LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvan hallinta tietoteknisten turvallisuusjärjestelmien urakointitehtävissä

Syrén, Mikael

2012 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Tietoturvan hallinta tietoteknisten turvallisuusjärjestelmien urakointitehävissä

Syrén Mikael
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Joulukuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Syrén Mikael

Tietoturvan hallinta tietoteknisten turvallisuusjärjestelmien urakointitehtävissä

Vuosi 2012 Sivumäärä 57

Jokaisella yrityksellä on suojattavaa tietoa. Erityisesti liiketoiminnan kannalta kriittisen tiedon suojaaminen ja turvaaminen on yritysten menestyksellisen toiminnan ja sen jatkuvuuden kannalta tärkeää. Tietoturvan hallinnan avulla pyritään nykymäärittelyn mukaan varmistamaan tiedon käytettävyys, eheys, luottamuksellisuus sekä kiistämättömyys ja todentaminen.

Riippuvuus tietoteknisistä järjestelmistä tulee kaikessa liiketoiminnassa vain kasvamaan tulevaisuudessa, jolloin tietoturvan merkitys korostuu. Useissa yrityksissä ollaan siis muutoksen edessä, kun tietoturvakysymyksiä joudutaan perusteellisesti miettimään. Sama koskee myös turvaurakoitsijoita, jotka tietoteknisten turvallisuusjärjestelmien urakointitehtävissä käsittelevät paljon luottamuksellista tietoa. Teknisen puolen lisäksi tietoturvassa on huomioitava ihmisten työskentelytavat. Urakoitsijoiden on myös oltava tietoisia lainsäädännön velvoitteista tietojen turvaamiseen.

Opinnäytetyö toteutettiin yhteistyössä hankeyrityksen Seti Oy:n kanssa. Mukana oli myös Sähköinfo Oy:n edustaja. Työn tarkoituksena oli tutkia tietoturvaa ja sen tärkeimpiä tekijöitä olemassa olevan teorian avulla sekä lähestyä sitä kautta turvaurakoitsijan tietoturvan hallintaa urakointitehtävissä hankeyrityksen urakkaprosessimallin läpi. Tavoitteena oli, että opinnäytetyö itsessään tarjoaisi kuvauksen huomioitavista asioista tietoturvan hallinnassa itse yrityksen toiminnan sekä urakointitehtävien tarkastelukulmista. Lisäksi opinnäytetyö esittelee lopussa esimerkkikuvaukset turvaurakoitsijan tietoturvan menetelmäohjeista.

Opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä. Sen yhteydessä teetettiin myös kysely sähkö- ja turvaurakoitsijoiden keskuudessa. Työ tukee pääasiassa Sähköinfo Oy:n turvaurakoitsijoille kohdistamaa palvelutoimintaa (TU-koulutusta ja tietoturvaohjeistusta), mutta välillisesti myös Seti Oy:n TU-sertifiointia, koska urakoitsijalla on oltava käsitys tietoturvan merkityksestä ja mahdollisista menetelmistä sen hallintaan, jota sertifiointi edellyttää.

Asiasanat: tietoturva, tietoturvan hallinta, tietotekniset turvallisuusjärjestelmät, turvaurakointi

Laurea University of Applied Sciences **Abstract**
Leppävaara
Bachelor's Degree Programme in Security Management

Syrén Mikael

Information Security Management of Contracting Functions of Information Technology Security Systems

Year 2012 Pages 57

Every company has information that needs to be protected. In particular, protecting and securing the business-critical information is important in order to maintain successful operation and its continuity. According to the current definition information security management ensures the availability, integrity, confidentiality, non-repudiation and authentication of information.

Dependence on information technology systems in all business operations will only increase in the future, while information security is emphasized at the same time. Many companies are facing a change, when the security issues need to be thoroughly thought out. The same applies to security contractors who are dealing with a lot of confidential information in IT security system contracting tasks. In addition to the technical side of information security people's ways of working have to be taken into account. Contractors must also be aware of the obligations of the law for securing information.

The thesis project was carried out in cooperation with the company Seti Oy. There was also a representative from Sähköinfo Oy. The purpose was to examine the information security and the most important factors in the existing theory, and to approach its management in contracting tasks through the contracting process model of the project company. The objective was that the thesis itself provides a description of the important matters of information security management from the company's point of view, as well as from the contracting point of view. In addition, the thesis presents at the end examples of a description of the security methodology following the contractor's information security.

