttavat yrityksen koko toimintaan, esimerkiksi tuotettavuuteen ja yrityksen taloudellisuuteen. (Tietoturvallisuus ja tulosohjaus 2004, 15.)

Tässä luvussa käsitellään kehitystyön kannalta oleellisia tietoturvan osa-alueita ja jätetään pois hallinnollisen-, ohjelmisto-, sekä tietoliikenneturvallisuuden kuvaus. Nämä osa-alueet jäävät pois kehitystyöstä, koska ne eivät ole työn kannalta oleellisessa keskiössä ja koska toimeksiantajayritys käyttää osaksi pilvipohjaisia ratkaisuja ja nämä tietoturvan osa-alueet ovat palveluntarjoajan vastuulla.

2.1.1 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tietoturvan osa-aluetta, jonka päämääränä on varmistaa tietojen turvallinen säilyttäminen, palauttaminen ja tuhoaminen (Hakala ym. 2006, 11). Tietoaineistoturvallisuuden yksi oleellisista tehtävistä on myös varmistaa yrityksen tiedostojen ja tietojen oikeanlainen säilyttäminen. Tyypillisesti tietoaineistoturvallisuuden pohjalta tiedot voidaan myös jakaa eri turvaluokkiin. Näin yritys voi itse luokitella tietonsa niiden arkaluontoisuuden perusteella. (Tirronen 2003.)

VAHTI-ohjeen mukaan tietoaineistoturvallisuudelle määritellään erilaisia vaatimuksia. Tiedot tulee luokitella ja tiedostoille tulee antaa luokittelumerkintänsä. Tiedoille tulee olla rajattu pääsy niin, että vain henkilöt, jotka tarvitsevat tietoja työssään, pääsevät niihin käsiksi. Pääsyä voidaan rajata tietoihin esimerkiksi salasanoilla tai käyttöoikeuksin. Tiedonsiirto ja tallennusvälineiden käytölle tulee olla selkeät ohjeistukset: onko yrityksen tietoja sallittu tallentaa muistitikuille, ulkoisille kovalevyille tai Cd-levyille. Tiedot tulee hävittää turvallisesti niin, että tiedonluokituksen mukaan tiedot hävitetään oikeaoppisesti. Tietojenkäsittely tulee tapahtua käyttäjän henkilökohtaisin tunnuksin. Tämä tarkoittaa sitä, että yhteisiä tunnuksia ei saa käyttää tietojenkäsittelyyn. Näin voidaan varmistua siitä, että tietojenkäsittelijä voidaan tarpeen vaatiessa myös jäljittää. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 79–80.)

2.1.2 Tietolaitteistoturvallisuus

Laitteistoturvallisuus on tietokoneiden ja tietojärjestelmään kytkettyjen laitteiden mitoittamista, testausta, huoltamista sekä varautumista laitteiden kulumiseen niiden elinkaaren aikana. (Hakala ym. 2006, 12.)

VAHTI-ohje luokittelee laitteistoturvallisuudelle omat vaatimuksensa sekä vaatimuksen tarkemmat kuvaukset. VAHTI-ohjeen mukaan laitteen omistajuus tulee määritellä niin, että yrityksessä jokaisella laiteella on yksi omistaja, joka vastaa siitä. Laitteistoa tulee säännöllisesti ylläpitää sekä päivitykset tulee tehdä ajallaan laitteisiin. Kapasiteetin suunnittelua tulee toteuttaa siten, että tietojenkäsittelykapasiteetin tarve tulee ennakoida sekä investoida tarpeeksi ajoissa. Laitteiden käytöstä poisto tulee tehdä suunnitelmallisesti sekä siten, että käytöstä poiston jälkeen tietoihin ei pääse enää käsiksi. Haittaohjelmilta suojautumisesta tulee huolehtia niin, että laitteistot ovat suojattu asianmukaisesti sekä sellaisilla menetelmillä, jotka päivittyvät säännöllisesti haittaohjelmien mukana. (Valtiovarainministeriö 2004.)

2.1.3 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan niitä toimia, jolla voidaan varmistaa tietojärjestelmien käyttäjien toimintakyky ja heidän tehtävien mukainen pääsyoikeuksien rajaaminen. Pääsyoikeuksien rajaamisella tarkoitetaan sitä, että käyttäjä pääsee niihin resursseihin ja tiedostoihin kiinni, joita hänen työtehtävänsä vaativat. (Hakala ym. 2006, 11.) Työntekijöille tulee myös määrittää toimenkuva. Toimenkuvassa tulee märittää työntekijälle työtehtävät, oikeudet, velvollisuudet sekä vastuut. Toimenkuvan määrittelyn pohjalta työntekijälle voidaan määritellä edellä mainitsemat pääsyoikeudet resursseihin ja tiedostoihin. (Valtiovarainministeriö 2004.)

VAHTI-dokumenttien pohjalta henkilöstöturvallisuudelle määritellään seuraavia vaatimuksia. Työntekijän soveltuvuus tulee varmistaa niin, että se vastaa työtehtävän edellyttämää tasoa. Koulutuksen taso tulee olla sellainen, että työntekijä voi suoriutua työtehtävästä sekä on sopiva työtehtävään. Henkilöstön taustatarkastus tulee suorittaa niin, että henkilön koulutuksesta tulee varmistua sekä mahdollisten suositusten sekä työhistorian tarkastus tulee teettää, mikäli työtehtävä sen vaatii. Työntekijälle tulee teettää salassapitosopimus, jonka avulla voidaan varmistua siitä, että työntekijä on tietoinen omista velvoitteistaan sekä lainsäädännöstä salassapitovelvollisuuden suhteen. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 39–41.)

VAHTI-dokumentissa todetaan ulkoisen henkilöstön osalta siten, että ulkoiset työntekijät tulee olla yrityksen oman henkilöstön ohjauksessa sekä ydinosaamistaso pystytään pitämään yrityksen sisäisillä työntekijöillä. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 41.)

Henkilöstöturvallisuuden osa-alueella tietoturvariskejä voivat aiheuttaa myös erinäiset muutokset yhteiskunnassa, yrityksen kilpailutilanteen kiristäminen tai tietojenkäsittelyyn osallistuvien henkilöiden suuri määrä. Laadukkaalla henkilöstöturvallisuudella voidaan edellä mainittuja tietoturvariskejä minimoida. (Laaksonen ym. 2006, 138.)

2.1.4 Käyttöturvallisuus

Käyttöturvallisuutta luonnehditaan tietoturvallisuuden kahdeksanneksi osa-alueeksi. Käyttöturvallisuus usein sisällytetään tietoturvan jokaiseen osa-alueeseen, mutta sitä voidaan myös pitää tietoturvan omana osa-alueena. Käyttöturvallisuus käsitteenä kattaa järjestelmän käytöstä aiheutuvat riskit sekä niiden riskeihin varautumisen. (Hakala ym. 2006, 12.)

Käyttöturvallisuuden alaisuuteen kuuluvat käyttöjärjestelmien salasanat, yrityksen käytössä olevien ohjelmien oikeaoppinen käyttäminen sekä laitteistoiden virustorjuntaohjelmien käyttäminen. Käyttöturvallisuuden perusperiaatteena on luoda yritykselle sellaiset toimintatavat, joita käytetään yrityksen jokapäiväisessä toiminnassa. Näin voidaan varmistua siitä, että yrityksen tietoturvallisuuden taso pysyy mahdollisimman laadukkaana. (Tirronen 2003.)

VAHTI-dokumentaation pohjalta käyttöturvallisuudelle määritellään seuraavanlaisia vaatimuksia. Käyttäjien pääsyoikeudet tulee pystyä todentamaan turvallisesti. Yrityksen tehtäviä tulee eriyttää siten, että yrityksen koko tietojärjestelmän hallinta ei voi olla hallittavissa totaalisesti vain yhdellä käyttäjällä. Haittaohjelmilta suojautuminen tulee huolehtia siten, että yrityksen tietokoneilla on käytössä suojausohjelmia sekä niiden päivittämisestä on huolehdittu.

Tietojärjestelmään liittyvät riittävät ohjedokumentaatiot ovat huolehdittava siten, että ne ovat ajan tasalla sekä tarpeen tullen yrityksen henkilöstön käytettävissä. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 86–88.)

Yrityksen laitteiden käyttövarmuus on myös osa yrityksen käyttöturvallisuutta. Käyttövarmuudella tarkoitetaan, että yritys on varautunut laitteiden vikaantumiseen. Esimerkiksi, kun yrityksen tietokoneen kovalevy hajoaa ja käytössä olevan laitteen tiedostot muuttuvat käyttökelvottomiksi, tulee tiedostojen palautuksen olla ongelmatonta. (Tirronen 2003.)

