TAMPEREEN TEKNILLINEN YLIOPISTO

Tuotantotalouden osasto

ILONA ILVONEN

TIETOTURVALLISUUS PIRKANMAALAISISSA PK-YRITYKSISSÄ

Prof. Mika Hannula on hyväksytty
tarkastajaksi osastoneuvoston
kokouksessa 18.1.2006

TAMPEREEN TEKNILLINEN YLIOPISTO
Tuotantotalouden osasto, Tiedonhallinta
ILVONEN, ILONA: Tietoturvallisuus pirkanmaalaisissa pk-yrityksissä
Diplomityö: 80 sivua
Tarkastaja: professori Mika Hannula
Rahoittaja: Tiedonhallinnan laitos
Toukokuu 2006
Hakusanat: TIETOTURVALLISUUS, TIETOTURVALLISUUDEN JOHTAMINEN, TIETOTURVALLISUUSAUDITOINTI

Tietoturvallisuus on ajankohtainen teema niin kansainvälisessä kuin kotimaisessakin tutkimuksessa ja kirjallisuudessa. Tämän tutkimuksen tavoitteena on selvittää pirkanmaalaisten tietointensiivisten pk-yritysten tietoturvallisuuden yleistila sekä kehittämistarpeet. Tutkimuksessa on toiminta-analyyttisen tutkimuksen piirteitä. Tutkimusmenetelmänä on teoriaosuudessa kirjallisuusselvitys sekä empiriaosuudessa yksilö- tai ryhmähaastattelut. Empiirinen aineisto on kerätty haastattelemalla 16 yrityksen edustajia.

Tietoturvallisuus on käsitteenä hyvin monitahoinen. Tutkimuksen aluksi käsitettä lähestytään teoreettisesti niin tietoturvallisuuden osa-alueiden, ulottuvuuksien kuin tietoturvallisuuskulttuurinkin näkökulmista. Teoriakatsauksen pohjalta arvioidaan tietoturvallisuuden eri määritelmiä, sekä kuvataan tietoturvallisuus prosessina, joka suojaa organisaation tietoa. Prosessissa tietoturvallisuuden osa-alueiden avulla voidaan kuvata tiedon suojaustoimenpiteet sekä jäsentää tietoturvallisuuspolitiikkaa. Tietoturvallisuuspolitiikka ohjaa toimenpiteiden määrittelyä ja suoritusta. Tietoturvallisuuskulttuuri mahdollistaa tai estää tietoturvallisuustoimenpiteiden käytännön toteutumisen yrityksessä.

Haastattelujen perusteella tietoturvallisuus nähdään kohdeyrityksissä lähinnä teknisenä asiana. Teknisen turvallisuuden lisäksi tietojen luottamuksellisuuden säilyttäminen nähdään tietoturvallisuuden osana. Useammasta näkökulmasta huolimatta kokonaiskuvaa tietoturvallisuudesta ja sen toteuttamisesta ei ole muodostunut kaikkiin yrityksiin, vaikka tietointensiivisissä yrityksissä tiedolla on merkittävä rooli liiketoiminnan toteuttamisessa. Yrityksissä tulisi pyrkiä systemaattisempaan tietoturvallisuuden kehittämiseen dokumentoinnin ja koulutuksen avulla. Tutkimuksen päätelmissä esitetään prosessimalli, jonka avulla tietoturvallisuustyötä voitaisiin organisoida tutkimuksen yrityksissä. Nelivaiheinen prosessi on sovellettu ja kevennetty kansainvälisessä kirjallisuudessa löytyvistä tietoturvallisuuden kehittämisen malleista.

TAMPERE UNIVERSITY OF TECHNOLOGY
Industrial Engineering and Management, Business Information Management
ILVONEN, ILONA: Information security in SME's in Tampere region
Master of Science Thesis: 80 pages
Examiner: professor Mika Hannula
Funding: Institute of Business Information Management
May 2006
Keywords: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY ASSESSMENT

Information security is a current theme in research and literature. The aim of this study is to find out the overall status and main deficiencies of information security management in knowledge-intensive SME's in the Tampere region. The study is performed by a literature review and single- and group interviews. The empirical data is collected by interviewing the representatives of 16 companies over issues concerning information security management.

Information security is a complex concept. At first it is approached theoretically through different domains of information security, critical characteristics of information and information security culture. Based on the theory different definitions to information security are discussed, and information security is described as a process to secure organizational information. In the process the actions to secure information can be described through the domains on information security. Information security policy sets the guidelines to the execution of these measures, and information security culture either enables or hinders the formation of information security practises in the organization.

Based on the interviews, information security is seen mainly as a technical issue in the companies. In addition to technical issues, confidentiality of information is seen as a part of information security. Despite several views to information security were present, the overall picture of information security has yet to be developed, although in knowledge-intensive companies information has a significant role in business. The companies should aim for a more systematic process of improving information security with the help of documentation and personnel training. The study introduces a process model which could be utilized in the studied companies to better organise information security efforts. The four-phased model is applied from models found presented in the literature. It is developed especially for the needs of SME's.

ALKUSANAT

Diplomityö on alkuvaiheessaan vuoren kokoinen möykky, joka odottaa valloittajaansa. Vaikka sainkin alusta asti itse määritellä työn tavoitteita ja aikatauluja minulle annetuissa raameissa, tuntui että projekti tulee kestämään ikuisuuden, ja että valmistuminen tapahtuu sitten joskus. Kuten aina, aika on kuitenkin kulunut työn touhussa nopeasti, ja tässä se nyt on, valmis diplomityö.

Haluan lämpimästi kiittää Tiedonhallinnan laitosta työn rahoittamisesta, joka mahdollisti pysymiseni laitoksella töissä myös diplomityöprojektin ajan. Rahoituksen lisäksi olen saanut tukea työprosessin aikana kaikilta työtovereiltani, mikä on auttanut valtavasti. Erityisesti haluan kiittää työtäni ohjannutta Nina Helanderia kannustavasta ja kriittisestä ohjauksesta, joka on mahdollistanut onnistuneen lopputuloksen. Kiitokset kuuluvat myös työn tarkastaneelle Mika Hannulalle rakentavista kommenteista ja keskustelusta työn loppuvaiheessa.

Ulkopuolinenkin apu on usein tarpeen, joten haluan kiittää Tuija Kuusistoa sekä aviomiestäni Ville Ilvosta työn teoriaosuuden kommentoinnista työprosessin aikana.

Perhe on minulle tärkeä tuki, loputtomat kiitokset tuesta niin Villelle kuin pojalleni Matiakselle. Myös vanhemmiltani ja siskoiltani olen saanut kannustusta koko opiskeluajan, tuhannet kiitokset siitä!

Tampereella 23.5.2006

Ilona Ilvonen

SISÄLLYSLUETTELO

TIIVISTELMÄ
ABSTRACT
SISÄLLYSLUETTELO
1 JOHDANTO 1
1.1 Tutkimuskenttä ja tutkimuksen tausta 1
1.2 Tutkimuksen tavoitteet ja rajaukset 3
1.3 Tutkimusote ja tutkimusmenetelmät 5
1.3.1 Tieteenkäsitys ja taustafilosofia 5
1.3.2 Tutkimusote 7
1.4 Tutkimuksen toteutus 8
1.5 Tutkimuksen rakenne 8
2 TIETOTURVALLISUUS KÄSITTEENÄ 10
2.1 Tietoturvallisuuden osa-alueet 10
2.2 Tietoturvallisuuden ulottuvuudet 25
2.3 Tietoturvallisuuspolitiikka 26
2.4 Tietoturvallisuuskulttuuri 27
2.5 Yhteenveto tietoturvallisuudesta käsitteenä 30
3 TUTKIMUKSEN TOTEUTUS 32
3.1 Tietoturvallisuusauditoinnit 32
3.2 Kohdeyritykset ja haastattelujen toteutus 34
3.3 Auditoinneissa käytetyt kysymykset 35
3.4 Aineiston analyysi 41
4 AUDITOINTIEN TULOKSET 42
4.1 Tietoturvallisuuden määrittely sekä käsiteltävät tiedot 42
4.2 Hallinnollinen turvallisuus 43
4.3 Henkilöturvallisuus 45
4.4 Ohjelmisto-, laitteisto- ja tietoliikenteen turvallisuus 48
4.5 Fyysinen turvallisuus 50
4.6 Tietoaineisto- ja käyttöturvallisuus 52
4.7 Riskienhallinta ja tietoturvallisuudesta viestiminen 54
5 TUTKIMUKSEN JOHTOPÄÄTÖKSET 56
5.1 Tietoturvallisuuden tilan selvittäminen 56
5.2 Tietoturvallisuuden nykytila tutkituissa yrityksissä 57
5.2.1 Tietoturvallisuuden hallinnointi 58
5.2.2 Tekninen turvallisuus ja tietojen luokittelu 59
5.2.3 Tietoturvallisuuden ylläpitotoimet 62
5.3 Keskeisimmät puutteet tietoturvallisuuden hoidossa 63
5.4 Parannusehdotuksia tutkituille yrityksille 65
5.4.1 Vastuiden ja tavoitteiden määrittely 67
5.4.2 Tietoturvallisuuden arviointi ja riskikartoitus 67
5.4.3 Tietoturvallisuuspolitiikan määrittely 69
5.4.4 Tietoturvallisuuden ylläpito 69
6 YHTEENVETO 72
6.1 Tutkimuksen keskeiset havainnot 72
6.2 Jatkotutkimusajatuksia 73
6.3 Työn onnistumisen arviointi 74
LÄHTEET 76

1 JOHDANTO

Tieto on yritysten toiminnan perusta. Yrityksen toiminnan kannalta tärkeän tiedon suojaaminen, tietoturvallisuus, on yhä tärkeämpi osa yritysten toimintaa. Onko tietoturvallisuuden tärkeyttä kuitenkaan huomioitu tarpeeksi yritysten toiminnassa? Millä tavalla pienissä yrityksissä, joissa tieto on hyvin tärkeässä roolissa, suhtaudutaan tärkeiden tietojen suojaamiseen? Tässä diplomityössä pohditaan vastauksia näihin kysymyksiin.

1.1 Tutkimuskenttä ja tutkimuksen tausta

Tietoturvallisuuteen liittyvä kansainvälinen kirjallisuus ja tutkimus on painottunut suuriin yrityksiin. Myös kotimaisessa tutkimuksessa on kuvattu isompien yritysten tilannetta lähinnä teknisistä lähtökohdista (Helenius 2005, s.16-20). Tässä tutkimuksessa keskitytään tarkastelemaan tietoturvallisuutta pienissä ja keskisuurissa yrityksissä johtamisen näkökulmasta.

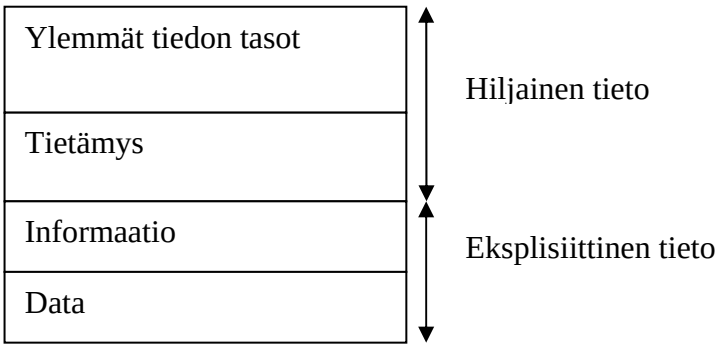
Käsite tietoturvallisuus muodostuu sanaparista ”tieto” ja ”turvallisuus”. Turvallisuus on tila, jossa kohde on turvassa eli suojattuna siihen kohdistuvilta uhkilta[1]. Tietoturvallisuuden tapauksessa kohde on tieto. Tieto puolestaan on monitahoinen käsite, jota ovat määritelleet useat kirjoittajat (e.g. Thierauf 2001, Nonaka & Takeuchi 1995, Choo 2002, Awad & Ghaziri 2003, Davenport & Prusak 1998).

Tieto voidaan määritellä esimerkiksi tasojen tai lajien avulla. Tiedon tasoja voidaan eritellä kolmesta kuuteen (e.g. Thierauf 2001, Awad & Ghaziri 2003, Davenport & Prusak 1998). Alin tiedon taso on data, joka on irrallisia tiedonmurusia, joita esimerkiksi tietokoneiden lokitietoihin kerätään isoja määriä. Kun dataa tulkitaan ja siihen liitetään merkityksiä, saadaan informaatiota. Suuri osa esimerkiksi yrityksen tietojärjestelmiin talletetusta tiedosta on informaatiota. Tietämys on pääosin ihmisiin sitoutunutta tietoa, jonka avulla dataa ja informaatiota tulkitaan. Tietämyksen olennainen tuottaja on kokemus, ja kyky soveltaa sitä uusiin ongelmiin. Tietämystä korkeampien tiedon tasojen tarkastelu ei tämän tutkimuksen puitteissa ole tarpeellista, sillä tietoturvallisuuden keinoin suojattava tieto on lähinnä dataa, informaatiota tai tietämystä.

Tietoa voidaan tarkastella myös Nonakan ja Takeuchin (1995) suuren yleisön tietoisuuteen tuomien tiedon lajien avulla. Tiedon lajit ovat hiljainen ja eksplisiittinen tieto. Hiljainen tieto on ihmisiin sitoutunutta kokemusperäistä tietoa, jonka pukeminen sanoiksi ja jakaminen muiden kanssa on vaikeaa. Eksplisiittinen tieto taas on nimensä

[1] security (Merriam-Webster Online Dictionary)

mukaisesti kirjallisessa muodossa olevaa tietoa, jonka levittäminen näin ollen on helpompaa. Tiedon lajien ja tasojen voidaan nähdä suhteutuvan toisiinsa esimerkiksi kuvan 1 mukaisesti.



Kuva 1. Tiedon tasot ja lajit

Koska tietämys on lähinnä ihmisiin sitoutunutta tietoa, voidaan katsoa, että kuvan jaottelu pätee useimmissa tapauksissa. Eksplisiittisessä muodossa olevan tiedon voidaan katsoa olevan sinänsä aina tasoltaan korkeintaan informaatiota. Jotta siitä tulisi tietämystä, tarvitaan vastaanottajan tulkinta, hiljaista tietoa, tätä informaatiota täydentämään. Tiedon tasojen ja lajien yhdistäminen voitaisiin tehdä myös toisella tavalla, eikä tässä esitetty jako ole yksikäsitteinen. Tässä tutkimuksessa keskitytään pääosin tarkastelemaan eksplisiittisen tiedon, eli datan ja informaation suojaamista. Kuitenkin myös hiljaisen tiedon suojaamista tarkastellaan.

Tutkimuksen kohteena ovat pienet ja keskisuuret yritykset. Botha ja von Solms (2004, s.330) ovat listanneet kirjallisuuskatsauksen perusteella seuraavia pk-yritysten erityispiiirteitä:

- Taloudellinen suoriutuminen. Yritykset tekevät suhteessa kokoonsa parempaa tulosta kuin isot yritykset
- Innovaatiot. Pienissä yrityksissä ympäristö on avoimempi luovuudelle ja uusille ideoille. Henkilöstön toimenkuva on myös laajempi kuin suurissa yrityksissä, mikä myös antaa tilaa innovatiivisuudelle.
- Kasvu ja työpaikkojen luominen. Pienet yritykset luovat kasvun kautta uusia työpaikkoja suhteessa enemmän kuin suuret yritykset.
- Alihankintasuhteet. Pienet yritykset ovat usein toimitussuhteessa isoihin organisaatioihin.
- Toimintaympäristö. Pienet yritykset ovat hyvin alttiita markkinoiden muutoksille, ja niiden täytyy siksi kyetä nopeisiin muutoksiin selvitäkseen. Ympäristö on siinä mielessä dynaamisempi kuin isoilla yrityksillä.
- Organisaatiorakenne. Pienen työntekijämäärän vuoksi organisaatio on matala, ja johtajat lähellä alaisiaan.

- Infrastruktuurin tarve. Pienten yritysten käytössä olevat tietojärjestelmät ovat yksinkertaisempia kuin isojen yritysten. Esimerkiksi poikkeustilanteista selviäminen voi näin olla helpompaa.
- Budjetti. Koska yritysten koko on pieni ja liikevaihtokin siksi rajallinen, muuhun kuin suoraan tuottavaan työhön budjetoitavat varat ovat rajallisia.
- Toiminnan kontrolli. Koska yrityksissä on matala organisaatio, ei päivittäisten toimintojen ohjaus ole niin hierarkkista.

Edellä listatut piirteet voivat olla tietoturvallisuuden näkökulmasta joko vahvuuksia tai heikkouksia. Haasteena on löytää tarpeeksi resursseja kehittää tietoturvallisuutta ympäristössä, joka muuttuu jatkuvasti. Erityisesti johtavassa asemassa olevien henkilöiden toimenkuvat ovat jo valmiiksi laajoja, jolloin yhden tehtävän lisääminen edelleen lisää haasteellisuutta. Toisaalta pienet yritykset joutuvat jatkuvasti sopeutumaan muutoksiin, jolloin tietoturvallisuuden kehittäminen on haaste muiden muutosten joukossa. Tämä voi olla myös etu verrattuna staattisempiin isoihin organisaatioihin. Toisaalta isoilta yrityksiltä voi alihankintasuhteiden kautta tulla vaatimuksia esimerkiksi tietoturvallisuuden tasoon liittyen, jolloin yrityksen koosta huolimatta tietoturvallisuuden tason tulisi vastata asiakasorganisaation vaatimuksia.

Tutkimus täydentää rakoa, joka on pienten yritysten tarpeiden ja tarjolla olevan kirjallisuuden välissä. Tutkimus lähtee tutkijan henkilökohtaisesta kiinnostuksesta tietoturvallisuuskäytäntöjen ja –kulttuurin muotoutumisen mekanismeja kohtaan.

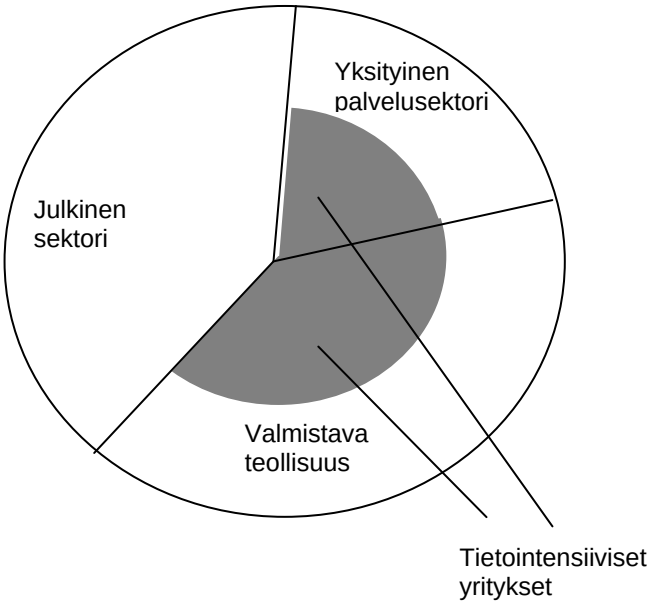
1.2 Tutkimuksen tavoitteet ja rajaukset

Tutkimuksen tavoitteena on selvittää tietoturvallisuuden tilaa pienissä tietointensiivisissä pirkanmaalaisissa yrityksissä. Alvessonin (2004, s. 21) mukaan tietointensiivisellä yrityksellä tarkoitetaan yritystä, jonka

- henkilöstö on korkeasti koulutettua ja työ vaatii tietämyksen soveltamista
- työ on hyvin itsenäistä ja organisaatiohierarkia matala
- organisaation rakenteet ovat satunnaisesti muodostuvia
- koordinointi ja ongelmanratkaisu vaatii laajaa kommunikointia työntekijöiden kesken
- asiakkaille tarjottavat palvelut ovat erityislaatuisia
- työntekijöillä on tietoa, jota asiakkailla ei ole
- työn laadun arviointi on subjektiivista.

Kaikkien edellä mainittujen kriteerien ei tarvitse täyttyä, jotta yritys voitaisiin määritellä tietointensiiviseksi, mutta usein tietointensiivisessä yrityksessä useampi piirre on läsnä (ibid.). Ei siis ole tiettyä määrää kriteereitä, joiden täyttymisen jälkeen yritystä voitaisiin yksiselitteisesti kutsua tietointensiiviseksi. Tärkeimpinä piirteinä voidaan kuitenkin pitää tietämyksen soveltamisen tärkeyttä sekä tiedon epätasapainoa, eli

tietointensiivisen työn tekijällä on usein tietoa, jota asiakkaalla ei ole. Tietointensiivisellä yrityksellä tarkoitetaan tässä yhteydessä siis yritystä, jonka keskeisenä tuotannontekijänä tai tuotteena on tieto eri muodoissaan. Kuvassa 2 on havainnollistettu tutkimuksen kohdeyritysten viitteellistä sijoittumista yrityskenttään.



Kuva 2. Kohdeyritysten sijoittuminen yrityskenttään

Tutkimuksessa ei tarkastella julkisen sektorin organisaatioita, vaan keskitytään tarkastelemaan itsenäisiä yrityksiä. Julkisen sektorin puolella valtionhallinnon ohjeistukset ja lainsäädäntö vaikuttavat voimakkaasti organisaatioiden toimintaan, jolloin itsenäisesti laadittujen ohjeiden ja yleispätevien ohjeistusten rajan erottaminen on vaikeaa. Sekä yksityisellä palvelusektorilla että valmistavan teollisuuden puolella on yrityksiä, jotka voidaan ymmärtää tietointensiivisiksi. Tietointensiivisyys myös hämärtää rajaa teollisuuden fyysisten tuotteiden ja palvelun välillä, sillä tieto voidaan monessa yhteydessä ymmärtää joko tuotteeksi tai palveluksi. Edellisten määritelmien ja rajausten perusteella tietointensiivisiksi toimialoiksi jäsentyvät esimerkiksi ohjelmistoala, korkean teknologian tutkimus ja tuotekehitys, bioala, yksityisen terveydenhuollon palvelut, konsultointipalvelut sekä muut tietointensiiviset palvelut, kuten esimerkiksi kirjanpito. Tietointensiivisyyden lisäksi tutkimuksen kohdeyritykset rajataan tutkimuksessa sijainnin ja henkilöstömäärän mukaan. Kohteena ovat pirkanmaalaiset tietointensiiviset pk-yritykset[2].

[2] Pk-yritykseksi luetaan yritys, jonka henkilöstön määrä on alle 250 henkeä **ja** vuotuinen liikevaihto on enintään 50 milj. euroa **tai** tase enintään 43 milj. euroa. Pienellä yrityksellä tarkoitetaan yritystä, jonka palveluksessa on vähemmän kuin 50 työntekijää, jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa. (Tekes 2005)

Tutkimuksen tavoite on **selvittää tietoturvallisuuden tila ja kehittämistarpeet pirkanmaalaisissa tietointensiivisissä pk-yrityksissä**. Tavoitetta lähestytään seuraavien tutkimuskysymysten avulla

1. Miten tietoturvallisuuden tilaa ko. yrityksissä voidaan selvittää?
2. Millä tavalla tietoturvallisuus on ko. yrityksissä hoidettu?
3. Minkälaisia ovat yleisimmät puutteet tietoturvallisuudessa ja mistä ne voisivat johtua?
4. Millaisia kehittämistoimenpiteitä yrityksissä tulisi tehdä puutteiden korjaamiseksi?

Ensimmäinen tutkimuskysymys on luonteeltaan teoreettinen, toinen kysymys empiirinen. Kolmas kysymys on sekä teoreettinen että empiirinen ja neljäs kysymys teoriaa empiriaan soveltava. Tutkimuskysymykset viestivät taustalla olevasta oletuksesta, jonka mukaan kohdeyritysten tietoturvallisuudessa on puutteita. Tämä oletus perustuu aiempina vuosina tehtyihin tietoturvallisuusauditointeihin ja niistä tehtyihin yhteenvetoihin (e.g. Kuusisto & Ilvonen 2003). Lisäksi taustalla on kirjallisuudessa esiintyvä tieto siitä, että tietoturvallisuuden organisointi ei aina toimi, kuten on aiottu (e.g. von Solms & von Solms 2004b).

1.3 Tutkimusote ja tutkimusmenetelmät

Tutkimusotteen ja tutkimusmenetelmän tulee perustua selkeään käsitykseen siitä, minkälaisesta tutkimuksesta on kyse ja miten se parhaiten tulisi suoritetuksi. Seuraavassa tutustutaan hieman tieteenkäsityksiin, tutkimusotteisiin ja -menetelmiin. Näiden pohjalta rajataan tämän työn taustalla oleva tutkimusote sekä menetelmät.

1.3.1 Tieteenkäsitys ja taustafilosofia

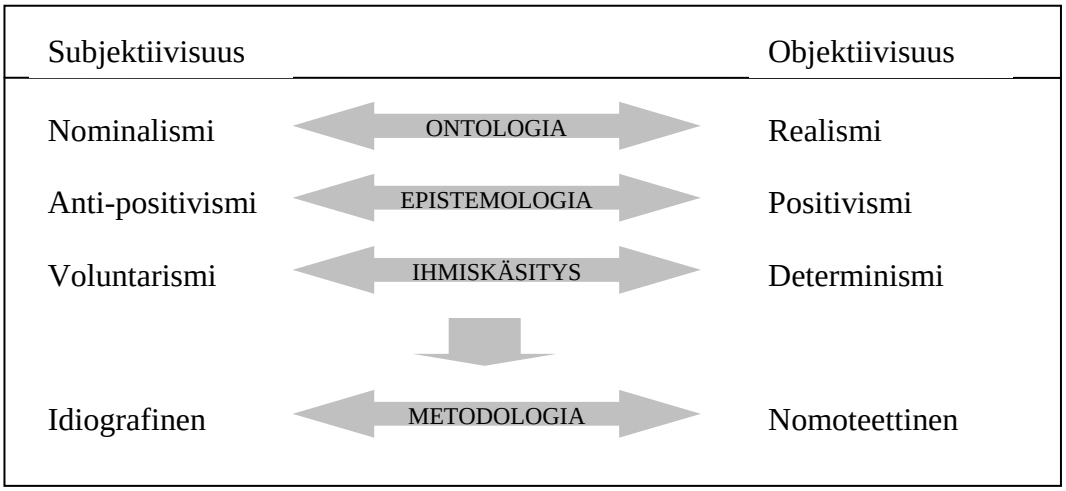
Olkkosen (1994, s. 26-30) mukaan tieteen taustalla on kaksi toisistaan eroavaa tieteenkäsitystä: positivismi ja hermeneutiikka. Positivismi painottaa kvantitatiivisuutta ja asioiden yksiselitteisyyttä: asiat joko johtuvat tai eivät johdu jostakin ilmiöstä. Positivismiin perustuvat tutkimusotteet perustuvat laajojen aineistojen keruuseen ja analysointiin tilastollisin menetelmin. Hermeneutiikka taas on ihmistieteiden lähestymistapa tieteeseen, se painottaa asioiden syvempää ymmärtämistä. Tutkimusmenetelmät ovat laadullisia ja aineistot huomattavasti suppeampia.

Guba ja Lincoln (2000, lähteessä Metsämuuronen 2005, s. 199) vertailevat neljää eri tutkimuksen tekemisen paradigmaa eli perususkomusta. Näitä ovat positivismi, postpositivismi, kriittinen teoria ja konstruktivismi. Paradigmalla on osa-alueet, joita

ovat ontologia, epistemologia ja metodologia. Ontologia tarkoittaa käsitystä siitä, mikä on todellista ja mitä näin ollen voidaan tutkia. Epistemologia on oppi siitä, minkälaista tietoa todellisuudesta on olemassa. Metodologia taas tarkoittaa sitä, kuinka voidaan saada tietoa siitä, minkä uskotaan olevan tiedettävissä. Yksittäiset tutkimusmetodit valitaan metodologian perusteella. (Guba ja Lincoln 2000, lähteessä Metsämuuronen 2005, s.199-201.) Paradigma siis vaikuttaa tiedonhankinnan taustalla ja määrittelee minkälaista tutkimusmetodologiaa ja tiedonhankinnan strategiaa tullaan käyttämään.

Positivismi on paradigmoista esitelty jo edellä. Postpositivismi on positivismin pohjalta kritiikin kautta syntynyt käsitys siitä, että aivan kaikkea tietoa ei ole konkreettisesti saatavilla. Kriittinen teoria on useiden filosofioiden pohjalta syntynyt tutkimusfilosofia, jonka mukaan tutkimus on subjektiivista, historiallista ja perustuu tutkittavan ja tutkijan dialogiin. Konstruktivismi on tieteenkäsitys, jonka perusajatus on, että todellisuus on suhteellista, kun taas muissa tieteenfilosofioissa pohjataan realismiin. Aineistoa kerätään vuorovaikutuksen avulla ja tulokset perustuvat tulkintaan. (Metsämuuronen 2005, s. 200-201.)

Tieteenfilosofiaa lähestyvät myös Burrell ja Morgan (1979, s. 3), jotka käsittelevät tieteenfilosofiaa subjektiivisen ja objektiivisen lähestymisen kautta. Tätä ajattelutapaa on havainnollistettu kuvassa 3.



Kuva 3. Tieteenkäsitys subjektiivisuuden ja objektiivisuuden näkökulmasta (Mukailtu lähteestä Burrell & Morgan 1979, s. 3)

Kuvan 2 mallissa kolme ylintä, eli ontologia, epistemologia ja käsitys ihmisluonnosta vaikuttavat suoraan siihen, minkälainen on tutkimuksessa käytettävä metodologia. Vastakkain ovat subjektiivinen näkemys, jossa todellisuus on suhteellista ja tutkimuksen tekemiseen vaikuttaa voimakkaasti tutkijan tulkinta. Toisella puolella on näkemys objektiivisuudesta, jossa totuus on olemassa ja siitä voidaan saada tietoa ulkopuolelta tarkkailemalla ja analysoimalla kvantitatiivisesti kerättyä tietoa.

Tämän tutkimuksen taustalla oleva tieteenkäsitys on lähinnä konstruktiivista teoriaa ja lähempänä subjektiivista kuin objektiivista lähestymistä kuvan 3 jaottelussa. Todellisuus tietoturvallisuuteen liittyvissä asioissa on suhteellista, sillä esimerkiksi yritysten tietoturvallisuustilanne voi näyttää hyvinkin erilaiselta riippuen siitä, ketä yrityksissä haastatellaan. Myös haastattelijan oma käsitys siitä, mitä tietoturvallisuuteen liittyvillä termeillä tarkoitetaan vaikuttaa tutkimustuloksiin eli tulkintaan siitä, mikä on tietoturvallisuuden tila kohdeyrityksissä. Tämän käsityksen pohjalta valittava tutkimusmetodologia ja sen pohjalta valittavat menetelmät keskittyvät laadullisen tiedon hankintaan, jonka pohjalta tehdään tulkintoja. Positivistiset piirteet tutkimuksessa näkyvät niin, että tutkimuksessa pyritään objektiiviseen havainnointiin.

1.3.2 Tutkimusote

Neilimo ja Näsi (lähteessä Olkkonen 1994, s. 61) kuvaavat toiminta-analyyttisen tutkimusotteen olevan kohtuullisen suppeaan empiriaan keskittyvä tutkimusote, jonka avulla pyritään ymmärtämään tutkittavaa ilmiötä tai organisaatiota. Tutkimusotteessa on piirteitä positivismista, eli ilmiöitä pyritään tarkastelemaan ulkopuolelta, mutta suppeamman empirian tarkastelu on enemmänkin laadullista, eikä tilastollista, kuten nomoteettisessa tutkimusotteessa.

Edellä käsitellyn tieteenkäsityksen pohjalta tässä tutkimuksessa tiedon keruumenetelmä on laadullinen. Aineiston pohjalta pyritään tekemään ilmiötä ymmärtäviä päätelmiä, joka on toiminta-analyyttisen tutkimuksen piirre. Tällä perusteella tutkimus perustuu lähinnä hermeneuttiseen tieteenkäsitykseen positivismin vaikuttaessa taustalla. Molempien läsnäolo sekä useiden tutkimusotteiden käyttö samassa tutkimuksessa on Olkkosen (1994, s.59) mukaan liiketaloustieteessä tyypillistä. Tässä tutkimuksessa on kuitenkin eniten toiminta-analyyttisen tutkimuksen piirteitä.

Tutkimuksen tavoitteena on nykytilan analysoinnin lisäksi pohtia syitä, jotka ovat tietoturvallisuuden nykytilan takana. Aineistoa analysoidaan muodostamalla kategorioita ja pyrkimällä saturoimaan niitä. Aineistosta pyritään löytämään selkeitä toimintatyylejä tutkituissa yrityksissä eri tietoturvallisuuden osa-alueilla, sekä esittämään parannusehdotuksia. Edellä esiteltyjen tutkimusotteiden piirteiden perusteella voidaan todeta, että tässä diplomityössä on pääosin toiminta-analyyttisen tutkimuksen piirteitä.