The thesis was carried out as exploratory development work. An inquiry was also implemented among the electrical and security contractors. The work primarily supports the focused services of Sähköinfo Oy for the security contractors (the TU-training and the guidance for security), but also, indirectly, the TU-certification of Seti Oy, because the contractor needs to have understanding of the importance of information security and the possible methods of its management, which are required in order to receive certification.

Keywords: Information Security, Information Security Management, IT Security Systems, Security Contracting

Sisällys

1 Johdanto

Tärkeän tiedon suojaaminen on yrityksissä yksi menestyksellisen liiketoiminnan edellytyksistä. Näiden tietojen puuttuminen, virheellisyys tai paljastuminen voi pahimmillaan aiheuttaa yritykselle merkittäviä taloudellisia tai muita vahinkoja. Esimerkkinä tästä on, kun vuonna 2009 liittovaltion poliisi FBI ilmoitti Coca Colan johdolle, että heidän tarkoin varjeltuun yrityskauppaa koskevaan materiaaliin oli päästy käsiksi. Arkaluontoisten tietojen vuotamisen arvellaan kaataneen 2,4 miljardin dollarin arvoisen kaupan toisesta juomavalmistajasta. Kyseisessä tapauksessa hakkerit pääsivät Coca Colan verkkoihin lähettämällä sähköpostia, jonka liitteenä oli tiedostoksi naamioitu vakoiluohjelma. (Bloomberg 2012.)

Jatkuvasti lisääntyvien tietojen ja tietojärjestelmien määrä asettaa yrityksille, joissa minkäänlaista tietoa käsitellään, uusia haasteita. Tietoturvan hallinnalla pyritään vastaamaan näihin haasteisiin. Yleisesti ottaen sillä tarkoitetaan tietojen, erilaisten järjestelmien ja palveluiden riittävää suojaamista lainsäädännön asettamien vaatimuksien sekä muiden toimenpiteiden puitteissa. Haasteellista tästä tekee sen, että riittävän tietoturvatason määrittäminen on yritysten omalla vastuulla, kun varsinaista pakottavaa lainsäädäntöä ei ole ja standardisointi etenee hitaasti. Lisäksi tietoturvan hallinta koetaan usein niin kauan jäykäksi ja hitaaksi ennen kuin jotain haitallista yrityksen liiketoiminnalle tapahtuu.

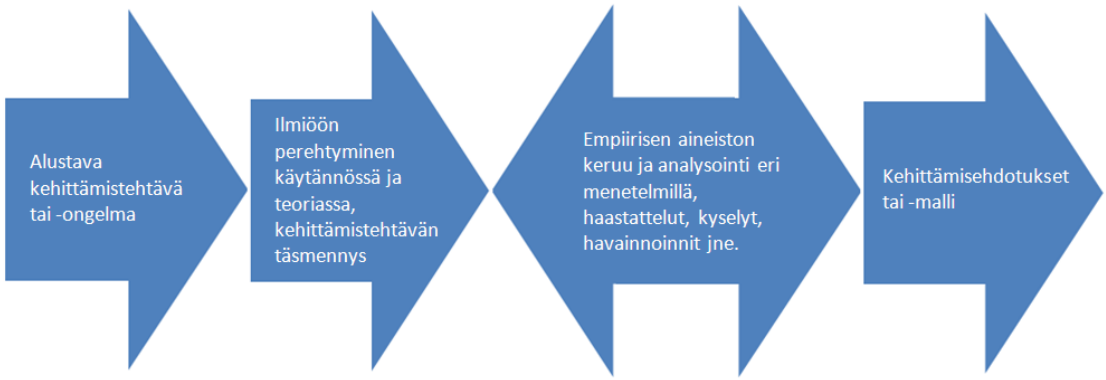
Periaatteessa kaikissa työtehtävissä on tilanteita, joissa tietoturva tulisi varmistaa. Jos ongelmia tulee, tiedetäänkö miten pitäisi toimia? Näitä seikkoja on tässä tutkimuksellisessa kehittämistyössä lähdetty selvittämään. Tietoturvaa ja sen hallintaa on työssä ensin tarkasteltu hyvin yksinkertaisella tasolla lähinnä yritysturvallisuuden näkökulmasta. Tämän jälkeen tarkastelukulmaa on ohjattu enemmän kohti varsinaista tarkoitusta eli turvaurakointia. Sitten aihetta on lähestytty hankeyrityksen turvaurakointiprosessiajattelua silmällä pitäen. Lopussa kyselyn jälkeen on pohdinnan yhteydessä esitelty yksi työn lopputuotoksista eli esimerkkikuvaukset turvaurakoitsijan menetelmäohjeista.