2.1.5 Fyysinen turvallisuus

Tietoturvassa fyysinen turvallisuus tarkoittaa yrityksen käytössä olevan rakennuksen tai tilojen sekä niihin sijoitettujen laitteiden suojaamista. Fyysiseen turvallisuuteen liittyvät uhat ovat pääsääntöisesti ilkivallasta aihetuvat teot, yrityksen tiloihin murtautuminen sekä ympäristöstä aihetutuvat uhat, kuten vesivahingot tai sähkökatkokset. (Hakala ym. 2006, 12.)

Hyvin keskeinen yrityksiä ohjaava tietoturvastandardi on ISO/IEC 17799. Tämä standardi on eräänlainen tietoturvallisuuden yleinen menettelytapaohje, joka määrittelee yritykselle osa-alueet, jotka on huomioitava tietoturvallisuudessa. (Hakala ym. 2006, 46.) ISO/IEC 17799 standardi määrittää yrityksen tilojen kohteiden turvallisuudelle seuraavia taulukossa kuvattuja kontrolleja:

Standardin numerointi	Kohde	Kontrolli
9.1.1	Fyysiset turvatoimet	Yrityksen on huolehdittava asianmukaisesta kulunvalvonnasta.
9.1.2	Fyysinen pääsyvalvonta	Turvatut tilat on suojattava niin, että vain sallitulla henkilöstöllä on pääsy tiloihin.
9.1.3	Toimisto- ja muiden tilojen sekä järjestelmien suojaus	Tilojen fyysinen suojaaminen on suunniteltava sekä toteutettava.

Taulukko 1: Tilojen fyysinen turvallisuus ja ympäristö turvallisuus (Hakala ym. 2006, 304).

VAHTI-dokumentaation mukaan fyysisen turvallisuuden toimina tulee ottaa myös huomioon paloturvallisuus. Paloturvallisuuden toimenpiteenä tiloissa tulee olla paloilmoituslaitteisto asennettuna ja käytössä. Lisäksi sammutinpullo tai peitto tulee löytyä tiloista. Pöly voi itsessään muodostaa suuren uhan sähkölaitteille ja sitä myöden koko rakennukselle. Tämän johdosta osa fyysistä turvallisuutta on tilojen puhtaanapito ja riittävästä siivouksesta huolehtiminen. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 47–48.)

3 Tutkimusmenetelmä

Tämä opinnäytetyö on tapaustutkimus. Tapaustutkimus on tutkimusstrategia, jossa pyritään tutkimaan syvällisesti tapauksen kohdetta tai koko kokonaisuutta. Tapaustutkimukselle olennaista on pyrkiä tuottamaan tarkkaa sekä yksityiskohtaista tietoa valitusta tapauskohteesta. (Koppa 2015a.) Tässä opinnäytetyössä tapaustutkimuksen kohteina ovat yrityksen valittujen tietoturvaosa-alueiden ongelmakohtien havaitseminen sekä ratkaiseminen.

Tutkimuksen aineistonkeruu toteutettiin teemahaastatteluiden ja havainnoinnin menetelmiä käyttämällä. Haastattelut toteutettiin toimeksiantajayrityksen henkilökunnan kanssa, jotta saatiin mahdollisimman tarkkaa informaatiota yrityksen toimintatavoista. Täten tulokset oli mahdollista personoitua yrityksen tarpeita vastaavaksi. Jokaisen Pk-yrityksen toimintatavat ovat erilaisia, minkä takia on tärkeää, että tietoturvan toimintatavat vastaavat juuri kyseisen yrityksen tarpeita. Tässä opinnäytetyössä ei nähdä määrällisellä tutkimuksella olevan näkyvää lisäarvoa tutkimukseen, sillä laadullisin tutkimusmenetelmin saadaan syvällistä tietoa tutkittavaan aiheeseen (Juuti & Puusa 2020, Johdanto).

Seuraavaksi käsitellään opinnäytetyössä käytettyjä tiedonkeruumenetelmiä sekä analysointimenetelmää, joiden avulla saadaan arvokasta tietoa ja pystytään tarjoamaan toimeksiantajayritykselle kehitysehdotuksia sekä parempia toimintatapoja tietoturvan valittujen osa-alueiden parantamiseksi. Tutkimus etenee haastatteluiden sekä havainnoinnin kautta tutkimustulosten analysointiin.

3.1 Teemahaastattelu

Haastattelut toteutettiin teemahaastatteluina. Haastattelut ovat osa laadullisia tutkimusmenetelmiä. Laadullinen tutkimus pyrkii ymmärtämään kohteen laadun lisäksi kohteen ominaisuuksia ja merkityksiä tavalla, jolla kokonaisvaltainen kuva voidaan saavuttaa. (Koppa 2015b.) Teemahaastattelut mahdollistavat monien ilmiöiden tutkimisen ja oletuksena teemahaastatteluissa on, että haastateltavat ovat kokeneet tai läpikäyneet tutkimuksen kohteena olevan aihealueen. Ennen teemahaastattelua tutkija selvittää olennaiset tekijät liittyen tutkimuskohteeseen tutustumalla teoriaan. (Puusa & Juuti 2020, 106.)

Teemahaastattelulle olennaista on eteneminen etukäteen valittujen teemojen ympärillä. Lisäksi tutkija esittää tarkentavia kysymyksiä liittyen valittuihin teemoihin. Haastattelumuotona teemahaastattelut mahdollistavat joustavuuden, sillä teemojen järjestys, laajuus sekä kysymisen tapa saattavat vaihdella. Haastattelussa valittujen teemojen tarkoituksena on antaa tutkijalle mahdollisimman laajaa tietoa, jota tutkija pystyy hyödyntämään myöhemmin myös teorian avulla. (Puusa & Juuti 2020, 106–108.)

3.2 Havainnointi

Havainnointi on yksi aineistonhankinnan perusmenetelmistä. Tyypillisesti havainnointia voidaan käyttää joko pääasiallisena aineistonkeruumenetelmänä tai muita keruumenetelmiä tukevana menetelmänä. Havainnoinnin erityisetuna on se, että tutkijan on mahdollista seurata todellisia tilanteita reaaliaikaisesti. Havainnoinnin avulla tutkijan on mahdollista varmistaa asioiden oikeellisuus ja miten haastatteluissa tutkittavasta kohteesta on kerrottu. (Puusa & Juuti 2020, 127.)

3.3 Teemoittelu

Tutkimustulosten analysointimenetelmäksi valittiin teemoittelu. Teemoittelu on yksi laadullisen analyysin perusmentelemistä, jonka avulla tutkimusaineistosta pyritään hahmottamaan tutkimukselle keskeisiä teemoja. Teemoiksi analyysissä voidaan hahmottaa aiheita, jotka toistuvat aineistossa. Teemoittelu analyysimenetelmänä on aiheiden ja aineiston pilkkomista sekä ryhmittelyä niiden yksityiskohtaisempaa tarkastelua varten. (Koppa 2015c; Kajaanin Ammattikorkeakoulu 2021.)

Teemoittelu soveltuu erityisesti tutkimustulosten analysointimenetelmäksi, kun kyse on laadullisen aineiston analysoimisesta. Tutkimuksen aineistonkeruumenetelmänä käytettiin teemahaastatteluita, joissa kysymykset rajataan teemojen mukaan. Teemahaastatteluiden avulla tutkimustulosten jakaminen eri teemoihin on sujuvaa, jolloin teemoittelu on hyödyllisin analysointimenetelmä (Tuomi & Sarajärvi 2011, 93).

4 Tutkimuksen toteutus

Haastattelut toteutettiin toimeksiantajayrityksen Suomessa toimivien toimihenkilöiden kanssa. Henkilöstön haastatteleminen mahdollistaa yksityiskohtaisen ja tutkimukselle oleellisen tiedon saamisen, sillä henkilöstöllä on tarkka ja ajankohtainen tieto tutkimuksen aiheeseen liittyen. Haastateltavina toimivat yrityksen toimitusjohtaja (CEO), Myynti – sekä työturvallisuusjohtaja (Sales Director and Safety Manager), Tuotepäällikkö (Product Manager), Kehityspäällikkö (R&D Manager). Haastattelut toteutettiin yksilöhaastatteluina ja haastattelun kysymykset olivat etukäteen laadittuja, minkä avulla saatiin keskustelua valittujen teemojen ympärille.

Haastatteluiden kysymykset sisältävät kaikki opinnäytetyön aiheeseen liittyvät tietoturvan osa-alueet. Nämä osa-alueet toimivat haastatteluissa teemoina. Haastattelut etenivät osa-alue kerrallaan, jotta teemoille saadaan yksityiskohtaiset tulokset.

Tulokset analysoidaan käyttäen teemoittelua analysointimenetelmänä. Teemoittelun avulla tutkija merkitsee tutkimuksen kannalta olennaisia asioita, mikä auttaa aineiston sisällön selkeyttämisessä ja tulkitsemisessa.