Tutkimusmenetelmiksi on valittu kirjallisuusselvitys ja puolistrukturoidut haastattelut. Tutkimuksen teoriapohja rakentuu kirjallisuusselvitykseen niin tietoturvallisuuden johtamisen kuin auditointien tekemisen alueelta. Tutkimusaineisto kerättiin puolistrukturoiduilla haastatteluilla. Haastattelu tutkimusmenetelmänä sekä aineiston analyysitavat on esitelty tarkemmin luvuissa 3.2 ja 3.4.

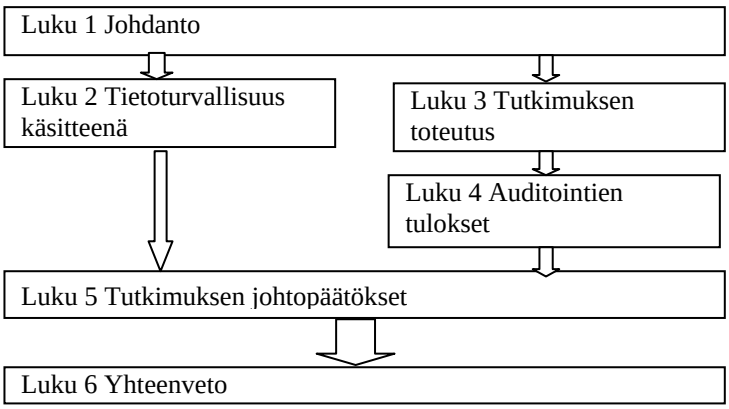
1.4 Tutkimuksen toteutus

Keväällä 2003 Tampereen teknillisen yliopiston tiedonhallinnan laitoksen tietoturvallisuuden johtaminen –kurssilla tehtiin ensimmäistä kertaa harjoitustöinä tietoturvallisuusauditointeja. Yhteensä kolmena keväänä kurssin suorittajat ovat neljän hengen ryhmätöinä tehneet tietoturvallisuusauditoinnin erilaisiin yrityksiin haastattelemalla yrityksen tietoturvallisuudesta vastaavaa henkilöä. Koska auditoituja yrityksiä ei ole valittu mukaan millään erityisellä perusteella, on yritysten kirjo ollut varsin suuri. Harjoitustöinä tehdyistä auditointiraporteista on tehty joka vuosi yhteenveto, josta yritysten edustajat ovat voineet arvioida oman yrityksensä tietoturvallisuuden tilaa verrattuna muihin.

Koska näinä kolmena vuotena yritysten kirjo on ollut laaja ja raportointi tapahtunut pelkästään opiskelijoiden toimesta ilman selkeää raportointipohjaa, ei yhteenvetojen perusteella ole voitu tehdä laajempia tieteellisiä päätelmiä. Siksi lukuvuonna 2005-2006 toteutettujen auditointien suunnittelussa panostettiin entistä paremmin niin yritysten valintaan kuin auditointien tekemisen ja raportoinnin yhdenmukaisuuteen. Tutkija valitsi auditoidut yritykset itsenäisesti. Auditoinneissa käytettävä kysymysrunko on tehty tutkimuksen tarpeita vastaavaksi. Tutkimuksen toteutus on kuvattu tarkemmin luvussa 3.

1.5 Tutkimuksen rakenne

Tutkimuksen rakenne noudattelee tavanomaisen empiirisen tutkimuksen rakennetta. Lukujen suhteet toisiinsa on kuvattu kuvassa 4.



Kuva 4. Tutkimuksen rakenne

Luvussa 2 pureudutaan käsitteen tietoturvallisuus määrittelyyn. Tietoturvallisuutta lähestytään sen osa-alueiden ja ulottuvuuksien kautta sekä johtamisen ja

organisaatiokulttuurin näkökulmista. Luku pohjustaa vastausta kaikkiin tutkimuskysymyksiin.

Luvussa 3 esitellään käytetty tutkimusmenetelmä, haastattelu, sekä tarkastellaan tietoturvallisuusauditointien tekemistä. Lisäksi esitellään haastatteluissa käytetyt kysymykset sekä tarkastellaan kerätyn aineiston analyysimenetelmiä. Luvussa esitetään näin vastaus tutkimuskysymykseen 1.

Luvussa 4 esitellään haastattelujen tulokset. Luku esittää vastauksen tutkimuskysymykseen 2.

Luvussa 5 esitetään vastaukset tutkimuskysymyksiin 3 ja 4 esittämällä analyysi aineistosta ja tekemällä parannusehdotuksia tutkituille yrityksille.

Luvussa 6 tehdään lyhyt yhteenveto tutkimuksen tuloksista, sekä esitetään jatkotutkimusehdotuksia ja arvioidaan tutkimuksen onnistumista.

2 TIETOTURVALLISUUS KÄSITTEENÄ

Tietoturvallisuus on tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä (VAHTI 1/2001, s. 7.). Tietoturvallisuuden tavoite on tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta (ibid.).

BS 7799 -standardissa tietoturvallisuus määritellään tiedon ja liiketoiminnan näkökulmasta. Tieto on suojattava kohde, jolla on tietty arvo organisaatiolle. Tietoturvallisuusjärjestelyt suojaavat tätä tietoa siihen kohdistuvilta uhkilta liiketoiminnan jatkuvuuden varmistamiseksi, liiketoiminnallisten vahinkojen minimoimiseksi ja investoinneista sekä liiketoiminnan mahdollisuuksista saadun tuoton maksimoimiseksi (BS 7799-1:fi). Whitmanin ja Mattordin (2003, s. 41) mukaan tietoturvallisuus pelkistettynä tarkoittaa organisaation kannalta neljän tärkeän toiminnon suorittamista:

- Varmistetaan organisaation toimintakyky
- Mahdollistetaan organisaation tietoteknisten sovellusten turvallinen käyttö
- Turvataan organisaation keräämä ja käyttämä tieto
- Suojellaan organisaation teknisiä resursseja

Tässä luvussa määritellään tietoturvallisuuden osa-alueet ja ulottuvuudet, sekä tarkastellaan tietoturvapolitiikkaa sekä tietoturvallisuuskulttuuria, jotka olennaisesti vaikuttavat tietoturvallisuuden toteutumiseen yrityksessä. Tietoturvallisuuden kannalta suojattavana asiana tarkastellaan joko fyysisessä muodossa olevaa tai tietojärjestelmiin talletettua tietoa. Lisäksi pohditaan henkilöihin sitoutuneen hiljaisen tiedon suojaamista.

2.1 Tietoturvallisuuden osa-alueet

Tietoturvallisuus määritellään sekä osa-alueiden että ulottuvuuksien avulla (e.g. VAHTI 1/2001, Peltier et. al. 2005). Tietoturvallisuus voidaan käsittää myös toimintana, joka tähtää tiedon suojaamiseen sen luvattomalta käytöltä tai tuhoutumiselta (Whitman & Mattord 2003, s. 9). Tämä määritelmä saa selkeyttä kun tietoa tarkastellaan eri toiminnan osissa tietoturvallisuuden osa-alueiden kautta. Valtioneuvosto jakaa tietoturvallisuuden kahdeksaan osa-alueeseen, joita ovat hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoaineistoturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja käyttöturvallisuus (VM 1998, s. 4).

Osa-aluejakoja on löydettävissä useita ja tämän alaluvun lopussa on verrattu tässä työssä käytettävää jakoa kansainvälisistä lähteistä (Tipton & Krause 2004, Whitman & Mattord 2003, BS 7799-1:fi) löytyviin jaotteluihin. Koska työ on tehty suomeksi suomalaisten yritysten toimiessa empirian lähteenä, on tarkoituksenmukaista käyttää Valtionhallinnon julkaisemaa osa-aluejakoa. Tähän jakoon tuodaan kuitenkin mukaan myös liiketoiminnan jatkuvuuden suunnittelu, sillä se nähdään tässä tutkimuksessa tasa-arvoisena tietoturvallisuuden osa-alueena muihin verrattuna. Jatkuvuussuunnittelu on tärkeää erityisesti pienissä yrityksissä, joissa yhden avainhenkilön poissaolo voi vaikuttaa olennaisesti yrityksen toimintaedellytyksiin. Kaikkia osa-alueita käsitellään lähinnä hallinnollisesta näkökulmasta työn rajauksen takia. Osa-aluejako esitellään, jotta saadaan kattava kuva tietoturvallisuuden hallinnointiin liittyvistä asioista.

Hallinnollinen tietoturvallisuus

Hallinnollinen turvallisuus on turvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostama kokonaisuus (VAHTI 1/2001, Liite 2). Osa-alue pitää siis sisällään sekä vastuiden määrittelyn, tietoturvallisuusorganisaation määrittelyn että valvonnan järjestelyt. Tietoturvallisuuspolitiikan luominen ja sen pohjalta tietoturvallisuusohjeistusten laatiminen sekä tarvittavan koulutuksen järjestäminen ovat olennainen osa hallinnollista tietoturvallisuutta.

Englanninkielisessä kirjallisuudessa suoraa vastinetta termille hallinnollinen tietoturvallisuus ei ole. Peltier et al. (2005, s.18-19) mainitsevat tietoturvallisuuspolitiikan[3] ja organisaation tietoturvallisuustoimet[4] joilla tarkoitetaan politiikan luomista ja tietoturvallisuuden vastuiden määrittelyä. He näkevät tietoturvallisuuspolitiikan tietoturvallisuuden keskipisteenä, joka hermojärjestelmän tavoin ohjaa organisaation toimintaa. Organisaation tietoturvallisuustoimilla he tarkoittavat toimia, joilla tietoturvallisuuspolitiikka viedään käytäntöön. Erityisesti he korostavat ylimmän johdon tukea tietoturvallisuuspolitiikassa kirjatuille tavoitteille. Nämä määritelmät vastaavat VAHTI-ryhmän määrittelemää hallinnollista tietoturvallisuutta.

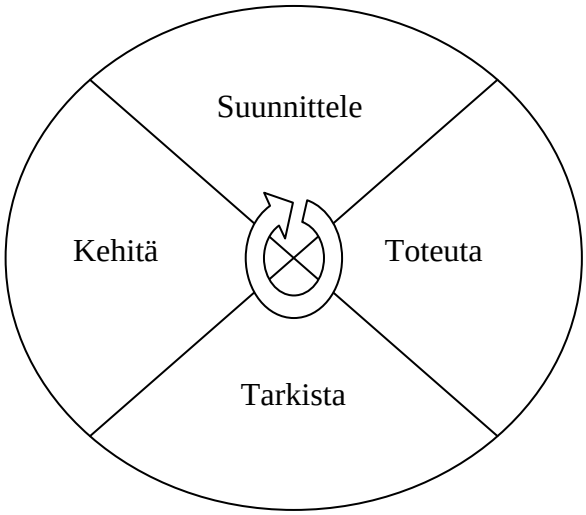
Tipton ja Krause (1999, s. 193) mainitsevat tietoturvallisuuden hallintatoimien[5] olevan tärkeitä tietoturvallisuuden kokonaisuuden kannalta. Hallintatoimiksi mainitaan esimerkiksi tietoturvallisuustietouden ohjelma[6], joka tukee tietoturvallisuuspolitiikan, organisoinnin ja ohjeistusten ylläpitoa. Kirjoittajat toteavat, että hyvin toteutettu

[3] information security policy
[4] organisational security
[5] security management practices
[6] information security awareness program

turvallisuusohjelma on edellytys sille, että teknisistä turvallisuustoimista on mitään hyötyä. Myös tämän määritelmän perusteella kuvattu osa-alue vastaa varsin tarkasti suomenkielistä termiä hallinnollinen tietoturvallisuus.

Whitman ja Mattord (2003, s.192) käsittelevät tietoturvallisuutta lähinnä prosessina, joten kaikki osa-alueet eivät heidän kuvauksessaan näy selkeinä. Hallinnollisen turvallisuuden piirteet tulevat esiin prosessin alkuvaiheessa, kun yrityksen tietoturvallisuudesta vastaavat henkilöt nimetään ja tietoturvallisuuden päälinjaukset[7] luodaan. Prosessiin kuuluvat tietoturvallisuuspolitiikan luominen, sen ylläpito ja siitä viestiminen. Kuten Tipton ja Krause (2004), myös Whitman ja Mattord (2003) käyttävät toiminnasta termiä tietoturvallisuuden hallintatoimet.

Tietoturvallisuuden hallinnoinnin voidaan nähdä noudattelevan laatuympyränä tunnettua prosessia; suunnittele, toteuta, tarkista, kehitä[8] (BS 7799-2:fi, s. 6). Ympyrämalli on kuvattu kuvassa 5.



Kuva 5. Tietoturvallisuuden hallinnoinnin ympyrämalli

Tietoturvallisuuden organisoinnin tulee lähteä hallintorakenteen suunnittelusta (BS 7799-1:fi, s.14). Kun hallintorakenne on kunnossa, tulee muokata tietoturvallisuuspolitiikat ja ohjeistukset, joiden pohjalta tietoturvallisuutta lähdetään organisaatiossa kehittämään (Posthumus & von Solms 2004, s. 644). Toteutusvaiheessa tietoturvallisuuspolitiikka pyritään viemään käytäntöön. Posthumus ja von Solms (2004, s.645) erottavat tietoturvallisuuden hallinnointiprosessissa kaksi osaa: hallinnollisen[9] ja johtamisen[10] osan. Hallinnollinen puoli huolehtii suunnittelusta, johtamisen puoli siitä miten suunnitelmat toteutetaan ja miten niitä kontrolloidaan. Tietoturvallisuuden

[7] Security Program Policy
[8] plan, do, check, act - PDCA
[9] governance
[10] management

tarkistus ja arviointi on olennainen osa tietoturvallisuuden organisointia. Arvioinnin suorittajan tulisi olla riippumaton tietoturvallisuustoimien toteuttajasta (BS 7799-1:fi, s.18). Toteutuksen ja arvioinnin palaute vaikuttaa paitsi suoraan toteutukseen, mahdollisesti myös hallinnolliseen suunnitteluun suunnitelmien kehittämisen myötä. Tietoturvallisuuden hallinnoinnin tulisi pyöriä jatkuvana prosessina ja edellä esitelty ympyrämalli on yksi vaihtoehto prosessiluonteen kuvaamiseen.

Hallinnollinen tietoturvallisuus tarkoittaa sitä, että tietoturvallisuusvastuut yrityksessä on organisoitu selkeästi. Tietoturvallisuutta hallinnoidaan tietoturvallisuuspolitiikalla ja –ohjeistuksilla. Tietoturvallisuuden tilaa seurataan ja seurannan pohjalta suunnitelmiin ja toteutukseen tehdään tarvittaessa muutoksia. Tietoturvallisuuspolitiikkaa tarkastellaan tarkemmin luvussa 2.3.

Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisuusjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen järjestelyihin liittyvien turvallisuustekijöiden hoitamista (VAHTI 1/2001, Liite 2). Osa-alue pitää sisällään henkilöstön luotettavuudesta ja käyttöoikeuksista huolehtimisen niin, että henkilön oikeudet eri tietoihin ovat tiedossa ja hän on tietoinen oikeuksistaan ja velvollisuuksistaan. Myös henkilöstöä koskevat tiedot tulee säilyttää asianmukaisesti. Sijaisuusjärjestelyt viittaavat varahenkilöjärjestelyjen suunnitteluun ennalta niin, että poissaolot eivät vaaranna yrityksen kannalta tärkeiden tietojen viiveetöntä saatavuutta.

Tipton ja Krause (2004) mainitsevat tietoturvallisuuden hallintatoimet, johon viitattiin hallinnollisen turvallisuuden yhteydessä. Tämän alueen alla on mainittu työsuhteeseen liittyvät tietoturvallisuustoimet[11] sekä tietoturvallisuuskoulutus[12], jotka voidaan nähdä henkilöturvallisuutta vastaavana. Fenton ja Wolfe (2004, s. 887-896) nostavat henkilöstöön ja tietoturvallisuuteen liittyen esiin tehtävänkuvaukset ja tietoturvallisuusroolit sekä riittävän koulutuksen. Heidän mukaansa tehtävänkuvausten tarkka laatiminen helpottaa sen miettimisessä, minkälaisia työntekijöitä tarvitaan, sekä minkälaisia tietoja henkilöt työssään tarvitsevat. Kun tehtävänkuva on määritelty, on rekrytointiprosessi askelta helpompi suorittaa. Yritysten täytyy heidän mukaansa tässäkin asiassa muistaa, että tehdyt kuvaukset ovat dynaamisia ja parhaillaan töissä olevan työntekijän tehtävät todennäköisesti eivät vastaa sitä työnkuvaa, joka hänelle on rekrytointivaiheessa määritelty. Henkilöstön rooli tietoturvallisuuden toteuttajana on tärkeä ja kirjoittajat korostavat turvallisten toimintatapojen viemistä rutiinitoiminnaksi, jolloin mahdolliset tietoturvallisuuspuutteetkin huomataan helpommin.

[11] Employment policies and practices
[12] Security awareness training

Hansche (2004, s. 999) toteaa suuren osan tietoturvallisuusuhkista aiheutuvan henkilöstön tietämättömyydestä. Riittävä koulutus ja tietoisuuden lisääminen luovat yritykseen tietoturvallisuudelle otollisempaa ympäristöä, jossa henkilöstö tietää mitä tehdä tai ei tehdä. Tietoturvalliset toimintatavat muodostuvat rutiiniksi. Henkilöturvallisuuden voisikin jakaa kahteen alueeseen, joista toisessa keskitytään henkilön ja häntä koskevien tietojen suojaamiseen ja toisessa yrityksen tärkeiden tietojen suojaamiseen henkilöltä. von Solms ja von Solms (2004b, s.375) mainitsevat yleiseksi johdon virheeksi henkilöstön koulutuksen ja tietoturvallisuudesta viestimisen laiminlyönnin. He toteavat, että henkilöstön koulutukseen tehty investointi on monessa tilanteessa osoittautunut erittäin kannattavaksi. Koulutuksen avulla vältetään tietämättömyydestä johtuvia virheitä sekä vahvistetaan henkilöstön tietoisuutta vastuistaan, eli suojellaan yritystä henkilöistä aiheutuvilta uhkilta. Jos toimintatavoista ja vastuista ei olla tietoisia, ei henkilöstöä voida myöskään vaatia vastuuseen teoistaan.

Whitman ja Mattord (2003, s. 435-440) mainitsevat myös työsuhteeseen liittyvät asiat[13] tietoturvallisuuden kannalta. Heidän mukaansa tietoturvallisuuden kannalta tärkeitä asioita liittyy työsuhteen kaikkiin vaiheisiin työnkuvauksen laatimisesta sopivan henkilön palkkaamiseen, sopimuspykäliin ja koulutukseen sekä työsuhteen päättämiseen saakka. Henkilöturvallisuus ei ole erillinen asia, vaan tietoturvallisuus tulisi viedä kiinteäksi osaksi henkilöstöhallintoa. Tällöin tietoturvallisuuteen liittyvät sopimukset ja perehdytys ovat normaali käytäntö ja saavat riittävästi huomiota ja arvostusta henkilöstöltä.

Kun henkilö aloittaa työt organisaatiossa, tulee huolehtia siitä että hän on tietoinen käsittelemiensä tietojen luottamuksellisuudesta esimerkiksi salassapitosopimuksen avulla (BS 7799-1:fi, s. 26). Kun työnkuvassa tapahtuu olennainen muutos, tai henkilö lähtee pois organisaatiosta, tulee tämän sopimuksen sisältö tarkistaa, että se vastaa vallitsevaa tilannetta. Myös työsopimuksesta tulee käydä ilmi henkilön velvollisuudet tietoturvallisuuden suhteen (ibid.). Salassapitosopimuksilla ja tietoturvallisuusvelvollisuuksien kirjaamisella pyritään suojelemaan yritystä henkilön tahallisia tai tahattomia toimia vastaan. Sopimusrikkomuksesta seuraavat sanktiot osaltaan motivoivat tietoturvalliseen toimintaan. Sopimusten lisäksi tietoturvallisuussäännösten noudattamista tulisi myös valvoa erilaisin kontrollikeinoin. Suurin osa kontrollikeinoista on tehty, jotta rehelliset ihmiset pysyisivät rehellisinä (Haugen & Selin 1999, s. 341). Kontrollikeinoilla ja turvallisuuden arvioinneilla voidaan toki tunnistaa jo tapahtuneita rikkomuksia, jolloin sopimusten sanktiot astuvat voimaan, mutta tärkeintä on sopimusten ja velvoitteiden ennaltaehkäisevä teho (BS 7799-1:fi, s.28). Velvollisuuksista ja sopimuksista tulee muistuttaa myös työsuhteen päättyessä.

[13] Employment policies and practices

Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa yrityksen toimitilojen turvaamista. Tavoitteena on luoda ja ylläpitää turvalliset toimintaolosuhteet yrityksen tietotekniselle käyttöympäristölle sekä suojata kiinteistö ja sen erikoistilat luvattomia tai rikollisia toimia vastaan, onnettomuuksilta ja luonnontuhoilta. Fyysiseen turvallisuuteen kuuluu myös teknisten järjestelmien toiminnan varmistaminen. Tämä osa-alue käsittää kiinteistön rakenteellisen turvallisuuden, valvontatekniikan, valvonnan ja vartioinnin. (VAHTI 1/2001, Liite 2.) Fyysinen turvallisuus on siis tietoturvallisuuden näkökulmasta sekä tietoteknisten laitteiden toiminnan takaamista, että fyysisessä muodossa olevan tiedon turvallisuuden takaamista.

Tipton ja Krause (2004, s.1922) toteavat fyysisen turvallisuuden[14] olevan osin perinteistä toimitilojen turvallisuuden varmistamista kulunvalvonnan ja pääsyrajoitusten avulla. Nykyään kuitenkin yritykselle tärkeää tietoa on fyysisesti paljon hajallaan tiloissa ja sen turvaamiseen pelkät perinteisen valvonnan keinot eivät riitä. Tietoturvallisuudesta vastaavien sekä perinteistä vartiointia hoitavien tulisi tehdä yhteistyötä, jotta yrityksen tietoa suojellaan parhaiten sopivilla toimilla (ibid.). Yrityksen avaintoiminnot tulee sijoittaa niin, että ulkopuolisten pääsy niihin voidaan estää (BS 7799-1:fi, s.30). Esimerkiksi yrityksen toiminnan kannalta välttämätön palvelin tulee sijoittaa niin, etteivät asiattomat pääse siihen käsiksi.

Whitman ja Mattord (2003, s. 357) määrittelevät fyysisen turvallisuuden toimiksi, joilla suunnitellaan, toteutetaan ja ylläpidetään yrityksen fyysisten resurssien turvaamista. Määrittely on hyvin pitkälle sama edellä esitetyn VAHTI-ohjeiden määrittelyn kanssa, sillä fyysisiä resursseja ovat niin fyysiset tilat kuin fyysisessä muodossa oleva tieto ja laitteet, joilla tietoa käsitellään. VAHTI-ohjeissa on kuitenkin erilliset osa-alueet laitteistoturvallisuudelle ja tietoaineistoturvallisuudelle, jotka taas Whitmanin ja Mattordin (2003) määrittelyssä ovat tulkittavissa osaksi fyysistä turvallisuutta.

Fyysisen turvallisuuden takaamiseksi yrityksen ovet ja ikkunat tulee olla asianmukaisesti lukittuina, kulunvalvonnan tulee olla toiminnassa aina ja hälytysjärjestelmien aina kun kyseisellä turva-alueella ei työskennellä (Miettinen 1999, s. 177-183). Laitteistot tulee sijoittaa siten, että fyysisistä uhkista, esimerkiksi lattialle vuotavasta vedestä olisi mahdollisimman vähän haittaa (ibid.). Yrityksessä tulee olla käsillä alkusammutusvälineet ja henkilökunnan tulee osata käyttää niitä. Fyysinen turvallisuus on siis tiedon suojaamista sen fyysisessä olinpaikassa niin luvatonta pääsyä kuin vahingoista tai onnettomuuksista johtuvia uhkia vastaan. Myös fyysisten toimintaedellytyksen, kuten esimerkiksi sähkön saannin, varmistaminen kuuluu fyysisen turvallisuuden piiriin (Miettinen 1999, s. 184). Sähkön saanti on tärkeää tietokonelaitteiden toiminnan kannalta ja se voidaan joko varmistaa UPS-laittein

[14] Physical security

hallittua laitteiston alasajoa varten, tai hankkia varavirtageneraattori, joka varmistaa sähkön saannin pitemmäksikin aikaa, mikäli se on tarpeellista.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tiedon ja tietoaineiston saatavuutta, oikeellisuutta, salassa pitämistä, turvallista käsittelyä ja säilyttämistä sekä tietojätteen hävittämistä (VAHTI 1/2001, Liite 2). Toimenpiteet kohdistuvat niin digitaalisessa kuin fyysisessäkin muodossa oleviin tietoaineistoihin niiden koko elinkaaren ajan, eli tietoaineistoturvallisuuden suojauksen kohteena ovat pääasiassa data ja informaatio. Esimerkiksi tietojen luokittelu säilytyssääntöjen luomiseksi on olennainen osa tietoaineistoturvallisuutta. Tietojen luokittelulla tarkoitetaan tiedon turvallisuustarpeen arvioimista ja sen mukaisten suojauskeinojen valitsemista (BS 7799-1:fi, s.22). Mitä tärkeämpi tieto, sitä isompi on sen paljastumisen aiheuttama uhka ja sitä paremman tarvitsee olla suojaustaso. Yksinkertaisimmillaan luokittelu voidaan tehdä julkisiin ja salaisiin tietoihin, jolloin salaiselle tiedolle on määritelty tietyt säännöt joiden mukaan sitä käsitellään. Monimutkaisempiakin luokituksia voidaan tarvita, mutta eri turvallisuusluokkien ja suojausohjeiden määrä pitäisi selkeyden vuoksi pyrkiä pitämään pienenä (BS 7799-1:fi, s.24).

Tipton ja Krause (2004) eivät mainitse tietoaineistoturvallisuutta omana osa-alueenaan. Appleyard (2004, s.715-720) käsittelee tietojen luokittelua tietoturvallisuuden prosessin yhtenä osana. Lähteessä tarkastellaan asiaa hallinnollisesta näkökulmasta ja sen mukaan luokittelun tulee perustua tietoturvallisuuspolitiikkaan ja edetä prosessina muun tietoturvallisuustyön ohella. Kirjoittaja mukaan tärkeää prosessissa on, että tietojen oikeat omistajat määrittelevät kuka tietoja saa käyttää ja minkälaiseen salaisuusluokkaan ne kuuluvat. Kuitenkin näitä päätöksiä tekevät usein tietohallinnon ihmiset, joiden tulisi toimia ainoastaan oikeuksien ylläpitäjinä, ei sen määrittelijöinä kuka tietoa tarvitsee. Myös Peltier et al. (2005, s.114) korostavat tiedon omistajan tarpeellisuutta. Tiedon omistaja voi olla esimerkiksi yrityksen yksikkö, jossa tietoa tuotetaan ja käytetään, jolloin varsinainen omistaja, tai tiedosta vastuullinen henkilö on tämän yksikön johtaja. Tiedon omistajan vastuulla on huolehtia, että tiedon luokittelu on ajan tasalla, että tiedon suojaustoimenpiteet ovat riittävät ja että tietoon on pääsy vain niillä henkilöillä, jotka tietoa tarvitsevat (ibid.).

Whitman ja Mattord (2003, s. 206) mainitsevat tietoturvallisuuspolitiikan yhteydessä tietojen luokittelun. Heidän mukaansa luokittelusääntöjen tulee kuvata miten yrityksen sisäiseen käyttöön tarkoitettua materiaalia säilytetään ja käsitellään, jotta se ei pääse paljastumaan ulkopuolisille. Esimerkiksi puhtaan pöydän politiikka, eli käytäntö että mitään papereita ei jätetä pöydille lojumaan, on yksi tapa suojata fyysisiä tietoaineistoja asiattomien silmiltä.

Tietoaineistoturvallisuus määrittelee miten eri tietoja käsitellään, millä tavalla niitä suojataan ja kenellä niihin on oikeus. Oikeushallinnan kautta osa-alue on tiiviissä yhteydessä toisaalta henkilöturvallisuuteen (luku 2.1.2), toisaalta käyttöturvallisuuteen (luku 2.1.8). Tiedon säilytyksen osalta tietoaineistoturvallisuudella on voimakas kytkös fyysiseen turvallisuuteen (luku 2.1.3). Käsittelysäännöt tulee määritellä tietojen koko elinkaarta varten, eli myös tietoja hävitettäessä on huolehdittava luottamuksellisuuden säilymisestä mikäli se on tarpeen.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien saatavuuteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen sekä verkon varmistamiseen liittyvät turvallisuustoimenpiteet (VAHTI 1/2001, Liite 2). Tämän osa-alueen alle kuuluvat etäyhteyksien ja yrityksen sisäisen sekä yrityksen ulkopuolelle suuntautuvan tietoliikenteen turvallinen hoito.

Tietoliikenneturvallisuus on osa-alueista selkeimmin löydettävissä myös kansainvälisistä lähteistä. Esimerkiksi Tipton ja Krause (2004, s. 198) nostavat tietoliikenneturvallisuuden[15] yhdeksi osa-alueeksi. Tietoliikenteen turvallisuus on se alue tietoturvallisuudesta, joka yleisesti mielletään tietoturvallisuudeksi. Näissä tapauksissa tietoturvalla tarkoitetaan virustorjuntaa ja palomuuria. Tietoliikenneturvallisuus tarkoittaakin Tiptonin ja Krausen (ibid.) mukaan yrityksessä sisällä kulkevan sekä ulospäin lähtevän ja ulkoa tulevan tiedon turvaamista niin, että sen eheys, saatavuus ja luottamuksellisuus säilyvät. Apuna tässä käytetään mm. palomuureja, suojattuja yhteyksiä ja virustorjuntaohjelmistoja.

GAISP-standardissa (GAISP 3.0, s.18-19) määritellään tietoliikenteen turvallista organisointia teknisistä lähtökohdista. Kun tietoliikennettä lähdetään suojaamaan, tulee ottaa huomioon sekä verkosta tuleva uhka yrityksen järjestelmään, että järjestelmän itsensä aiheuttama uhka verkon muille toimijoille. Esimerkiksi etätyöskentelyä hoidettaessa tulee huolehtia yhteyden oikeellisuudesta, tiedon riittävästä salauksesta sen liikkuessa julkisessa verkossa sekä käyttäjän tunnistuksesta. Etäyhteyttä otettaessa on siis varmistettava että etälaitetta käyttää oikea henkilö. Tähän on keinoina esimerkiksi käyttäjätunnus ja salasana sekä tarvittaessa toimikortti. Yhteyden tulee olla salattu niin, että käsiteltävä luottamuksellinen tieto ei liiku verkossa selväkielisenä. Tämä voidaan toteuttaa useilla eri salaustekniikoilla, esimerkkinä VPN-tekniikat[16]. Lisäksi voidaan varmistaa, että etäyhteys otetaan juuri siihen koneeseen, johon yhteys halutaan

[15] Telecommunications, network and internet security
[16] VPN = Virtual Private Network. Erilaisin salausmenetelmin toteutettu suojattu yhteys fyysisesti eri verkkoihin kuuluvien tietokoneiden välillä

muodostaa, jolloin vältetään yhteyden ohjaaminen kolmannen osapuolen kautta, eli ns. välimieshyökkäys.

Tietoliikenteen turvallisuuteen kuuluu, paitsi verkkoliikenne yleensä, olennaisesti sähköpostin turvallisuus. Sähköpostia käytetään suuressa osassa yrityksiä jokapäiväisenä viestintäkanavana, jonka välityksellä lähetetään suuria määriä työhön liittyvää tietoa ja materiaalia. Sähköposti ei sinällään kuitenkaan ole yhtä luotettava viestintämuoto kuin esimerkiksi puhelin tai perinteinen kirje. Organisaation tuleekin pohtia minkälaista tietoa sähköpostilla voidaan käsitellä, miten liitetiedostoihin suhtaudutaan ja minkälaisia salaustekniikoita mahdollisesti käytetään sähköpostiviestinnän turvaamiseksi (BS 7799-1:fi, s.52).

Tietoliikenteen turvallisuuteen liittyy myös haittaohjelmien torjunta. Haittaohjelmia ovat ohjelmat, joiden on tarkoitus aiheuttaa haittaa verkossa toimiville tietokoneille (Viestintävirasto 2001). Haittaohjelmilta voidaan suojautua palomuurien ja virustorjuntaohjelmistojen avulla. Palomuurit suojaavat itsenäisesti toimivia haittaohjelmia vastaan valvomalla verkkoliikennettä. Virustorjuntaohjelmistot taas havaitsevat ja tuhoavat haitallisesti toimivia ohjelmia, viruksia, jotka liikkuvat esimerkiksi sähköpostien liitetiedostoina (ibid.).

Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteiston saatavuuteen, toimintaan, ylläpitoon sekä laitteiden ja tarvikkeiden saatavuuteen liittyviä toimenpiteitä (VAHTI 1/2001, Liite 2). Osa-alue on lähellä fyysistä turvallisuutta, mutta keskittyy enemmän itse laitteisiin eikä niiden fyysiseen ympäristöön. Tiedonkäsittelyn ollessa nykyään digitaalista miltei kaikkialla, laitteistojen saatavuus ja toimintavarmuus on yritysten toiminnan kannalta erittäin tärkeää. Laitteistoturvallisuus tietoturvallisuuden kannalta keskittyy tiedon tuottamiseen, käsittelyyn ja säilyttämiseen käytettävien laitteistojen turvaamiseen. Tietokoneet ja kommunikaattorit esimerkiksi ovat itsestään selviä laitteistoturvallisuuden piiriin kuuluvia laitteita, mutta esimerkiksi tutkimustoiminnassa käytettäviä mittalaitteita käytetään tiedon tuottamiseen, jolloin niiden säilyminen ehjinä ja toimintakykyisinä on niitä käyttävän organisaation kannalta myös erittäin tärkeää.

Tipton ja Krause (2004) eivät mainitse laitteistoturvallisuutta omana osa-alueenaan, eikä laitteistoturvallisuutta käsitellä missään kirjan artikkeleista ainakaan otsikkotasolla. Voidaan olettaa, että kirjoittajat ymmärtävät laitteistoturvallisuuden osaksi fyysistä turvallisuutta, eikä siihen tarvitse erikseen kiinnittää huomiota. Nykyisin kuitenkin laitteistoja käytetään muuallakin kuin yrityksen liiketiloissa, jolloin laitteistojen saatavuudelle ja turvaamiselle syntyy aikaisempaa isompia vaatimuksia. Whitman ja Mattord (2003, s. 381) käsittelevät laitteistoturvallisuutta fyysiseen turvallisuuteen

kuuluvana. Heidän mukaansa esimerkiksi kannettavan tietokoneen käsittelystä ja säilyttämisestä tulisi ohjeistaa huolellisesti, sillä kannettavat ovat alttiina varkaudelle sekä laitteen itsensä että sen sisältämän tiedon takia.

BS 7799 –standardi (BS 7799-1:fi, s.32) määrittelee laitteistoturvallisuuden osaksi fyysistä turvallisuutta ja esimerkiksi laitteistojen turvallisen sijoittelun osalta näin onkin. Standardin mukaan laitteistoturvallisuuden tavoite on estää omaisuuden häviäminen, vahingoittuminen tai vaarantuminen ja sitä kautta liiketoiminnan jatkuvuuden vaarantuminen. Laitteistojen fyysisen toimintaympäristön turvaaminen on kuvattu luvussa 2.1.3. Laitteistot voidaan välillä kuitenkin viedä pois fyysisen suojauksen piiristä, esimerkiksi kantamalla kannettavaa tietokonetta mukana. Tällöin laitteen turvallisesta säilytyksestä huolehtii työntekijä, jota on ohjeistettava perusteellisesti (BS 7799-1:fi, s.34). Suojaustoimenpiteet on sovitettava laitteiston sisältämän tiedon arkaluonteisuuden mukaan. Mukana kuljetettavia laitteita ovat myös mm. erilaiset muistivälineet kuten USB-muistitikut. Myös näiden huolellisesta säilytyksestä ja suojaamisesta tulee ohjeistaa.

Ohjelmistoturvallisuus

Ohjelmistoturvallisuus tarkoittaa käyttöjärjestelmien ja muiden ohjelmien suojausominaisuuksien hallintaa, ohjelmien lokitiedostojen keräämistä ja käytön valvontaa sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä (VAHTI 1/2001, Liite 2). Tipton ja Krause (2004, s. 1074) tuovat edellä mainittuun määrittelyyn lisäksi ohjelmistojen kehityksen näkökulman, eli jo ohjelmistojen kehitysvaiheessa tulee huomioida kehitettävän ohjelmiston turvallisuus sekä kehitysympäristön turvallisuus. Ohjelmistoturvallisuus[17] on tässä muodossaan nostettu yhdeksi tietoturvallisuuden osa-alueeksi.

Ohjelmistoturvallisuus tarkoittaa siis niin käytettävien ohjelmistojen turvallisuuden takaamista päivittämällä ja keräämällä ohjelmien toiminnasta lokitietoja kuin ohjelmien turvallista kehittämistä. Turvallinen kehittäminen tarkoittaa sitä ettei ohjelmaan jää tai jätetä vahingonteon mahdollistavia turva-aukkoja. Jos ja kun näitä aukkoja kuitenkin syntyy, tulee niiden tukkimisesta huolehtia päivittämällä esimerkiksi käyttöjärjestelmä aina, kun uusi päivitys on saatavilla (BS 7799-1:fi, s.44).

Ohjelmistoturvallisuus on läheisesti kytköksissä laitteistoturvallisuuteen (2.1.6) sekä tietoliikenteen turvallisuuteen (2.1.5). Näiden osa-alueiden rajat ovat hyvin häilyvät. Osittain ohjelmistoturvallisuuteen kuuluvia asioita on käsitelty jo edellä mainittujen osa-alueiden yhteydessä. Lisäksi ohjelmistojen ylläpitoon ja käyttöoikeuksiin otetaan kantaa käyttöturvallisuuden (2.1.8) yhteydessä.

[17] Applications and systems development security

Käyttöturvallisuus

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteitä, varmuus- ja suojakopioinnista sekä häiriöraportoinnista (VAHTI 1/2001, Liite 2). Ohjelmistojen ja laitteistojen toimivuuden hallintaa on käsitelty jo ohjelmistoturvallisuuden (luku 2.1.7) ja laitteistoturvallisuuden (luku 2.1.6) yhteydessä.

Henry (2004a, s. 1559) määrittelee käyttöturvallisuuden[18] koostuvan käyttöympäristön valvonnasta ja tuesta sekä liiketoimintaedellytysten suojaamisesta varmuuskopioiden, ylläpidon ja tilanteisiin reagoinnin avulla. Käyttöturvallisuudesta vastaavat henkilöt huolehtivat yritykselle tärkeän tiedon säilyttämisestä ja varmuuskopioinnista, sekä teknisen tietojenkäsittely-ympäristön ylläpidosta (ibid.). Monesti tekninen ylläpito ei välttämättä ole tietoinen roolistaan yrityksen liiketoimintaedellytysten ylläpitäjänä. Tämä voi luoda hankalia tilanteita yrityksessä, vaikka tietoturvallisuusasiat muilta osin olisivatkin kunnossa. Siksi tietoturvallisuustietoisuuden kohentaminen ja varmistaminen erityisesti käyttöympäristöstä vastaavien keskuudessa on erittäin tärkeää.

BS 7799 standardin yhtenä lukuna on pääsyoikeuksien valvonta. Pääsynvalvonnan tavoitteena on valvoa pääsyä tietoon ja liiketoimintaprosesseihin turvallisuusohjeistusten määritelmien mukaisesti (BS 7799-1:fi s. 54). Kontrolli toteutetaan yleisimmin henkilökohtaisten käyttäjätunnusten ja salasanojen avulla. Käyttäjille voidaan eri toimenpitein määritellä oikeudet juuri niihin tietoihin joihin heillä on tarve. Tietojen luokittelu (luku 2.1.4) liittyy läheisesti käyttöoikeuksien määrittelyyn, sillä yhtenä perusteena käyttöoikeuksien määrittelylle voivat olla eri tietoluokat.

Käyttöturvallisuuden tavoitteena on myös turvata tietojen eheys ja saatavuus kaikissa tilanteissa (BS 7799-1:fi, s. 44). Tähän tavoitteeseen pyritään esimerkiksi huolehtimalla tietojen varmuuskopioinnista. Varmuuskopioita tulisi säilyttää fyysisesti erillään alkuperäisestä laitteistosta, jotta tietojen saatavuus voitaisiin varmistaa myös esimerkiksi tulipalon sattuessa. Varmuuskopioita tulee myös testata, jotta voidaan varmistaa, että ne toimivat silloin kun niitä tarvitaan (ibid.).

[18] Operations security

Liiketoiminnan jatkuvuus

Liiketoiminnan jatkuvuuden suunnittelu voidaan nähdä osana edellä esiteltyjä tietoturvallisuuden osa-alueita. Se tuodaan tässä kuitenkin esiin omana osa-alueenaan, sillä yrityksen tiedon tarkasteleminen erityisesti liiketoiminnallisesta näkökulmasta saattaa unohtua tietoturvallisuudesta vastaavilta henkilöiltä (Peltier et al. 2005, s.209). Liiketoiminnan jatkuvuuden suunnittelu[19] on yrityksen toiminnan kannalta tärkeän tiedon ja tietojärjestelmien saatavuuden varmistamista poikkeustilanteissa, joissa normaalit toiminnot eivät ole käytettävissä (Botha & von Solms 2004, s.328). Vaikka valtionhallinnon tietoturvallisuusohjeistukset koskevat yhteiskunnan tärkeitä toimintoja ylläpitäviä organisaatiota, ei niissä ole nostettu toiminnan jatkuvuuden suunnittelua omaksi teemakseen, mikä on yllättävää. Osaltaan tämä on puute VAHTI-ohjeistuksissa.

Whitman ja Mattord (2003, s. 260) määrittelevät liiketoiminnan jatkuvuuden suunnittelun tarkoittavan suunnitelmia sen varalle, että toiminta yrityksen ensisijaisissa toimitiloissa estyy. Tämä estyminen saattaa johtua esimerkiksi tulipalosta tai luonnonkatastrofista. Jatkuvuussuunnitelman tavoite on kartoittaa mitä toimintoja voidaan siirtää muualle, kuinka nopeasti tämä tulee tehdä ja mihin ne siirretään. Liiketoiminnan jatkuvuussuunnittelun lisäksi Whitman ja Mattord (2003, s. 160) mainitsevat myös poikkeustilannesuunnitelmat[20] ja toipumissuunnitelmat[21] pienemmistä poikkeustilanteista ja katastrofeista, kuten luvattomasta tietojen kopioinnista tai palvelinhuoneen vesivahingosta, selviämiseen. Pienemmätkin suunnitelmat tähtäävät liiketoiminnan mahdollisimman häiriöttömään jatkumiseen ja voidaan näin ymmärtää osaksi liiketoiminnan jatkuvuuden suunnittelua.

Tipton ja Krause (2004, s.1642) nostavat liiketoiminnan jatkuvuuden yhdeksi osaotsikoksi ja näkevät sen näin erittäin tärkeänä osana tietoturvallisuutta ja liiketoimintaa yleensä. Liiketoiminnan jatkuvuuden suunnittelulla he tarkoittavat varautumista siihen, että normaali liiketoiminta häiriintyy joko luonnon tai ihmisen aiheuttaman tapahtuman johdosta. Jatkuvuussuunnittelu on tärkeää, mutta myös haastavaa, sillä vaikka yritys omistaisi tietoresursseja, niitä saattaa hallinnoida joku aivan muu taho kuin yritys itse esimerkiksi laitteistojen ylläpidon ulkoistamisen takia. Jatkuvuussuunnittelun ytimenä on riskien tunnistaminen ja niiden toteutumiseen varautuminen. Jotkin riskit voidaan eliminoida esimerkiksi toimintatapoja muuttamalla, mutta suurten riskien varalle on tehtävä suunnitelmia, vaikka riskin toteutumisen todennäköisyys olisikin pieni. Tässä määrittelyssä liiketoiminnan jatkuvuuden suunnittelu nähdään laajaksi asiaksi ja se selkeästi sisältää Whitmanin ja Mattordin (2003, s.160) erittelemän poikkeustilanne- ja toipumissuunnittelun.

[19] Business Continuity Planning
[20] Incident Response Plan
[21] Disaster Recovery Plan

Liiketoiminnan jatkuvuuden suunnittelu, kuten tietoturvallisuuden hallinnointi ylipäätäänkin, on jatkuva prosessi. Syklisen prosessiluonteen mainitsevat useat kirjoittajat (e.g. Karakasidis 1997, Heng 1996, Jackson 2004). Yksi lähestymistapa vaiheittaiseen liiketoiminnan jatkuvuuden suunnitteluun on Bothan ja von Solmsin (2004, s. 331-332) spiraalimalli. Siinä perinteinen jatkuvuussuunnitteluprosessi käydään läpi systemaattisesti useita kertoja, jolloin jokainen kierros rakentaa jo aiemmin tehtyjen suunnitelmien pohjalle ja parantaa turvallisuutta ennestään. Yksittäisen kierroksen vaiheita ovat projektisuunnittelu, liiketoiminnan vaikutusten analysointi, jatkuvuusstrategioiden suunnittelu ja toteutus, jatkuvuuskoulutus ja -testaus sekä ylläpito. Tärkeää jatkuvuussuunnittelussa on saada prosessille ylimmän johdon tuki, jotta suunnitelmat voidaan tehdä huolellisesti ja esimerkiksi liiketoiminnan vaikutusten analyysissa esille tuleviin riskeihin voidaan aidosti vastata. Jatkuvuussuunnitteluprosessi voi toimia myös yrityksen sisäisenä tietoturvallisuusarviointina, sillä siinä käydään läpi liiketoimintaa uhkaavia riskejä sekä pyritään poistamaan riskejä ja varautumaan niiden toteutumiseen. Aiemmin kuvatut tietoturvallisuuden osa-alueet ovat kaikki jollakin tasolla mukana jatkuvuussuunnittelussa.

Yhteenveto tietoturvallisuuden osa-alueista

Edellä on määritelty sekä kotimaisten että ulkomaisten lähteiden avulla tietoturvallisuuden osa-alueet. Taulukossa 1 esitetään yhteenveto osa-aluejaosta ja osa-alueiden nimityksistä tietoturvallisuuden johtamisen keskeisessä kirjallisuudessa.

Taulukko 1. Yhteenveto tietoturvallisuuden osa-alueista kirjallisuudessa

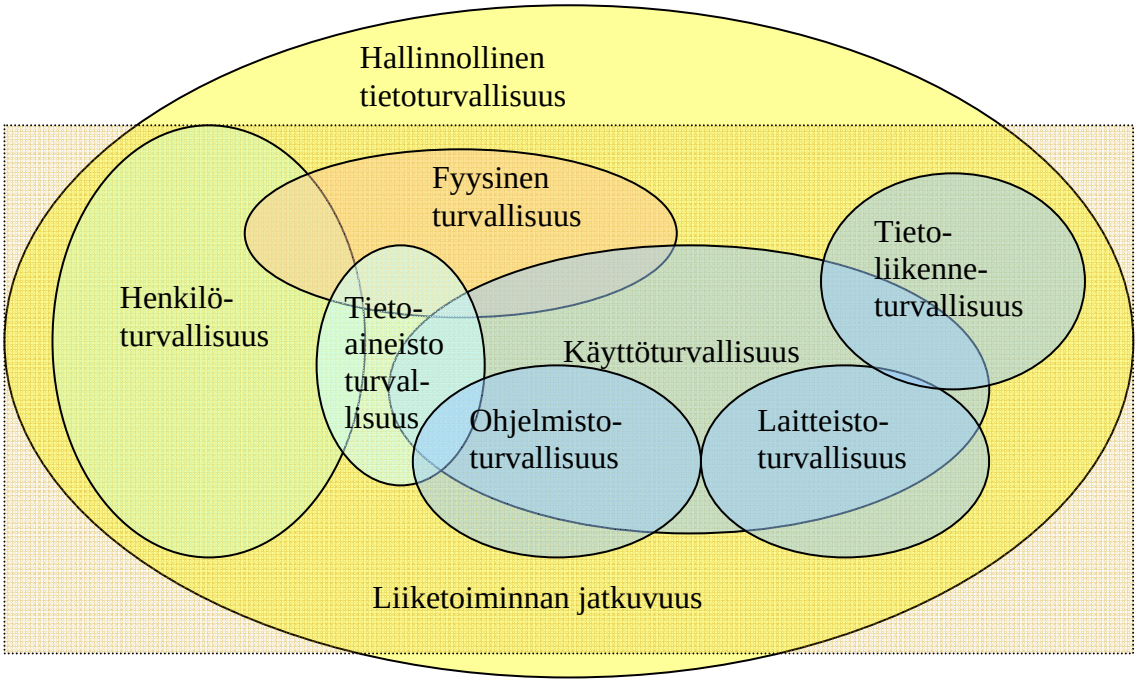
VAHTI-ohjeet	Tipton ja Krause 2004	BS 7799-1:fi	Whitman ja Mattord 2003
Hallinnollinen tietoturvallisuus	Information security management, management practices	Tietoturvallisuuden organisointi	Security management practices, security program policy
Henkilöstöturvallisuus	Employment policies and practices	Henkilöstöturvallisuus	Employment practices, personnel security
Fyysinen turvallisuus	Physical security	Fyysinen turvallisuus ja ympäristön turvallisuus	Physical security
Tietoaineistoturvallisuus		Suojattavien kohteiden luokitus ja valvonta	
Tietoliikenneturvallisuus	Telecommunications, network and internet security	Tietoliikenteen ja käyttötoimintojen hallinta	Security technology
Laitteistoturvallisuus		Järjestemien	Physical security

Ohjelmistoturvallisuus	Applications and systems development security	kehittäminen ja ylläpito	Security technology
Käyttöturvallisuus	Operations security		
	Business continuity planning	Liiketoiminnan jatkuvuuden hallinta	Business continuity planning
	Access control systems and methodology	Pääsyoikeuksien valvonta	
	Cryptography		
	Enterprise security architecture		Implementation and maintenance
		Vaatimustenmukaisuus	

Kaikki osa-alueet eivät esiinny samanlaisina eri lähteissä, vaan osa-aluejaottelu vaihtelee kirjoittajan ja kirjan tarkoituksen mukaan. VAHTI-ohjeissa liiketoiminnan jatkuvuussuunnittelua ei mainita, sillä ohjeet on kehitetty julkisten organisaatioiden tietoturvallisuusohjeistuksiksi. Toiminnan jatkuvuuden suunnittelua tarvitaan näissäkin organisaatioissa, mutta se ei ole niiden olemassaolon kannalta niin keskeisessä roolissa kuin yritysten kohdalla, joissa lyhytkestoinenkin häiriö liiketoiminnalle voi muodostua kohtalokkaaksi. Toisaalta monien julkisten organisaatioiden toimintavalmius kriisitilanteissa on tärkeää jopa kansallisen turvallisuuden takia, minkä takia on yllättävää että jatkuvuussuunnittelu ei ole saanut roolia VAHTI-ohjeissa lainkaan. Taulukossa 1 eri lähteissä esiintyviä osa-alueita on sijoiteltu niin, että toisiaan suunnilleen vastaavat osa-alueet ovat rinnakkain. Osa-aluekuvaukset, kuten yllä monen osa-alueen kohdalla on todettu, eivät kuitenkaan täysin vastaa toisiaan. Joitakin osa-alueita on lähteissä ryhmitelty keskenään, jolloin joitakin taulukon kohdista jää tyhjäksi, tai sama nimitys toistuu useammassa kohdassa.

Tiptonin ja Krausen (2004) osa-alueet vastaavat muuten hyvin pitkälle muita, mutta kryptografia on omana osa-alueenaan laajempien kokonaisuuksien joukossa. Muut jaottelut käsittelevät erilaisia salausmenetelmiä tietoaineistoturvallisuuden ja tietoliikenteen turvallisuuden yhteydessä, eikä niille ole annettu kovin suurta roolia. Myöskään tässä työssä ei katsota tarpeelliseksi tutustua erilaisiin salausmenetelmiin sen tarkemmin, koska työ on tehty johtamisen näkökulmasta.

Tietoturvallisuuden osa-alueiden määrittelyjä on olemassa useita ja osa-alueiden määrä sekä suhteet toisiinsa vaihtelevat jo senkin mukaan, mikä on yrityksen kannalta tärkeää. Vaikka täysin yleispätevää jaottelua ei tämän takia olekaan olemassa, voidaan esittää kuhunkin tilanteeseen sopiva yleiskuvaus osa-alueista. Kuva 6 esittää yhteenvetona tässä työssä määritellyt tietoturvallisuuden osa-alueet sekä sen, miten niiden nähdään suhteutuvan toisiinsa.



Kuva 6. Tietoturvallisuuden osa-alueiden kenttä

Hallinnollinen tietoturvallisuus pitää sisällään kaikkien muiden osa-alueiden vastuiden määrittelyn sekä sen, miten yrityksessä suhtaudutaan tietoturvallisuuteen. Käyttöturvallisuus pyrkii takaamaan tietoaineistojen, ohjelmistojen ja laitteistojen turvallisuuden, mutta näihin liittyy muutakin kuin niiden turvallinen käyttö. Tietoaineistoturvallisuuden takaa loppukädessä se, että henkilöstö tiedostaa käsittelemänsä tiedon arvon ja noudattaa sen käsittelystä annettuja ohjeita. Fyysisen toimintaympäristön turvaaminen on osa käyttöturvallisuutta, tai päinvastoin.

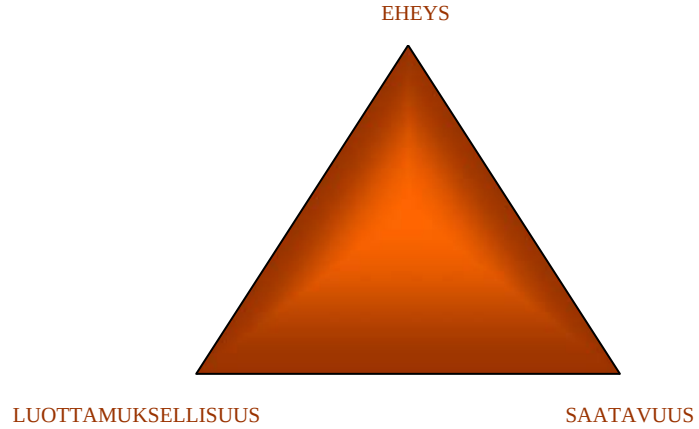
Kuten huomataan, osa-alueiden rajat ovat häilyvät. Eri lähteet painottavat eri asioita, jolloin jossakin yhteydessä erilliset osa-alueet muuttuvatkin toisilleen sisäkkäisiksi. Kuvassa 6 keskeisintä on, että hallinnollinen turvallisuus kattaa kaikki muut osa-alueet, eli siinä luodaan kokonaiskuva tietoturvallisuudesta. Yksittäisten osa-alueiden turvallisuudesta huolehtiminen on kuitenkin tärkeää, minkä takia ne ansaitsevat tulla mainituksi itsenäisinä osa-alueina vaikka ne voidaankin mieltää kuuluvaksi johonkin toiseen osa-alueeseen ja hallinnolliseen turvallisuuteen.

Liiketoiminnan jatkuvuus ei ole samalla tavalla erillinen osa-alue kuin muut kuvassa esiintyvät osa-alueet. Se on prosessi, jonka tulee kattaa kaikki tietoturvallisuuden osa-alueet ja joka toimii osana sisäistä tietoturvallisuuden arviointia ja riskienhallintaa. Jatkuvuussuunnittelun avulla yksittäisillä osa-alueilla olevia puutteita voidaan tunnistaa ja niihin voidaan tehdä parannuksia.

2.2 Tietoturvallisuuden ulottuvuudet

Tiedon ulottuvuudet eli ominaisuudet tietoturvallisuuden kannalta ovat luottamuksellisuus, eheys ja saatavuus. Tietoturvallisuus prosessina tähtää näiden ulottuvuuksien turvaamiseen. Termin saatavuus tilalla suomenkielisessä kirjallisuudessa käytetään usein termiä käytettävyys, ja esimerkiksi VAHTI-ohjeet suosittelevat tämän termin käyttöä. Käytettävyys tarkoittaa käyttökelpoisuutta ja käytettävissä oloa (Haarala et. al. 2001a, s.638). Termi on vakiintunut toisen tutkimusalan käyttöön vastaamaan englanninkielistä termiä usability, jonka suomennokseksi sanakirjat tarjoavatkin käytettävyyttä. Vakiintumisen takia saman termin käyttäminen tarkoittamaan tiedon jatkuvaa saatavilla oloa aiheuttaisi sekaannusta. Saatavuus terminä tarkoittaa esimerkiksi tiedon jatkuvaa saatavilla oloa (Haarala et. al. 2001b, s.6). Sanakirjat tarjoavat myös termin availability suomennokseksi termiä saatavuus. Tässä tutkimuksessa englanninkielisen termin availability suomennoksena käytetään termiä saatavuus merkityssekaannuksien välttämiseksi.

Luottamuksellisuus tarkoittaa sitä, että tieto on vain niiden henkilöiden saatavilla, joilla on pääsyoikeus ko. tietoon (BS 7799-1:fi s. 8). Eheydellä tarkoitetaan sitä, että tieto ja sen käsittelytavat ovat täydellisiä ja virheettömiä (ibid), eli tieto ei pääse muuttumaan tai tuhoutumaan käsittelyn tai säilytyksen aikana. Saatavuus tarkoittaa että tieto ja sen käsittelytavat ovat aina tarvittaessa niiden käyttöön valtuutettujen saatavilla (ibid.). Nämä kolme ulottuvuutta ovat tasa-arvoisia tiedon kannalta ja ne on havainnollistettu kuvassa 7. Myös Tipton ja Krause (2004) mainitsevat yleisesti nämä kolme ulottuvuutta tietoon kohdistuvien uhkien analysoinnin yhteydessä.



Kuva 7. Tiedon kolme ulottuvuutta eli CIA-kolmio

Whitman ja Mattord esittelevät CIA-kolmion, joka toimii oivana muistisääntönä ulottuvuuksia opettelevalle. Englanninkielisessä kirjallisuudessa ulottuvuuksia esiintyy vaihteleva määrä näiden kolmen perusulottuvuuden lisäksi. Whitman ja Mattord (2003, s.10-14) mainitsevat yhteensä seitsemän ulottuvuutta, joita ovat saatavuus[22],

[22] availability

täsmällisyys[23], autenttisuus[24], luottamuksellisuus[25], eheys[26], hyödyllisyys[27] ja hallussapito[28]. Edellä mainittu standardissa käytetty jako kolmeen ulottuvuuteen on kuitenkin löydettävissä myös tästä jaottelusta. Saatavuus ja hyödyllisyys yhdessä vastaavat aiemmin määriteltyä saatavuutta, täsmällisyys, autenttisuus ja eheys vastaavat eheyttä, luottamuksellisuus ja hallussapito aiemmin määriteltyä luottamuksellisuutta. Voidaan ajatella, että standardin määritelmissä toisilleen läheiset käsitteet on niputettu yhteen selkeyden vuoksi. Toisaalta voidaan nähdä, että on tarpeen eritellä useampia ulottuvuuksia esimerkiksi riskianalyysien tekemisen avuksi.

2.3 Tietoturvallisuuspolitiikka

Shortenin (2004, s. 917) mukaan tietoturvallisuuden kehittämisen tulisi lähteä tietoturvallisuuspolitiikan määrittelystä. Hän painottaa, että politiikan tulee olla johdon allekirjoittama asiakirja, josta selviävät tietoturvallisuuteen liittyvät velvollisuudet ja vastuut. Höne ja Eloff (2002, s.402) määrittelevät, että tietoturvapolitiikka on yleensä lyhyt ja varsin yleisluontoinen dokumentti, joka viestii tietoturvallisuuden tärkeydestä kaikille tiedon käyttäjille yrityksessä. Sen tulee olla yhteensopiva yrityksen liiketoiminnan tavoitteiden kanssa ja johdon tukema, jotta se viestii turvallisuuden tärkeydestä oikealla tavalla.

Luvussa 2.1 kuvatuilla tietoturvallisuuden osa-alueilla pyritään turvaamaan tiedon ulottuvuuksia (luku 2.2). Hallinnollisen tietoturvallisuuden yhteydessä todettiin myös, että tietoturvallisuuspolitiikka kuuluu olennaisena osana siihen. Politiikan laatiminen ei kuitenkaan ole yksinkertaista, minkä vuoksi yrityksissä monesti päädytään muualta melko suoraan kopioituun politiikkaan, joka jää yrityksen toiminnasta irralliseksi (Höne & Eloff 2002, s. 403). Tämä voi johtua politiikan laatijoiden heikosta tietotasosta tai puhtaasti ajan ja resurssien puutteesta. Muualta kopioitu politiikka jää kuitenkin helposti liian yleiseksi sekä kieleltään vieraaksi yrityksen työntekijöille. Jos politiikka tuntuu kopioidulta dokumentilta, johon toimitusjohtaja on nopeasti laittanut nimensä alle, eivät työntekijätkään välitä siitä sen enempää.

Tietoturvallisuuspolitiikan tulee BS 7799 -standardin mukaan (BS 7799-1:fi, s. 12) sisältää vähintään seuraavat ohjeet tiiviissä ja helppolukuisessa muodossa:

- tietoturvallisuuden, sen yleistavoitteiden, soveltamisalan ja merkityksen määrittely yrityksen kannalta
- yrityksen johdon tuki tietoturvallisuuden tavoitteille ja periaatteille

[23] accuracy
[24] authenticity
[25] confidentiality
[26] integrity
[27] utility
[28] possession

- organisaation kannalta tärkeiden tietoturvallisuuden menettelytapojen, periaatteiden, standardien ja vaatimusten noudattamista koskeva selvitys
    - lainsäädäntö ja sopimukset sekä niiden noudattaminen
    - koulutus
    - virustorjunta
    - liiketoiminnan jatkuvuuden hallinta
    - politiikan rikkomusten seuraamukset
- yleisten ja erityisten velvollisuuksien määrittely
- viittaukset politiikkaa tukeviin asiakirjoihin, esim. tarkemmat ohjeistukset eri osa-alueille

Mielenkiintoista on, että standardi kuvaa muuten hyvin yleisluontoisen listan siitä, mitä politiikka pitää sisällään, mutta virustorjunnan hoitaminen mainitaan yhtenä kohtana. Tänä päivänä tietokonevirukset ovat niin yleisiä, että virustorjunnan asianmukainen hoitaminen on päivittäisen liiketoiminnan perusedellytys, jolloin erityinen lauseke niinkin yleisluontoisessa dokumentissa kuin tietoturvallisuuspolitiikka on, on tarpeeton.

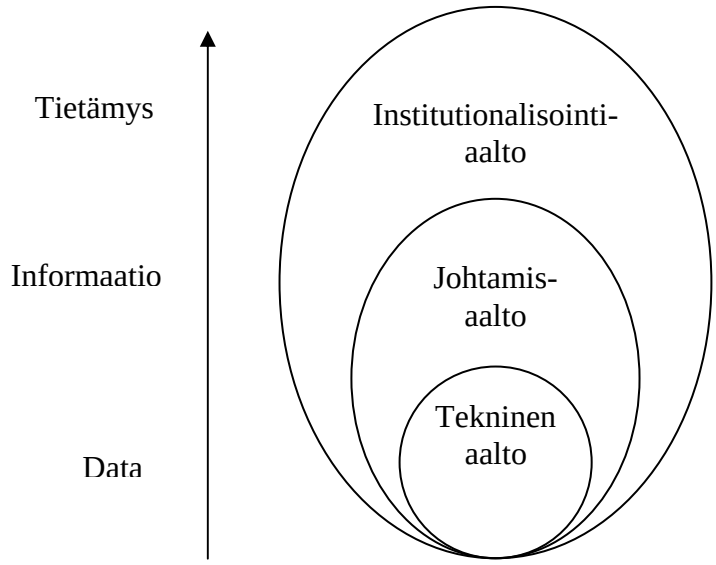
Tietoturvallisuuspolitiikan tarkoituksena on kuvata tietoturvallisuuden tehokkaat toimintatavat yrityksessä (GAISP 3.0, s. 11). Jos tietoturvallisuuden tavoitteita ja prosesseja ei tarkkaan määritellä, voi syntyä tilanne jossa riskejä ei arvioida kattavasti ja jossakin kohtaa suojataan riittämättömästi ja jossakin liikaa (ibid.). Molemmat tapaukset ovat tehokkuuden kannalta huono ratkaisu. Tietoturvallisuuspolitiikan tulee olla siis siinäkin mielessä yhteydessä yrityksen muuhun strategiaan, että riskejä arvioidaan yrityksen omista lähtökohdista ja suojauksen tarve arvioidaan jokaisen riskin kohdalla erikseen. Pieni yritys, jonka liiketoiminta ei kärsi palvelimen kaatumisesta yöllä, tuskin tarvitsee 24 tunnin reaaliaikaista ylläpitoa, kun taas yritys, joka tarjoaa www-palvelintilaa toisille yrityksille tarvitsee sitä ehdottomasti, sillä pienikin katkos voi aiheuttaa vahinkoa liiketoiminnalle. Yrityskohtaisuus on politiikassa tärkeää siis sekä henkilöstön aidon sitoutumisen että riskienhallinnan järkevyyden kannalta.