Opinnäytetyön itsessään voidaan ajatella toimivan turvaurakoitsijoille johdatteluna aiheeseen. Raportti etenee seuraavasti: ensiksi esitellään työn tutkimuksellinen ote, jota seuraa teoriaosuus. Teoria seuraa vahvasti myös, kun työssä seuraavaksi perehdytään menetelmiin tietoturvan hallitsemiseksi sekä turvaurakkaprosessin sitomiseen tietoturvaan liittyviin kohtiin. Tämän jälkeen syvennytään kehittämistyön yhteydessä toteutettuun kyselyyn ja sen analysointiin. Kaiken edellä mainitun pohjalta on lopussa pohdittu tietoturvan hallintaa tietoteknisten turvallisuusjärjestelmien urakointitehtävissä sekä turvaurakoitsijan tietoturvan menetelmäohjeiden esimerkkikuvauksia. Viimeiseen lukuun on pyritty yhteenvedon muodossa tiivistämään kaikki kehittämistyön kannalta oleellinen.

2 Tutkimuksellinen kehittämistyö

Tässä luvussa esitellään tarkemmin opinnäytetyön tutkimuksellista otetta. Siinä käydään läpi työn taustat, tavoitteet, työssä käytetyt menetelmät, määritellään keskeiset käsitteet ja kuvataan hankeyritys lyhyesti. Työn luonteen takia opinnäytetyöstä muodostui tutkimuksellinen kehittämistyö, jonka tukena on käytetty Ojasalon, Moilasen ja Ritalahden (2009) teosta Kehittämistyön menetelmät.

Opinnäytetyö on toteutettu alla olevassa kuviossa kuvattujen tapaustutkimuksen vaiheiden mukaan vaikka työssä on löydettävissä myös toiminta- ja konstruktiiviselle tutkimukselle ominaisia piirteitä. Alustava kehittämistehtävä, josta työssä lähdettiin liikkeelle, on tarkemmin avattu seuraavassa kappaleessa. Tämän jälkeen ilmiöön perehtymistä on käyty läpi palavereissa sekä aihetta käsittelevän kirjallisuuden avuin, mitä kautta kehittämistehtävää tarkennettiin. Sittemmin opinnäytetyössä toteutettiin kysely aiheeseen liittyen. Näiden pohjalta on muodostettu pohdinnassa esitellyt kehittämisehdotukset tai toisin sanoen esimerkkikuvaukset turvaurakoitsijan menetelmäohjeista.



Kuvio 1: Tapaustutkimuksen vaiheet (Ojasalo, Moilanen & Ritalahti 2009, 54.)

2.1 Opinnäytetyön tausta ja tavoitteet

Opinnäytetyö on toteutettu yhteistyössä hankeyrityksen Seti Oy:n kanssa. Mukana suunnittelussa ja palavereissa on ollut myös Sähköinfo Oy:n edustaja. Kehittämistarpeet yrityksellä liittyivät hyvin pitkälti tietoturvan pariin. Hankeyrityksessä koettiin, että turvaurakoitsijan tietoturvan hallinta erinäisissä asennus- ja ylläpitotoiminnassa vaati selvitystä sekä ohjeisto kehitystä.

Tämä lähestymiskulma johtui siitä, että hankeyrityksessä oli tunnistettu tietoturvaan liittyvien asioiden merkityksen korostuminen nyt ja lähitulevaisuudessa, jolloin heillä oli tarve kehittää palvelutoimintaansa ja sertifiointiaan vastamaan näihin haasteisiin. Turvaurakoinnissa ja

siihen liittyvissä työtehtävissä liikkuu paljon tietoa, ja luottamuksellisia tietoja joudutaan käsittelemään myös päivittäisessä työssä. Heidän haltuunsa uskotaan merkittävä määrä sellaista tietoa, joka joutuessaan vääriin käsiin, voisi aiheuttaa eri osapuolille suuria vahinkoja. Täten voidaan sanoa, että tietoturvan kunnollisella hallinnalla on tai ainakin tulisi olla iso merkitys turvaurakointitehtävissä jo pelkän liiketoiminnan jatkuvuuden kannalta.