Haastattelut toteutettiin monissa eri osissa yrityksen sisällä johtuen siitä, että haastateltavia ei ollut mahdollista saada samanaikaisesti paikan päälle haastateltaviksi. Haastatteluiden henkilöt olivat jaettuna myös kahteen eri ryhmään. Ryhmäjako toteutettiin sen takia, että haastatteluissa yrityksen perustajat muodostivat oman ryhmänsä ja yrityksessä palkkalistoilla työskentelevät muodostivat oman ryhmänsä. Jaottelu toteutettiin, jotta haastateltavien vastauksiin ei mahdollisesti vaikuttaisi esimiesten läsnäolo.

Ryhmäjako toteutettiin seuraavalla tavalla: ryhmän numero yksi muodostivat yrityksen toimitusjohtaja sekä myyntijohtaja/työturvallisuusjohtaja. Ryhmä numero kahden muodostivat tuotepäällikkö sekä kehityspäällikkö. Molemmille ryhmille esitettiin samat kysymykset, joihin jokainen haastateltava vastasi omassa haastattelussaan.

4.1 Yrityksen johdon haastattelut

Haastatteluiden alussa kartoitettiin yrityksen yleinen tietoturvallisuustilanne. Johdon haastattelussa kävi ilmi, että yrityksessä ei olla mietitty juurikaan tietoturvaa perustamisen jälkeen. Toimitusjohtajan mukaan yritys on kasvanut sellaista vauhtia, että yksinkertaisesti tietoturvan kehittämiselle ei ole ollut yrityksen sisällä aikaa eikä resursseja. Toimitusjohtaja sekä myyntijohtaja kertoivat myös, että ongelmana on ollut osaamattomuus tietoturvasta sekä yleisesti IT-järjestelmistä. Aikaisemmin yrityksessä työskenteli vielä kolmas omistaja, joka oli itse IT-taustainen henkilö. Kuitenkin kolmas omistaja on siirtynyt yrityksen ulkopuolelle muihin tehtäviin, eikä enää osallistu yrityksen päivittäiseen toimintaan operatiivisella tasolla.

Haastattelut etenivät kysymyksellä liittyen mahdollisiin ongelmiin tietoturvaan liittyen ja että onko kriittisiä ongelmia esiintynyt viime vuosien aikana. Haastattelussa vastaus oli yksimielinen. Haastateltavat kertoivat, että yrityksellä on ollut haasteita tiedostojen jaon kanssa ulkopuolisille tahoille. Toimitusjohtajan mukaan yrityksellä ei tällä hetkellä ole ohjeistusta siitä, kuinka ulkopuolisille tiedostoja tulisi jakaa sekä tiedostojen jaon kanssa on ollut tietoturvan näkökulmasta ongelmia. Yritys on muun muassa jakanut salaisia tiedostoja yrityksen julkisessa Sharepoint -sivulla johtuen siitä, että yritys ei ole keksinyt muuta tapaa kuinka tiedostoja voidaan jakaa. Myyntijohtaja totesi myös, että yrityksen tiedostot ovat sekavassa järjestyksessä, eikä niitä ole luokiteltu omiin tietoturvallisuusluokkiin. Haastattelun perusteella yrityksessä ei ole kuitenkaan ilmennyt kriittisiä tietoturvaloukkauksia, mutta haastateltavat mainitsivat, että on ollut tilanteita, jotka olisivat voineet johtaa vakaviin seurauksiin.

Tietoaineistoturvallisuus

Seuraavaksi haastattelut etenivät tietoturvan osa-alueiden teemojen mukaisesti. Ensimmäisenä käsiteltiin yrityksen tietoaineistoturvallisuutta. Toimitusjohtajan sekä myyntijohtajan mukaan yritys ei ole muodostanut yrityksen käyttäjätileille oikeusryhmiä, jotka voisivat rajoittaa sitä, kuka yrityksen sisällä pääsee mihinkin tietoihin kiinni. Yritys on kuitenkin jaotellut Sharepoint -sivut niin, että yrityksellä on kaksi eri sivua, julkinen sekä yrityksen sisäinen. Kuitenkin jos yritys haluaa antaa työntekijälle pääsyn yrityksen sisäiseen Sharepoint -sivustoon, tulee hän pääsemään kaikkiin tietoihin käsiksi.

Aikaisemman vastauksen perustella tiedostojen tallentamisen sekavuudesta haastattelussa kysyttiin myös, että minne yritys tallentaa tiedostonsa ja onko yrityksellä selkeää ohjeistusta siitä, miten ja minne tiedostot tulee tallentaa. Toimitusjohtajan mukaan yrityksellä ei ole ohjeistusta siitä, että saako tiedostoja tallentaa ulkoisille tallennusvälineille. Tiedostot tulee aina tallentaa yrityksen OneDriveen. Yrityksellä ei myöskään ole ohjeistusta siitä, miten sellaiset tiedot, jotka eivät ole enää tarpeellisia, tulisi hävittää.

Viimeiseksi ensimmäisestä osa-alueesta selvitettiin yrityksen yhteiskäyttötunnuksien politiikkaa. Myyntijohtaja totesi haastattelussa, että jokaisella yrityksen työntekijällä on henkilökohtaiset tunnukset yrityksen verkkoon, mutta yrityksen verkon admin -tunnuksiin on pääsy kahdella henkilöllä. Toinen henkilöistä on yrityksen yksi omistajista, joka ei ole enää mukana yrityksen operatiivisessa toiminnassa ja toinen henkilö on myyntijohtaja.

Tietolaitteistoturvallisuus

Seuraavaksi haastatteluiden teema vaihtui tietolaitteisturvallisuuden osa-alueeseen. Osa-alueen vaihdos aloitettiin käsittelemällä yrityksen toimintatapaa yrityksen omistamien laitteiden osalta. Tässä haastattelussa laitteilla tarkoitetaan yrityksen käytössä olevia tietokoneita sekä matkapuhelimia. Haastattelussa kävi ilmi, että yritys järjestää aina uudelle työntekijälle puhelimen sekä tietokoneen työvälineiksi. Henkilö, jolle laiteet luovutetaan, vastaa niistä itse. Kuitenkin myyntijohtaja totesi, että yrityksellä ei ole virallista nimikointijärjestelmää tai rekisteriä, jonne laitteen tiedot sekä käyttäjän tiedot syötettäisiin ja tallennettaisiin.

Seuraavaksi kysymykseksi haastattelussa esitettiin, onko yrityksellä ohjeistettua toimintatapaa, miten laitteiden käyttöjärjestelmät sekä käytetyt sovellukset pidetään ajan tasalla, jotta käyttö olisi mahdollisimman tietoturvallista. Toimitusjohtajan mukaan yrityksellä ei ole ohjeistusta siitä, kuinka usein järjestelmien päivityksiä on haettava tai asennettava.

Jatkumona järjestelmien käytettävyyteen haastattelussa selvitettiin, pyrkiikö yritys ennakoimaan laitteiden kulumista tai vaihtoa ennen kuin on liian myöhäistä. Haastattelussa kävi ilmi, että yritys ei ole ennakoinut laitteiden vaihtoa tai kulumista muulla tavalla, kuin että henkilökohtaisesti jollain käyttäjillä on huolenpitosopimuksia laitteillensa. Yritys on myös kohdannut ongelmia liittyen tähän aihepiiriin. Myyntijohtajan mukaan viimeksi vuoden 2020 kesällä yrityksen tietokone oli lopettanut äkillisesti toimintansa, jonka vuoksi kaikkia tietoja ei tuhoutuneesta laitteesta saatu palautettua. Tämän tiedon johdosta esitettiin tarkentava kysymys siitä, onko yrityksellä ohjeistusta siitä, kuinka vanha toimimaton laite hävitetään ja jos on niin miten. Toimitusjohtajan sekä myyntijohtajan mukaan yrityksellä ei ole käytössä ohjeistusta siitä, miten vanhat tai toimimattomat laitteet tulisi hävittää.

Viimeisenä tietolaitteistoturvallisuus teemasta kysyttiin, kuinka yritys suojaa laitteistonsa haittaohjelmilta. Myyntijohtajan mukaan yrityksellä ei ole käytössä haittaohjelmia varten erilisiä sovelluksia. Kuitenkin käyttäjät itse ovat ladanneet virustorjuntaohjelmiston laitteillensa. Vastauksen johdosta tarkennettiin kysymystä, että koskeeko virustorjuntaohjelmien asentaminen tietokoneita sekä puhelimia vai pelkästään tietokoneita. Toimitusjohtajan sekä myyntijohtajan mukaan torjuntaohjelmistojen asentaminen koskee vain tietokoneita.