2.4 Tietoturvallisuuskulttuuri

Tietoturvallisuuskulttuuri muodostuu yritykseen sitä mukaa, kun yrityksen ohjeistukset, politiikat ja toimintatavat tulevat osaksi päivittäistä toimintaa. Kulttuurin muodostumista ajan myötä käsittelee esimerkiksi von Solms (2000, s.615) esittäessään tietoturvallisuuden aallot. Ensimmäinen aalto on tekninen aalto, eli tietoturvallisuus on yrityksessä lähinnä tekninen kysymys ja turvallisuusratkaisut myös teknisiä. Toisena on johtamisaalto, jonka aikana tietoturvallisuus nousee myös johdon mielenkiinnon kohteeksi ja teknisten ratkaisujen lisäksi pohditaan toimintatapoja ja muodostetaan tietoturvallisuuspolitiikka ja muita ohjeistuksia. Kolmantena tulee institutionalisointiaalto, jonka aikana muodostetaan tietoturvallisuuskulttuuria

yritykseen vertaamalla aiemmin dokumentoituja toimintaperiaatteita esim. standardeihin. Tietoturvallisuus muuttuu institutionalisointiaallon myötä osaksi normaalia työrutiinia, jonka toimintamalli pohjautuu kansainvälisesti tunnettuihin standardeihin ja hyväksi havaittuihin käytäntöihin.

Tietoturvallisuuden aallot voidaan nähdä liittyvän siihen, minkälaista tietoa yrityksessä pääosin suojataan (Kuusisto et. al. 2004, s. 2) . Kuvassa 8 esitetään kuinka aallot liittyvät tiedon tasoihin, eli dataan, informaatioon ja tietämykseen.



Kuva 8. Tietoturvallisuuden aallot ja tiedon tasot (mukailtu lähteestä Kuusisto et. al. 2004, s.2)

Teknisen aallon vaiheessa suojaustoimenpiteet kohdistuvat lähinnä dataan ja tietokoneiden suojaamiseen. Johtamisaallon mukana pyritään suojaamaan kaikkea yrityksen hallussa olevaa informaatiota, niin tietokoneilla kuin fyysisessäkin muodossa olevaa. Institutionalisointiaallon mukana mukaan tulee myös työntekijöiden tietämyksen suojaaminen yrityksen tärkeänä voimavarana. Tällöin voidaan puhua tietoturvallisuuskulttuuriin vaikuttamisesta.

Dhillon (1997, s. 59) määrittelee tietoturvallisuuskulttuurin toimintamalleiksi, joita yrityksessä noudatetaan tiedon suojaamiseksi. Tietoturvallisuuskulttuuri näkyy siis yrityksen päivittäisessä toiminnassa normaalien toimien kautta. Tietoturvallisuuskulttuuri voi olla tietoturvallisuuspolitiikan ilmentymä, mutta nämä kaksi voivat myös olla ristiriidassa keskenään. Voidaan ajatella, että jos yrityksessä ei ole dokumentoitua tietoturvallisuuspolitiikkaa, tietoturvallisuuskulttuuri muodostaa kirjoittamattoman politiikan. Joskus kuitenkin yrityksissä on olemassa kirjoittamattomia sääntöjä esimerkiksi salasanojen muotovaatimuksista, joita tulisi noudattaa, mutta joita

ei kuitenkaan noudateta. Tällöin dokumentoimatonkin politiikka on ristiriidassa vallitsevan kulttuurin kanssa.

Dhillon (1997, s. 59) mainitsee tietoturvallisuuskulttuurin puutteen aiheuttavan ongelmia koko organisaation yhtenäisyyden ylläpitoon, sekä erityisesti määriteltyjen tietoturvallisuusprosessien yhtenäisyyteen. Scheinin (lähteessä Thomson & von Solms 2005, s.5) mukaan organisaatiokulttuuri ilmenee useammalla tasolla, joista syvintä tasoa tulee ymmärtää jotta kulttuurin johtaminen olisi mahdollista. Organisaatiokulttuurin syvin taso on jaettujen arvojen ja uskomusten taso, joka syntyy kun asioista tulee itsestäänselvyyksiä. Kulttuuri on siis olemassa joka tapauksessa jonkinlaisena. Yrityksessä voi esimerkiksi vallita tilanne, että ”kaikki tietävät” ettei salasanaa tarvitse vaihtaa, vaikkei kukaan osaa sanoa mistä ”tieto” on peräisin. Olettamuksesta on muodostunut yhteinen itsestäänselvyys. Dhillonin (1997, s. 59) mainitsema tietoturvakulttuurin puute on enemmänkin tietoturvallisuuden näkymättömyyttä organisaation kulttuurissa. Tällaisen organisaation tietoturvakulttuuri on hyvin kehittymätön, mutta se on kuitenkin olemassa yleisenä toimintana, joka ei ota tietoturvallisuutta huomioon. Voidaankin ajatella, että tietoturvallisuuskulttuuri on osa organisaatiokulttuuria ja yleensä tietoturvallisuuskulttuurina siitä puhutaan silloin kun tietoturvalliset toimintatavat ovat vakiintuneet tai vakiintumassa osaksi työntekijöiden perusoletuksia työstään.

Tietoturvakulttuurin kehittämiseksi johdon tulisi pyrkiä vaikuttamaan organisaatiokulttuurin syvimpään tasoon, jotta tietoturvallisuus olisi osa työntekijöiden päivittäistä rutiinia (Thomson & von Solms 2005, s.7). Hallinnolliseen ja henkilöturvallisuuteen kuuluva tietoturvallisuustietoisuuden ylläpito esimerkiksi koulutuksin, sekä tietoturvallisuusohjeistusten tekeminen hyvin muotoillun tietoturvallisuuspolitiikan pohjalta ovat esimerkkejä keinoista, joilla kulttuuriin voi pyrkiä vaikuttamaan. Johdon tulee ymmärtää, että tietoturvallisuuskäytäntöjen noudattamiseen tulee kannustaa ja niiden noudattamista tulee valvoa (von Solms & von Solms 2004b, s. 372). Johdon esimerkin ja kannustuksen kautta tietoturvallisuuskäytänteet voidaan saada osaksi päivittäistä toimintaa, jota kautta tietoturvallisuuskulttuuri yrityksessä kehittyy.

von Solms ja von Solms (2004a, s. 277) toteavat, että jos johto haluaa työntekijöiden toimivan tietyllä tavalla, täytyy tuo toiminta kuvata heille tavalla tai toisella. Tietoturvapolitiikan ja käytäntöjen tulee heidän mukaansa heijastaa johdon arvoja ja suhtautumista tietoturvallisuuteen, jotta yrityksen tietoturvakulttuuria voitaisiin kehittää niiden avulla. Kirjoittajat vertaavatkin tietoturvallisuuspolitiikkaa Raamatun kymmeneen käskyyn, jotka edelleen, tuhansia vuosia niiden kirjoittamisen jälkeen, ohjaavat kulttuurisina perusarvoina ihmisten toimintaa. Jotta tietoturvallisuuspolitiikka voi toimia tietoturvallisuuskulttuurin kehityksen pohjana, tulee sen olla yleisluontoinen ja mahdollisimman pysyvä dokumentti. Sen tulee myös olla kaikkein ylimmän johdon

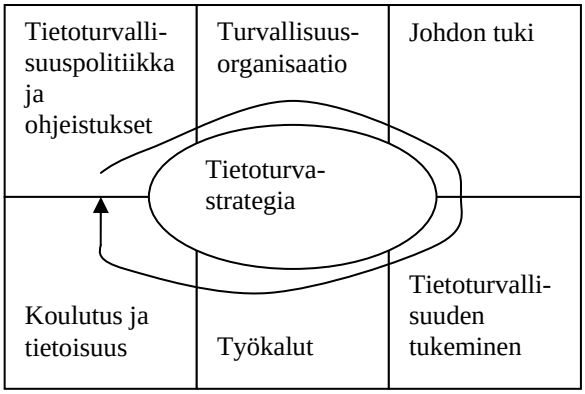
hyväksymä ja vahvistama, jotta se on uskottava ja työntekijät hyväksyvät sen toimintaa ohjaavaksi dokumentiksi.

Tietoturvallisuuskulttuuri on siis jotain, joka ohjaa työntekijöiden toimintaa heidän päivittäisessä työssään. Vaikka kulttuuriin vaikuttaminen ei ole helppoa, tietoturvallisuuskulttuuria voidaan pyrkiä kehittämään esimerkiksi tietoturvallisuuspolitiikan ja koulutuksen sekä tietoisuuden lisäämisen avulla. Johdon sitoutuminen tähän tehtävään on hyvin tärkeää, jotta vaikutus ulottuisi kulttuurin syvimmälle tasolle asti.

2.5 Yhteenveto tietoturvallisuudesta käsitteenä

Tietoturvallisuus on monimutkainen käsite, jonka yksiselitteinen määrittely on hankalaa. Toisaalta tietoturvallisuus voidaan nähdä joukkona toimenpiteitä, joiden avulla varmistetaan tietojen luottamuksellisuus. Toisaalta turvallisuus on osa normaalia toimintaa ja sisältyy jokapäiväiseen liiketoimintaan sen perusedellytyksenä.

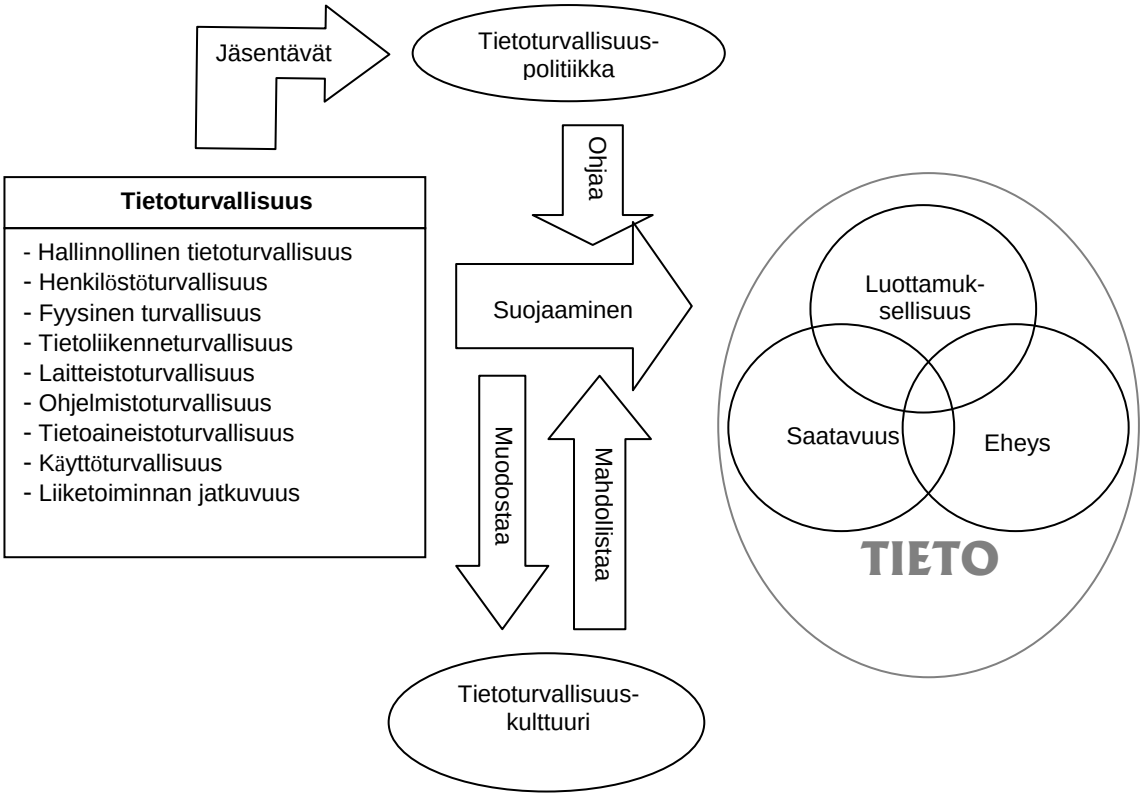
Kairab (2005, s. 46) esittää tietoturvallisuuden jatkuvana prosessina, jossa toteutetaan yrityksen turvallisuusstrategiaa ja varmistetaan näin liiketoiminnan mahdollisuudet kaikissa tilanteissa. Tämä prosessi on kuvattu kuvassa 9.



Kuva 9. Tietoturvallisuuden prosessi (mukailtu lähteestä Kairab 2005, s.46)

Kairabin malli lähtee tietoturvallisuuspolitiikan määrittelystä, tietoturvallisuuden organisoinnista ja johdon tuesta. Kun nämä on saatu kuntoon, voidaan lähteä tukemaan ja levittämään tietoturvallisuustietoutta yrityksessä erilaisten työkalujen ja koulutuksen avulla. Koko tätä prosessia ohjaa johdon määrittelemä tietoturvastrategia. Prosessi on syklinen, eli koulutuksen ja tietoisuuden ylläpidon kautta päästään päivittämään tietoturvallisuuspolitiikkaa.

Tietoturvallisuus nähdään tässä työssä edellä käsiteltyjen määritelmien kautta prosessina, jonka tavoite on suojata tiedon ominaisuuksia. Prosessin osina mainitaan hallinnolliset, tekniset ja muut toimenpiteet. Nämä toimenpiteet voidaan nähdä tietoturvallisuuden osa-alueina, jotka on ensimmäisessä alaluvussa määritelty. Kuvassa 10 on havainnollistettu tutkimuksen keskeisten käsitteiden suhteita toisiinsa.



Kuva 10. Tietoturvallisuuteen liittyvien käsitteiden suhteet

Tietoturvallisuuden osa-alueiden kautta kuvataan toimenpiteet, joilla suojataan tiedon ominaisuuksia. Kaikki osa-alueet kattava tietoturvallisuuspolitiikka toimii pohjana suojaustoimenpiteiden kuvaukselle ja ylimmän johdon kannanottona se ohjaa suhtautumista tietoturvallisuuteen yrityksessä. Suojaustoimenpiteiden ja tietoturvapolitiikan viestimien asenteiden kautta yritykseen muodostuu tietoturvallisuuskulttuuri, joka voi mahdollistaa tai myös vaikeuttaa suojaustoimenpiteitä. Koko prosessin tavoitteena on suojata yrityksen toiminnan kannalta keskeisen tiedon säilyminen vain siihen oikeutettujen henkilöiden hallussa ja saatavilla muuttumattomana. Tätä kautta taataan yrityksen liiketoiminnan edellytykset tiedon osalta kaikissa tilanteissa.

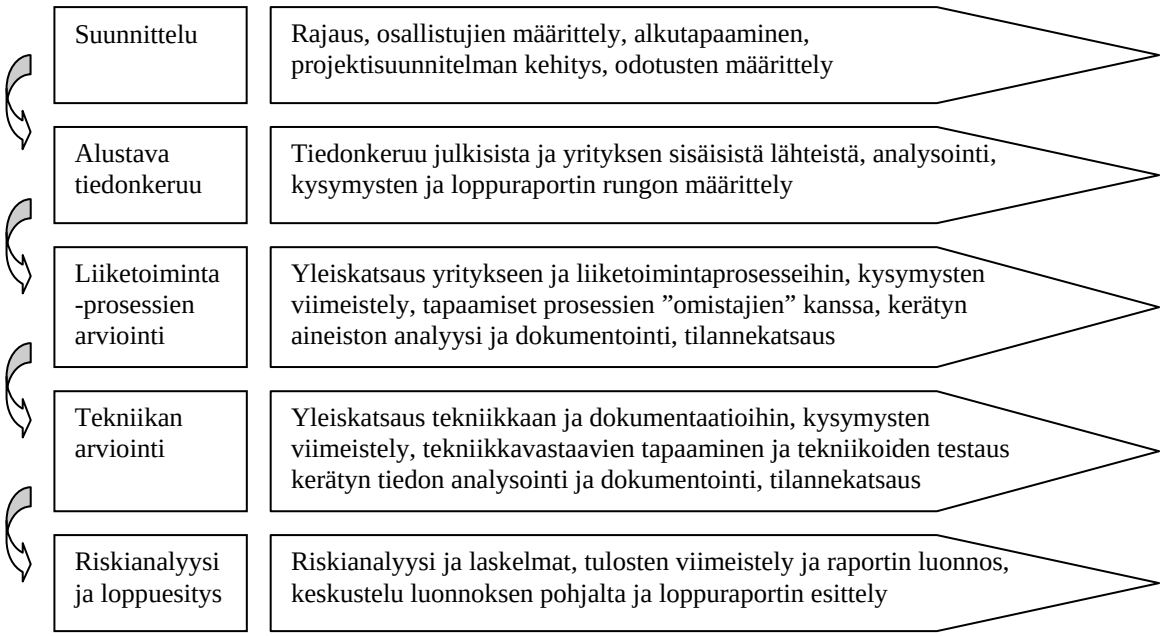
3 TUTKIMUKSEN TOTEUTUS

Englanninkielisessä kirjallisuudessa (e.g. Kairab 2005, CEM) tietoturvallisuuden arvioinnista käytetään yleensä termiä ”assessment”. Tämä termi kääntyisi suomen kielessä sanaksi arviointi. Audit-sana englannin kielessä viittaa lähinnä tilintarkastukseen, ja yleensä myös standardia vastaan tehtävää, sertifikaattiin tähtäävää tietoturvallisuuden arviointia kutsutaan sanalla ”assesment”. Suomessa esimerkiksi konsulttiyritykset tarjoavat tietoturvallisuuden arviointipalveluita nimikkeellä tietoturvallisuusauditointi. Tämän takia tässä työssä englanninkielisen termin ”assessment” käännöksenä käytetään sanaa auditointi ja työssä puhutaan tietoturvallisuusauditoinneista.

3.1 Tietoturvallisuusauditoinnit

Tietoturvallisuusauditointi voidaan tehdä monella eri tavalla. Monet kuvaukset auditointimenetelmistä (e.g. CEM, Kairab 2005) ovat hyvin yksityiskohtaisia ja ne sisältävät sekä haastatteluja että dokumenttien tarkistusta ja järjestelmien testausta. Tässä tutkimuksessa auditoinnit on toteutettu haastattelemalla, koska olennaista oli valita menetelmä, jonka avulla on mahdollista yhdistää opiskelijoiden harjoitustyön tekeminen tutkimusaineiston keruuseen.

Auditoinnin tekemiseen löytyy useita malleja, joissa on tietyt pääkohdat. Esimerkiksi Kairab (2005, s.63) esittelee hyvin monisyisen mallin, joka kuvaa yksityiskohtaisesti auditointiprosessin. Prosessi on kuvattu kuvassa 11. Prosessikuvaus on tehty auditoinnin suorittavan yrityksen tai yhteisön näkökulmasta.



Kuva 11. Tietoturvallisuusauditointiprosessi (Mukailtu lähteestä Kairab 2005 s.63)

Toinen malli auditoinnin suorittamiselle löytyy Common Evaluation Methodista (CEM). Tämä malli esittelee pääkohdat, jotka ovat alkuehdot, vastuullisten nimeäminen sekä auditoinnin suoritus ja analyysi (CEM v3.0, s.23). Tämä malli on tavallaan yksinkertaistettu versio Kairabin esittelemästä auditointimallista. Vaikka arviointimalli sinänsä on yksinkertainen, CEM on tietotekninen auditointimenetelmä, jonka avulla käydään yrityksen tietotekninen turvallisuus erittäin systemaattisesti läpi. Auditoinnit sertifikaattia vastaan voivat sisältää huomattavan tiukkoja kriteerejä sille, hyväksytäänkö vai hylätäänkö yrityksen ”suoritus” kyseisellä alueella (esim. CEM). Tässä tutkimuksessa ei kuitenkaan myönnetä sertifikaatteja tai anneta yksiselitteistä lausuntoa yrityksen tietoturvallisuuden tilasta, joten myöskään tiukkoja kriteerejä sille, mikä on hyväksyttävä ja mikä huono tilanne ei ole asetettu.

Yksi tapa lähestyä tietoturvallisuuden auditointia on yrityksen haavoittuvuuksien etsintä. Hale et. al (2004) esittelevät haavoittuvuusanalyysin tietojen turvaamisen työkaluna. Heidän lähestymistapansa on tarjota kevytkäyttöinen työkalu johdolle tietoturvallisuusriskien arviointiin. Mallissa on kolme porrasta: tietovarantojen arvon määritys, uhkien analyysi ja turvaamisen kustannusten määrittely (Hale et. al. 2004, s. 60-61). Malli on riskianalyysimalli, joka keveytensä ja liiketaloudellisen näkökulmansa puolesta soveltuu hyvin tietoturvallisuuden yleistilan arviointiin ja suojaustoimenpiteiden valintaan.

Tutkimuksen tarkoituksena on selvittää tietoturvallisuuden ja erityisesti sen johtamisen nykytilaa, sekä pohtia miten sitä voitaisiin parantaa. Liian yksityiskohtaisiin asioihin ei pureuduttu, sillä erityisesti teknisen tietoturvan osalta kriteeristöjä ja arviointiohjeita on runsaasti ja teknisten yksityiskohtien selvittäminen olisi vienyt turhan paljon aikaa.

Tekniset yksityiskohdat eivät myöskään kuulu tutkimuksen taustalla olevan kurssin aihepiiriin. Yksittäiset yritykset saavat opiskelijoiden tekemän auditointiraportin, jossa on jonkin verran otettu kantaa turvallisuustoimenpiteiden kustannuksiin. Laajempaa riskianalyysia tai kustannusarvioita tässä tutkimuksessa ei kuitenkaan tehdä.

3.2 Kohdeyritykset ja haastattelujen toteutus

Haastatteluja on erilaisia, esimerkiksi strukturoitu haastattelu, teemahaastattelu ja avoin haastattelu (Fontana & Frey 2005). Strukturoitu haastattelu on haastattelu, joka suoritetaan valmiin kysymyssarjan avulla niin, että kysymysten muoto ja järjestys on määrätty (Hirsjärvi et al. 2004, s.197). Teemahaastattelu taas on haastattelu, jossa haastattelu etenee mietittyjen teemojen puitteissa, mutta kysymysten tarkkaa muotoa ja järjestystä ei ole mietitty (ibid.). Tässä tutkimuksessa auditoinnit suoritettiin valmiin kysymysrungon mukaan, mutta niin, että kysymysten ei tarvinnut olla valmiiksi määrätyssä järjestyksessä. Tarkentavia kysymyksiä oli mahdollista lisätä valmiita kysymyksiä täydentämään. Kysymysten vastauksia ei myös ollut etukäteen rajattu ennalta määrättyihin vaihtoehtoihin, kuten strukturoidussa haastattelussa usein on (Fontana & Frey 2005, s.702). Tällä perusteella haastattelu on strukturoidun ja teemahaastattelun välimuoto ja sitä kutsutaan tässä tutkimuksessa puolistrukturoiduksi haastatteluksi.

Haastatteluin voidaan kerätä sekä laadullista että kvantitatiivista tietoa. Tässä tutkimuksessa kerättävä tieto on lähinnä laadullista. Kysymykset ovat pääosin luonteeltaan avoimia. Osassa kysymyksiä on nähtävissä suljetut vastausvaihtoehdot, vaikka niitä ei ole erikseen määritelty. Näissä tilanteissa kerättyä tietoa voidaan käsitellä myös kvantitatiivisesti.

Tutkimukseen osallistui 16 yritystä, joiden koko vaihteli 6 ja 120 työntekijän välillä. 10:ssä yrityksistä oli yli 10 mutta alle 30 ja 5:ssä yli 30 työntekijää. Tutkimus painottuu siis lähinnä pieniin yrityksiin. Yritysten toimialat on esitetty taulukossa 2.

Taulukko 2. Kohdeyritysten toimialat

Toimiala	Yrityksiä
Ohjelmistosuunnittelu ja -tuotanto	4
Konsultointipalvelut	5
Terveydenhuollon palvelut ja tutkimus	4
Kirjanpito- ja markkinointipalvelut	3

Yrityksistä haastatteluun osallistui yleensä yksi henkilö, mutta neljässä yrityksessä haastateltavia oli kaksi ja kahdessa yrityksessä kolme. Seitsemässä yrityksessä

toimitusjohtaja oli mukana haastattelussa. Haastateltavat olivat yrityksessä tietoturvallisuudesta vastaavia henkilöitä.

Haastateltavien määrän vaihtelu saattaa aiheuttaa erilaisia vastauksia esitettyihin kysymyksiin. Toisaalta useampi kuin yksi haastateltava varmistaa, että kaikkiin kysymyksiin saadaan vastaus, sillä henkilöiden vastaukset täydentävät toisiaan. Kun paikalla on useampia henkilöitä, he kuitenkin helpommin saattavat vastata ryhmäpaineen takia ”ohjekirjan mukaan” sen sijaan, että vastaus kuvastaisi todellisia käytäntöjä. Koska haastatteluissa kartoitettiin lähinnä yleisen tason asioita ja esimerkiksi sitä, onko politiikkoja ja ohjeistuksia olemassa, ei ryhmäpaineen vaikutus merkittävästi vääristä tuloksia. Jatkokysymyksinä kysyttiin myös käytännön tilanteista, mutta näistä puhuttiin vaihtelevasti eri yrityksissä muutenkin, joten haastateltavien määrä ei olennaisesti vaikuta tuloksiin. Hyvä kontrollikeino olisi ollut haastatella useampaa saman yrityksen edustajaa toisistaan riippumatta, mutta tähän ei tässä tutkimuksessa ollut mahdollisuutta. Haastattelijoina toimivat tietoturvallisuuden johtaminen –kurssin opiskelijaryhmät tutkijan ohjauksessa.

Haastattelut nauhoitettiin ja osa vastauksista litteroitiin jatkoanalyysia varten. Haastattelut tehtiin yritysten tiloissa, jolloin voitiin luoda yleissilmäys yritysten toimitiloihin. Varsinaisia tutustumiskiertoja tehtiin vain parissa yrityksessä, joten fyysiseen turvallisuuteen liittyvät asiat on selvitetty lähinnä haastattelukysymysten perusteella. Yritysten edustajat saivat haastattelukysymykset nähtäväkseen ennen haastattelua siihen valmistautumista varten. Valmistautumisen mahdollisuus oli käytetty hyväksi vaihtelevasti.

3.3 Auditoinneissa käytetyt kysymykset

Auditointikysymyksillä pyrittiin selvittämään mahdollisimman kattavasti yrityksen tietoturvallisuuden yleinen tila. Haastatteluun käytettävissä olevan ajan puitteissa käsiteltävien kysymysten määrä on rajallinen, joten yhtä osa-aluetta ei voitu käsitellä kovin monella kysymyksellä. Erityisesti teknisten tietoturvallisuusratkaisujen kohdalla kysymykset eivät mene yksityiskohtiin. Lähinnä selvitettiin, onko tiettyjä teknisiä ratkaisuja olemassa, ei sitä, minkälaisia nämä ratkaisut yksityiskohtaisesti ovat.

Kysymykset on ryhmitelty tietoturvallisuuden osa-alueiden mukaan niin, että tiettyjä osa-alueita on työn painotuksen takia yhdistelty keskenään. Osa-alueet on määritelty luvussa 2.1. Kysymykset on valittu niin, että ne ovat luonteeltaan yleisiä, ja käsittelevät lähinnä tietoturvallisuuden nykytilannetta. Osa jatkokysymyksistä pyrkii kartoittamaan syitä siihen, miksi yrityksissä toimitaan niin kuin toimitaan. Kysymykset ovat muotoutuneet tietoturvallisuuden osa-alueiden määrittelyn myötä niin, että kaikki osa-

alueet tulisivat katetuksi. Pääpaino on kuitenkin työn rajauksen takia hallinnollisilla asioilla.

Taustatiedot

Yrityksen taustatietoja kysyttiin pääosin yksittäisten auditointiraporttien arviointia varten. Yrityksen koko ja toimiala vaikuttavat siihen, minkälaiset toimenpide-ehdotukset ovat järkeviä. Esimerkiksi kymmenen henkilön yrityksessä tarvittavan dokumentaation laajuus tai koulutuksen määrän ja laadun tarve voi olla eri luokkaa kuin 100 hengen yrityksessä. Taustatietoihin liittyvät kysymykset on listattu taulukossa 3.

Taulukko 3. Yrityksen taustatietoja kartoittavat kysymykset

1. Yrityksen toiminnan lyhyt kuvaus (toimiala, asiakkaat, toimittajat)
2. Tilojen kuvaus (mm. toimistoympäristö, tuotantolaitteet, onko jaettu muiden yritysten kanssa?)
3. Työntekijöiden määrä yrityksessä
4. Mitä tietoturvallisuus on?
5. Minkälaista tietoa yrityksessä käsitellään?
6. Mitä toimintoja yrityksessä on ulkoistettu (esim. siivous, vartiointi, IT-palvelut – nimeä palveluiden tarjoaja)?
7. Onko yrityksellä tietoturvallisuuteen liittyviä sertifikaatteja? (ISO 9001, ISO 17799, ISO 18045, CMM, BSI, WebTrust tms.).
8. Onko yrityksen arvot määritelty? Onko arvoissa tai niitä selittävässä dokumentaatiossa viittauksia tietoturvallisuuden arvoihin eli tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen?

Kysymyksen 4 tarkoituksena on kartoittaa, miten haastateltavat ymmärtävät käsitteen tietoturvallisuus ja asettaa haastattelijoita samalle kartalle haastateltavan kanssa. Tämän kysymyksen kaikki vastaukset litteroitiin analysointia varten. Kysymys 5 kartoittaa paitsi sitä, minkälaista tietoa yritys käsittelee, myös sitä onko yrityksessä oikeasti pohdittu, minkälaista tietoa siellä käsitellään ja mitkä tiedot ovat toiminnan kannalta tärkeitä.

Hallinnollinen tietoturvallisuus

Hallinnollisen tietoturvallisuuden alle kuuluvat tietoturvallisuuspolitiikan luominen ja ylläpito, vastuiden jako sekä tietoturvallisuustoiminnan valvonta. Hallinnolliseen tietoturvallisuuteen liittyvät kysymykset on esitetty taulukossa 4.

Taulukko 4. Hallinnolliseen tietoturvallisuuteen liittyvät kysymykset

9. Kuvaile tietoturvallisuuspolitiikkaanne (tavoitteet, laajuus, onko

dokumentoitu?). Millaisella dokumenttikokonaisuudella tietoturvallisuutta hallitaan, ts. onko eri osa-alueille muodostettu omaa tietoturvallisuuspolitiikkaa (esim. yleinen tietoturvallisuuspolitiikka, verkon tietoturvallisuuspolitiikka jne.)?
10. Miten vastuu tietoturvallisuudesta on jaettu eri organisaatiotasoille? Kuinka tietoturvallisuusvastuista viestitään?
11. Järjestetäänkö yrityksessä sisäistä tietoturvallisuuden arviointia? Kuinka usein?
12. Valvotaanko tietoturvallisuuspolitiikan tai -ohjeistusten noudattamista? Miten?

Kysymyksen 9 kohdalla tärkeää on huomata, että yrityksessä voi olla olemassa epävirallinen tietoturvallisuuspolitiikka, vaikka sitä ei olisikaan dokumentoitu. Myös politiikan dokumentoinnin tavassa voi olla eroja, joita pyritään kysymyksin selvittämään.

Henkilöstöturvallisuus

Henkilöstöturvallisuus pitää sisällään henkilöstön työsuhteen aikaiset tietoturvallisuuteen liittyvät asiat. Tähän kuuluvat niin rekrytointiin, työssäoloon kuin irtisanomiseen liittyvät toiminnot. Näihin liittyvät kysymykset on listattu taulukossa 5.

Taulukko 5. Henkilöstöturvallisuuteen liittyvät kysymykset

13. Miten yrityksessä kehitetään tietoturvallisuustietoisuutta, eli henkilökunnan asenteita ja motivaatiota tietoturvallisuutta kohtaan?
14. Miten työntekijöitä koulutetaan tietoturvallisuuteen liittyvissä asioissa? Onko uusille työntekijöille olemassa valmista koulutuspakettia tai ohjeistusta (esim. heti rekrytoinnin jälkeen)? Jos henkilöstöä ei kouluteta, mitkä ovat suurimmat syyt siihen?
15. Kuinka työntekijöiden taustat selvitetään rekrytointitilanteessa (rikosrekisteri, suosittelijoiden lausunnot yms.)?
16. Millaisia turvallisuusmääräyksiä ja ehtoja kirjataan työsopimuksiin?
17. Onko työntekijöillä mahdollisuus etätyöskentelyyn? Kuinka etätyöskentely on hoidettu?
18. Onko yrityksessä dokumentoituja tai muuten vakiintuneita toimintatapoja työsuhteen päättyessä (pääsy/käyttöoikeuksien hallinta, työhön liittyvän materiaalin luovutus)?

Kysymysten avulla saadaan yleiskuva henkilöstöturvallisuuden luomiseen ja ylläpitämiseen liittyvistä toimista, joita yrityksessä tehdään. Vastaukset viestivät yleisestä asenteesta tietoturvallisuuden käytännön hoitamisesta.