Työn tarkoituksena oli tukea pääasiassa Sähköinfon turvaurakoitsijoille kohdistamaa palvelutoimintaa (TU-koulutusta ja tietoturvaohjeistusta), mutta välillisesti myös Setin TU-sertifiointia, koska urakoitsijalla on oltava käsitys tietoturvan merkityksestä ja mahdollisista menetelmistä sen hallintaan, jota sertifiointi edellyttää. Tätä ajatusta voidaan oikeastaan pitää punaisena lankana koko työlle. Lisäksi sen tarkoituksena oli tutkia tietoturvaa ja sen tärkeimpiä tekijöitä olemassa olevan teorian avulla sekä sitä kautta lähestyä turvaurakoitsijan tietoturvan hallintaa urakointitehtävissä muun muassa hankeyrityksen urakkaprosessimallin läpi.

Tavoitteena oli, että opinnäytetyö itsessään tarjoaisi kuvauksen huomioitavista asioista tietoturvan hallinnassa sekä itse yrityksien toiminnan, että urakointitehtävien tarkastelukulmista. Tästä johtuen työ ei siis kokonaisuutena ole täysin tasapainossa teorian ja empirian suhteen. Lisäksi pohdintojen yhteydessä tuli esittää esimerkkikuvaus turvaurakoitsijan tietoturvan menetelmäohjeesta. Menetelmäohjeen osalta päädyttiin tekemään kaksi esimerkkikuvausta edellä mainittujen eri tarkastelukulmien takia. Tavoitteisiin lukeutui myös kyselyn toteuttaminen, jota on tarkemmin käyty läpi työn loppu puolella.

2.2 Keskeiset käsitteet

Tietoturva (information security) käsitettä *k*äytetään tässä työssä terminä muiden synonyymien kuten tietoturvallisuuden sijaan. Tietoturva on kokonaisvaltaisen yritysturvallisuuden ja riskienhallinnan osa-alue. (VAHTI 8/2008, 107, 109.) Sen tarkoituksena on varmistaa tiedon käytettävyys, eheys ja luottamuksellisuus hallinnollisilla, teknisillä ja muilla toimenpiteillä ja järjestelyillä (KATAKRI 2011, 125). Tietojen suojaamisen lisäksi siihen kuuluu järjestelmien ja palveluiden suojaaminen sekä normaali- että poikkeusoloissa (Viestintävirasto 2012.)

Tietoturvan hallinnalla (managing information security) tarkoitetaan tässä tekstissä niitä toimia, joilla tietoa pyritään suojaamaan, kuten tietoturvan organisointi ja ohjeistukset. Jos tietoturvan tarkoituksena on varmistaa tiedon käytettävyys, eheys ja luottamuksellisuus, niin sen hallinta tarjoaa pohjan sen varmistamiseksi. Kokonaisvaltaisen tietoturvan hallinnan toteutus on yleisesti jaoteltu kahdeksaan osa-alueeseen: hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Tietotekniset turvallisuusjärjestelmät (IT security systems) käsittävät kaikki havaitsemiseen ja hälyttämiseen liitettävät järjestelmät kuten kamera- ja kulunvalvonnan. Tarkemmin sanottuna sillä tarkoitetaan yritysten turvajärjestelmien ja tietoteknisten järjestelmien yhdistämistä. Tietoteknisten turvallisuusjärjestelmien urakointitehtävissä yleisten perusvalmiuksien ja teknisen puolen ymmärtäminen korostuvat.

Turvaurakoinnilla (security contracting) tarkoitetaan asiakkaalle tehtävää projektia, jossa pyritään tarjoamaan kaikki tarvittava turvatekniikka samassa paketissa. Tämä voi tarkoittaa edellä mainittujen kamera- ja kulunvalvontajärjestelmien lisäksi esimerkiksi murtoilmaisu- ja paloilmoitinjärjestelmien urakointia. Turvaurakoinnissa voidaan yleisesti nähdä kolme päävaihetta, jotka koostuvat myyntiprosessista, järjestelmien asennuksesta ja, sopimuksen mukaan, mahdollisesta ylläpidosta.