Henkilöstöturvallisuus

Kolmantena osa-alueena käsiteltiin henkilöturvallisuutta ja esitettiin haastateltaville kyseiseen osa-alueeseen liittyviä kysymyksiä. Ensimmäiseksi kartoitettiin sitä, millä tavalla henkilöstön taitojen vastaavuus tarkastetaan vaadittua tehtävää varten. Toimitusjohtaja kertoi, että yritys pyrkii palkkaamaan henkilöstöä suosittelijoiden sekä tuttujen kautta, jotta työntekijän taidoista olisi mahdollisimman tarkka ymmärrys ja että työntekijä olisi tarpeeksi kokenut tehtävää varten. Myös työntekijän työtausta tarkastetaan työtodistuksista sekä soitetaan mahdollisille suosittelijoille. Vastauksen johdosta haastattelussa esitettiin tarkentava kysymys, että tarkastaako yritys myös työntekijän koulutustaustan ja jos tarkastaa niin miten. Toimitusjohtajan mukaan yritys ei ole palkkaustilanteessa tarkastanut henkilöiden koulutustaustaa, koska pääsääntöisesti palkatut henkilöt ovat olleet jollain tavalla tuttuja.

Seuraavaksi haastattelussa yrityksen johdolta kysyttiin teettääkö yritys salassapitosopimuksia työntekijöillensä. Toimitusjohtajan mukaan yritys ei teetätä henkilöstölle salassapitosopimuksia, mutta yrityksen edustajille teetätetään salassapitosopimus. Salassapitosopimukset teetätetään myös jokaisen yrityksen tai henkilön kohdalla, joka osallistuu yrityksen erikoiskoneiden tai -laitteiden tuotanto sekä suunnitteluprosessiin.

Haastattelua jatkettiin selvittämällä, määritteleekö yritys käyttäjän työtehtävän mukaan työntekijäntilin käyttöoikeuksia tiedostoihin tai kansioihin. Jos yritys määrittelee, niin millä tavoin tätä toteutetaan, onko esimerkiksi kansioille muodostettu luku- tai muokkausoikeuksia. Myyntijohtajan mukaan yritys ei ole muodostanut kansioille käyttöoikeuksia, joten niitä ei voida räätälöidä työtehtävän mukaan. Joitain rajoituksia yritys on silti muodostanut, koska yrityksen kaikki työntekijät eivät pääse käsiksi johdon kansioihin.

Viimeisenä henkilöstöturvallisuuden teeman kysymyksissä selvitettiin, millä tavoin yrityksen edustajien tilit eroavat yrityksen omien työntekijöiden tunnuksista. Myyntijohtaja kertoi, että edustajien tilit ovat niin sanottuja External-status-tilejä. External-status tunnustenhallinta puolella rajoittaa käyttäjän pääsyä yrityksen tiedostoihin. Myyntijohtajan esimerkin mukaan työntekijä, jolla on External-käyttötili, ei pääse käsiksi yrityksen sisäisille työntekijöille tarkoitettuihin Sharepoint -sivustoihin.

Käyttöturvallisuus

Seuraavaksi haastatteluiden teema vaihtui käyttöturvallisuuden osa-alueeseen. Aluksi käyttöturvallisuudesta haluttiin selvittää, miten henkilöstö huolehtii käytettyjen tilien salasanoista ja onko yrityksellä käytössä ohjelmaa salasanojen tallennusta varten. Haastattelussa kävi ilmi se, että yrityksellä ei ole käytössä ohjelmaa, joka on tarkoitettu salasanojen säilyttämiseen. Myyntijohtajan mukaan yrityksen käyttäjät tallentavat kaikki käytetyt tunnukset sekä salasanat suoraan selaimeen. Tämän tiedon johdosta, haastattelussa esitettiin tarkentava kysymys salasanojen politiikasta yrityksessä, onko yrityksellä määritelty käyttäjätunnuksien salasanoille minimivaatimuksia. Myyntijohtajan mukaan yrityksen salasanoille ei ole määritelty minimivaatimuksia, mutta kaksivaiheinen todennus on pakotettuna jokaiselle käyttäjätilille. Tämä tarkoittaa sitä, että kirjautuessaan yrityksen tunnuksilla, käyttäjän tulee kirjautua sisään ensiksi salasanalla, jonka jälkeen kirjautumisruutu pyytää koodia, jonka työntekijä saa tekstiviestillä puhelimeen. Vasta tämän prosessin jälkeen käyttäjä pääsee kirjautumaan yrityksen sivuille.

Seuraavaksi käyttöturvallisuuden osa-alueesta haastattelussa selvitettiin yrityksen toimintatapaa tehdä dokumentaatiota ja ohjeistusta yrityksen käyttämistä tietojärjestelmistä tai sovelluksista. Haastateltavilta kysyttiin, onko yritys varautunut tilanteisiin, jossa työntekijä lähtee riitaisesti yrityksestä ja että pystyvätkö muu henkilöstö jatkamaan tällöin lähteneen työntekijän toimintaa yrityksessä olevien ohjeistusten pohjalta. Toimitusjohtajan mukaan dokumentaatiota tai ohjeistusta ei yrityksessä ole tehty, mutta toimintaa on pyritty tekemään niin, että aina kaksi henkilöä osaavat käyttää yrityksen käyttämiä järjestelmiä sekä sovelluksia.

Viimeisinä kysymyksinä käyttöturvallisuuden osa-alueesta selvitettiin yrityksen toimintatapaa varautua laitteiden rikkoutumiseen sekä tiedostojen palauttamiseen rikki menneestä laitteesta. Aikaisemmin haastattelussa selvisi, että yritys ei ole varautunut rikki meneviin laitteisiin.

Myös aikaisemmista haastattelun vastuksista ilmeni, että yritys ei voi enää palauttaa rikki menneen laitteen tiedostoja, jotka ovat tallennettuna suoraan laitteen omalle kovalevylle. Kuitenkin yrityksellä on ohjeistettu, että tiedot pitää tallentaa aina yrityksen pilveen, jotta tiedostot ovat aina saatavilla. Tästä kysymyksestä jatkettiin kysymällä, että onko yritys varautunut mitenkään siihen, että tiedostot voivat tuhoutua tai kadota kokonaan pilvestä. Toimitus- sekä myyntijohtajan mukaan ei ole. Yrityksen kaikki liiketoimintakriittiset tiedostot ovat tallennettuna yrityksen O365 palvelun OneDriveen.

Fyysinen turvallisuus

Viimeisenä teemana haastatteluissa käsiteltiin yrityksen fyysistä turvallisuutta. Haastattelussa selvitettiin, onko yrityksellä käytössä kulunhallintaa yrityksen toimistotiloissa. Myyntijohtajan mukaan toimitiloihin pääsee avaimella ja se toimii yrityksen kulunhallintana. Kortinlukijoita ja kulukortteja yrityksellä ei ole käytössä. Haastattelua jatkettiin tarkentavalla kysymyksellä, että millaista valvontaa rakennuksessa suoritetaan, onko yrityksellä esimerkiksi käytössä valvontakameroita. Toimitusjohtajan mukaan yritys ei käytä valvontakameroita toimitiloissaan, mutta rakennus on suojattu liiketunnistimin sekä vartiointiliike huolehtii koko rakennuksen vartioinnista.

Viimeisinä kysymyksinä haastattelussa selvitettiin yrityksen varautumista paloturvallisuuteen sekä pölyn aiheuttamiin riskitekijöihin sähkölaitteille. Molempien haastateltavien mukaan yrityksessä ei varauduta pölyn aiheuttamiin riskeihin. Paloturvallisuudesta puolestaan on huolehdittu siten, että koko rakennuksella on käytössä poistumissuunnitelma tulipalon sattuessa. Lisäksi haastatteluiden vastausten mukaan yrityksen toimistosta löytyy palosammutin sekä hälytin.

4.2 Työntekijöiden haastattelut

Ryhmä numero kahden haastattelu toteutettiin samalla kaavalla, kuin ensimmäisen ryhmän haastattelu. Haastattelun teema käytiin seuraavassa järjestyksessä: Tietoaineisto-, tietolaitteisto-, henkilöstö-, käyttö- sekä fyysinen turvallisuus. Toisen ryhmän haastatteluissa esiintyi paljon yhtäläisyyksiä ensimmäisen haastatteluryhmän tuloksiin. Toisen ryhmän haastattelussa nousi esille samat ongelmakohdat kuin ensimmäisessä ryhmässä teemahaastattelukysymysten vastausten perusteella.

Kuitenkin toisen ryhmän haastatteluissa esiintyi myös lisäyksiä edellisen haastattelun tuloksiin. Seuraavissa kappaleissa käsitellään löydökset tietoturvan osa-alueittain, joita ei ilmennyt ensimmäisen ryhmän haastatteluissa.