Kysymysten 13 ja 14 kohdalla saadaan vastausten perusteella myös kuvaa siitä, millaisiksi asenteisiin ja motivaatioon vaikuttavat toimenpiteet koetaan. Kysymykset kartoittavat tavallaan samaa asiaa, mutta hieman eri sanamuodoin ja eri näkökulmasta.

Ohjelmisto- , laitteisto- ja tietoliikenteen turvallisuus

Ohjelmisto-, laitteisto- ja tietoliikenteen turvallisuus on tässä yhteydessä niputettu yhteen, sillä niistä selvitetään lähinnä yleistasoa. Nämä osa-alueet voivat olla hyvinkin tarkasti hoidettuja ja dokumentoituja, mutta kuten edellä on mainittu, ne eivät ole tämän työn ja kurssin kannalta keskeisessä roolissa. Kysymysten avulla selvitetään pääpiirteittäin, onko yrityksen tekninen tietoturvallisuus riittävällä tasolla hoidettu. Kysymykset on esitetty taulukossa 6.

Taulukko 6. Ohjelmisto-, laitteisto- ja tietoliikenteen turvallisuuteen liittyvät kysymykset

19. Onko työntekijöillä oikeus asentaa ohjelmia tietokoneilleen? Miten käytössä olevien ohjelmien ylläpito on organisoitu?
20. Mitä siirrettäviä medioita yrityksessä on lupa käyttää (esim. USB-muistit, CD, DVD)? Onko siirrettäviä medioita suojattu luvattomalta pääsyltä, väärinkäytöltä tai muuttumiselta? Miten?
21. Onko kannettavien tietokoneiden kovalevyjä salattu? Jos ei, niin miksi?
22. Kuinka virustarkastus on organisoitu yrityksessä (esim. ohjelmistot, päivitykset, tarkastettujen tiedostojen tyypit)?
23. Minkälaisia menetelmiä yrityksessä käytetään tietoliikenteen salaamiseen (esim. sähköpostin salausohjelmat, käytettävät salausprotokollat)? Valvotaanko näiden käyttöä?
24. Kuinka käyttäjien autentikointi (oikeaksi tunnistaminen) ulkopuolisista yhteyksistä on järjestetty?

Ohjelmistoturvallisuuden osalta kartoitetaan lähinnä sitä, miten vastuu ylläpidosta on jaettu. Vaikka tämä kuuluu osittain hallinnollisen turvallisuuden alle, on kysymys kuitenkin ryhmitelty ohjelmistoturvallisuuden kohdalle.

Laitteistoturvallisuuden kohdalla kartoitetaan lähinnä yleisiä toimintaperiaatteita, yksittäisiin suojausmenetelmiin ei ole tarkoituksenmukaista mennä muuta kuin esimerkin tasolla. Laitteistoturvallisuudessa aiemmin eniten puutteita on ollut kannettavien laitteiden käytön ohjeistuksessa ja salaamisessa. Kysymyksen tarkoituksena onkin herättää ajatuksia laitteiden merkityksestä. Tietoliikenteen turvallisuuteen liittyvien kysymysten kohdalla kysymykset johdattivat puhumaan tietoliikenteen turvallisuudesta yleisemminkin.

Fyysinen turvallisuus

Fyysisen turvallisuuden kohdalta kartoitetaan nimenomaan tietojen fyysistä käsittely- ja säilytysympäristöä ja sitä, miten sen turvallisuus on hoidettu. Esimerkiksi tulipalojen torjunnan kohdalla on tietenkin tärkeää huolehtia myös henkilöstön turvallisuudesta.

Tietoturvallisuudesta on todettu, että jos helpoin keino varastaa yrityksen tietoja on kävellä yritykseen sisään ja varastaa tietokone, on turvallisuus hoidettu hyvin. On kuitenkin tärkeää varmistaa, että em. toimenpiteen suorittaminen ei ole sekään helppoa. Siksi fyysinen turvallisuus on olennainen osa tietoturvallisuutta. Fyysistä turvallisuutta käsittelevät kysymykset on esitetty taulukossa 7.

Taulukko 7. Yrityksen fyysiseen turvallisuuteen liittyvät kysymykset

25. Onko toimitiloissa kulunvalvontajärjestelmä? Minkälainen? Kuinka toimitilan kulkuoikeudet ja -säännöt on määritelty? Käytetäänkö videovalvontaa, miten?
26. Onko henkilökunnalla kuvallisia henkilökortteja ja väliaikaisia kortteja vierailijoille? Jos ei, miten yrityksessä tunnistetaan henkilökunta ja vierailijat? Onko yrityksessä määritelty sääntöjä vierailijoita koskien?
27. Kuinka pääsy tietoturvallisuuden kannalta merkittäviin paikkoihin on järjestetty (esim. palvelinhuone)?
28. Kuinka tulipalon ja vesivahingon tunnistus, hälytys ja torjunta on järjestetty?

Vierailijakäytäntöjä ja vartiointia kartoitetaan juuri sen varalta, että joskus tietojen varastaminen yllä kuvatulla tavalla voi olla aivan liian helppoa. Jos kukaan ei kiinnitä huomiota yrityksessä itsevarmasti liikkuvaan vieraaseen, on ohjeistuksissa tai niiden noudattamisessa jotakin vikaa.

Fyysisen turvallisuuden kohdalla on tärkeää muistaa tietoteknisten laitteiden herkkyys normaaleille sammutustoimenpiteille ja tämän huomioonottamista selvitetään tulipalon- ja vesivahingon torjuntaa kartoittavilla kysymyksillä. Aikaisempina vuosina etenkin pienissä yrityksissä fyysisessä turvallisuudessa on ollut puutteita, jotka ovat olleet korjattavissa hyvin yksinkertaisin toimenpitein.

Tietoaineisto- ja käyttöturvallisuus

Tietoaineisto- ja käyttöturvallisuus ovat hyvin läheisiä osa-alueita, joten ne on tässä yhteydessä niputettu yhteen. Molempiin liittyvät kysymykset on listattu taulukossa 8.

Taulukko 8. Tietoaineisto- ja käyttöturvallisuus

29. Onko yrityksessä määritelty politiikka tietojärjestelmiin pääsylle? (esim. käytetäänkö henkilökohtaista käyttäjätunnusta ja salasanaa?)
30. Minkälainen salasanapolitiikka yrityksessä on? Miten sen noudattamista

valvotaan?
31. Kuinka tieto on luokiteltu (luokittelulutapa, kuinka käsitellään, hävittäminen jne.)? Onko lajittelutapa dokumentoitu?
32. Onko työntekijöiden pääsyoikeuksia rajoitettu vain heidän työtehtävissään tarvitsemiin tietoihin? Onko henkilöstön tehtävien jaossa kiinnitetty huomiota turvattomiin/vaarallisiin työyhdistelmiin?
33. Onko tiedoilla ja tietojärjestelmillä nimetty vastuuhenkilö? (tiedon/järjestelmän omistaja). Jos vastuuhenkilöä ei ole, kuvaile korvaavia toimintatapoja.
34. Minkälainen varmuuskopiointipolitiikka yrityksessä on? Miten varmuuskopiointi on käytännössä organisoitu? Missä varmuuskopioita säilytetään?

Näistäkin kysymyksistä on löydettävissä hallinnolliseen turvallisuuteen liittyviä piirteitä, mutta kysymykset on kuitenkin selvyyden vuoksi ryhmitelty omien osa-alueidensa alle. Myös näiden kysymysten kohdalla on syytä huomata, että yrityksessä voi olla olemassa politiikka esimerkiksi salasanojen suhteen, vaikka sitä ei olisi kirjallisesti dokumentoitu.

Liiketoiminnan jatkuvuus ja riskienhallinta

Liiketoiminnan jatkuvuuden suunnittelu on tärkeää, vaikka muut tietoturvallisuuden osa-alueetkin osaltaan vaikuttavat liiketoiminnan jatkuvuuden turvaamiseen poikkeustilanteissa. Tämän työn yhteydessä liiketoiminnan jatkuvuus ja riskienhallinta on kuitenkin haluttu nostaa omaksi osa-alueekseen esille. Näihin asioihin liittyvät kysymykset on kuvattu taulukossa 9.

Taulukko 9. Liiketoiminnan jatkuvuuden suunnitteluun ja riskienhallintaan liittyvät kysymykset

35. Millä tavalla yrityksessä arvioidaan tietoturvallisuuteen liittyviä riskejä? Kuka niitä arvioi? Kuinka usein?
36. Kuvaile menettelytapoja liiketoiminnan jatkuvuuden varmistamiseksi ongelma/häiriötilanteissa (esim. liiketoiminnan jatkuvuussuunnitelma, suunnitelma onnettomuustilanteista selviämiseksi, onko varahenkilöitä avainhenkilöiden tilalle)
37. Käytetäänkö agenttien, jällenmyyjien, alihankkijoiden tai yhteistyökumppaneiden kanssa salassapitosopimuksia (non-disclosure agreement)?
38. Miten yrityksenne käsityksestä tietoturvallisuudesta viestitään asiakkaille ja toimittajille?

Liiketoiminnan jatkuvuuden suunnittelusta kysytään varsin suoraan, mutta hyvin laajalla kysymyksellä. Vastauksesta käy näin laajan kysymyksen avulla ilmi, mitä

liiketoiminnan jatkuvuuden suunnittelulla yrityksessä ymmärretään ja se, miten tämä asia on yrityksessä hoidettu.

3.4 Aineiston analyysi

Haastatteluaineistoa käsitellään kokonaisuutena, jota analysoidaan vertaillen ja kategorisoiden vastauksia. Osa kysymyksistä on on/ei/eos –tyyppisiä, joiden perusteella voidaan luoda määrällistä tietoa kuvaajien avulla. Toisten kysymysten kohdalla vastaukset ovat niin erilaisia, että niistä on etsitty yhteisiä tai eroavia piirteitä, eikä raportointi onnistu graafisesti.

Haastatteluaineistosta osa on litteroitu analyyseja varten. Varsinaista keskusteluanalyysia, jossa analysoidaan vastausten sisällön lisäksi niiden esittämistapaa ja keskustelua haastattelijan kanssa (Peräkylä 2005, s.875) aineistosta ei tehdä, jonka vuoksi haastattelujen täydellinen litterointi ei ollut tarpeen. Litterointien yhteydessä aineisto anonymisoitiin, eli yksittäisen vastauksen viittaukset haastateltavan yritykseen poistettiin. Näin vastauksia voidaan säilyttää pitempään kuin yrityskohtaista aineistoa ja niitä voidaan käyttää vertailuaineistona mahdollisissa jatkotutkimuksissa.

Aineiston analysointi tehdään kysymys kerrallaan niin pitkälle kuin se on mahdollista. Välittömästi haastattelujen jälkeen tutkimuksen tekijä purki haastattelun aikana tehdyt muistiinpanot auki haastattelunauhan tukemana. Nämä muistiinpanot purettiin kysymys kerrallaan niin, että eri yritysten vastaukset eri kysymyksiin olivat nähtävissä kerralla. Analyysi tapahtui kirjoitusprosessin myötä.

Tulokset esitellään osin kysymyskohtaisesti, osin kysymyksiä yhdistellen. Varsinainen aineiston analyysi on tehty tutkimuskysymysten pohjalta niin että hallinnollinen turvallisuus on keskeisimmässä roolissa. Muidenkin osa-alueiden alle ryhmitellyt kysymykset kartoittavat myös hallinnollisen turvallisuuden tilannetta. Pääosin analyysissa on keskitytty yleistilan analysointiin, mutta joidenkin kysymysten kohdalla vastausten yksityiskohtaisuus on antanut mahdollisuuden tarkempaan analyysiin ja parannusehdotusten pohtimiseen.

4 AUDITOINTIEN TULOKSET

Tässä luvussa käydään läpi luvussa 3 esiteltyjen auditointihaastatteluiden tulokset pääosin kysymyskohtaisesti. Luvussa 3.2.1 esitellyt taustatietokysymykset kartoittavat yrityksen taustaa lähinnä Tietoturvallisuuden johtaminen –kurssilla harjoitustöinä tehtyjä auditointiraportteja varten. Taustakysymyksien osalta tässä tutkimuksessa käsitellään ainoastaan sitä, miten haastateltavat määrittelevät käsitteen tietoturvallisuus sekä miten yrityksissä on tunnistettu minkälaista tietoa niissä käsitellään.

4.1 Tietoturvallisuuden määrittely sekä käsiteltävät tiedot

Tietoturvallisuuden ytimekäs määrittely oli haastateltavien mielestä vaikea tehtävä. Tämä ei liene yllätys ottaen huomioon että tässäkin tutkimuksessa luvussa 2 on käytetty yli 20 sivua käsitteen sisällön jäsentämiseen ja määrittelyyn. Lähes kaikissa vastauksissa oli esillä tiedon luottamuksellisuuden takaaminen tietoturvallisuuden keskeisimpänä tehtävänä. Yrityksissä nähtiin, että koska niissä käsitellään paljon esimerkiksi asiakkaita koskevia henkilötietoja tai tuotekehitystietoja, näiden tietojen luottamuksellisuuden turvaaminen on yrityksen liiketoiminnan kannalta tärkeintä. Vastauksista esille nousevat teemat ja niiden esiintyminen on kuvattu taulukossa 10.

Taulukko 10. Tietoturvallisuuden määrittelyn teemat yrityksissä

Tietojen luottamuksellisuuden säilyttäminen	Tietotekniikkaan ja tietoliikenneyhteyksiin liittyvä turvallisuus	Vastuunjako ja henkilöstön toiminnan vaikutus
x	x	x
x	x	
x	x	
x	x	
	x	
x	x	x
x	x	
x	x	
x	x	
x	x	
x	x	
x	x	
x	x	x
x		
x		
x		x

Neljässä vastauksessa tulee esiin selkeästi henkilöstön toiminnan ja vastuunjaon merkitys tietoturvallisuudelle. Henkilöstön osuutta tietoturvan toteuttajina ei

varsinaisesti mainita muissa vastauksissa, mutta rivien välistä voidaan tulkita, että tietoturvallisuus on näissäkin yrityksissä tärkeä asia, eikä sitä nähdä pelkästään teknisenä asiana. Ainoastaan yhdessä haastattelussa haastateltava määritteli tietoturvallisuuden aluksi lähinnä tietojen tekniseen säilyttämiseen liittyvänä asiana. Haastattelun jatkuessa kävi kuitenkin ilmi, ettei alun tekninen määritelmä vastannut yrityksen koko käsitystä tietoturvallisuudesta, vaan muitakin näkökulmia oli jo otettu huomioon.

Yllättävästi kaikista vastauksista ei tekninen turvallisuus nouse konkreettiseksi teemaksi. Näissä vastauksissa keskityttiin tietojen luottamuksellisuuden korostamiseen. Voidaan kuitenkin tulkita, että myös näissä yrityksissä tekniset ratkaisut koettiin osaksi luottamuksellisuuden turvaamista. Tietojen luottamuksellisuuden turvaaminen onkin lähinnä yleistason teema, jonka moni vastaaja on tarkoittanut johdannoksi tietoturvallisuuden merkityksen pohtimiseen. Joissakin yrityksissä vastauksen keskeinen sisältö kuitenkin oli, että tietoturvallisuus tarkoittaa luottamuksellisten tietojen säilyttämistä luottamuksellisina.

Yhdessä yrityksessä tietoturvallisuuden määrittely johti haastateltavaa pohtimaan, että tietoturvallisuus on itse asiassa kompromissi riittävän tietojen suojaamisen ja liiketoiminnan mahdollistamisen välillä. Haastateltava koki, että mikäli tiedot on täysin turvattu, ei niitä voi käyttää liiketoiminnan pohjanakaan.

Yrityksissä oli pohdittu minkälaista tietoa niissä käsitellään. Tärkeimpänä suojauskohteena mainittiin asiakkaisiin liittyvät tiedot, jotka sisälsivät niin asiakkaiden henkilötietoja kuin projektitietoja. Lisäksi omaan tuotekehitykseen liittyvät tiedot mainittiin tärkeinä. Suurin osa yrityksistä oli myös tunnistanut, että päivittäisessä toiminnassa syntyy yrityksen tilaa koskevaa tietoa esimerkiksi kirjanpitotietojen muodossa, vaikka näitä ei ensimmäisenä koettu tietoturvallisuuden kannalta tärkeiksi tiedoiksi.

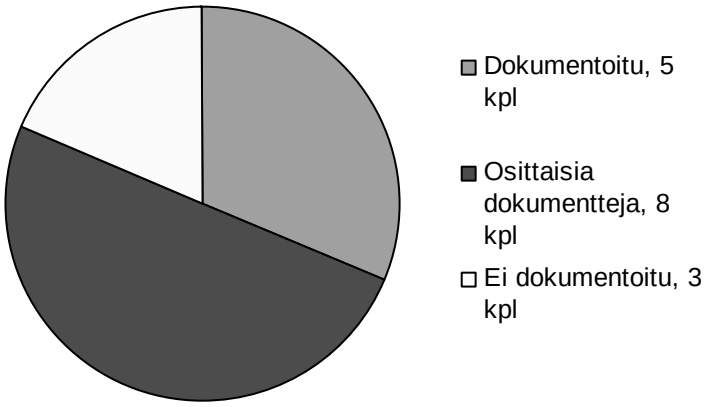
4.2 Hallinnollinen turvallisuus

Hallinnolliseen turvallisuuteen liittyvät haastattelukysymykset käsittelivät tietoturvallisuuspolitiikan tai –ohjeistusten olemassaoloa sekä tietoturvallisuuden vastuunjakoa. Lisäksi kartoitettiin, millä keinoilla yritykset valvovat politiikan ja ohjeiden noudattamista, sekä millä tavalla tietoturvallisuutta arvioidaan yrityksissä.

Tietoturvallisuuspolitiikka

16:sta yrityksestä viidessä oli dokumentoitu tietoturvallisuuspolitiikka. Lisäksi kahdeksassa yrityksessä oli tietoturvallisuuden perusperiaatteita dokumentoituna tai

muuten toimintaa erittäin voimakkaasti ohjaavat kirjoittamattomat säännöt toimintatavoista. Tietoturvallisuuspolitiikan dokumentoinnin tilannetta on kuvattu kuvassa 12.



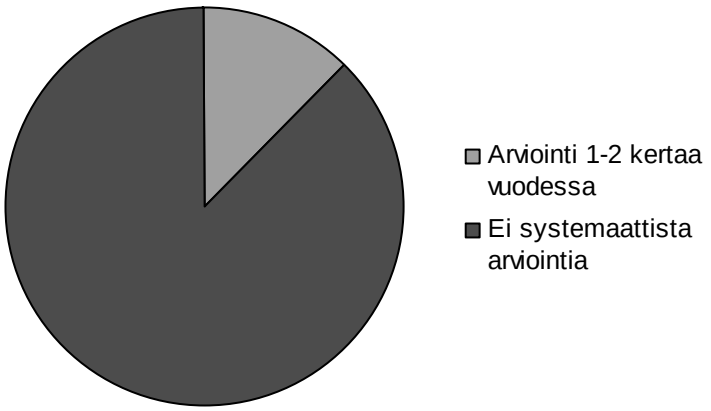
Kuva 12. Tietoturvallisuuspolitiikan dokumentointi tutkituissa yrityksissä

Tietoturvallisuuspolitiikkadokumentin laajuus vaihteli parista sivusta varsin laajaan ohjeistuspakettiin. Yhdessä yrityksessä tietoturvallisuuspolitiikan tekemiseen oli hiljattain panostettu. Prosessi oli havaittu varsin työlääksi ja päivityksiä vaivalla tehtyyn dokumenttiin aiottiin tehdä erittäin säästeliäästi. Toisessa yrityksessä olemassa oleva tietoturvallisuuspolitiikka itsessään oli havaittu liian raskaaksi ja hankalaksi noudattaa ja sen päivitys oli suunnitteilla. Yrityksissä, joissa ei ollut varsinaista tietoturvallisuuspolitiikkaa asiaa ei oltu lähestytty kokonaisvaltaisesti. Käytössä olevat ohjeistukset ja toimintaperiaatteet koskivat joko henkilötietojen käsittelyä ja pohjautuivat tietosuojalakiin, tai ohjeistivat tietoteknisten välineiden turvalliseen käyttöön.

Tietoturvallisuuspolitiikat sisälsivät tietoturvallisuuden vastuiden määrittelyn. Näiden viiden yrityksen lisäksi neljässä yrityksessä oli tehty selvä vastuunjako tietoturvallisuuden suunnittelun ja käytännön toteutuksen suhteen. Teknisistä tietoturvaratkaisuista ja varsinkin niiden ylläpidosta vastasivat henkilöt, jotka muutenkin vastaavat tietotekniikasta, esimerkiksi ATK-tukihenkilö tai IT-toimittajan edustaja. Lopuissa yrityksistä vastuunjako ei ollut yhtä selkeä, vaan todettiin, että johto vastaa suunnittelusta ja toteutumisesta. Työntekijöiden vastuu käytännön tietoturvallisuustoimien toteutumisesta mainittiin suurimmassa osassa vastauksista.

Arviointi ja valvonta

Sisäistä arviointia tehtiin säännöllisesti kahdessa yrityksessä. Toisessa laatukäsikirjan edellyttämän vuosittaisen arvioinnin yhteydessä, toisessa tietoturvavastaava arvioi tilannetta pari kertaa vuodessa. Muissa yrityksissä sisäistä arviointia ei tehty. Tilanne on kuvattu kuvassa 13. Arviointiprosessin kehittäminen nähtiin vaikeaksi. Teknisten ratkaisujen osalta todettiin, että tietoturvatarvetta arvioidaan tarpeen mukaan, yleisin esimerkki oli Windows-käyttöjärjestelmän tietoturvapäivitystarpeen seuraaminen, joka haastattelujen aikaan oli paljon julkisuudessa.



Kuva 13. Tietoturvallisuuden arvioinnin järjestäminen

Tietoturvallisuuspolitiikan ja –ohjeistusten valvominen koettiin tutkituissa yrityksissä pääosin hankalaksi kuten sisäisten arviointienkin tekeminen. Miltei kaikissa yrityksissä todettiin, että valvonta toteutuu lähinnä päivittäisen työnjohdon myötä ja että vakavien rikkomusten uskotaan tulevan ilmi ilman systemaattista valvontaakin. Päivittäisvalvonnan puitteissa esimerkiksi ohjeiden vastaisista toimintatavoista pyrittiin huomauttamaan. Erityisesti kotona tapahtuvan työskentelyn valvonta katsottiin käytännössä mahdottomaksi. Monissa tilanteissa tietoturvallisuuden toteutuminen on kiinni ainoastaan henkilöstön toiminnasta, jolloin systemaattisen tietoturvallisuuden valvonnan toteuttaminen on hankalaa ilman jokaisen henkilön olkapään takana seisovaa ”poliisia”.

4.3 Henkilöstöturvallisuus

Henkilöstöturvallisuuteen liittyvät kysymykset käsittelivät työntekijöille tarjottavaa tietoturvallisuuskoulutusta sekä keinoja, joilla tietoturvallisuustietoutta pidetään yllä. Lisäksi henkilöturvallisuuteen liittyy työsuhteen elinkaareen kuuluvat toimenpiteet,

kuten rekrytointivaiheen taustantarkistukset ja turvallisuustoimet työsuhteen aikana sekä sen päättyessä.

Tietoturvallisuustietoisuus ja -koulutus

Henkilöstön tietoturvallisuustietoutta pidetään yrityksissä yllä lähinnä ajankohtaisista asioista sähköpostitse tiedottamalla. Tietoturva-asiat voivat olla esillä esim. viikkopalavereissa tai vastaavissa mikäli tähän on tarvetta. Lähinnä ajankohtaiset asiat joista on tärkeää tiedottaa liittyvät teknisestä tietoturvallisuudesta huolehtimiseen, esimerkkeinä käyttöjärjestelmien turva-aukoista tiedottaminen ja virussuojauksen toimivuuden varmistaminen. Varsinaisia tietoturvallisuuskoulutuksia tai järjestelmällistä tietoturvallisuustietoisuuden ylläpitoa yrityksissä ei järjestetty. Suurin osa yrityksistä kuitenkin tiedosti, että tietojen salassapito ja turvaaminen on yritykselle imagokysymys ja siksi erittäin tärkeää. Tämän ymmärtäminen oli kaikille yrityksille olennaista ja sitä myös korostettiin työntekijöille.

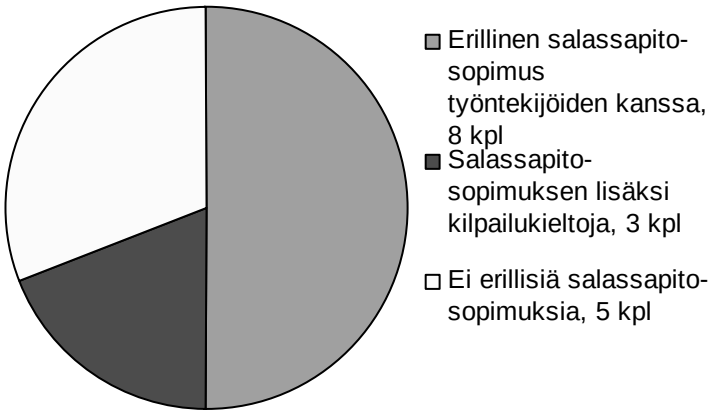
Ainoa tietoturvallisuuteen liittyvä koulutus mitä yrityksissä tarjottiin oli perehdytysvaiheessa tapahtuva tutustuminen tekniseen toimintaympäristöön. Yrityksissä joissa oli dokumentoitu tietoturvallisuuspolitiikka tai dokumentoituja ohjeistuksia, ohjeistuksiin tutustuminen oli osa perehdytystä. Muissakin yrityksissä perusasiat käytiin läpi työhön tutustumisen yhteydessä. Kolmessa yrityksessä todettiin että tarvetta laajemmalle ja systemaattiselle tietoturvakoulutukselle olisi. Yhdessä yrityksessä koulutuksen suunnittelu nähtiin erittäin vaikeaksi työntekijöiden koulutustaustan takia. Tässä yrityksessä haastateltava koki, että korkeasti koulutetut tietotekniikan ammattilaiset eivät olisi motivoituneita osallistumaan tietoturvallisuuskoulutukseen.

Työsuhteeseen liittyvät asiat

Uutta työntekijää rekrytoidessaan yritykset eivät pääsääntöisesti tee työntekijöiden rikostaustojen tarkistuksia. Suurin osa yrityksistä tarkastaa suosittelijoiden lausunnot työntekijästä, mikäli suosittelijoita on käytetty. Edelliseen työnantajaan otetaan myös mahdollisesti yhteyttä joissakin yrityksissä. Yhdessä yrityksessä tehdään rekrytoitavista SUPOn taustantarkistus, mikäli tarkistus on tehtävän kannalta tarpeellinen. Koulutustaustan oikeellisuus tarkistetaan joissakin yrityksissä, mikäli on syytä epäillä rekrytoitavan antaneen virheellisiä tietoja.

Kaikissa yrityksissä huolehdittiin työntekijöiden salassapitovelvoitteesta. Yritysten tilanne on kuvattu kuvassa 14. Yksitoista yritystä teki työntekijöiden kanssa joko erillisen salassapitosopimuksen tai salassapitositoumuksen työsopimuksen yhteydessä. Viisi yritystä tukeutui työsopimuslain tai alan ammattisääntöjen salassapitovelvoitteisiin, eikä erillisiä sopimuksia tai mainintoja työsopimukseen ollut

tehty. Osassa yrityksiä yleisen salassapitosopimuksen lisäksi tehtiin vielä projektikohtaisia salassapitositoumuksia. Salassapitosopimusten kestot ja sisältö vaihtelivat tehtävän ja sopimuksen tarkoittaman tiedon mukaan. Kolmessa yrityksessä mainittiin että myös kilpailukieltosopimuksia tehdään tehtävänkuvasta riippuen.

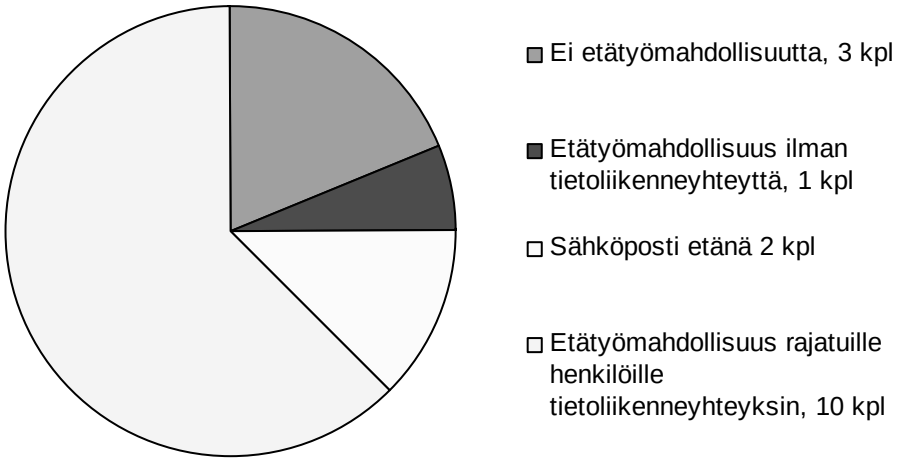


Kuva 14. Salassapitosopimustilanne yrityksissä

Työnsuhteen päättyessä hoidettavia toimintoja oli dokumentoitu kuudessa yrityksessä. Dokumentointi pyrki enemmänkin takaamaan fyysisen turvallisuuden, eli toimitilan avaimet ja kulkuoikeudet otettiin pois. Lisäksi dokumenteissa oli tarkistuslistoja henkilöstöhallinnon asioista jotka pitää hoitaa työsuhteen päättyessä. Yrityksissä, joissa dokumentoituja ohjeita ei ollut pyrittiin samoihin toimenpiteisiin, eli fyysinen pääsy toimitiloihin suljettiin sekä tietojärjestelmien käyttäjätunnukset suljettiin. Joissakin yrityksissä muistutettiin allekirjoitettujen salassapitosopimusten ja kilpailukieltojen olemassaolosta myös työsuhteen päätyttyä. Jos henkilöllä on hallussaan yrityksen materiaaleja tulee ne luovuttaa pois työsuhteen päättyessä kaikissa yrityksissä. Haastateltavat kokivat vaikeaksi valvoa esimerkiksi paperimateriaalien palauttamista, sillä materiaaleista pidetään harvoin kirjaa.

Etätyöskentely

Suhtautuminen etätyöskentelyyn vaihteli yrityksissä jonkin verran. Eri etätyöskentelymuodot on kuvattu kuvassa 15. Kolmessa yrityksessä etätyöskentelyä ei tehty, kahdessa näistä etätyö oli toimialan takia hankalaa. Kolmannessa yrityksessä tietoliikenneyhteyksiä etätyöskentelyyn ei tarjottu, mutta kannettavalla tietokoneella oli mahdollisuus työskennellä myös etänä. Kahdessa yrityksessä vain sähköpostin lukeminen etänä oli mahdollista, muita yhteyksiä etätyöskentelyyn ei tarjottu. Lopuissa yrityksissä etätyöskentely oli mahdollista, mutta suurimmassa osassa vain rajatulle määrälle henkilöitä. Etäyhteydet oli toteutettu VPN-tekniikoilla tai muuten salatuilla yhteyksillä.



Kuva 15. Etätyöskentelykäytännöt yrityksissä

Yleisesti etätyöksi mielletään työskentely kotona, joka kuvastuu myös valtaosasta haastateltavien vastauksia. Useiden yritysten kohdalla työskentelyä tapahtuu kuitenkin esimerkiksi asiakkaiden tiloissa, jolloin voidaan myös puhua etätyöskentelystä. Tietoliikenneyhteyksien tarjoaminen yrityksen palvelimille tuntui olevan usein etätyöskentelymahdollisuuden määritelmä. Useammassa yrityksessä asiaa tarkemmin tiedusteltaessa kävi kuitenkin ilmi, että myös henkilöt joille tietoliikenneyhteyttä ei tarjota voivat etätyöskennellä käyttämällä esimerkiksi kannettavaa tietokonetta tai ottamalla työhön liittyviä paperidokumentteja mukaansa.

4.4 Ohjelmisto-, laitteisto- ja tietoliikenteen turvallisuus

Ohjelmisto- laitteisto- ja tietoliikenteen turvallisuus ovat kaikki varsin teknisiä osa-alueita, joten kysymykset koskivat lähinnä työntekijöiden oikeuksia ja vastuita näihin osa-alueisiin liittyen. Kysymykset käsittelivät oikeuksia ohjelmien asentamiseen sekä kannettavien laitteiden käyttöä ja virustorjuntaa. Tietoliikenneyhteyksien hoitoa kartoitettiin varsin pintapuolisesti.