2.3 Hankeyritys

”Henkilö- ja yritysarviointi Seti Oy on Turvatekniikan keskuksen nimeämä puolueeton ja riippumaton sähköturvallisuuslakien mukaisten sähköpätevyystodistusten arvioija. Lakisääteisten pätevyystodistusten lisäksi Henkilö- ja yritysarviointi Seti Oy myöntää tele-, turva- ja kuntotutkijapätevyyksiä sekä vaaditut ehdot täyttäville yrityksille SETI-, tele- ja turvaurakoitsijahyväksyntöjä”. (Henkilö- ja Yritysarviointi Seti Oy 2012.) Turva-alan yrittäjät ry suosittelee jäsenilleen Seti Oy:n myöntämää TU-yritystssertifikaatia. Sertifikaatin avulla turvaurakoitsijat voivat osoittaa asiakkailleen muun muassa tietoturvateknisen osaamisensa.

Julkisesti hankeyrityksestä saatavien tietojen perusteella mainittakoon, että kaupparekisterin päivämäärä sijoittuu vuodelle 1996. Yritys sijaitsee tällä hetkellä Espoon Leppävaarassa. Joulukuussa 2009 siellä työskenteli neljä henkilöä. Tämän jälkeen henkilöstön lukumäärää ei kaupparekisteriin ole päivitetty. Yrityksen verkkosivuilta löytyvien yhteystietojen mukaan henkilökuntaa on kuitenkin tällä hetkellä viiden henkilön verran. Liikevaihdosta saadaan muodostettua nousujohteinen viiva aina vuodesta 2007 vuoteen 2011, jolloin ilmoitettu liikevaihto oli 764 000 euroa.

Sähköinfo Oy puolestaan tekee tiivistä yhteistyötä koulutusten järjestämisessä Seti Oy:n kanssa. Lyhyesti sanottuna se on STUL ry:n omistama koulutus- ja kustannusyhtiö, joka on perustettu jo vuonna 1968. Sähköinfo Oy tuottaa sähköalaa koskevaa kirjallisuutta, koulutusta ja muita palveluita, joista tämän työn yhteydessä on keskitytty siis koulutukseen ja tietoturvaohjeistuksen kehittämiseen. (Sähköinfo 2012.) Hankeyrityksestä puhuttaessa viitataan molempiin kyseisiin yrityksiin.

Kehittämistyön painopiste on turvaurakoitsijoissa (ja hankeyrityksen heille suunnatussa palvelutoiminnassa ja sertifioinnissa), jotka asentavat ja/tai ylläpitävät tietoteknisiä turvallisuusjärjestelmiä, kuten paloilmoitin- ja murtoilmaisujärjestelmiä, kamera- ja kulunvalvontajärjestelmiä ja henkilöturvallisuusjärjestelmiä. Kuten aiemmin on mainittu, tulee urakoitsijoilla olla käsitys tietoturvan merkityksestä ja menetelmistä sen hallintaan sertifioinnin kriteerien täyttämiseksi. Tietoturvan hallintaa tullaan kehittämistyön myöhemmässä vaiheessa tarkastelemaan muun muassa Seti Oy:n TU-yritystssertifioinnin vaatimuksien näkökulmasta yrityksen toiminnanohjaukselle, jota on kuvattu alla olevassa kuviossa. Siitä voidaan myös hyvin nähdä, mitä asioita urakka pitää sisällään.

Kuvio 2: Turvaurakointiprosessi

2.4 Työn menetelmällinen perusta

Kuten aiemmin on mainittu, niin opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä. Tutkimuksellinen kehittämistyö eroaa hyvinkin paljon tieteellisestä tutkimuksesta. Siinä perinteiset seikat, kuten tutkimusongelma ja siihen vastaaminen käyttämällä tarkoin vain yleisesti hyväksyttyjä menetelmiä, eivät nouse niin suureen rooliin. Kyseisessä opinnäytetyössä lähtökohtina ovat yrityksen kehittämistarpeet ja niiden saavuttaminen eli pyrkimys ratkaista käytännön ongelmia ja tuottaa uusia ideoita ja käytäntöjä heidän tarpeisiinsa. Toisin sanoen työssä halutaan tuoda esille käytännön parannuksia, eikä luoda uutta teoriaa. (Ojasalo ym. 2009, 18–20.)