Tietolaitteistoturvallisuus

Haastatteluryhmä kahden vastauksissa esiintyi samoja vastauksia, mitä aikaisempi ryhmä haastattelussa antoi. Haastatteluissa nousi vastausten eroavaisuus tietolaitteistoturvallisuuden osalta liittyen yrityksen ennakoimiseen laitteiden kulumiseen tai rikkoutumiseen. Kehityspäällikön mukaan yritys on osaksi ennakoinut laitteiden vaihtoa, ennen kuin on ollut liian myöhäistä. Esimerkiksi kehityspäällikön tietokone vaihdettiin jokin aika sitten sen takia, koska vanha laite alkoi olemaan hidas ja käyttäjällä heräsi huoli siitä, että laite ei enää kestä käyttöä kauhean pitkään. Kuitenkin kehityspäällikkö kertoi, että yritys ei itsessään suoraan ohjeista laitteiden vaihtoon, vaan ehdotus laitteen uusimisesta tuli häneltä itseltään.

Käyttöturvallisuus

Käyttöturvallisuuden osalta eroavaisuus ilmeni käyttäjien tavasta huolehtia salasanojensa tallentamisesti tietoturvallisesti. Tuotepäällikön sekä kehityspäällikön mukaan he käyttävät salasanojen tallentamiseen erillisitä sovellusta, joka on tarkoitettu pelkästään käyttötunnusten sekä salasanojen tallentamiseen. Sovellus itsessään tallentaa kaikki salasanat tietokantaan, jonka jälkeen ohjelma salaa tietokannan tiedot. Tietokannan saa auki itselleen käytettäväksi ennalta määritetyllä salasanalla. Tämän tiedon johdosta haastattelussa esitettiin tarkentava kysymys, onko salasanojen tallentamiseen tullut määräyksiä tai ohjeistuksia yrityksen johdolta. Molempien haastateltavien mukaan ohjeistusta ei ollut tullut yrityksen johdolta, vaan he ovat itse kokeneet tallennusohjelman hyödylliseksi ja turvalliseksi ja näin ollen ottaneet ohjelman käyttöönsä.

Toisena uutena löydöksenä käyttöturvallisuuden osalta tuli vastaukset yrityksen toiminnasta varautua rikkimeneviin laitteisiin. Kehityspäällikön mukaan yritys on osittain varautunut laitteiden rikkoutumiseen. Jokaisella työntekijällä on kaksi puhelinta siitä syystä, mikäli käyttäjän puhelin menisi rikki. Näin käyttäjä voisi vaihtaa puhelinta toiseen ja käyttää vanhempaa mallia niin kauan kunnes puhelin saadaan uusittua. Myös osalla työntekijöistä on huolenpitosopimuksia laitteisiin, jotta vikatilanteissa laite saadaan nopeasti huollettua tai tarvittaessa vaihdettua. Huolenpitosopimuksista kuitenkin kehityspäällikkö mainitsi, että ne ovat hoidettu omatoimisesti ja henkilökohtaisesi. Yritys maksaa tarvittaessa huolenpitosopimuksen, mutta ei automaattisesti sitä itse osta laitteille.

Fyysinen turvallisuus

Fyysisen turvallisuuden osa-alueelta uutena asiana haastattelussa nousi esiin yrityksen varautuminen pölyn aiheuttamiin riskeihin. Tuotepäällikön mukaan yritys varautuu pölyn kerääntymiseen siivoamalla tarkasti sähkölaitteiden ympäriltä pölyt kerran viikossa. Näin ollen pölyä ei pääse kerääntymään liikaa ja se ei aiheuta uhkaa toimitilojen sähkölaitteille.

4.3 Havainnoinnin tulokset

Tässä opinnäytetyössä havainnointia on käytetty haastatteluja tukevana aineistonkeruumenetelmänä. Havainnoinnin tarkoituksena oli keskittyä teemahaastatteluissa ilmenneisiin ongelmakohtiin ja varmistaa haastatteluissa tulleiden johtopäätösten oikeellisuus. Havainnointi toteutettiin useana eri päivänä sekä ajallisesti yrityksen toimintatapoja seurattiin muutamia tunteja kerralla. Havainnoinnin kohteena oli toimitusjohtajan ja myyntijohtajan toiminta sekä yrityksen toimitilat. Seuraavassa kappaleessa käsitellään havainnoinnin tuloksia tietoturvan osa-alueittain. Havainnoinnin tulokset rajautuivat tietoaineisto-, käyttö- sekä fyysiseen turvallisuuteen.

Tietoaineistoturvallisuus

Havainnoinnin yhteydessä tutkija huomasi, että yrityksen tiedostot ovat hyvin sekavalla tavalla rakennettu Sharepoint-sivustolle. Yrityksen tiedostoja ei olla luokiteltu ja työtä hankaloittaa ja hidastaa tiedostojen suuri määrä. Yrityksellä näytti olevan haasteita siinä, että tiedostoja ei tahtonut löytää nopeasti eikä kansiorakenteita ollut rakennettu loogisella tavalla. Yritys myös pohti observoinnin aikana, kuinka tärkeä ja arkaluontoinen tiedosto voidaan jakaa ulkopuoliselle toimijalle. Ongelmaksi muodostui se, että ilman käyttäjätilin luomista yrityksen verkkoon, tiedostoa ei saatu jaettua. Yritys päätyi lisäämään tiedon julkiseen kansioon, josta ulkopuolinen toimija pystyi lataamaan tiedoston. Lataamisen jälkeen tiedosto kuitenkin poistettiin nopeasti.

Käyttöturvallisuus

Havaintoina seurantajakson aikana tutkija huomasi, että myyntijohtaja sekä toimitusjohtaja molemmat käyttävät selainmuistissa tallennettuja tunnuksia yrityksen tietojärjestelmiin kirjautuessa. Kumpikaan havainnoinnin kohteena olleista käyttäjistä ei käyttänyt salasanojentallennukseen soveltuvia sovelluksia. Käyttäjätiedot olivat luettavissa selainmuistissa, mikäli laitteen saisi aukaistua.

Toisena huomiona seurantajakson aikana huomattiin, että yritys tallentaa huomattavan paljon tiedostoja suoraan tietokoneen omalle muistille. Vain valmiit tiedostot, joita ei tarvinnut enää muokata siirrettiin yrityksen pilveen. Kuitenkin tiedostoja myös muokattiin suoraan pilvestä, jolloin tiedostot tallentuivat automaattisesti, kun niitä oli muokattu.

Fyysinen turvallisuus

Seurantajakson aikana tutkija pyrki tarkastelemaan yrityksen fyysisen turvallisuuden tilannetta. Seurantajakson aikana kävi ilmi, että yrityksen toimitilat ovat vartioitu tarpeellisin menetelmin. Yrityksen toimitiloissa on huomattava määrä liiketunnistimia ja rakennus on vartioitu ulkopuolisen variointiyrityksen toimesta 24 tuntia vuoden jokaisena päivänä. Seurantajakson aikana yrityksen tiloista huomattiin, että kulunhallintana toimistotiloihin käytettiin avainta. Rakennuksessa ei ollut käytössä kortinlukijoita, jolla voisi seurata tarkemmin henkilöstön liikkumista.

4.4 Aineiston analyysi

Tässä kappaleessa käsitellään tietoturvakartoituksen lopputuloksia tietoturvan eri osa-alueittain. Aineiston analyysimenetelmänä käytettiin teemoittelua. Teemoittelun avulla kartoituksessa ilmenneitä ongelmakohtia pystyttiin jäsentämään oikeisiin tietoturvallisuuden osa-alueisiin ja tällä tavalla aineiston kokonaisuutta pystyttiin selventämään. Teemoina tutkimuksessa käytettiin tietoturvan eri osa-alueiden nimiä ja näin yrityksen tietoturvan kartoituksesta pystyttiin rakentamaan analyysitaulukko, joka antaa pohjan tulevalle kehitystyölle. Kehitystyön keskiössä on ratkaista tietoturvan ongelmat, jotka ilmenevät analyysitaulukosta.

Tutkimustulosten mukaan suurimmat tietoturvaongelmat jakaantuivat tietoaineisto- ja käyttöturvallisuuteen. Yrityksen suurimmaksi ongelmaksi ilmeni tiedostojen luokittelemattomuus ja sekavuus. Tiedostojen kansiorakennetta ei ole järjestelty loogisesti ja tästä johtuen yrityksellä on ollut tilanteita, joissa salaisia tiedostoja on jaettu ulkopuolisille. Tiedostojen luokittelemattomuus ja sekavuus voivat aiheuttaa salaisten ja arkaluontoisten tietojen vuotamisen ulkopuolisille tahoille. Ulkopuoliset tahot voivat käyttää yritykselle arkaluontoista tietoa väärin ja yritykselle voi koitua vakavia seurauksia, kuten mahdollisia tappioita tietojen väärin jakamisen vuoksi. Tiedostojen sekavuus voi aiheuttaa tiedostojen katoamisen tai päälle tallentamisen, jolloin tiedosto tuhoutuu. Lisäksi tiedostojen sekava järjestys voi johtaa tiedostojen vahinkohävittämiseen. Tiedostojen sekavuus johtuu usein siitä, että ohjeistusta tietojen tallennukseen ja tallennuskohteisiin ei ole. Hyvällä tiedostojenluokittelulla voidaan varmistaa, että jokainen tietojenkäsittelijä on tietoinen tiedoston tärkeydestä ja merkityksestä yritykselle.