Tietotekniikkaympäristön ylläpito oli neljässätoista yrityksessä hoidettu keskitetysti. Päivityksistä vastasi joko yrityksen oma ATK-tuki tai ulkopuolinen yritys, jolle ylläpito oli ulkoistettu. Kahdessa yrityksessä työntekijät itse olivat vastuussa käytössä olevien ohjelmien päivityksestä. Kahdeksassa yrityksessä työntekijöillä on mahdollisuus asentaa ohjelmia tietokoneilleen huolimatta siitä, että kuudessa näistä ohjelmistoympäristön ylläpito hoidettiin keskitetysti. Kaikissa näissä yrityksissä sallitut ohjelmat on kuitenkin rajoitettu työn kannalta tärkeisiin ohjelmiin. Käytännössä joissakin yrityksissä koneilta on löytynyt muitakin kuin työssä tarvittavia ohjelmia.

Kannettavat tietokoneet ja siirrettävät tallennusvälineet

Siirrettävien medioiden käyttöä ei ole rajoitettu suurimmassa osassa yrityksiä. Neljässä yrityksessä siirrettäviä medioita, lähinnä USB-muistitikkuja, salataan ajoittain mikäli niillä kuljetetaan luottamuksellista tietoa. Suurimmassa osassa yrityksiä siirrettäviä medioita ei käytetä toimintaan liittyvän tiedon, vaan lähinnä työntekijöiden henkilökohtaisten tiedostojen, siirtämiseen, jolloin tikkujen sisällöstä huolehtiminen ja salaaminen on työntekijöiden vastuulla. Salassapitovelvoitteet kieltävät useimmissa yrityksissä salaisen tiedon viemisen turhaan pois yrityksen tiloista. Tämän käytännön valvominen koettiin erittäin hankalaksi.

Kannettavia tietokoneita on yrityksissä käytössä vaihtelevasti. Pääosin vain johtavassa tai muuten vastuullisessa asemassa olevilla on käytössään työkannettava. Kahdessa yrityksessä kannettavien tietokoneiden kovalevyt oli salattu ja kolmessa salausta oltiin suunnittelemassa tai ottamassa käyttöön. Lopuissa yrityksissä koneelle kirjautumiseen vaadittavat käyttäjätunnus ja salasana katsottiin riittäväksi suojaukseksi. Salauksen todettiin olevan myös riski esimerkiksi kovalevyn rikkoutumisen yhteydessä.

Virustorjunta ja tietoliikenneyhteydet

Kaikissa yrityksissä oli käytössä automaattisesti päivittyvä virustorjuntaohjelmisto, joka on koko ajan päällä. Yhdessä yrityksessä eri koneilla oli eri virustorjuntaohjelmistoja, mutta kirjavasta tilanteesta oli tavoitteena siirtyä keskitetympään ratkaisuun lähiaikoina. Tässäkin yrityksessä kaikki koneet oli kuitenkin suojattu viruksia vastaan.

Kuten jo teoriaosuudessa (luku 2.3) todettiin, virustorjunnan hoitaminen on jo perusedellytys toimimiselle julkisessa verkossa. Tältä pohjalta oli odotettavissa, että virustorjunta on hoidettu kaikissa yrityksissä hyvin. Virustorjunnan apuvälineinä toimivat virustorjuntaohjelmistojen lisäksi palomuurit, jotka estävät esimerkiksi verkkomatojen pääsyn tietokoneelle. Kaikissa yrityksissä oli käytössä ainakin ohjelmallinen palomuuri, useissa yrityksissä sekä verkkopalvelun tarjoajan palomuuri että lisäksi omat palomuurit. Lisäksi viruksiin liittyvät asiat olivat niitä, joista useimmiten tiedotettiin henkilöstölle ajankohtaisina asioina, joten myös henkilöstön tietoisuus virustorjunnasta oli hyvällä tasolla.

Kuten luvussa 4.3 todettiin, osassa yrityksistä etätyöskentely oli mahdollista VPN-yhteyden avulla. Myös esimerkiksi asiakkaille päin suunnattuja yhteyksiä oli toteutettu VPN-tekniikoilla. Salatun yhteyden muodostamiseen ulkopuolelta yrityksen palvelimelle käytettiin yleensä käyttäjätunnusta ja salasanaa. Kahdessa yrityksessä pääsy tapahtui etäkäytössä olevan tietokoneen IP-numeron ja jo kirjautuneen käyttäjän tunnuksen avulla. Yhdessä yrityksessä oli käytössä HST-kortti tunnuksen ja salasanan

lisäksi. Yrityksillä oli käytössä palomuureja, joiden avulla pääsyä palvelimille valvottiin. Palomuurien olemassaoloa ja konfigurointia ei kuitenkaan käsitelty kaikissa haastatteluissa.

4.5 Fyysinen turvallisuus

Fyysisen turvallisuuteen liittyvillä kysymyksillä kartoitettiin yritysten toimitilojen kulkuoikeuksia sekä käytäntöjä vierailijoiden suhteen. Lisäksi pohdittiin esimerkiksi palvelinlaitteistojen sijoittamista sekä tulipalon ja vesivahinkojen torjuntaa.

Kulunvalvonta ja vierailijasäännöt

Yhdessätoista yrityksessä oli jonkunlainen kulunvalvontajärjestelmä käytössä. Osassa kulunvalvonta koski vain yrityksen toimitilojen pääovea, isommissa yrityksissä myös väliovissa oli kulunvalvontalaitteita. Kulunvalvonta oli toteutettu yleisimmin kulkukorteilla tai –napeilla, kahdessa yrityksessä oli käytössä sormenjälkitunnistin. Yrityksissä, joissa ei ole kulunvalvontaa käytössä, työntekijöillä on käytössään avaimet, joilla toimitiloihin pääsee. Myös yrityksissä, joissa on kulunvalvonta työtiloja oli avaimen takana. Kolmessa yrityksessä ei ollut toimitilojen sisällä lukittavia työtiloja, vaan ainoa lukko oli ulko-ovessa. Muissa yrityksissä pääsyä eri tiloihin oli porrastettu työntekijöiden tarpeen mukaan.

Fyysisten tilojen suojaustaso vaihtelee paljon sen mukaan, minkälaisessa rakennuksessa yrityksen tilat sijaitsevat. Tutkitut yritykset olivat sen verran pieniä, että ainoastaan yhdellä yrityksellä oli oma toimitalo, jota ei ollut jaettu muiden yritysten tai yksityishenkilöiden kanssa. Jos toimitaan uudehkoissa useiden yritysten käyttöön tarkoitetuissa toimistotiloissa, on kulunvalvonta sekä muu fyysinen suojaus hoidettu yleensä kiinteistön puolesta hyvin ja kulunvalvonta toimii seurantana siitä, kuka yrityksen tiloihin on tullut ja milloin. Osassa yrityksiä kulunvalvontaa ei kuitenkaan ole, vaikka tarvetta vastaavalle fyysiselle turvallisuudelle, kuin muissa tutkimuksen yrityksissä, olisikin.

Useissa auditoiduissa yrityksissä fyysinen murtosuojaus rajoittui toimitilojen pääoveen. Yksittäiset työhuoneet eivät usein olleet lukittavia ja lukollisia kaappeja asiakirjojen säilytykseenkin käytettiin yllättävän vähän. Yrityksissä käsiteltiin kuitenkin hyvinkin arkaluonteisia tietoja erityisesti asiakkaita koskien. Tästä näkökulmasta katsottuna fyysisessä turvallisuudessa oli huomattavastikin parantamisen varaa, vaikkakin lukkojen lisäämisen kohteet tulee jokaisessa yrityksessä päättää yrityskohtaisen riskianalyysin perusteella. Osassa yrityksiä kulkusäännöt ja –oikeudet oli hoidettu hyvinkin tiukasti ja tiedot olivat tältä osin erittäin hyvin suojattuja.

Neljässä yrityksessä oli käytössä kuvalliset henkilökortit, yhteen näistä kortit oli juuri tilattu. Henkilökortit koettiin tärkeiksi myös vierailtaessa asiakkaiden luona. Yhden yrityksen kohdalla henkilökortteja käytettiinkin juuri vierailtaessa asiakkaiden ja yhteistyökumppaneiden luona, ei niinkään omissa tiloissa. Yhdessä yrityksessä oli käytössä vierailijakortit ja toisessa yrityksessä vierailijat kirjattiin, mutta kortteja ei ollut käytössä. Kaikissa yrityksissä oli käytäntö, ettei vierailijoita pitäisi jättää yksin ja että heidät ohjataan neuvottelutiloihin. Vierailijakorttien puutetta perusteltiin juuri sillä, että vieraita ei jätetä yksin. Haastateltavien mukaan kaikki työntekijät tuntevat toisensa ja ylimääräiset henkilöt kyllä huomataan.

Hälytysjärjestelmät ja palvelinten suojaus

Suurimmassa osassa yrityksiä oli käytössä vartiointiliikkeen hälytysjärjestelmä, joka oli päällä, mikäli kukaan ei ollut paikalla. Suurimmassa osassa yrityksiä työntekoaikoja ei ollut rajoitettu, eli hälytysjärjestelmien koodit olivat tiedossa valtaosalla työntekijöistä. Sääntöjä eri vuorokauden aikoihin liikkumisesta oli käytössä, eli vaikka töitä olikin lupa tehdä vaikka yöllä, pääsääntöisesti yritysten tiloihin ei saanut tuoda vierailijoita virka-ajan ulkopuolella. Hälytysjärjestelmät toimivat samalla tulipalon tunnistus- ja hälytysjärjestelminä. Tulipaloihin ei pääsääntöisesti ollut varauduttu muuten kuin hälyttimin ja mahdollisesti automaattisammutuksella, jos semmoinen kiinteistön puolesta oli olemassa. Vesivahinkoihin oli varauduttu nostamalla laitteita pois lattialta, mutta kaikissa yrityksissä tätä ei oltu huomioitu. Videovalvonta oli käytössä kuudessa yrityksessä, mutta tarvetta nauhojen käytölle ei ollut ilmennyt ja osin käyttö oli satunnaista.

Tietoturvallisuuden kannalta merkittäviä paikkoja ovat tietointensiivisissä yrityksissä kaikki toimitilat, joissa säilytetään työhön liittyviä materiaaleja. Erityishuomio kohdennettiin palvelinten säilyttämiseen, sillä useimmissa yrityksissä oli käytössä verkkolevytalletus, eli tiedot talletettiin palvelimille pöytäkoneiden sijasta tai lisäksi. Palvelinten sijoittelu oli kirjavaa. Osassa yrityksiä palvelin oli kahvitilan tai siivouskomeron lattialla. Osassa yrityksiä palvelin oli sijoitettu asianmukaiseen telineeseen tai hyllylle lukittuun ja ilmastoituun huoneeseen. Lukollisia kaappeja tärkeiden papereiden säilytykseen oli käytössä suurimmassa osassa yrityksiä. Puhtaan pöydän politiikka oli käytössä joissakin yrityksissä, mutta paperimateriaalien säilytyssääntöjä ei käsitelty tarkemmin kaikissa haastatteluissa.

Kuten edellä kuvatusta huomataan, fyysisen turvallisuuden huomiointi esimerkiksi tietojenkäsittelylaitteiden sijoittelussa oli kirjavaa. Yrityksissä, joissa työskenteli myös tietotekniikka-alan ammattilaisia, koneiden sijoittelu oli hoidettu asianmukaisesti. Yrityksissä, joissa osaaminen kohdistui muille aloille, tietotekniset välineet olivat enemmän vain välttämättömiä välineitä työn suorittamiseksi, jolloin niiden turvallinen

sijoittaminen oli jäänyt vähemmälle huomiolle, tai esimerkiksi lattiatasoon asettamiseen liittyviä riskejä ei ollut tiedostettu.

4.6 Tietoaineisto- ja käyttöturvallisuus

Tietoaineistoturvallisuuden yhteydessä kartoitettiin sitä, miten yritykset luokittelevat tärkeitä tietojaan, sekä miten eri tavoin luokiteltuja tietoja käsitellään. Lisäksi kysymykset selvittivät käyttöoikeuspolitiikkaa sekä salasanojen ja käyttäjätunnusten käyttöä yrityksissä, varmuuskopiointia, sekä tietojen vastuuhenkilöiden määrittelyä.

Pääsyoikeudet ja tietojen luokittelu

Kolmessatoista yrityksessä tietokoneille ja tietojärjestelmiin pääsyyn vaadittiin henkilökohtainen käyttäjätunnus ja salasana. Kolmessa yrityksessä salasanat olivat konekohtaisia ja koneen vieressä näkyvillä. Osittain samalla salasanalla pääsi kaikkiin käytössä oleviin järjestelmiin, osittain eri järjestelmät vaativat omat tunnuksensa ja kirjautumisensa jolloin käyttöoikeus määriteltiin henkilön työnkuvan mukaan. Salasanapolitiikkoja yrityksissä joissa käytetään henkilökohtaisia käyttäjätunnuksia on havainnollistettu taulukossa 11. Yritykset on esitetty taulukossa satunnaisessa järjestyksessä.

Taulukko 11. Yritysten salasanapolitiikat henkilökohtaisen salasanan suhteen

Salasana muidenkin tiedossa	Salasanan muotovaatimukset	Säännöllinen vaihtoväli	Koneellinen valvonta	Muu valvonta
	x	2 kk		
	x	6 kk	x	
x	x	ei		x
	x	n. 6 kk	x	
	x	ei		
x	x	ei		x
	x	3 kk	x	
	x	tulossa	x	
(x)	x	ei		
	ei	ei		
	x	ei	x	
	x	3 kk	x	
	x	3 kk	x	

Kahdessa yrityksessä salasanat määriteltiin yhden henkilön toimesta, jolla oli hallussaan lista kaikkien työntekijöiden tunnuksista ja salasanoista. Yhdessä yrityksessä tiedettiin että työntekijät jakoivat salasanojaan keskenään esimerkiksi sairaus- tai lomatilanteissa, jotta yrityksessä paikalla olevilla olisi pääsy tarvittaviin tietoihin. Salasanan

muotovaatimuksien määrittelyssä oli vaihtelua. Osassa oli vaatimuksena minimipituus ja suullinen ohjeistus hyvästä salasanassa, joissakin yrityksissä erilaisten merkkien määrä oli tarkkaan määritelty ja ohjelmallisesti myös valvottu. Koneellinen valvonta tarkoittaa sitä että esimerkiksi käyttöjärjestelmä edellyttää salasanan vaihtamista määritellyin väliajoin ja tarkistaa myös salasanan muodon sitä määriteltäessä. Kahdessa tutkitussa yrityksessä oli päädytty ratkaisuun, jossa salasanat määriteltiin työntekijöiden puolesta, jolloin salasanat tekevälle henkilölle jää tieto kaikkien salasanoista.

Kahdeksassa yrityksessä oli dokumentoitu tietojen luokittelukäytäntö, kahdeksassa yrityksessä taas tukeuduttiin maalaisjärjen käyttöön tai suulliseen periaatteeseen, että kaikki tieto jota käsitellään on salaista. Esimerkiksi salaisten paperidokumenttien tuhoamiseen oli käytössä joko silppureita tai lukollisia laatikoita joiden sisältö vietiin tuhottavaksi. Yhdessä yrityksessä oli tietoturvapolitiikkaan dokumentoitu varsin yksityiskohtainen tietojen luokittelusäännöstö, mutta se oli havaittu turhan raskaaksi ja yksinkertaistamista oli jo suunniteltu. Muissa yrityksissä salaisuusluokkia oli käytössä yksi tai kaksi, jolloin dokumentti sisälsi lähinnä tiedon siitä mitkä tiedot ovat julkisia.

Kaikissa yrityksissä oli rajoitettu tietojen käyttöoikeutta edes jollakin tasolla. Kolmessa yrityksessä oikeuksia oli rajattu lähinnä yrityksen omien talous- ja palkkatietojen osalta. Muissa yrityksissä tietojärjestelmissä oleviin tietoihin pääsyä oli rajattu vain niihin tietoihin, joihin henkilöllä on tarve. Pääsyoikeutta paperidokumentteihin rajattiin lukollisilla kaapeilla, joita oli kuitenkin käytössä varsin vähän. Yrityksissä joissa tietojärjestelmiin ei vaadittu henkilökohtaista käyttäjätunnusta pääsyä tietoihin pystyttiin rajaamaan vain rajoittamalla pääsyä tietyille tietokoneille.

Vastuut ja varmuuskopiointi

Vaarallisiin työyhdistelmiin oli kiinnitetty huomiota vaihtelevasti. Osassa yrityksiä todettiin, että pienessä yrityksessä valtaa ja tietoa tahtoo keskittyä paljon toimitusjohtajalle ja muille johdon jäsenille, mutta tätä ei oikein voi välttää. Työyhdistelmiin kiinnitettiin huomiota lähinnä tilanteissa, joissa sama henkilö oli tekemisissä kahden toistensa kanssa kilpailevan asiakkaan kanssa. Osassa yrityksiä näitä tilanteita pyrittiin välttämään, mutta esimerkiksi tilitoimistoissa kyseisen tilanteen välttäminen on hankalaa. Osassa yrityksiä vaarallisia työyhdistelmiä ei ollut mietitty, mutta haastattelutilanteessa haastateltavat eivät nähneet sellaisille mahdollisuuttakaan.

Kaikissa yrityksissä oli taho joka oli vastuussa tietojärjestelmistä. Yleensä tämä taho oli ATK-laitteistojen ylläpidosta vastaava henkilö. Osassa yrityksiä järjestelmien tietosisällöstä vastasivat kunkin projektin päälliköt tai esimiehet muuten, osassa todettiin vastuun tiedoista olevan kullakin työntekijällä mutta viimekädessä toimitusjohtajalla, joka viittasi siihen ettei vastuuhenkilöitä ollut tietolaji- tai projektikohtaisesti mietitty.

Varmuuskopiointi on yksi tärkeimmistä liiketoiminnan kannalta kriittisen tiedon suojaustoimenpiteistä. Varmuuskopioita otettiin tärkeistä tiedoista kaikissa auditoiduissa yrityksissä. Kahdeksassa yrityksessä kopioita säilytettiin myös yrityksen toimitilojen ulkopuolella, tällöin paikkana oli pankkiholvi tai lukollinen kaappi työntekijän kotona. Muissa yrityksissä varmistuksia tehtiin esimerkiksi peilaamalla kahta palvelinta keskenään tai kovalevypeilauksella saman palvelimen sisällä. Varmistuksia otettiin myös nauhoille tai DVD-levyille, mutta näissä yrityksissä niitä säilytettiin samassa tilassa varmennettavan koneen kanssa.

4.7 Riskienhallinta ja tietoturvallisuudesta viestiminen

Viimeinen kysymyskategoria kartoitti riskienhallinnan organisointia yrityksessä, liiketoiminnan jatkuvuuden suunnittelua sekä tietoturvallisuudesta viestimistä. Hallinnollisen turvallisuuden yhteydessä kartoitettiin tietoturvallisuuden arviointia, tässä yhteydessä lähestytään samaa asiaa kysymällä kuka tietoturvallisuuteen liittyviä riskejä arvioi.

Riskienhallinta ja liiketoiminnan jatkuvuussuunnittelu

Tietoturvallisuuteen liittyviä riskejä arvioidaan valtaosassa yrityksiä satunnaisesti. Yhdessä yrityksessä tehdään riskikartoitus vuosittain laatuarvioinnin yhteydessä. Muissa yrityksissä riskien arviointi on osa päivittäistä toimintaa, jolloin riskejä mietitään esimerkiksi projektien yhteydessä tai ongelmien ilmaantuessa. Seitsemässä yrityksessä tuli esille tietty henkilö tai henkilöt, jotka ovat vastuussa riskikartoitusten tekemisestä. Vastuuhenkilöt olivat yrityksessä tietoturvasta vastuussa olevia henkilöitä, yleensä johdon edustajia. Muissa yrityksissä arvioinnista puhuttiin passiivissa, jolloin on tulkittavissa, että arviointi on johdon tai kulloisenkin projektijohdon tehtävä.

Dokumentoituja suunnitelmia liiketoiminnan jatkuvuuden varmistamiseksi ei ollut tehtynä suurimmassa osassa yrityksiä. Dokumentointeja oli tehty lähinnä työtehtävien osalta. Varahenkilöjärjestelyjä oli sovittu osassa yrityksiä. Yleisin tapa varautua poissaoloihin esimerkiksi sairauden takia oli tallentaa tietoja verkkolevyille niin, että niihin on pääsy vaikka työntekijä itse ei olisi saapuvilla. Varsinaisiin onnettomuustilanteisiin, joissa liiketoiminta vaarantuisi, ei oltu varauduttu varmuuskopioita kummemmin. Yhdessä yrityksessä varalaitekanta oli olemassa, mutta sitä säilytettiin yrityksen tiloissa. Lisäksi joissakin yrityksissä oli varmistettu virransaantia sähkökatkon varalta, jotta kriittiset toiminnot eivät vaarantuisi.

Liiketoiminnan jatkuvuuden suunnittelu oli käsitteenä varsin outo pääosalle haastatelluista. Tämän takia vastaukset sen suhteen, minkälaisia toimenpiteitä

yrityksissä on tehty vaihtelivat suuresti. Jatkokysymyksin kuitenkin yleensä selvisi, ettei jatkuvuuden suunnitteluun oltu kovin paljon paneuduttu riippumatta siitä, millä nimellä suunnittelua kutsuttiin.

Sopimuskäytännöt ja tietoturvallisuudesta viestiminen

Salassapitosopimuksia tehtiin paitsi työntekijöiden, myös yhteistyötahojen kanssa. Yritysten käytännöt salassapitosopimusten tekemisen suhteen vaihtelivat varsin paljon. Neljä yritystä vaati haastattelijoita allekirjoittamaan salassapitosopimuksen ennen kuin haastattelu aloitettiin. Näissä yrityksissä salassapitosopimusten tekeminen oli yleinen käytäntö muutenkin. Sopimukset olivat yrityksissä laadittuja. Yhdeksässä yrityksessä salassapitosopimuksia tehtiin aina tarvittaessa, yleensä osana useimpia toimeksiantosopimuksia.

Tietoturvallisuudesta ei pääsääntöisesti viestitä ulospäin. Yhtenä viestinnän keinona voitaisiin pitää tietoturvallisuuteen liittyvien sertifikaattien hankkimista ja niiden käyttöä markkinoinnissa. Yhdelläkään haastatelluista yrityksistä ei kuitenkaan ollut tietoturvallisuuteen liittyviä sertifikaatteja. Suurin osa totesi, ettei sertifiointiin ole syytä jatkossakaan, sillä sertifiointi on kallista ja turvalliset toimintatavat voi osoittaa asiakkaille muillakin keinoin. Osassa yrityksiä oli käytössä dokumentoidut yrityksen arvot. Kolmessa yrityksessä todettiin arvoihin kirjatun luotettavuuden sisältävän myös viittauksen luottamuksellisuuteen. Suoria viittauksia tietoturvallisuuteen arvoissa tai niitä selittävässä dokumentaatiossa ei ollut yhdessäkään yrityksessä.

Yritykset esittelevät tietoturvallisuuteen liittyviä käytäntöjään mikäli asiakkaat niistä haluavat tietää. Kahdessa yrityksessä asiakkaat olivat tehneet pienimuotoisia auditointeja yrityksen tiloihin varmistuakseen yhteistyökumppanin luotettavuudesta. Suurin osa yrityksistä koki, että tietoturvallisuudesta ei ole tarvetta viestiä erikseen, vaan että paras mainos yrityksen turvallisuudesta on turvalliset toimintatavat ja luottamuksen säilyttäminen. Kuten luvussa 4.3.1 mainittiin, yritykset kokivat luottamuksen säilymisen perusedellytykseksi yrityksen liiketoiminnalle. Kolmessa yrityksessä todettiin, että hyvin hoidetusta tietoturvallisuudesta maininta olisi joissakin tapauksissa mainosvaltti. Toisissa yrityksissä taas koettiin, että jos tietoturvallisuudesta ”huudellaan” julkisesti, herää kysymys kuinka huonosti asiat onkaan hoidettu, jos itsestäänselvyyksiä käytetään mainostuksessa. Rivien välistä on myös tulkittavissa tietoturvallisuudesta viestimisen kääntöpuoli: jos mainostetaan tietoturvallisuuden olevan viimeisen päälle kunnossa, yritys on pulassa, jos jotakin sattuu. Yrityksissä koettiin, etteivät asiat ole niin hyvin hoidossa, että niistä kannattaisi erikseen kehuskella. Toisaalta esimerkiksi salassapitosopimusten sisältö ja olemassaolo viestittää asiakkaille yrityksen suhtautumisesta tietojen suojaamiseen. Tällöin erillistä tietoturvallisuuden markkinointia ei tarvita.

5 TUTKIMUKSEN JOHTOPÄÄTÖKSET

Tietoturvallisuus on hyvin monitahoinen käsite, jonka yksiselitteinen määrittely on hankala tehtävä. Tämän työn teoriaselvityksen tuloksena tietoturvallisuus nähdään prosessina, joka tähtää yrityksen tietojen suojaamiseen. Prosessin muodostavat tekniset suojausprosessit, systemaattinen riskienarviointi sekä riskiarvioinnin pohjalta määritellyt suojaustoimenpiteet. Yrityksen tietopääomaa ovat niin tietokoneilla ja papereilla olevat data ja informaatio kuin sen henkilöstön tietämys. Tietoturvallisuuden toteutusta yrityksessä ohjaa tietoturvallisuuspolitiikka ja yrityksessä vallitseva tietoturvallisuuskulttuuri on osaltaan vaikuttamassa siihen, kuinka tietoturvallisuus yrityksessä toteutuu.

Tässä luvussa analysoidaan luvussa 4 esitettyjä auditointien tuloksia sekä esitetään kehitysehdotuksia paitsi tutkituille yrityksille, myös yleisesti. Tulosten yleistettävyys kaikkiin tietointensiivisiin pk-yrityksiin voidaan kyseenalaistaa, mutta kun otetaan huomioon tutkimuksessa mukana olleiden yritysten määrä ja aineiston varsin hyvä yhtenäisyys, voidaan olettaa, että samankaltaisia ongelmia todennäköisesti esiintyy myös muissa vastaavissa yrityksissä.

5.1 Tietoturvallisuuden tilan selvittäminen

Luvussa 3.1 kuvattiin tietoturvallisuusauditointien menetelmiä. Kirjallisuudessa (e.g. Kairab 2005, CEM) esiintyvät menetelmät yrityksen tietoturvallisuuden tilan selvittämiseksi ovat hyvin perusteellisia ja yksityiskohtaisia. Kairabin (2005) auditointimallin täydellinen suorittaminen edellyttäisi useita haastatteluja auditoitavassa yrityksessä. Lisäksi auditointiprosessi vaatisi yrityksen dokumentaatioiden huolellista läpikäyntiä. Tutkimuksen tavoitteena on kuitenkin selvittää tietoturvallisuuden yleistila mukana olleissa yrityksissä, jolloin yksityiskohtainen dokumentaatioiden ja prosessien läpikäyminen ei ole tarpeellista. Tutkimuksessa valittiin kevyempi lähestymistapa, jossa yrityksissä tehtiin yksi haastattelu, jonka pohjalta muodostettiin arvio tietoturvallisuuden yleistilasta. Pienten yritysten kohdalla valittu menettely on perusteltua, sillä kuten luvussa 1.1 todetaan, pienten yritysten työntekijöiden toimenkuvat ovat laajoja, ja johdolla on läheinen kosketus yrityksen päivittäiseen toimintaan. Näin yhdellä tai kahdella haastateltavalla johdon edustajalla on käsitys sekä yrityksen teknisistä ratkaisuista että liiketoimintaprosesseista. Kairabin (2005, s. 63) mallissa liiketoimintaprosessien ja teknisten ratkaisujen arviointi on eriytetty toisistaan.

Tutkimuksen kysymysrungon pohjaksi valittiin tietoturvallisuuden osa-alueet, joiden perusteella käytettävät kysymykset valittiin ja ryhmiteltiin. Teoriaosuuden myötä käy kuitenkin ilmi, että osa-aluejako on eri lähteissä erilainen ja lisäksi paikoin hyvin keinotekoinen koska selkeitä rajoja osa-alueiden välillä ei ole. Haastattelukysymysten

ryhmittely olisi voitu tehdä monella eri tavalla ja silti osa-alueiden määrittelyn mukaan oikein. Osa-aluerajojen häilyvyyden takia tietoturvallisuus onkin helpompi määritellä prosessina, jonka osana käytetään eri osa-alueiden yhteydessä kuvattuja suojauskeinoja. Kysymykset kuitenkin olivat toimivia riippumatta siitä mikä niiden otsikkona oli.

Haastattelukysymyksiä oli 38. Haastattelulle oli varattu aikaa kaksi tuntia, mutta useimmiten kysymykset käytiin läpi huomattavasti nopeammin. Tällä perusteella kysymyksiä olisi voinut olla enemmänkin, jolloin näinkin lyhyessä ajassa olisi voitu pureutua myös syvemmälle yritysten ratkaisujen syihin. Haastattelujen avulla saatiin kuitenkin selvitettyä tietoturvallisuuden nykytila yrityksissä, mikä oli tutkimuksen tavoite.

Haastattelijoina toimivat tietoturvallisuuden johtaminen -kurssin opiskelijaryhmät diplomityön tekijän ohjauksessa. Haastattelijat olivat tehtävässään kokemattomia ja haastatteleva ryhmä vaihtui joka yritykseen. Ohjeistuksista ja tutkimuksen tekijän opastuksesta huolimatta kerätyn haastatteluaineiston yhtenäisyys hieman kärsi haastattelijoiden vaihtumisesta. Tutkimuksen tekijä esitti täydentäviä kysymyksiä ja tarvittaessa muotoili kysymyksiä uudestaan. Vastausten laajuus vaihteli kuitenkin yrityskohtaisesti. Koska haastattelutilaisuus toimi oppimistilanteena opiskelijaryhmille jatkuva puuttuminen tutkimuksen tekijän toimesta olisi johtanut turhautumiseen, minkä takia tutkimuksen tekijä pyrki puuttumaan kysymysten esittämiseen mahdollisimman vähän. Jälkikäteen analysoiden haastatteluaineisto olisi voinut olla yhtenäisempää, jos tutkimuksen tekijä olisi tarkemmin huolehtinut, että kysymyksiin vastataan yhtä laajasti kaikissa yrityksissä. Toisaalta puuttuminen ei välttämättä olisi johtanut laajempaan aineistoon, sillä tietoturvallisuus on yrityksille varsin arka aihe ja osassa yrityksistä haastattelukysymyksiin vastattiin tarkoituksellisesti mahdollisimman niukasti.

5.2 Tietoturvallisuuden nykytila tutkituissa yrityksissä

Tietoturvallisuuden nykytila haastattelujen perusteella on kuvattu osa-alueittain luvussa 4. Tietoturvallisuutta oli pohdittu ainakin teknisellä tasolla kaikissa yrityksissä. Koska yritykset käsittelevät päivittäisessä toiminnassaan suuria määriä tietoa, on niiden pakko varmistaa teknisten järjestelmien toimivuus ja tietojen saatavuus. Lisäksi haastatteluista käy ilmi, että tietoturvallisuuden hoitaminen on yrityksille elinehto asiakassuhteiden säilyttämisen kannalta. Käsitys siitä, miten tietoturvallisuus hoidetaan hyvin, vaihteli kuitenkin suuresti. Yrityksissä myös todettiin, että tietoturvallisuuden kokonaisvaltaiselle kehittämiselle olisi tarvetta.

Seuraavassa esitetään analyysia tietoturvallisuuden nykytilasta tutkituissa yrityksissä, ja annetaan parannusehdotuksia pienempiin havaittuihin puutteisiin. Keskeiset puutteet on nostettu erikseen esiin luvussa 5.3.

5.2.1 Tietoturvallisuuden hallinnointi

Tietoturvallisuuden tarkasteleminen kokonaisuutena ei ollut yrityksissä yleistä, lähinnä kokonaiskuva oli syntynyt niissä yrityksissä, joissa tietoturvallisuuspolitiikka oli dokumentoitu. Yrityksissä, joissa oli olemassa yksittäisiä toimintaohjeistuksia tietoturvallisuuteen liittyen ohjeistukset olivat luonteeltaan lähinnä teknisiä, eivätkä ne auttaneet työntekijöitä muodostamaan kokonaiskäsitystä yrityksen tietoturvallisuustavoitteista.

Yrityksissä oli hyvin mietitty minkälaista tietoa yritys käsittelee ja mitkä tiedoista ovat tärkeitä. Asiakastiedot suojattavana kohteena olivat tärkeimpiä kaikkien yritysten kohdalla. Tulos ei ole yllättävä ottaen huomioon yritysten toimialat ja toiminnan luonteen. Omaan normaaliin liiketoimintaan liittyviä tietoja ei tunnistettu tärkeiksi kaikissa yrityksissä, mutta nämäkin tiedot mainittiin suurimmassa osassa vastauksia. Useimmissa yrityksissä lähtökohta oli, että kaikki tieto jota yrityksessä käsitellään on tärkeää ja sitä tulee suojata. Tietointensiivisten yritysten kyseessä ollessa tämä on luonnollinen tilanne. Silloin tärkeimpien tietojen tunnistaminen erikseen ei välttämättä ole tarpeen.