Teoriaa käydään toki myös tässä opinnäytetyössä läpi tarvittavan tietoperustan ja kuvauksen luomiseksi, mutta sitä ohjaa enemmänkin yrityksen kanssa asetutetut käytännölliset tavoit-

teet, joita tuetaan teorialla. Tietoperusta pohjautuu hyvin pitkälti yritysturvallisuuden käytäntöihin, kansainväliseen turvallisuusauditiointikriteeristöön (KATAKRI) sekä VAHTI-ohjeistuksiin tietoturvasta. Lisäksi työssä on läpi projektin oltu vuorovaikutuksessa hankeyritykseen, jotta ongelmia voitaisiin paremmin havainnoida ja sitä kautta ratkaista. (Ojasalo ym. 2009, 20–21.)

Teoreettisella viitekehyksellä tarkoitetaan tässä työssä näkökulmaa, josta aihetta tarkastellaan. Kuten aikaisemmin on mainittu, niin näkökulmana on tietoteknisten turvallisuusjärjestelmien urakointitehtäviin liittyvän tietoturvan hallinta. Aihetta on kuitenkin jouduttu lähestymään paljon laajemmasta tarkastelukulmasta kokonaisuuden hahmottamiseksi ja ymmärtämiseksi sekä halutun lopputuloksen saavuttamiseksi. Lisäksi sitä on tarkastelu hankeyrityksen turvaurakointiprosessin läpi.

Tietoperustan ilmeneminen tapahtuu ”oivalluttava – perinteinen” – mallin mukaan, jossa tietoperusta on erillinen kokonaisuus tekijän omaa ajattelua lisättynä. Varsinaisten tulosten esittelyä ei vielä sen yhteydessä tehdä. (Ojasalo ym. 2009, 36.) Teoriaosuudessa pyritään vastaamaan kysymyksiin: mitä tietoturva on? Miksi sitä tarvitaan? Miten sitä voisi toteuttaa ja millä menetelmillä? Lähestymistapana käytetään alustavan suunnitelman mukaan sovellettua tapaus-, toiminta- ja konstruktiivista tutkimusta.

Tämä johtuu siitä, että kehittämistyössä on tarkoituksena tuottaa yritykselle kehittämisehdotuksia, jolloin lähestymistapana on tapaustutkimus. Toisaalta taas toimintatutkimukselle tyypillisesti työssä painottuu yhtäaikaisesti tutkitun tiedon tuottaminen ja käytännön muutoksen aikaansaaminen. Konstruktiivisessa tutkimuksessa tehtävänä on tuottaa jotain konkreettista, joka tässä tapauksessa on esimerkkikuvaukset menetelmäohjeista. (Ojasalo ym. 2009, 36–38.)

Jo aiemmin mainitun kyselyn lisäksi muita menetelmiä ovat yhteisölliset menetelmät kuten aivoriihityöskentely hankeyrityksen edustajien kanssa sekä yhteiset palaverit. Kysely valittiin niin sanotuksi tutkimusmenetelmäksi, koska sen uskottiin palvelevan parhaiten lopullista tarkoitusta ja tuottavan eniten tutkimusaineistoa käytettävissä olevaan aikatauluun suhteutettuna. Lisäksi sen toteuttaminen oli muihin vaihtoehtoihin nähden joustavaa ja hankeyrityksellä oli laaja verkosto käytettävissään, joille kyselylomake oli mahdollista lähettää.

Menetelmänä kyselylomake on hyvin tyypillinen määrällinen menetelmä. Kuitenkaan sen tarkoituksena ei niinkään ollut testata teorian paikkaansa pitävyyttä, vaan muodostaa käsitystä turvaurakoitsijoiden tietoturvan hallinnasta. Tutkimuksellisessa kehittämistyössä menetelmät ovat hyvin pitkälti vain välinearvon roolissa, auttamassa työtä parhaaseen mahdolliseen lopputulokseen, mikä oli kyselyn rooli myös tässä opinnäytetyössä. (Ojasalo ym. 2009, 93–95.)

Projektiluontoisen opinnäytetyön onnistumista joudutaan arvioimaan ja mittamaan eri tavoin kuin puhdasta tutkimuksellista työtä. Ajatuksena oli, että opinnäytetyön onnistumista arvioitaisiin yhteistyöyrityksen kanssa arviointipalaverin yhteydessä. Palaverissa voitaisiin käydä läpi koko prosessin onnistumista sekä lopullisen tuotoksen hyödyllisyyttä heidän palvelutoimintaansa ajatellen. Tiukan aikataulun takia arviointiosuutta ei ole itse raporttiin keritty sisällyttää.