Haastatteluiden tuloksissa ilmeni myös, että yrityksessä tiedostoja tallennetaan ainoastaan pilvipalveluihin. Pilvipalveluihin tallentaminen on suotavaa, mutta tilanteissa, joissa tiedostot ovat ainoastaan pilvipalveluissa, on suuri riski. Pilvipalveluun tallennetut tiedostot ovat tällöin vain yhdessä paikassa ja jos kyseinen tiedosto poistetaan joko vahingossa tai tahallisesti, ei tiedostoa pystytä varmuudella aina palauttamaan. Tiedostoja kannattaa säilyttää pilvipalveluissa, mutta tärkeiden tiedostojen saatavuus tulisi varmistaa tallentamalla tiedot useaan eri paikkaan.

Salasalojen käyttö yrityksessä on tutkimuksen mukaan myös heikolla tasolla. Salasanoille ei ole asetettu minimivaatimuksia. Vaatimukset tulisi asettaa salasanoille, jotta salasanat olisivat tietoturvallisia. Heikot ja lyhyet salasanat ovat tietoturvauhka, sillä ulkopuolisilla tahoilla on täten suurempi mahdollisuus päästä yrityksen käyttämiin tunnuksiin käsiksi. Tietomurrot ovat todella yleisiä nykypäivänä, jolloin vahvojen salasanojen merkitys korostuu.

Muiden tietoturvan osa-alueiden osalta haastatteluissa ilmeni ongelmia, jotka vaativat myös kehitysehdotuksia, mutta eivät ole kriittisimpiä. Yrityksen fyysinen ja henkilöstöturvallisuus ovat kohtalaisella tasolla ja merkittäviä tietoturvariskejä ei ole havaittavissa tutkimustulosten perusteella.

4.5 Riskimatriisi

Tietoturvakartoituksessa ilmenneet ongelmakohdat analysoidaan riskimatriisin avulla tärkeysjärjestykseen. Riskimatriisi on työkalu, jonka avulla voidaan kuvata riskien eri tasoja. Riskimatriisin tulosten avulla voidaan karkeasti rajata riskien käsittelyn tarve. Riskimariisi rakennetaan asteikoilla 1–4, jossa vaakatasossa arvioidaan riskin vaikutusta ja pystyasennossa riskin todennäköisyyttä. Riskimatriisin arviointiasteikon tulos saadaan, kun riskin vaikutus kerrotaan todennäköisyyden luvulla. Alla on kuvattuna VAHTI-dokumentissa esitetty asteikko todennäköisyyden määritelmille.

Taso 1. Epätodennäköinen

Tapahtuman toteutuminen ilmenee vain poikkeuksellisissa oloissa ja mahdollisuus toteutumiseen on enimmäkseen teoreettinen. Tapahtuma on epätodennäköinen esimerkiksi tilanteissa, kun riskin ei tiedetä toteutuneen aikaisemmin.

Taso 2. Mahdollinen
Tapahtuma saattaa toteutua tietyissä tapauksissa tai olosuhteissa ja on toteutunut joskus oman yrityksen sisällä tai muualla.
Taso 3. Todennäköinen
Tapahtuman toteutuminen on odotettavissa tai tapahtuman toteutuminen tiedostetaan toteutuvan mitä suurimmalla todennäköisyydellä.
Taso 4. Lähes varma
Tapahtuma toteutuu tai on usein toteutunut. Tapahtumassa on tapahtunut useita ”läheltä piti tilanteita”.

Taulukko 2: Todennäköisyyden tasot (Ohje riskienhallintaan 2017, 23)

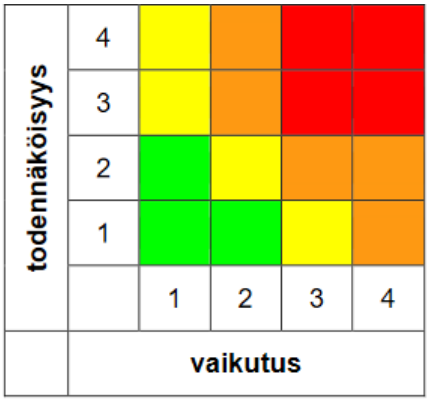
Vaikutusta arvioidaan riskimatriisissa seuraavilla luvuilla:

Taso 1. Vähäinen
Riskin toteutumisen vaikutus yrityksen toimintaan on vähäinen ja voi aiheuttaa vähäistä haittaa yrityksen strategisen tavoitteen saavuttamiseksi.
Taso 2. Kohtalainen
Riskin toteutuessa mahdollisuudet saavuttaa yhtä tai useampia strategisia tavoitteita viivästyvät ja heikentyvät. Riskin toteutumisen seurauksena ei vaadita toiminnan keskeyttämistä, mutta toiminnallisia suunnitelmia saatetaan joutua muuttamaan. Tapahtumasta voi aiheutua yritykselle vähäisiä kustannuksia.
Taso 3. Merkittävä
Riskin toteuttaminen hidastaa, vaikeuttaa sekä vaarantaa merkittävällä tavalla tärkeän strategian saavuttamista. Riskin toteutuminen voi aiheuttaa suurta vahinkoa ja merkittäviä kustannuksia sekä omaisuuden rikkoontumista. Riskin toteutuessa yksittäisten ihmisten terveys ja henki voivat vaarantua.

Taso 4. Kriittinen
Riskin toteutuessa esimerkiksi yritykselle toiminnan kannalta tärkeä strateginen tavoite estyy tai kriittinen prosessi tai palvelu keskeytyy. Riskin toteutuminen voi luoda suurta vahinkoa tai kustannuksia myös muille tahoille. Riskin seurauksena toiminta joudutaan keskeyttämään pitkähköksi ajaksi ja merkittäviä kustannuksia voi aiheutua yrityksen tai valtionhallinnon näkökulmasta katsottuna. Suuren ihmisjoukon henki tai terveys vaarantuu ja riskin toteutuminen voi vaikuttaa koko yhteiskunnan toimintaan.

Taulukko 3: Vaikutuksen tasot (Ohje riskienhallintaan 2017, 24)

Analyysitaulukon ongelmakohdat on arvioitu riskimatriisin avulla, jotta tutkija voi asettaa ongelmakohdat kriittisyysjärjestykseen. Riskimatriisin tasot jaetaan neljään eri pääluokkaan: Kriittinen riski (9–16), merkittävä riski (4–8), kohtalainen riski (3–4) sekä matalariski (1–2).



Kuva 1: Riskimatriisi (Ohje riskienhallintaan, liite 2017)

4.6 Ongelmakohtien yhteenveto

Tietoturvakartoituksen tulokset ovat kuvattuna alla olevassa taulukossa, joka toimii myös yhteenvetona haastatteluissa ja havainnoinnissa ilmenneille ongelmakohdille. Taulukossa esitetään tietoturva-alueeseen liittyvät ilmenneet ongelmakohdat sekä niiden arvioitu riskien taso.

Tietoturvan osa-alue	Ongelmakohdat	Riskin taso
Tietoaineisto-turvallisuus	▪ Tiedostojen jakaminen sisäisesti ja ulkoisesti	16
	▪ Tiedostojen käyttöoikeudet	6
	▪ Ohjeiden puute	4
	▪ Tiedostojen suojaus	4
	▪ Tiedostojen tallentaminen	12
	▪ Yhteiskäyttötunnukset (admin)	4
	▪ Tiedostojen luokittelemattomuus	16
Tietolaitteis-toturvallisuus	▪ Ei nimikoituja laitteitta	1
	▪ Ei ohjeistusta järjestelmäpäivitysten suhteen	2
	▪ Ei ohjeistusta vanhojen tai toimimattomien laitteiden hävittämiseksi	4
	▪ Ei yrityksen määrittelemää tietoturvaohjelmistoa käytössä	2
Henkilöstö-turvallisuus	▪ Ei salassapitosopimuksia henkilöstölle	1
	▪ Henkilöstön koulutustaustaa ei tarkasteta	1
	▪ Käyttöoikeuksia ei määritellä työtehtävän mukaan	2
Käyttöturvallisuus	▪ Ei ohjeistusta käyttää salasanan säilöntäsovelluksia	1
	▪ Tunnusten tallentaminen suoraan selaimeen	3
	▪ Salasanoille ei ole asetettu minimivaatimuksia	2
	▪ Ei ohjeistuksia tai dokumentaatiota käytetyistä sovelluksista tai järjestelmistä.	1
	▪ Kaikki tiedostot tallennettuna vain pilveen	4
Fyysinen turvallisuus	▪ Avain ainoastaan kulunhallintana toimistotilohin	1

Taulukko 4: Analyysitaulukko

5 Tulokset

Tässä luvussa käsitellään tietoturvakartoitukseen perustuvia kehitysehdotuksia toimeksiantajayrityksen tietoturvan parantamiseksi. Opinnäytetyön tavoitteena on tuottaa toimeksiantajayritykselle kehitysehdotukset kartoituksessa ilmenneille ongelmakohdille. Nämä kehitysehdotukset täyttävät VAHTI-dokumentaation vaatimukset yrityksille. Kehitysehdotukset esitetään tietoturvan osa-alueittain ongelmakohta kerrallaan. Kehitysehdotukset ovat luotu toimeksiantajayrityksen tarpeisiin sekä kokoon nähden.