Luvussa 2.1.1 todetaan, että tietoturvallisuuden hallinnoinnin prosessi lähtee liikkeelle vastuunjaosta. Vastuunjako tekniseen turvallisuuteen ja yleiseen tietoturvallisuuden toteuttamiseen on askel kokonaisvaltaisempaa lähestymistä kohden. Mikäli tietoturvallisuusohjeistusten ja toimintojen suunnittelu ja toteutus on ainoastaan tietotekniikasta huolehtivien vastuulla, viestii se siitä, että yrityksen käsitys tietoturvallisuudesta on varsin tekninen. Jos yrityksen peruskäsitys on, että tietoturvallisuus on tekninen asia, ei työntekijöillekään muodostu käsitystä tietoturvallisuuden kokonaismerkityksestä (von Solms & von Solms 2004b, s.372). Kun politiikat ja ohjeistukset tulevat johdon edustajalta, ne todennäköisemmin edesauttavat kokonaisvaltaisemman tietoturvallisuuskulttuurin muotoutumista. Käytännön teknisten ratkaisujen toteutus kannattaa toki jättää tietotekniikkavastaavien huoleksi. Aivan pienessä yrityksessä tietotekniikkavastaava voi olla myös johdon edustaja, jolloin tietoturvallisuuden kokonaisvastuun määrittäminen hänelle on ymmärrettävää. Tällaisessakin yrityksessä kuitenkin myös toimitusjohtajan tulee olla kiinteästi mukana kehittämässä tietoturvallisuutta.

Henkilöturvallisuuteen kuuluvat kaikki henkilöstön työsuhteen elinkaaren aikana esille tulevat turvallisuusasiat (luku 2.1.2). Palkkausvaiheessa työntekijöiden taustojen tarkastaminen on tärkeää, jotta voidaan varmistua työnhakijan olevan sitä mitä hän väittää olevansa. Monissa tapauksissa työ- ja koulutodistusten tarkistaminen voi riittää, mutta suosittelijoiden lausuntojen tarkastaminen on hyvä tehdä aina kun siihen on mahdollisuus. Positiivinen huomio on myös, että useissa yrityksissä tarkistetaan työntekijän tietoja edelliseltä työnantajalta. Taustojen tarkistamisen motiivina lienee

kuitenkin yleensä selvittää onko henkilö pätevä työntekijä, ei niinkään selvittää onko hän mahdollinen uhka yrityksen tietoturvallisuudelle. Mikäli taustalta jotakin epäselvää löytyy, voi tämä olla varoittava merkki työntekijän motiiveista hakea yrityksen palvelukseen ja näin merkki potentiaalisesta tietoturvauhasta. Ahkera ja tunnollinen henkilö ei todennäköisemmin aiheuta uhkaa yrityksen tietoturvalle esimerkiksi huolimattomalla tietojen käsittelyllä, joten työntekijän pätevyyden ja työtaustan selvittäminen on siltäkin osin myös tietoturvallisuuden kannalta tärkeää.

Työsuhteen päättymisen yhteydessä tietoturvallisuuden kannalta useimmiten on korostettu käyttäjätunnusten sulkemista välittömästi työsuhteen päättyessä, jotta henkilölle ei jää mahdollisuutta esimerkiksi muuttaa yrityksen tiedostojen sisältöä (e.g. Whitman & Mattord 2003, Peltier et. al. 2005). Ongelma ei ole suuri, mikäli henkilöllä olisi mahdollisuus kirjautua yrityksen järjestelmiin ainoastaan toimitilojen sisällä. Siinä tapauksessa fyysisten kulkuoikeuksien poistaminen riittää myös tietojärjestelmiin pääsyn sulkemiseksi. On kuitenkin tärkeää huolehtia myös järjestelmien käyttöoikeuksien sulkemisesta työsuhteen päättyessä, jotta henkilö ei pääse yrityksen tiedostoihin niin toimitiloista kuin niiden ulkopuoleltakaan etäyhteyksien kautta. Tärkeää on myös tiedottaa muuta henkilökuntaa työsuhteen päättymisestä, jotta kaikki ovat tietoisia siitä. Näin ei pääse syntymään tilannetta, jossa henkilölle luovutettaisiin yrityksen materiaalia luullen, että hän vielä työskentelee yrityksessä. Pienen yrityksen kohdalla tällainen tilanne on hyvin epätodennäköinen, mutta riski on myös torjuttavissa pienellä toimenpiteellä.

5.2.2 Tekninen turvallisuus ja tietojen luokittelu

Etätyöskentely on usein teknisin ratkaisuin toteutettua työskentelyä esimerkiksi kotoa käsin. Myös yritysten vastauksissa käy ilmi, että etätyöskentelyksi mielletään lähinnä tietoliikenneyhteyksin muodostettu etäyhteys yrityksen palvelimille. Etätyötä kuitenkin olla voi olla mikä tahansa yrityksen toimitilojen ulkopuolella tehtävä työ. Etätyöskentelyyn liittyen on tärkeää huomioida, että yrityksen tietoturvallisuuspolitiikka ja tietojenkäsittelysäännökset ovat voimassa myös yrityksen tilojen ulkopuolella. Erityisesti paperidokumenttien kohdalla olisikin tärkeää määritellä minkälaista tietoa on luvallista kuljettaa yrityksen tilojen ulkopuolelle ja saako esimerkiksi alkuperäisiä dokumentteja kuljettaa mukana. Kysymys on relevantti esimerkiksi kirjanpitoyrityksen kohdalla, joka saattaa säilyttää asiakkaan kuittien originaalikappaleita kirjanpidon tekemisen ajan, jolloin näiden kuittien kuljettaminen yrityksen tilojen ulkopuolelle voi kasvattaa niihin kohdistuvaa fyysisen tuhoutumisen uhkaa.

Etätyöskentelyyn ja teknisten välineiden käyttöön liittyy myös siirrettävien medioiden käyttö yrityksissä. Koska varsinaisia dokumentoituja käytäntöjä siitä, miten siirrettäviä medioita käytetään, ei juurikaan ollut, on siirrettävien laitteiden käsittelyyn hankala

ottaa kantaa. Mikäli esimerkiksi USB-muistitikkuja käytetään paljon, tulisi niiden käytöstä tehdä selkeät ohjeet, sekä ainakin harkita tikkujen salausta. Tietointensiivisen yrityksen kohdalla siirrettävien medioiden käytön estäminen olisi hankalaa, sillä tietokoneet ovat keskeisiä työkaluja ja siirrettäviä medioita käytetään päivittäisessä toiminnassa. Tällaisessa tapauksessa on hyvin pitkälle luotettava siihen, että ohjeistuksia ja sopimuksia tiedostojen käsittelystä noudatetaan, sillä sen valvonta, minkälaista tietoa työntekijät tallettavat muistitikuilleen ja miten he tikkuja käsittelevät ja säilyttävät on erittäin vaikeaa.

Teknisen tietoturvallisuuden keskeinen asia on käytettävien tietojärjestelmien ja ohjelmistojen ylläpito. Keskitetyn ylläpidon ratkaisun yleisyys kuvastaa sitä, että on paitsi turvallista, myös kustannustehokasta huolehtia ohjelmistojen päivityksistä ja valinnasta keskitetysti. Joissakin tapauksissa, erityisesti hyvin pienissä yrityksissä, voi olla tehokkaampaa että esimerkiksi ohjelmistokehittäjä huolehtii oman kehitysympäristönsä päivittämisestä, sillä hänellä on tarvittava osaaminen ylläpidon suorittamiseksi. Päivitys- ja asennusoikeuksien jakaminen kaikille käyttäjille johtaa kuitenkin helposti hyvin kirjavaan tilanteeseen, jossa yrityksessä on yhtä monta erilaista työympäristöä kuin on tietokoneita. Lisäksi esimerkiksi tärkeiden tietoturvapäivitysten tekemisen jättäminen työntekijöiden vastuulle altistaa yrityksen tietoverkosta tuleville hyökkäyksille, mikäli päivitykset jäävät kiireen tai unohduksen takia tekemättä. Yritykset olivat hoitaneet esimerkiksi virusohjelmien päivityksen keskitetysti, jolloin virusten aiheuttamia uhkia vastaan on suojauduttu varsin hyvin.

Tietointensiivisten yritysten kyseessä ollessa fyysinen turvallisuus on kaksitahoinen asia. Toisaalta yrityksen liiketoiminnan jatkuvuuden kannalta fyysisten tilojen merkitys voi olla hyvinkin pieni, mikäli toiminnassa tarvittavien tietojen saatavuus ei ole sidoksissa toimitiloihin. Toisaalta toimitiloissa voidaan säilyttää paljon arkaluonteista tietoa, jonka fyysinen suojaaminen vääriin käsiin joutumiselta on erittäin tärkeää. Riittävä murtosuojaus ja kulunvalvonta niin, että toimitiloihin ei pääse asiattomia henkilöitä ilman valvontaa on yksi fyysisen turvallisuuden tavoite (Tipton & Krause 2004, s.1922).

Kulkusääntöjen määrittely kulkukorttien avulla helpottaa porrastetun pääsyn toteuttamista niin, että yrityksellä on useamman tasoisia kulkuoikeusalueita ja tärkeimmät tiedot säilytetään paikoissa joihin vain harvoilla henkilöillä on pääsy. Tällainen porrastettu pääsyrakenne toimii yhtenä fyysisen turvallisuuden elementtinä (Steinke 2004, s.1931). Sähköisen kulkukortin sekä kuvallisen henkilökortin tulisi yhdessä toimia varmistuksina siitä, että henkilöllä on oikeus kulkea yrityksen tiloissa (Whitman & Mattord 2003, s.360). Vaikka tutkitut yritykset ovatkin pieniä, jolloin todennäköisesti suurin osa työntekijöistä tuntee toisensa, saattaa syntyä tilanteita joissa kuvallinen henkilökortti olisi tarpeen. Joissakin yrityksissä tarve oli huomattu asiakkaiden puolelta, kun työntekijät liikkuivat asiakkaiden luona.

Kulunvalvonnan lisäksi tietoihin pääsyä rajataan käyttäjätunnuksien ja salasanojen avulla. Salasanapolitiikan tulisi olla tasapainossa yrityksen turvan tarpeen kanssa. Mikäli yrityksen tietokoneilta ei pääse ilman erillistä autentikointia käsiksi kriittisiin tietoihin, eikä koneella itsellään säilytetä tärkeitä tietoja, ei kirjautumissuojan tarvitse olla kovin vahva. Tällöin lyhyempikin salasana sekä pitkä vaihtoväli riittävät. Mikäli kuitenkin koneelta kirjaudutaan suoraan myös palvelimille, joka oli tilanne useassa tutkitussa yrityksessä, tulee salasanasuojauksen olla riittävän vahva. Salasanapolitiikan tulee yksiselitteisesti kuvata kuinka usein salasana vaihdetaan, mitä muotovaatimuksia sille asetetaan, sekä kenellä on oikeus pitää salasanaa hallussaan. Paras tilanne on, jos kaikki salasanat yrityksessä ovat henkilökohtaisia, jolloin voidaan esimerkiksi kerätä lokitietoja henkilötasolla. Kolmessa yrityksessä oli kuitenkin päädytty ratkaisuun, jossa salasanoja oli myös muiden kuin käyttäjän itsensä tiedossa. Näissä yrityksissä turvallisempaan käytäntöön voitaisiin päästä esimerkiksi järjestämällä koulutus hyvän salasanan määrittelystä sekä järjestämällä esimerkiksi salasanat aiemmin määritelleelle henkilölle pääkäyttäjän oikeudet henkilöstön tietokoneille, jolloin pääsy tärkeisiin tietoihin olisi varmistettu myös poissaolotilanteissa. Tällöin salasanat säilyisivät aidosti henkilökohtaisina.

Sekä fyysisen pääsyn rajoittaminen että käyttöoikeuksien määrittely tähtäävät tiedon saannin rajoittamiseen. Rajoittamisen pohjana tulisi olla tietojen luokittelu. Yksinkertaisena tietojen luokittelukäytäntönä voi toimia jako julkisiin, yrityksen sisäisiin sekä salaisiin tietoihin (Appleyard 2004, s.719). Tietojen suojausmekanismit valitaan tiedon kriittisyyden perusteella niin, että kaikkein liiketoimintakriittisin tieto on vain tiettyjen henkilöiden saatavilla ja sitä suojaavat toimet ovat vahvimpia. Yrityksen sisäiset tiedot ovat tietoja, joista työntekijät saavat keskustella keskenään, mutta joiden paljastuminen yrityksen ulkopuolelle olisi vahingollista. Näitä tietoja on valtaosa esimerkiksi tuotekehitystä tekevän yrityksen tiedoista. Julkista tietoa ovat tiedot, jotka on tarkoitettu julkisiksi, esimerkiksi internet-sivujen sisältö. Näiden luokkien lisäksi esimerkiksi projektiliiketoimintaa harjoittavissa yrityksissä voi syntyä tietoluokkia projektien mukaan. Oli tietoluokkien määräytymistapa mikä tahansa, tulee se dokumentoida. Dokumentissa tulee lisäksi määritellä, minkälaisia suojauskeinoja kuhunkin tietoluokkaan sovelletaan (Appleyard 2004, s. 725). Tutkimuksen yrityksissä tietojen luokittelukäytännöt vaihtelivat, mutta ainakin salaisten tietojen määrittelyyn oli kaikissa yrityksissä kiinnitetty huomiota. Kaikissa yrityksissä tulisi kuitenkin jollakin aikavälillä pohtia tarkemman luokittelun tarpeellisuutta.

Tiedon luokittelun lisäksi tulisi tunnistaa kustakin tiedoista vastaavat henkilöt. Tietojen vastuuhenkilö tai omistaja tulisi olla kaikille tärkeille tiedoille määriteltynä ja tämän omistajan tulisi olla johdon edustaja (Appleyard 2004, s.721). Tietojen omistajan rooli on määritellä tietojen luokitus, tarkistaa luokitustarve säännöllisesti sekä tarkastaa, että tiedoille määritellyt suojaustoimenpiteet ovat riittävät. Tämän vastuun pitää olla

liiketoimintajohdon edustajalla, sillä IT-ylläpitäjät eivät määrittele tiedon tärkeyttä liiketoiminnalle. IT-ylläpito voi olla vastuussa suojaustoimenpiteiden toteutuksesta, mutta ei niiden määrittelystä (Appleyard 2004, s.723). Tutkimuksen yrityksissä tietojen vastuuhenkilöitä ei ollut tarkemmin pohdittu, vaan heidän olemassaolonsa oli puolittainen itsestäänselvyys. Tärkeää olisi kuitenkin nimetä tietojen omistajat niin, että vastuu on oikeasti tiedon sisällöstä vastaavalla henkilöllä. Joissakin yrityksissä tämä voi tarkoittaa vallitsevan käytännön dokumentointia, toisaalla voidaan joutua muuttamaan käsityksiä relevantista vastuuhenkilöstä.

Tärkeän tiedon suojaamiseen liittyy olennaisesti varmuuskopiointi. Varmuuskopioinnin järkevä tapa riippuu varmistettavan tiedon määrästä, laitteistosta joka on käytettävissä sekä varmistuksen aikaviiveestä. Mikäli yrityksessä vaaditaan reaaliaikainen varmuuskopiointi, eräs tapa on käyttää peilaavaa varmennusta esimerkiksi kahden palvelimen välillä. Kun palvelimet sijoitetaan eri paikkoihin, saavutetaan peilauksella myös varmennuksen toinen tavoite, eli sijoitus eri tiloihin varmistettavan tiedon kanssa. Mikäli varmuuskopioinnille ei ole reaaliaikaista tarvetta, varmistusten tekeminen siirrettäville medioille, esimerkiksi nauhalle tai DVD-levylle voi toimia yrityksen kannalta riittävänä ratkaisuna. Lisäksi on syytä pohtia onko automaattisesti tapahtuva säännöllinen varmuuskopiointi tarpeen, vai riittääkö prosessi, jossa varmistuksen tekeminen on tietyn henkilön tai henkilöiden vastuulla. Tutkittujen yritysten kohdalla olisi hyvä tarkistaa, minkälaisia vaatimuksia varmuuskopioinnille yrityksen vakuutusyhtiö mahdollisesti asettaa, sekä etsiä ja ottaa käyttöön yrityksen kannalta järkevin varmuuskopiointikäytäntö. Osassa yrityksiä näin oli jo tehtykin, mutta osassa yrityksiä varmuuskopiointi ei ollut systemaattista, jolloin kehittämisen varaa olisi.

5.2.3 Tietoturvallisuuden ylläpitotoimet

Riskienhallinta on osa tietoturvallisuuden hallinnan prosessia. Riskienarvioinnin tulisi toteutua yrityksen omista lähtökohdista ja liiketoiminnan erityispiirteet huomioiden. Jotta riskiarviointi on kattavaa, tulee riskien hallinnasta ja arvioinnista vastuussa olevan henkilön olla johdon edustaja. Tämän tutkimuksen yritysten kohdalla vastuuhenkilö automaattisesti kuuluu johdon edustajiin, sillä pienissä yrityksissä organisaatiotasoja on vähän. Riskienhallintaan kuuluva tietoturvallisuuden arviointi koettiin yrityksissä hankalaksi. Arviointiprosessin sinänsä ei tarvitse olla monimutkainen, vaan jo esimerkiksi kuukausittainen tarkistuslistan läpikäynti voi toimia tietoturvallisuuden sisäisenä arviointina. Tällaisen tarkistuslistan luomisessa on tärkeää tunnistaa yrityksen itsensä kannalta keskeiset tietoturvallisuusriskit ja pohtia suojaustarvetta. Kun suojaustoimet on määritetty, valitaan tietotuvallisuuden valvonnan tarkistuslistaan tärkeimmät kohdat, joita seurataan määritellyin aikavälein. Tärkeintä sisäisen arvioinnin tekemisessä onkin arvioinnin systemaattisuus sekä sen kohdistuminen yrityksen kannalta olennaisiin asioihin.

Yritykset tekivät varsin usein salassapitosopimuksia yhteistyökumppanien ja työntekijöiden kanssa. Yllättävää oli, että vaikka salassapitosopimusten tekeminen yhteistyökumppanien kanssa on näin yleistä, sopimusta ei vaadittu tehtäväksi haastattelun suorittaneen opiskelijaryhmän kanssa kuin muutamassa yrityksessä. Haastatteluissa mukana ollutta diplomityön tekijää sitoo toki virkavelvollisuuden kautta salassapitovelvollisuus haastatteluaineiston suhteen, mutta opiskelijaryhmät eivät ole sopimussuhteessa yliopistoon, eivätkä näin automaattisesti salassapitovelvollisia. Neljän salassapitosopimuksen vaatineen yrityksen lisäksi vain kaksi yritystä muistutti suullisesti haastattelussa esillä olevien asioiden luottamuksellisuudesta. Loput yritykset joko luottivat siihen, että tiedot pysyvät luottamuksellisina tai kokivat, ettei haastattelussa käsitelty niin arkaluonteista tietoa, että salassapitosopimus olisi ollut tarpeen.

Suurin osa haastatelluista yrityksistä voidaan sijoittaa von Solmsin (2000) aalloilla teknisen aallon ja johtamisaallon välimaastoon. Yrityksissä joissa tietoturvallisuuspolitiikka oli luotuna oltiin jo pidemmällä johtamisaallon puolella. Systemaattinen tietoturvallisuuden kehittäminen ja tietoturvallisuustietoisuuden lisääminen veisivät yritykset institutionalisointiaallolle, jossa tietoturvalliset toimintatavat saataisiin luonnolliseksi osaksi yrityksen toimintakulttuuria.

5.3 Keskeisimmät puutteet tietoturvallisuuden hoidossa

Tietoturvallisuuspolitiikan dokumentointi on yrityksen tietoturvallisuuden toteutumisen kannalta erittäin tärkeää (e.g. Höne & Eloff 2002, von Solms & von Solms 2004a ja b). Politiikkadokumentin avulla toisaalta viestitään tietoturvallisuuden tärkeydestä yritykselle ja sitä kautta kasvatetaan tietoturvallisuustietoutta, toisaalta sen avulla varmistetaan yhteinen näkemys siitä mitä tietoa yrityksessä pitäisi suojella ja miten sitä suojellaan. Tutkituissa yrityksissä tietoturvallisuuden dokumentointi on toisaalta hyvällä mallilla, sillä vain kolmesta yrityksestä tietoturvallisuuden ohjeistukseen liittyvä dokumentointi puuttui kokonaan. Vastaavassa tutkimuksessa vuonna 2003 kolmessa yrityksessä oli dokumentoitu politiikka ja kolmessa osittaisia dokumentteja, yhteensä tutkittuja yrityksiä oli tuolloin 11 (Kuusisto & Ilvonen 2003, s.435). Dokumentointitilanne voisi kuitenkin olla parempikin, sillä osittaiset tietoturvallisuusohjeistukset keskittyivät lähinnä yksittäisten käytäntöjen ohjaamiseen ja kokonaiskuva tietoturvallisuudesta puuttuu suurimmasta osasta yrityksiä. Osittaiset ohjeistukset voidaan ottaa kuitenkin huomioon kun tietoturvallisuuspolitiikkaa koostetaan, jolloin voidaan myös arvioida ohjeistusten päivitystarvetta. Kuten luvussa 2.3 todetaan, tietoturvallisuuspolitiikan tulisi olla laadittu yrityksen näkökulmasta. Yhdessä haastatelluista yrityksistä politiikan laatiminen todettiin hyvin raskaaksi, joka viestii siitä että politiikan tekoon on oikeasti panostettu eikä sitä ole vain kopioitu

kirjallisuudessa esitetystä esimerkistä. Mallin ottaminen kirjallisuudesta saattaa kuitenkin helpottaa prosessia ja varmistaa, että tietoturvallisuutta käsitellään kokonaisuutena yksittäisten osa-alueiden sijaan.

Yrityksissä koettiin ohjeistusten noudattamisen valvominen erittäin haasteelliseksi. Valvonnan vaikeuden myöntävät myös Vroom ja von Solms (2004) toteamalla, että vaikka henkilökohtaista valvontaa voitaisiin toteuttaa, henkilöiden normaaleista toimintatavoista on vaikea saada selvyyttä heitä seuraamalla. Tietoturvallisuustietoisuuden lisääminen koulutuksen avulla voisi lisätä henkilöstön sisäistä valvontaa, kun tietoturvallisuuden merkitys yritykselle on paremmin henkilöstön tiedossa. Sisäisellä valvonnalla tässä tarkoitetaan sekä yksilön oman toiminnan tietoisempaa seurantaa että vertaisseurantaa, jossa työntekijät ”valvovat” toisiaan. Salassapitosopimukset ja muut määräykset toimivat osaltaan motivaattoreina sääntöjen noudattamiseen.

Suomessa työsopimuslaki velvoittaa työntekijän pitämään työnantajansa liike- ja ammattisalaisuudet salassa (L 26.1.2001/55, 3. luku). Tätä kautta jo pelkästään työsopimus toimii yleisenä salassapitosopimuksena, vaikka siinä ei salassapitovelvoitetta sen tarkemmin olisi määritelty. Laki on kuitenkin sen verran yleisluontoinen ilmaisussa liike- ja ammattisalaisuudet, että erityisesti tietointensiivisten yritysten kohdalla voi olla tarpeen tehdä erillinen salassapitosopimus jossa tarkemmin selvitetään mitkä tiedot työntekijän on pidettävä salassa, kenelle hänellä on oikeus asioista puhua ja kuinka kauan salassapitovelvoite on voimassa. Useammassa tutkitussa yrityksessä mainittiin projektikohtaiset salassapitosopimukset, jotka sitovat projektia koskevan tiedon ainoastaan projektiryhmän sisälle. Tämä voi olla tarpeen esimerkiksi jos yrityksessä tehdään projekteja keskenään kilpaileville asiakkaille. Useiden yritysten kohdalla asiakkaiden ja henkilökunnan henkilötietojen käsittelyä ohjaa henkilötietolaki ja esimerkiksi terveydenhuoltoalalla ammattieettiset säännöt. Nämä vahvistavat omalta osaltaan henkilöstön salassapitovelvoitetta yrityksen toimintaan liittyen, vaikka asiakastiedot sinänsä eivät liike- tai ammattisalaisuuksia olisikaan. Kuitenkin myös näiden lakien ja sääntöjen noudattamisesta on hyvä mainita joko työsopimuksessa tai erillisessä sopimuksessa jotta salassapitovelvoitteesta on yrityksen ja työntekijän kesken yhteinen näkemys.

Yksi keskeinen puute kaikissa tutkituissa yrityksissä oli järjestelmällisen tietoturvallisuuskoulutuksen puute. Syy tähän on pienten yritysten kohdalla varsin ilmeinen: ajan ja resurssien puute. Kaikki aika tulisi pyrkiä käyttämään tuottavaan työhön. Osittain koulutuksen puute saattaa johtua myös sanan koulutus sisällöstä. Koulutukseksi mielletään yleensä ainoastaan luentotyyppinen tilanne, jossa yksi henkilö puhuu ja loput kuuntelevat ja joka on erikseen järjestetty aihetta varten. Tietoturvallisuuskoulutus voidaan kuitenkin organisoida myös muulla tavalla.

Kannettavat tietokoneet voivat olla erittäinkin suuri riski yrityksen tärkeiden tietojen eheyden, saatavuuden ja luottamuksellisuuden kannalta. Usein kannettavia koneita on käytössä pääosin johtavassa asemassa olevilla henkilöillä, jotka tarvitsevat työssään miltei kaikkea yrityksen toiminnan kannalta kriittistä tietoa. Näin oli myös tämän tutkimuksen yrityksissä. Vaikka suurimmassa osassa yrityksiä tiedostettiin kannettavien koneiden sisältävän paljon liiketoimintakriittistä tietoa, ei salausta ollut tehty joko siksi, että se koettiin hankalaksi, tai sitten salausta ei oltu tultu ajatelleeksi. Mikäli yrityksissä oltaisiin tehty kattava riskikartoitus voidaan olettaa, että kannettavien tietokoneiden salaukseen suhtautuminen olisi erilaista. Kannettavat tietokoneet ovat houkutteleva varkauskohde jo rahallisen arvonsa takia, mutta joissakin tapauksissa houkuttimena voi toimia nimenomaan koneen sisältämä tieto. Olipa syy kannettavan tietokoneen menettämiseen mikä tahansa, koneen sisältämien tietojen paljastuminen ulkopuolisille voi olla yritykselle todella iso riski. Monissa tapauksissa jo pelkästään tietojen menettäminen ilman niiden paljastumistakin tuottaisi yritykselle ongelmia, mikäli koneen sisältöä ei ole varmuuskopioitu.

Kirjallisuudessa jatkuvuussuunnittelu kuvataan erityisesti onnettomuustilanteisiin varautumisena (e.g. Henry 2004b, Karakasidis 1997). Henry (2004b, s. 1700) korostaa jatkuvuussuunnittelun kokonaisvaltaisuutta, jossa eri osapuolet arvioivat yrityksen riskejä ja tekevät suunnitelmia kriisitilanteiden, joissa useampi riski toteutuu samanaikaisesti, varalle. Jatkuvuussuunnittelun alkuna voi toimia henkilöiden toimenkuvien dokumentointi ja tietojen saatavuuden varmistaminen. Tutkimuksen kohdeyritysten kaltaisissa pienissä yrityksissä olisi kuitenkin tarpeen pohtia myös laajemmin, minkälaiset tilanteet voisivat uhata yrityksen liiketoimintaa. Näitä tilanteita voi löytyä esimerkiksi riskianalyysin yhteydessä, jolloin voidaan pohtia sopivaa prosessia ja henkilöryhmää, joka toimii mikäli riskit toteutuvat (Henry 2004b, s.1700). Liiketoiminnan jatkuvuussuunnittelu ei saa olla toiminto, jota tehdään erillään tietoturvallisuuden muusta johtamisesta. Tietoturvallisuuden lisäksi jatkuvuussuunnittelu liittyy yritysturvallisuuteen ja henkilöstöjohtamiseen yleensä, jonka takia jatkuvuussuunnittelun tulee olla kokonaisvaltainen prosessi, vaikka yritys, jossa sitä tehdään, olisikin kooltaan pieni.

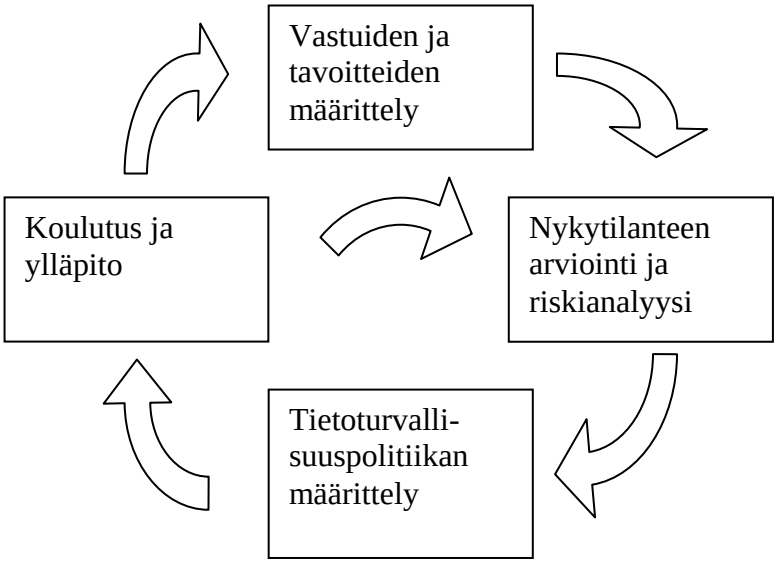
5.4 Parannusehdotuksia tutkituille yrityksille

Tietoturvallisuuden tila tutkituissa yrityksissä on teknisesti ottaen hyvä. Kokonaisvaltainen lähestymistapa tietoturvallisuuteen kuitenkin puuttuu, joka voi aiheuttaa vakaviakin ongelmia suunniteltujen tietoturvallisuustoimien käytännön toteutuksessa sekä kehittämisessä. Keskeisenä parannusehdotuksena tutkituille yrityksille onkin systemaattisen tietoturvallisuusprosessin käynnistäminen.

Teoriaosuudessa esiteltiin useampikin erilainen malli tai lähestymistapa tietoturvallisuuden organisointiin. Näiden mallien ongelma on se, että ne on suunniteltu

isojen yritysten käyttöön. Kun isossa yrityksessä käynnistetään tietoturvallisuuden kehittämisprosessi, voidaan sitä määrittelemään ja vetämään nimetä työryhmä, joka saa resurssit keskittyä nimenomaan tietoturvallisuustyöhön. Pienessä yrityksessä tähän ei yleensä ole mahdollisuutta, sillä etenkin johdon edustajien työnkuva on erittäin laaja. Mahdollisuutta keskittyä joksikin aikaa ainoastaan tietoturvallisuuden organisointiin ei noin vain löydy. Resurssien rajallisuus tulee huomioida käynnistettävässä prosessissa, vaikka tavoite tietoturvallisuudelle olisikin sama kuin isommassa yrityksessä: turvata yrityksen tiedot ja huolehtia että koko henkilöstö osaltaan toimii tavoitteiden mukaisesti.

Luvussa 1.1 kuvataan pk-yritysten erityispiirteinä budjetoinnin haasteet ja henkilöstön laajat toimenkuvat. Myös haastattelujen perusteella nähdään, että tietoturvallisuustyö tahtoo jäädä muiden tehtävien jalkoihin. Sen kehittämiseen panostetaan mikäli siitä on edes välillistä rahallista hyötyä, esimerkiksi potentiaalinen asiakas vaatii kehittämistoimenpiteitä ennen kuin hyväksyy yrityksen toimittajaksi. Haastatteluissa nousi esille yritysten tarve systemaattisempaan tietoturvallisuuden kehittämiseen niin, että aiheesta muotoutuisi kokonaiskuva jossa yrityksen tarpeet ja mahdollisuudet huomioidaan. Niukkojen resurssien ja kokonaiskuvan kehittämisen haasteeseen yritykset voivat vastata ottamalla käyttöön kuvan 16 mukaisen tietoturvallisuuden kehittämisen prosessin.



Kuva 16. Tietoturvallisuuden kehittämisen prosessimalli

Prosessi pohjautuu luvussa 2 esitettyihin malleihin tietoturvallisuuden johtamisen prosessiluonteesta, mutta siinä on otettu huomioon pk-yritysten erityispiirteet. Prosessi lähtee liikkeelle vastuiden ja tavoitteiden määrittelystä. Kairabin (2005) mallissa tämä vaihe vastaa tietoturvastrategian luomista. Tämän jälkeen arvioidaan yrityksen tilanne sekä tehdään riskianalyysi. Kolmannessa vaiheessa määritellään tietoturvallisuuden tavoitetila sekä muodostetaan tietoturvallisuuspolitiikka. Neljännessä vaiheessa suoritetaan ylläpitäviä toimenpiteitä, eli koulutetaan henkilöstöä ja pidetään ohjeistukset

ajan tasalla. Prosessi voi jatkua joko suoraan uudelle kierrokselle nykytilanteen arviointiin tai, mikäli tarvetta, vastuiden ja tavoitteiden uudelleen määrittelyyn. Vaiheiden sisältöä on kuvattu seuraavassa tarkemmin.