3 Teoriaa tietoturvasta

Seuraavien alalukujen pyrkimyksenä on tuoda esille tietoturvaan liitettyjä tekijöitä hyvin yleisellä tasolla, jotta ne muodostaisivat helposti yleiskuvan tietoturvasta, ja siten palvelisivat lopullista tarkoitusta mahdollisimman hyvin. Teoriaosuuden on tarkoitus esitellä niin sanotut kulmakivet tietoturvan osalta, jotta lukija saisi hyvän yleiskuvan lisäksi käsityksen tietoturva todellisesta laajuudesta ilman teknisten asioiden käsittelyä. Tässä vaiheessa ei vielä ole ajatuksena syventyä turvaurakointiprosessin kannalta oleellisimpiin tietoturvaseikkoihin vaan tuoda esille, että toimiva tietoturva vaatii kokonaisvaltaista tietoturvan hallintaa.

3.1 Tiedon turvaamisen lähtökohdat

Tietoturvan lähtökohtana yrityksen tai organisaation näkökulmasta pidetään lähes poikkeuksetta tiedon käytettävyyden, eheyden ja luottamuksellisuuden suojaamista. Lyhyesti sanottuna tällä tarkoitetaan sitä, että tieto on tarvittaessa saatavilla, se on vääristymätöntä ja tietoihin pääsevät käsiksi vain siihen oikeutetut käyttäjät. (Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen & Vesterinen 2008, 69; Leppänen 2006, 260—261.) Nykyään tätä lähestymistapaa ei kuitenkaan pidetä täysin riittävänä: kiistämättömyys ja todentaminen on lisätty tietoturvan lähtökotiin. Tiedon kiistämättömyydellä tarkoitetaan sitä, että käyttäjien väliset tapahtumat pystytään (jälkikäteen) todistamaan. Todentamisella puolestaan tarkoitetaan käyttäjän valtuuksien varmistamista, esimerkiksi tunnus- ja salasanayhdistelmillä, ennen kuin pääsy tietoihin sallitaan. (Raggad 2010, 20—23.)

Kuten käsitteiden avaamisen yhteydessä on tullut ilmi, on tietoturva yksi (tärkeimmistä) riskienhallinnan osa-alueista, joka tukee muun riskienhallinnan ohella yrityksen tai organisaation päätehtävää. Tämän johdosta toimivan tietoturvan rakentaminen myötäilee riskienhallintaprosessin perusperiaatteita: ensiksi kartoitetaan suojattavat kohteet, tehdään riskianalyysi ja luokitellaan tieto (Yrityksen tietoturvaopas 2012a). Tämä on ensisijaisen tärkeää, jotta tiedetään lähtökohtaisesti, mitä ylipäätään lähdetään suojaamaan. Näin suojaustoimenpiteet on myös helpompi tehokkaammin kohdistaa.

VAHTI Johdon tietoturvaoppaassa (2/2011, 16) painotetaan, että tietoturvatoimenpiteiden tulee perustua riskienarviointiin. Oppaassa käy myös hyvin ilmi, että säännönmukainen tietoriskien arviointi tulee olla integroituna osaksi muuta riskienhallintaa (ja toiminnan suunnittelua tai laatumallia). Esille nousevat myös lainsäädännölliset seikat, joita käsitellään myöhemmin tässä tekstissä.

Ruohonen (2002, 6) pitää tärkeänä osana tietoturvallisuutta tietoturvasuunnitelman tekemistä. Hänen mukaansa se helpottaa tunnistamaan tietoa uhkaavat riskit ja kohdistamaan suojauksen riittävällä tasolla ja tehokkaasti oikeisiin kohteisiin. Ruohonen huomauttaa myös, että tietoturvapolitiikkassa esitetään siihen liittyvistä kohdista, kuten tietoturvan tavoitteet, vastuut ja toimenpiteet, vain yleisluonteinen kuvaus, kun taas tietoturvasuunnitelmassa näiden kohtien määrittely on yksityiskohtaista. Kuitenkin myös tietoturvapolitiikan laatiminen on yksi tärkeimmistä lähtökohdista ja dokumenteista tietoturvan osalta.