Kehitysehdotukset ovat esitetty taulukoissa. Taulukot koostuvat haastatteluissa esiintyneistä ongelmakohdista, kehitysehdotuksista sekä perusteluista näille kehitysehdotuksille eli ratkaisuista kyseisiin ongelmakohtiin. Taulukossa esitetyt perusteet pohjautuvat VAHTI-dokumentaatiossa (Valtionhallinon keskeisten tietojärjestelmien turvaaminen 2004) esitettyihin vaatimuksiin.

5.1 Tietoaineistoturvallisuus

Ongelmakohta	Kehitysehdotus	Perustelut
Tiedostojen jakaminen sisäisesti ja ulkoisesti	Tiedostot voidaan jakaa sisäisesti SharePoint-sivustolla. Ulkopuolisille jaettavat tiedostot on jaettava tiedonsiirtoon tarkoitettujen sovelluksien kautta esim. Dropbox	VAHTI-ohjeistus vaatii yrityksiltä, että tiedon luottamuksellinen siirto tulee varmistaa. Tiedonsiirto tulee toteuttaa niin, että tiedot voidaan tarpeen tullen salata.
Tiedostojen käyttöoikeudet	Yrityksen tulee luoda tiedostokansioille käyttöoikeudet. Käyttöoikeuksia hallitaan admin-tunnuksella.	VAHTI-dokumenttien mukaan vain käyttäjät, jotka tarvitsevat työhönsä tietoja, saavat oikeudet tiedostokansioihin.
Ohjeiden puute tiedostojen tallentamisessa	Ohjeistus tulee luoda henkilöstölle tiedostojen tallentamiseen sekä hävittämiseen. Ohjeet voivat olla esim. PDF-muodossa.	VAHTI-dokumentin mukaan tiedostojen arkistoinnille sekä tietojenhävitykselle tulee olla olemassa oleva ohjeistus.

Tiedostojen suojaus	Erittäin arkaluontoiset tiedostot tulee suojata aina lähettäessä sekä niitä säilyttäessä. Esim. Tiedostojen kryptaaminen tai salasanasuojaus	VAHTI-ohjeistus toteaa, että tiedot, jotka eivät ole julkista tietoa, tulee salata.
Tiedostojen tallentaminen	Yrityksen tulee asettaa selkeät linjaukset siitä, minne tiedostot tallennetaan sekä saako tiedostoja ladata omalle laitteelle. Esim. verkkolevy	VAHTI-ohjeistuksen mukaan tiedontallentamispaikkojen käyttö ja rajoitukset tulee olla ohjeistettu.
Yhteiskäyttötunnukset (admin)	Admin-tunnukselle tulee määrittää vastuuhenkilö. Admintunnusta ei saa hallita, kuin yksi henkilö.	VAHTI-dokumentaatio toteaa, että yhteiskäyttötunnukset ovat kiellettyjä.
Tiedostojen luokittelemattomuus	Tiedostot tulee luokitella vähintään kolmeen eri tasoon: Julkinen, luottamuksellinen sekä erittäin salainen.	VAHTI-dokumentaatio velvoittaa yritystä luokittelemaan tiedot turvallisuusluokkiin.

Taulukko 5: Tietoaineistoturvallisuuden kehitysehdotukset

5.2 Tietolaitteistoturvallisuus

Ongelmakohta	Kehitysehdotus	Perustelut
Ei nimikoituja laitteita	Yritys nimikoi laitteensa sekä määrittää käyttäjän laitteelle.	VAHTI-ryhmän mukaan jokaisella laitteella tulee olla yksi omistaja.
Ei ohjeistusta järjestelmäpäivitysten suhteen	Yritys luo selkeät ohjeistukset työntekijöille, kuinka usein laitteiden järjestelmäpäivitykset tulee hakea ja asentaa, esimerkiksi kerran kuukaudessa	VAHTI-dokumenttien mukaan laitteiden ylläpito tulee olla suunnitelmallista.
Ei ohjeistusta vanhojen tai toimimattomien laitteiden hävittämiseksi	Yritys luo selkeät prosessit laitteiden hävitykseen, esimerkiksi kovalevyjen formatointi.	VAHTI-ohjeistuksen mukaan laitteen käytöstä poisto tulee olla suunnitelmallista.
Ei yrityksen määrittelemää tietoturvaohjelmistoa käytössä	Yritys ostaa lisenssit valitsemaansa tietoturvanohjelmaan. Ohjelmat vaaditaan asennettavaksi yrityksen jokaiselle laitteelle.	Dokumentaation mukaan laitteistot tulee olla suojattuna haittaohjelmilta asianmukaisella ohjelmistolla. Ohjelmistoon tulee olla saatavilla säännöllisesti päivityksiä.

Taulukko 6: Tietolaitteistoturvallisuuden kehitysehdotukset

5.3 Henkilöstöturvallisuus

Ongelmakohta	Kehitysehdotus	Perustelut
Ei salassapitosopimuksia henkilöstölle	Salassapitosopimukset tehdään yrityksen jokaiselle työntekijälle.	Ohjeistuksen mukaan yrityksen on huolehdittava siitä, että työntekijä allekirjoittaa salassapitosopimuksen.
Henkilöstön koulutustaustaa ei tarkisteta	Jokaisen palkattavan työntekijän taustat varmistetaan ennen koeajan päättymistä.	VAHTI-ohjeet velvoittavat yritystä tarkistamaan henkilöstön koulutustaustat.
Käyttöoikeuksia ei määritellä työtehtävän mukaan	Yrityksen työntekijöiden käyttöoikeudet tulee määritellä työtehtävää varten.	VAHTI-dokumentaatio vaatii, että työntekijöiden käyttöoikeudet rajataan työtehtävää varten.

Taulukko 7: Henkilöstöturvallisuuden kehitysehdotukset

5.4 Käyttöturvallisuus

Ongelmakohta	Kehitysehdotus	Perustelut
Ei ohjeistusta salasanan säilöntäsovelluksien käytöstä	Yritys asentaa sekä ohjeistaa jokaiselle käyttäjälle salasanan sälytysohjelman, esimerkiksi KeePass-ohjelman.	Salasanan säilönnälle ei ole erillistä määräystä VAHTI-dokumenttien toimesta. Dokumentti kuitenkin velvoittaa yrityksen salaamaan tärkeät tiedostot. Yrityksen käyttötunnusten salasanat luokitellaan tärkeiksi tiedoiksi.
Tunnusten tallentaminen suoraan selaimeen	Yritys tallentaa kaikki käytössä olevat tunnukset salasanan säilöntäohjelmaan.	VAHTI-ohjeet vaativat, että yrityksen tärkeät tiedot salataan ja säilytetään turvallisesti.
Salasanoille ei ole asetettu minimivaatimuksia	Vähintään yrityksen käyttötunnusten salasanoille määriteltävä vaatimukset. Esimerkiksi salasanan tulee olla 12 merkkiä pitkä ja sisältää ison kirjaimen, numeron sekä erikoismerkin.	Salasananoille ei ole erikseen määritelty minimivaatimuksia ohjeistuksessa. Vahvemmat salasanat parantavat yrityksen tietoturvaa.
Ei ohjeistuksia tai dokumentaatiota käytetyistä sovelluksista tai järjestelmistä	Yritys tekee selkeät ohjeet, kuinka tietojärjestelmiä ja sovelluksia käytetään. Ohjeet voivat olla esim. PDF muodossa.	VAHTI-ohjeet määrittävät, että yrityksen tulee tarjota henkilöstölle tietojärjestelmien käyttöön ohjeistukset.
Kaikki tiedostot tallennettuna vain pilveen	Yrityksen tulisi tallentaa tietoja myös lokaalisti. Esimerkiksi yrityksen tiedostoja voidaan jakaa sisäverkossa olevaan verkkolevyyn.	VAHTI-dokumenttien mukaan säilytettävät tiedot tulee kopioida ja tallentaa fyysisesti yrityksen tiloihin.