5.4.1 Vastuiden ja tavoitteiden määrittely

Pienen yrityksen kyseessä ollessa johdon tuki tietoturvallisuustyölle saadaan varmasti alusta asti, mutta mikäli aloite tietoturvallisuuden kehittämiseen tulee muualta kuin ylimmästä johdosta, tulee myös johdon edustajat saada mukaan prosessiin. Tietoturvallisuusprosessin alkuvaiheessa määritellään tietoturvallisuustyön päävastuuhenkilöt, sekä huolehditaan että heillä on mahdollisuus tehdä vastuullaan olevat tehtävät. Mikäli tietoturvallisuustyö on vain pieni osa henkilön tehtäviä, tulee tämä huomioida prosessin aikataulussa. Aikataulu on kuitenkin tärkeää laatia, jotta syntyy konkreettinen tavoite jota kohti pyritään.

Alkuvaiheessa tietoturvallisuustyön tavoite voi olla lähinnä yrityksen tietoturvallisuustason parantaminen tiettyyn ajankohtaan mennessä. Tavoite voi kuitenkin olla myös tarkempi, mikäli esimerkiksi jollakin osa-alueella on havaittu puutteita, jotka vaativat välitöntä korjaamista.

5.4.2 Tietoturvallisuuden arviointi ja riskikartoitus

Tietoturvallisuuden arviointi voidaan käynnistää esimerkiksi systemaattisella riskikartoituksella, jonka tavoitteena on löytää kaikki yritystä kohtaava uhat ja arvioida uhkien aiheuttama riski. Riskikartoitusprosessi on kuvattu taulukossa 12.

Taulukko 12. Riskikartoituksen vaiheet (mukailtu lähteestä Peltier et al. 2005, s.187-191)

Riskikartoituksen vaiheet
1.Tietovarantojen määrittely
2. Uhkien tunnistaminen
3.Uhkien toteutumisen todennäköisyyden arviointi
4. Vaikutusten arviointi
5. Torjuntakeinot
6. Dokumentointi

Riskikartoituksen ensimmäisenä vaiheena on määritellä, mitkä tietovarannot ovat yritykselle merkittäviä, sekä tunnistaa näihin varantoihin kohdistuvat uhat (Peltier et al. 2005, s.187-189). Uhat voidaan löytää mahdollisimman kattavasti esimerkiksi aivoriihi-

menetelmällä. Kun uhat ovat mahdollisimman kattavasti tiedossa voidaan arvioida eri uhkien toteutumisen todennäköisyyttä. Todennäköisyydet voidaan luokitella esimerkiksi kolmeen luokkaan, jotka on esitetty taulukossa 13. Taulukossa 13 on esitetty myös, miten todennäköisyyden ja uhan toteutumisen vaikutusten arvioinnin kautta voidaan selvittää uhan aiheuttama riski.

Taulukko 13. Riskimatriisi

Todennäköisyys	Vakavat vaikutukset	Keskivakavat vaikutukset	Ei vakavat vaikutukset
Suuri	Korkea riski, vaatii toimenpiteitä	Melko korkea riski, tulisi suojautua	Seurattava riski, toimenpiteitä harkittava
Keskimääräinen	Melko korkea riski, tulisi suojautua	Melko korkea riski, tulisi suojautua	Seurattava riski, toimenpiteitä harkittava
Pieni	Melko korkea riski, tulisi suojautua	Seurattava riski, toimenpiteitä harkittava	Ei merkittävä riski, ei vaadi toimenpiteitä

Kun on selvitetty kunkin uhkan aiheuttama riski, voidaan arvioida kuinka tarpeellista riskiä on torjua, sekä minkälaisia suojauskeinoja tulisi käyttää(Peltier et al. 2005, s. 191). Riskikartoitus on tärkeää dokumentoida, jotta sitä voidaan tehokkaasti käyttää päätöksenteon tukena tietoturvapolitiikasta ja suojauskeinoista päätettäessä (ibid.). Riskikartoituksen jälkeen tarkistetaan, vastaavatko nykyiset tietoturvallisuustoimet kaikkien riskien suojaustarvetta.

Riskianalyysi ja –kartoitus ovat olleet käytössä erityisesti aikoina, jolloin riskin toteutumistodennäköisyys ja sen toteutumisen vaikutukset, esimerkiksi tuhoutuvan laitteiston arvo, on ollut helposti määritettävissä. Nykyaikana riskianalyysin tekeminen perustuu pitkälle analyysin tekijän subjektiiviseen arvioon tiedon arvosta sekä uhan toteutumisen kustannuksista (Gerber & von Solms 2001, s.580). Gerber ja von Solms (2001, s.582) esittävätkin turvallisuusvaatimus-analyysin uudenlaisena työkaluna riskianalyysien tilalle tilanteessa, jossa riskikartoitus on muuttunut hyvin subjektiiviseksi. Heidän mallissaan otetaan huomioon liiketoiminnan vaatimukset tiedon luottamuksellisuuden, saatavuuden ja eheyden suhteen, lain asettamat vaatimukset sekä fyysiseen omaisuuteen kohdistuvat riskit. Myös perinteisen riskikartoituksen voidaan kuitenkin katsoa toimivan jälkimmäisenä mainitun mallin mukaisesti, sillä arvioitaessa tiedon arvoa yritykselle tulisi kyseiset asiat joka tapauksessa ottaa huomioon. Kun esimerkiksi liiketoiminnassa tarvittavan tiedon arvoa ei voida tarkasti mitata, tulee riskiarviosta automaattisesti subjektiivinen, jolloin menetelmällä jolla sitä arvioidaan ei ole olennaista merkitystä. Tässä esitellyt menetelmät ovat vain esimerkkejä, lisää tietoturvallisuuteen liittyviä

riskiarviointimalleja löytyy esimerkiksi Viestintäviraston julkaisemasta yrityksen tietoturvaoppaasta[29] tai pk-yrityksille suunnatusta, VTT:n ylläpitämästä riskienhallintaoppaasta[30] .

5.4.3 Tietoturvallisuuspolitiikan määrittely

Riskiarvioinnin perusteella tehdään tietoturvallisuusuhkien arviointi, ja kehitetään tietoturvallisuuspolitiikka jolla tähdätään riskien poistamiseen tai niiden pienentämiseen. Ytimekkään tietoturvallisuuspolitiikan lisäksi tulisi tehdä erilliset ohjeistukset ainakin yrityksen kannalta tärkeiden tietojen luokittelusta ja käsittelystä, tietoliikenneyhteyksien käytöstä sekä perehdytysvaiheessa ja työsuhteen päättyessä läpi käytävistä tietoturvallisuuteen liittyvistä asioista. Ohjeistukset voivat olla hyvinkin lyhyitä ja selkeitä, mutta tärkeää on että ne tehdään yhteisen tietoturvallisuusnäkemyksen luomiseksi.

Tietoturvallisuuspolitiikan luomiseen voidaan keskittyä lyhyen aikaa isommalla työryhmällä, jolloin se vie luomistyön aikana suuren osan mukana olevien henkilöiden työpanoksesta. Toinen vaihtoehto on kehittää politiikkaa vähitellen vertaillen sitä mahdollisesti tarjolla oleviin malleihin. Politiikan määrittely rinta rinnan yrityksen strategian kanssa on myös hyvä vaihtoehto, sillä tietoturvallisuuspolitiikan tulee olla linjassa yrityksen muiden toiminnallisten tavoitteiden kanssa. Pidemmän aikavälin vaihtoehdossa politiikan luominen ei vie prosentuaalisesti niin suurta osaa tekijöidensä työpanoksesta, jolloin tietoturvallisuustyö ei häiritse ”tuottavaa” työtä tarpeettomasti.

Tietoturvallisuuspolitiikan sisältöä on kuvattu tarkemmin luvussa 2.3. Politiikan luominen on prosessimallin vaiheista ainoa, jonka sisältö on suunnilleen sama yrityksen koosta riippumatta. Politiikkadokumentin laajuus ei merkittävästi vaihtele sen perusteella, kuinka suuresta yrityksestä on kysymys. Politiikan pohjalta muodostettavien yksittäisten toimintaohjeistusten määrä voi vaihdella paljonkin yrityksen koon mukaan, eli ohjeistusten tarve tulee arvioida yrityskohtaisesti.

5.4.4 Tietoturvallisuuden ylläpito

Tietoturvallisuuden ylläpitovaiheessa, joka on yrityksen päivittäistä toimintaa, tulee huolehtia henkilökunnan tietoisuudesta tietoturvallisuuden ajankohtaisista asioista. Tietoisuutta voidaan kasvattaa tietoturvallisuuskoulutuksin ja ylläpitää erilaisin tietoiskuin kulloinkin ajankohtaisesta aiheesta. Tietoturvallisuustietoisuutta voisi kasvattaa yrityksissä perinteistä luentotyylistä koulutusta kevyemmällä järjestelyllä,

[29] www.tietoturvaopas.fi
[30] www.pk-rh.fi

jossa esimerkiksi viikko- tai kuukausipalaverien yhdeksi aiheeksi otettaisiin kulloinkin ajankohtainen tietoturvallisuusteema. Tällä järjestelyllä tietoturvallisuus nähtäisiin yrityksessä osana normaalia toimintaa ja erityisesti asiantuntijatyötä tekevien vastarinta erikseen järjestettyä koulutusta kohtaan ajanhaaskauksena saataisiin matalammaksi. Yksi teema voisi olla esimerkiksi salasanan rakenne ja muistisääntöjen kehittäminen, toinen teema tietojen luovuttaminen puhelimitse tai sähköpostilla. Tietoiskut toisivat tietoturvallisuuden teemat yleiseen tietoisuuteen varsin pienellä resurssien käytöllä foorumissa, jossa kaikki ovat läsnä.

Koulutuksen on todettu olevan kannattava investointi tietoturvallisuuden parantamiseksi (von Solms & von Solms 2004b, s. 375). Vaikka tutkimuksen yritykset ovat pieniä ja resursseja erillisen tietoturvallisuuskoulutuksen järjestämiseen on rajallisesti, pienimuotoisenkin koulutuksen järjestäminen tietoiskujen lisäksi voisi olla yritysten kannalta järkevää. Koulutuksessa tulisi painottaa teknisten välineiden tietoturvallisuuden lisäksi sitä, miten jokainen työntekijä osaltaan voi vaikuttaa yrityksen tietojen turvaamiseen. Keinot, joilla turvallisuuteen voidaan vaikuttaa ovat yrityskohtaisia ja riippuvaisia yrityksen toiminnan luonteesta, esimerkiksi konsultointitoiminnassa koulutuksen tulisi korostaa mukana kuljetettavan tiedon huolellista käsittelyä, sillä konsultti asiakkaiden luona kulkiessaan usein kantaa mukanaan huomattavan salaisia tietoja. Koulutuksen tulisi perustua yritysten riskikartoituksessa tunnistamien riskien suojaustarpeeseen, näin koulutuksesta saadaan irti paras hyöty ja tietoturvallisuuden ylläpitoon yrityksessä punainen lanka.

Tietoturvallisuuskoulutusta suunniteltaessa voidaan ottaa tavoitteiksi esimerkiksi henkilökunnan tietoisuus (Hansche 2004, s.1000)

- talletettuun (fyysiseen ja sähköiseen) tietoon kohdistuvista uhista
- siitä, miten tärkeitä tietoja tunnistetaan ja suojataan
- verkkoympäristöön kohdistuvista uhista
- siitä, miten tietoa talletetaan, luokitellaan ja siirretään
- toiminnassa noudatettavista laeista (henkilötietolaki, tietosuojalaki, tekijänoikeuslait jne.)
- siitä, millä tavalla ja kenelle tietoturvallisuuteen liittyvistä tapahtumista tulisi raportoida, riippumatta siitä onko tapahtuma vain epäilys väärinkäytöstä vai todellinen tietoturvarike
- ohjeistuksista ja politiikoista joita heidän tulee noudattaa.

Siitä, minkälaisia asioita tulee ottaa huomioon koulutuksia ja tietoturvallisuustietoisuuden kehittämistä suunniteltaessa, ei voi antaa yleispätevää suositusta, vaan yllä esitetty lista on yksi vaihtoehto asioista, joiden tulisi olla koulutuksen tavoitteena. Mikäli koulutukseen ja tietoisuuden ylläpitämiseen käytettävät resurssit ovat rajalliset, kuten pienten yritysten kohdalla usein on, voidaan lähteä liikkeelle esimerkiksi tietoturvallisuuspolitiikan läpikäynnistä niin, että voidaan

varmistua kaikkien ymmärtävän politiikan sisällön ja tavoitteet. Sen jälkeen tietoisuutta ylläpitävänä prosessina yrityksessä voidaan kerätä säännöllisin tai epäsäännöllisin väliajoin tietoturvallisuutta koskevia ajankohtaisia asioita tiedotteiksi, jotka toimitetaan työntekijöille esimerkiksi sähköpostilla tai paperikopioina.

6 YHTEENVETO

Tässä luvussa esitetään yhteenveto tutkimuksen havainnoista ja johtopäätöksistä. Lisäksi pohditaan tutkimuksen pohjalta nousevia jatkotutkimusaiheita sekä arvioidaan tutkimuksen onnistumista.

6.1 Tutkimuksen keskeiset havainnot

Tietoturvallisuuden muotoutuminen yrityksessä tapahtuu vähitellen joko ohjattuna tai spontaanina prosessina. Kuten tietoturvallisuuskulttuurin yhteydessä todettiin, yrityksessä voi olla tietoturvallisuuskulttuuri, vaikka tietoturvallisuus ei olisi merkittävässä roolissa yrityksen toiminnassa. Kulttuuri kuitenkin on olemassa ja vaikuttaa siihen miten työntekijät ottavat tai eivät ota tietoturvallisuutta huomioon omassa työssään. Tähän kulttuuriin tietoisesti vaikuttamalla tietoturvallisuus voidaan nostaa työntekijöiden tietoisuuteen ja parantaa yrityksen tietoturvallisuuden tilaa. Teknisen aallon tietoturvallisuuskulttuurissa saavuttaneet yritykset ovat aloittaneet tietoturvallisuuden kehittämisen, mutta vasta johtamisaallon myötä alkaa tietoinen vaikuttaminen tietoturvallisuuskulttuuriin muun muassa tietoturvallisuuspolitiikan avulla. Erilaiset koulutukset ovat myös merkittävässä roolissa tietoturvallisuuskulttuurin muokkaamisessa.

Tutkimuksen keskeinen havainto on, että erityisesti tekninen tietoturvallisuus on hoidettu tutkituissa yrityksissä hyvin. Tietoturvallisuus nähdään kuitenkin usein lähinnä tekniikkaan liittyvänä asiana, eikä aihetta ole tarkasteltu yrityksissä kokonaisuutena, johon vaikuttaa myös johdon ja työntekijöiden toiminta. Ainoastaan viidessä yrityksessä tietoturvallisuutta oli tarkasteltu kokonaisvaltaisemmin tietoturvallisuuspolitiikan luomisen yhteydessä, mutta myös näissä yrityksissä oli huomattu, että politiikan tekeminen ja sen noudattamisen vieminen jokapäiväisen toiminnan osaksi ei ole helppoa. Tähän tulisi kuitenkin pyrkiä vahvan tietoturvallisuuskulttuurin luomiseksi yrityksiin. Pääsyy siihen, ettei tietoturvallisuutta tarkastella kokonaisuutena on se, että tietoturvallisuus on usein sälytetty yhden henkilön vastuulle, tai vastuuta ei ole pohdittu lainkaan. Jotta kokonaisvaltainen tarkastelu olisi mahdollista, tulee tietoturvallisuuden kehittämisessä olla mukana useampia henkilöitä, sekä ehdottomasti johdon edustaja. Kun kehittämistyö aloitetaan, tulee johdon myös huolehtia, että vastuullisilla henkilöillä on resurssit kehitystyön tekemiseen. Mikäli vastuu sälytetään jonnekin, jonka jälkeen sen olemassaolo unohdetaan ja se haudataan tärkeämpien työtehtävien alle, ei tietoturvallisuus kehity itsestään. Vastuunjaon merkitys tietoturvallisuuden kehittymiselle on suuri ja sitä tulisi pohtia kaikissa auditoiduissa yrityksissä.

Kaikissa tutkituissa yrityksissä olisi tilaa systemaattiselle tietoturvallisuuden kehittämiselle, mutta erityisesti kehittämiseen tulisi kiinnittää huomiota yrityksissä joissa tietoturvallisuuspolitiikkaa ei vielä ole olemassa. Tietoturvallisuuteen kuuluu niin teknisen puolen hyvin hoitaminen kuin henkilöstön tietoisuudesta ja koulutuksesta huolehtiminen. Näiden molempien puolien riittävä huomioiminen on ehto tietoturvallisuuden toteutumiselle (Eloff & Eloff 2003, s.130). Tietoturvallisuuden kehittämisen tulisi lähteä yrityksen omien riskien arvioinnista ja suojaustoimenpiteiden valinnasta riskianalyysiin perustuen. Koska tekniset asiat ovat jo verrattain hyvin hoidettuja, lähinnä yrityksissä tulisi kiinnittää huomiota tietoturvallisuuden vastuiden jakoon ja kehittämisen systemaattisuuteen. Tietoturvallisuuspolitiikan dokumentointi auttaisi näiden molempien tavoitteiden kanssa, sillä politiikassa määritellään tietoturvallisuudesta vastuussa olevat sekä tietoturvallisuuden prosessit. Kehittämistyön tulisi kuitenkin lähteä liikkeelle riskien arvioinnista, sillä kuten luvussa 2.3 todetaan, tietoturvallisuuspolitiikan tulee olla yrityskohtainen. Paras tapa varmistaa yrityskohtaisuus on pohjata politiikka yrityksessä tehdylle riskiarvioinnille.

Yritykset voisivat vastata kaikkiin mainittuihin tietoturvallisuuden puutteisiin kehittämällä systemaattisen tietoturvallisuuden johtamisen prosessin. Luvussa 5.3 esitetään prosessimalli, joka on kevennetty versio kirjallisuudessa esiintyneistä tietoturvallisuuden kehittämisen prosesseista. Malli tarjoaa työkalun pk-yrityksen tietoturvallisuuden kehittämiselle, mutta se ei vaadi raskasta organisaatiota taakseen, vaan huomioi pk-yritysten tilanteen, jossa tietoturvallisuudesta vastuullisten työnkuva sisältää runsaasti muitakin, usein liikevaihdon tuottamiseksi tärkeämpiä tehtäviä. Tietoturvallisuuden kehittäminen itsessään ei tuo yritykseen lisää rahaa. Tietoturvallisuuden hyvä hoitaminen on kuitenkin tärkeää yrityksen luotettavuuden takaamiseksi. Luotettavuus todettiin tutkimuksen yrityksissä ensiarvoisen tärkeäksi asiakassuhteiden säilyttämiseksi. Tätä kautta tietoturvallisuuden järjestelmälliselle kehittämiselle yrityksissä on tarvetta.

6.2 Jatkotutkimusajatuksia

Tietoturvallisuuden tilan tutkiminen pelkkien haastattelujen perusteella on haastava tehtävä. Vaikka haastateltavien määrä eri yrityksissä vaihteli, yleisellä tasolla kaikista yrityksistä saatiin vertailukelpoiset vastaukset joiden perusteella tutkimuskysymyksiin kyetään vastaamaan. Haastattelu ei kuitenkaan ole ainoana tutkimuskeinona paras mahdollinen, jos halutaan syvemmin selvittää tietoturvallisuuden tilaa organisaatiossa. Vallitsevien käytäntöjen selvittäminen vaatisi vähintäänkin useita toisistaan riippumatta tehtyjä haastatteluja organisaatiota kohden, sekä esimerkiksi seurantaa siitä, miten henkilöt toimivat jokapäiväisessä työssään. Seurannan toteutustapoja ei ole aivan helppo määritellä ja näiden tutkimuskeinojen pohdinta toimisikin oivana jatkona tälle tutkimukselle.

Tietointensiiviset yritykset toimivat ympäristössä, jossa tieto ja sen turvaaminen ovat tärkeitä edellytyksiä yritysten liiketoiminnalle. Mikäli tutkimuksen kohderyhmänä olisivat esimerkiksi fyysisiä tuotteita valmistavat pk-yritykset, olisivatko tulokset olleet erilaisia? Kuinka hyvin yritykset, joiden tuotteena ei ole tieto, tunnistavat toiminnan kannalta tärkeät tiedot? Ja kuinka näissä yrityksissä tiedon suojaamiseen suhtaudutaan? Tutkimuksen toistaminen toiselle kohderyhmälle olisi mielenkiintoista.

Luvussa 5.3 esitetään parannusehdotuksena kevennetty tietoturvallisuuden johtamisen ja kehittämisen prosessimalli. Kyseisen mallin testaaminen yhdessä tai useammassa pk-yrityksessä toisi tietoa siitä, vastaako se yritysten tarpeita paremmin kuin kansainvälisessä kirjallisuudessa esitetyt raskaammat ja monivaiheisemmat prosessimallit. Tämän työn puitteissa malli jää teoreettiseksi sovellukseksi.

6.3 Työn onnistumisen arviointi

Alkutilanteessa työn tekijä sai itsenäisesti määritellä työn rajaukset, aikataulutuksen sekä yritysten valinnan. Tukea tehdyille päätöksille on toki ollut työn ohjaajan puolesta jatkuvasti tarjolla. Joku viisas on sanonut parhaan keinon hiillostaa työntekijöitä olevan antaa heidän itse määritellä omat tavoitteensa. Tässäkin yhteydessä itsenäinen tavoitteiden ja aikataulujen määrittely on saattanut johtaa liian kireisiin tavoitteisiin, mutta alkuasetelmaan nähden tavoitteet on saavutettu alle aluksi asetetun aikataulun. Työn tekijä on myös huomannut, että mikään ei motivoi työntekoon niin kuin lähestyvä deadline, joten hyvin valittujen välietappien määrittely on rytmittänyt työn tekemistä mukavasti.

Työn rajaus tietointensiivisiin pk-yrityksiin Pirkanmaalla toimi lopulta hyvin, vaikka ajoittain aidosti pirkanmaalaisten yritysten löytäminen tuntui hankalalta. Lopulta yrityksiä saatiin mukaan riittävästi ja valittu kohderyhmä tuli katettua hyvin. Koska työn tekeminen oli sidoksissa TTY:llä järjestettyyn kurssiin, tuli työ tehtyä oikeassa järjestyksessä, eli teoriaosuus oli pääosin tehtynä ennen haastattelujen suorittamista. Haastattelujen jälkeen analyysivaiheessa teoriaosuus tosin vielä täydentyi aiemmin unohtuneilla teemoilla ja näkökulmilla. Tämä on merkki hyvästä työprosessista, jossa teoria ja empiria aidosti kohtaavat.

Päätelmien kohdalla ongelmaksi muodostui konkreettisten parannusehdotusten tekeminen perustellusti. Teoriaosuus on kirjoitettu varsin yleisellä tasolla, eikä yksittäisten osa-alueiden kohdalla ole määritelty kovinkaan tarkasti minkälaisia hyvät tai huonot suojaustoimenpiteet ovat. Päätelmien kirjoittamisen myötä korjauksia teoriaan tältä osalta syntyi ja näin ehdotuksille saatiin myös perusteluja. Kun otetaan huomioon, että parannusehdotukset itsessäänkin ovat hyvin yleisiä eivätkä jollekin

tietylle yritykselle kohdennettuja, voidaan katsoa ehdotusten olevan riittävästi perusteltuja. Lisäarvoa työlle olisi tuonut, jos kehitettyä tietoturvallisuuden johtamisen prosessimallia olisi voitu testata jossakin tutkimuksen yrityksessä, mutta koska lähtökohta oli että yritykset esiintyvät tutkimuksessa anonyymeina tämä ei ollut tutkimuksen puitteissa mahdollista. Lisäksi testaus olisi huomattavasti venyttänyt työn aikataulua ja vienyt sen jo diplomityön laajuuden ulkopuolelle.

Prosessina diplomityön tekeminen oli antoisa ja hyvin opettavainen kokemus. Koska aihe lähti työn tekijän omista kiinnostuksista ja tutkimusasetelmakin oli itse määritelty, on motivaatio työn tekemiseen ollut erittäin hyvä. Nyt, kun tulokset on analysoitu, asettaisi työn tekijä haastattelukysymykset eri tavalla ja tekisi haastattelutkin toisin, mutta diplomityön on tarkoituskin olla työ, jonka myötä opitaan asioita tutkimuksen tekemisestä. Siinä tarkoituksessaan tämä työ toimi hyvin.

LÄHTEET

Alvesson, M. 2004. Knowledge Work and Knowledge-Intensive Firms. New York, Oxford University Press. 271 s.

Appleyard, J. 2004. Information Classification: A Corporate Implementation Guide. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss.715-725

Awad, E. M. Ghaziri, H. M. 2003. Knowledge Management. Upper Saddle River, Prentice Hall. 456 s.

Botha, J. von Solms, R. 2004. A cyclic approach to business continuity planning. Information Management & Computer Security, vol 12, no 4. ss. 328-337

BS 7799-1:fi. 2000. Tietoturvallisuuden hallinta. Osa 1: Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen standardisoimisliitto SFS. 107 s.

BS 7799-2:fi. 2000. Tietoturvallisuuden hallintajärjestelmät. Osa 2: Vaatimukset ja soveltamisohjeet. Suomen standardisoimisliitto SFS. 38 s.

Burrell, G. Morgan, G. 1979. Sociological Paradigms and Organizational Analysis. Elements of the Sociology of Corporate Life. Gower Publishing Company Ltd, Lontoo.

CEM v3.0. Common Methodology for Information Technology Security Evaluation. ISO/IEC. 466 s.

Choo, C. W. 2002. Information Management fo the Intelligent Organization. The Art of Scanning the Environment. USA. Information Today. 325 s.

Davenport, T. H. Prusak, L. 1998. Working Knowledge. How Organizations Manage What They Know. Boston, Harvard Business School Press. 199 s.

Dhillon, G. 1997. Managing information system security. Hampshire, Macmillan press ltd. 210 s.

Fenton, J. Wolfe, J. 2004. Organizing for Success: Some Human Resources Issues in Information Security. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss.887-898

Fontana, A. Frey, J. 2005. The Interview. Denzin, N. Lincoln, Y. (toim.) The SAGE Handbook of Qualitative Research. 3rd edition. Thousand Oaks, SAGE Publication. ss. 695-727

GAISP V3.0. 2004. Generally Accepted Information Security Principles. Information Systems Security Association. 53 s.

Gerber, M. von Solms, R. 2001. From Risk Analysis to Security Requirements. Computers & Security, vol 20, no 7. ss.577-584

Haarala, R. Lehtinen, M. Grönros, E. Kolehmainen, T. Nissinen, I. (Toim.) 2001a. Suomen kielen perussanakirja, ensimmäinen osa. Kotimaisten kielten tutkimuskeskuksen julkaisuja 55. Helsinki, Edita. 646 s.

Haarala, R. Lehtinen, M. Grönros, E. Kolehmainen, T. Nissinen, I. (Toim.) 2001b. Suomen kielen perussanakirja, kolmas osa. Kotimaisten kielten tutkimuskeskuksen julkaisuja 55. Helsinki, Edita. 663 s.

Hansche, S. 2004. Making Security Awareness Happen. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss.999-1022

Hale, J. Landry, T. Wood, C. 2004. Susceptibility audits: A tool for safeguarding information assets. Business Horizons, vol 47, issue 3. ss.59-66.

Haugen, S. Selin, J. 1999. Identifying and controlling computer crime and employee fraud. Industrial Management & Data Systems. 99/8. ss. 340-344.

Helenius, M. 2005. Tietoturvallisuuden tutkimus ja opetus. Nykytilanne ja kehittämismahdollisuudet. Tampere, Tampereen yliopisto. Tietoyhteiskuntainstituutin raportteja 2/2005. 51 s.

Heng, G. M. 1996. Developing a suitable business continuity planning methodology. Information Management & Computer Security. vol 4, issue 2. ss.11-13

Henry, K. 2004a. Operations: The Center of Support and Control. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss. 1559-1568

Henry, K. 2004b. Business Continuity Planning: A Collaborative Approach. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss.1699-1707

Hirsjärvi, S. Remes, P. Sajavaara, P. 2004. Tutki ja kirjoita. 10, osin uud. painos. Helsinki, Kustannusosakeyhtiö Tammi. 436 s.

Höne, K. Eloff, J.H.P. 2002. Information security policy – what do international information security standards say? Computers & Security, Vol 21, Issue 5. ss. 402-409

Jackson, C. 2004. Reengineering the Business Continuity Planning Process. . Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss.1645-1656

Kairab, S. 2005. A Practical Guide to Security Assessments. Boca Raton, CRC Press. 498 s.

Karakasidis, K. 1997. A project planning process for business continuity. Information Management & Computer Security, vol 5, issue 2. ss.72-78

Kuusisto, T. Ilvonen, I. 2003. Information Security Culture in Small and Medium Size Enterprises. Hannula, M. Järvelin, A. Seppä, M.(toim.) Frontiers of e-Business Research 2003, eBRF 2003 Conference Proceedings. ss. 431-439

Kuusisto, T. Slay, J. Kuusisto, R. 2004. Information Security Culture Approach to Knowledge Security. Proc. of the 5th Australian Conference on Information Warfare and IT Security. 6 s.

L 26.1.2001/55. Työsopimuslaki. [http://www.finlex.fi/fi/laki/ajantasa/2001/20010055]. Luettu 8.3.2006.

Metsämuuronen, J. 2005. Tutkimuksen tekemisen perusteet ihmistieteissä. 3. laitos, Jyväskylä, International Methelp Ky. 1292s.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen –näin suojaat yrityksesi toiminnan. Helsinki, Kauppakaari. 318 s.

Nonaka, I. Takeuchi, H. 1995. The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York, Oxford University Press. 284 s.

Olkkonen, T. 1994. Johdatus teollisuustalouden tutkimustyöhön. 2. painos. Espoo, Teknillinen korkeakoulu. Raportti 152/1993/Teta. 143 s.

Peltier, T. Peltier, J. Blackley, J. 2005. Fundamentals of information security. Boca Raton, CRC Press.

Peräkylä, A. 2005 Analyzing talk and text. Denzin, N. Lincoln, Y. (toim.) The SAGE Handbook of Qualitative Research. 3rd edition. Thousand Oaks, SAGE Publication. ss. 869-886

Posthumus, S. von Solms, R. 2004. A framework for the governance of information security. Computers & Security. vol 23. ss. 638-646.

Shorten, B. 2004. Information Security Policies from the Ground Up. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss. 917-924

Steinke, C. 2004. Physical Security: A Foundation for Information Security. Tipton, H. Krause, M. (toim.) Information Security Management Handbook. 5th edition. Boca Raton, CRC Press. ss. 1925-1933

Tekes. 2005. Pk-yrityksen määritelmä. [http://www.tekes.fi/rahoitus/yritys/pk.html]. Luettu 21.9.2005.

Thierauf, J. R. 2001. Effective business intelligence systems. USA, Quorum Books. 370 s.

Thomson, K. von Solms, R. 2005. Information security obedience: a definition. Computers & Security, vol 24, issue 1. ss. 69-75

Tipton, H. Krause, M. (toim.) 1999. Information security management handbook. 4th edition. Boca Raton. CRC Press. 711 s.

Tipton, H. Krause, M. (toim.) 2004. Information security management handbook. 5th edition. Boca Raton, CRC Press. 2036 s.

VAHTI 1/2001. Valtion viranomaisen tietoturvallisuustyön yleisohje. Valtiovarainministeriö.

Viestintävirasto 2001. Tietoturvallisuuden perusteet: haittaohjelmat. [http://www.ficora.fi/suomi/tietoturva/haittaohj.htm]. Luettu 8.2.2006.

VM 0024:00/02/99/1998. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta. [http://www.vm.fi/tiedostot/pdf/fi/6294.pdf]. Luettu 6.3.2006.

von Solms, B. 2000. Information Security – The Third Wave? Computers & Security, vol 19. ss.615-620.

von Solms, R. von Solms, B. 2004a. From policies to culture. Computers & Security, vol 23. ss.275-279.

von Solms, B. von Solms, R. 2004b. The 10 deadly sins of information security management. Computers & Security. vol 23. ss. 371-376.

Vroom, C. von Solms, R. 2004. Towards information security behavioral compliance. Computers & Security. vol 23. ss.191-198

Whitman, M. E. Mattord, H. J. 2003. Principles of information security. Canada, Course Technology. 532 s.