Taulukko 8: Käyttöturvallisuuden kehitysehdotukset

5.5 Fyysinen turvallisuus

Ongelmakohta	Kehitysehdotus	Perustelu
Avain ainoastaan kulunhallintana toimistotilohin	Yritys järjestää toimitiloihin kortinlukijat sekä kulkukortit henkilöstölle.	Dokumenttien mukaan yrityksen kulunvalvonta tulee järjestää niin, että tiloihin ei voi saapua tai poistua ilman tulematta rekisteröidyksi.

Taulukko 9: Fyysisen turvallisuuden kehitysehdotukset

6 Johtopäätökset

Opinnäytetyö toteutettiin tapaustutkimuksena. Tapaustutkimuksessa toteutettiin toimeksiantajayritykselle tietoturvakartoitus. Kartoitus toteutettiin teemahaastatteluiden ja havainnoinnin avulla. Tutkimus eteni järjestelmällisesti, ja haastatteluiden sekä havainnoinnin tulosten avulla saatiin selkeästi esille yrityksen tietoturvan ongelmakohdat, joille tämän opinnäytetyön tuloksena esitettiin kehitysehdotukset. Sisäisen henkilöstön haastatteleminen ja heidän toimintansa seuraaminen mahdollisti sen, että kehitysehdotukset pystyttiin personoimaan juuri toimeksiantajayrityksen tarpeisiin ja esiintyneisiin ongelmakohtiin.

Tämän opinnäytetyön tietoturvankartoituksen perusteella yrityksellä oli todella paljon puutteita tietoturvan näkökulmasta. Tutkimuksen tulosten perusteella yrityksen suurimmaksi ongelmakohdaksi nousi esiin tietojenluokittelemattomuus. Toisena suurena ongelmakohtana kartoituksessa nousi yrityksen tiedostojen jakaminen ulkopuolisille henkilöille. Tämä ongelmakohta johtuu siitä, että yrityksen tietoja ei ole luokiteltu. Luokittelun puutteen vuoksi yrityksellä oli käynyt tilanne, jossa erittäin salassa pidettävä tiedosto oli jaettu yrityksen ulkopuolelle julkisella sivustolla. Osatekijänä tässä tapauksessa oli myös osaamattomuus, kuinka jakaa tiedosto vastaanottajalle tietoturvallisesti.

Näiden tulosten pohjalta tutkija on tehnyt kehittämisehdotukset toimeksiantajayritykselle tietoturvan parantamiseksi. Tutkija suosittelee yritystä käymään läpi tarkasti analyysitaulukon tulokset sekä kehittämisehdotukset. Näiden löydösten sekä kehittämisehdotusten pohjalta yritys voi lähteä rakentamaan tietoturvaansa parempaan suuntaan.

Tutkija suosittelee, että yritys palkkaa tai siirtää tietoturvavastuun työntekijälle, jolla on ymmärrystä yrityksen käyttämistä IT-järjestelmistä sekä tietoturvasta.

Vaikka yrityksen tietoturvan tila vaikuttaa tietoturvakartoituksen tuloksissa huonolta, on yrityksenjohto selkeästi motivoitunut tekemään korjausliikeitä tietoturvan parantamiseksi. Myös yrityksellä on paljon hyvää tietoturvan näkökulmasta, koska kriittisimpiä uhkia kartoituksessa löytyi kahdesta tietoturvan osa-alueesta.

Lähteet

Painetut

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell

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

Tuomi, J. & Sarajärvi, A. 2008. Laadullinen tutkimus ja sisällönanalyysi. 7. painos. Vantaa: Tammi

Sähköiset

Digi- ja väestötietovirasto. 2021. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. Viitattu 17.04.2021. https://dvv.fi/vahti

Elearn. 2003. Tietoturvan osa-alueet. Viitattu 189.04.2021. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html

Kajaanin Ammattikorkeakoulu. 2021. Viitattu 19.05.2021. https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Laadullisen-analyysi-ja-tulkinta/Teemoittelu

Koppa. 2015a. Tapaustutkimus. Viitattu 27.4.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/toimintatutkimus

Koppa. 2015b. Laadullinen tutkimus. Viitattu 24.4.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Koppa. 2015c. Teemoittelu. Viitattu 19.05.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/teemoittelu

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Koodaus. Viitattu 27.04.2021. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_2_2.html

Suomidigi. 2021. Tietoturvallisuus ja tulosohjaus. Viitattu 17.04.2021. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2004.pdf

Valtiovarainministeriö. 2004. Valtionhallinon keskeisten tietojärjestelmien turvaaminen. Viitattu 18.04.2021. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_5_2004.pdf

Valtiovarainministeriö. 2016. VAHTIn toimintakertomus vuodelta 2015. Viitattu 17.04.2021. https://vm.fi/julkaisut/vahti

Valtiovarainministeriö. 2021. Voimassa olevat tietoturvaohjeet ja -määräykset. Viitattu 17.04.2021. https://vm.fi/julkaisut/vahti

Valtiovarainministeriö. 2017. Ohje riskienhallintaan. Viitattu 20.05.2021. https://www.suomi-digi.fi/sites/default/files/2020-06/VM_22_2017_1.pdf

Julkaisemattomat

Toimeksiantajayrityksen toimitusjohtaja. Teemahaastattelu 15.04.2021.

Toimeksiantajayrityksen myyntijohtaja. Teemahaastattelu 15.04.2021.

Toimeksiantajayrityksen tuotepäällikkö ja kehityspäällikkö. Teemahaastattelut 20.04.2021.

Taulukot

Kuvat

Liitteet

Liite 1: Teemahaastatteluiden haastattelukysymykset

Tietoturva

Miten koet tietoturvan tilan olevan tällä hetkellä yrityksessä?

Onko yrityksessä ilmennyt ongelmia tietoturvan näkökulmasta?

Tietoaineistoturvallisuus

Ovatko yrityksenne tiedostot luokiteltu millään tavalla?

Onko käyttäjätileillänne minkäänlaisia oikeusryhmiä, jotka rajoittavat henkilöiden pääsyä tiedostoihin?

Minne yrityksen tiedostot tallennetaan? Saako tallennuksen tehdä ulkoisille tiedontallennusvälineille?

Onko teillä käytössä yhteiskäyttötunnuksia?

Miten arkaluontoiset tiedostot hävitetään ja onko hävittämiseen liittyen mitään ohjeistusta?

Tietolaitteistoturvallisuus

Onko yrityksessä nimikoidut laitteet jokaiselle työntekijälle?

Onko teillä ohjeistettu, että laitteet tulee päivittää kerran kuussa esim. kuun 1. pvä ajetaan ja tarkastetaan Windows -päivitykset?

Ennakoitteko koneiden vaihtoa ennen kuin on liian myöhäistä?

Onko teillä ohjeistusta, miten käytöstä poistuvat laitteet hävitetään?

Käytättekö virussuojausta?

Henkilöstöturvallisuus

Varmistatteko rekrytointitilanteissa, että työntekijän taidot vastaavat tehtävän vaatimaa tasoa?

Tarkastatteko työnhakijan koulutuspaperit?

Teettekö salassapitosopimukset?

Määritättekö työtehtävän mukaan käyttöoikeudet tiedostoihin?

Miten yrityksen edustajien käyttäjätilit eroavat firman sisällä työskentelevien kanssa?

Käyttöturvallisuus

Onko teillä ohjeistettu salasanoille tallennuspaikkoja? Ei ole mutta osa henkilöistä voi itse halutessaan ladata ohjelmia.

Tallennatteko salasanat selaimeen?

Onko yrityksen käyttäjätileihin määritelty salasanoille turvallisuuspolitiikkaa?

Käytättekö vahvaa tunnistautumista palveluihin?

Onko yrityksellä käytössä Admin -tili?

Kuka vastaa Admin -tilistä?

Teettekö tietojärjestelmien ja sovellusten käytöstä dokumentoituja ohjeita, jotta tilanteessa, jossa työntekijä lähtee riitaisasti yrityksestä, uusi työntekijä voi mutkattomasti jatkaa töitä?

Varaudutteko millään tavalla laitteiden rikkoutumiseen?

Tietokoneiden mennessä rikki pystyttekö palauttamaan tietokoneella olleet tiedostot?

Fyysinen turvallisuus

Onko teillä minkäänlaista kulunhallintaa toimistolla?

Onko paloturvallisuus otettu mitenkään huomioon työpaikalla?

Onko pölynaiheuttamia uhkia mietitty ollenkaan?

Onko minkäänlaista valvontaa tiloissa?