Tietoturvasuunnitelman laatiminen politiikan pohjalta onkin seuraava askel kohti toimivaa tietoturvaa. Ihmisten ja työntekijöiden toimintatavat korostuvat tietoturva-asioissa, joten tietoturvasuunnitelman ja -toimenpiteiden käyttöönottovaiheessa on huolehdittava henkilöstön tarvittavasta koulutuksesta ja perehdytyksestä. VTT:n Pk- yrityksien riskienhallinnan internet- sivustolla (PK-RH 2009) todetaankin, että ” riskejä hallittaessa on otettava lähtökohdaksi toiminnan kehittäminen - toimintatavat, osaaminen, johtaminen - ja vasta sen jälkeen tulevat tekniset suojauskeinot”. Tietoturvaa käsittelevässä kirjallisuudessa ja muissa ohjeistuksissa usein korostetaankin teknisten ratkaisujen lisäksi edellä mainittua ihmisten toimintaa yhtenä tärkeimmistä tekijöistä tietoturvan kannalta. On todettu, että 20 prosenttia tietoturvasta muodostuu teknisistä suojauskeinoista ja 80 prosenttia henkilöstön tietoturvatietoisuudesta ja – osaamisesta sekä näiden kehittämisestä (Halmevuo, Kyrölä, & Vuori 2004). Täten yksi tiedon turvaamisen lähtökohdista on tietoturvatietoinen ja osaava henkilöstö.

Jotta hyöty tietojen turvaamisesta olisi yritykselle mahdollisimman suuri, on huolehdittava riskienhallintaprosessille ominaisesti jo mainittujen kohtien lisäksi seurannasta ja jatkuvuudesta. Tietoturvan on täten oltava hallinassa myös muuttuneissa olosuhteissa. Seurannalla ja jatkuvuudella pyritään huolehtimaan siitä, että toiminta vastaa tarpeita ja, että häiriötilanteessa tai poikkeusoloissa toimintaa pystytään jatkamaan mahdollisimman nopeasti. (VAHTI 3/2007, 73.)

Yksinkeraisimmillaan tietoturvan lähtökohdat eli ne kohdat, jotka tulisivat jokaisessa yrityksessä tai organisaatiossa, joissa minkäänlaista tietoa käsitellään, voidaan esittää porrasaskelmien muodossa kuvion 3 mukaisesti:

Kuvio 3: Tietoturvan portaittainen toteutus (Yrityksen tietoturvaopas 2012b.)

3.2 Tavoitteet

Tietoturvan tärkeimmät perustavoitteet tulivat oikeastaan esille edellisen luvun yhteydessä: tiedon käytettävyyden, eheyden, luottamuksellisuuden, kiistämättömyyden ja todennettavuuden suojaaminen sekä varmistaminen. Tavoitteellisesti ajateltuna näillä voidaan tarkoittaa esimerkiksi sitä, että tiedot ja erilaiset tietojärjestelmät ovat käytettävissä kun niitä tarvitaan (käytettävyys), ne eivät vahingoitu (eheys), yrityksen toimintaan liittyvät luottamukselliset tiedot eivät joudu vääriin käsiin (luottamuksellisuus), väärinkäyttö on minimoitu (kiistämättömyys) ja tietoja ei valtuudetta muuteta (todentaminen).

Näiden tavoitteiden toeutuminen johtaa taas siihen, että yrityksessä pystytään hallitsemaan tietojen liikumista sen sisällä ja ulkopuolella. Lisäksi se vähentää turhia huolto- ja korjauskustannuksia, mikä puolestaan lisää yrityksen uskottavuutta, parantaa mainetta ja luo hyvän imagon. Näin yritys voi tehokkaammin keskittyä ydinliiketoimintaansa ja parantaa kannattavuuttaan. (Yrityksen tietoturvaopas 2012c.) Tietoturvan merkityksestä puhutaan työn myöhemmässä vaiheessa lisää.

Kehittämistyön kannalta on olennaista käsitellä tavoitteita myös operatiivisen tietoturvatoiminnan kannalta, johon turvaurakointiin liittyvät asennus- ja ylläpitotehtävät usein kuuluvat. VAHTI- julkaisussa (6/2006, 25) mainitaan, että juurikin operatiiviselle tietoturvatoiminnalle voidaan asettaa määrällisillä (kvantitatiivisilla) mittareilla mitattavissa olevia tuloksellisuus- ja laatutavoitteita. Julkaisussa listataan tyypillisiksi tavoitteiksi muun muassa:

- häiriöiden vähentyminen
- kolutuksen toteutuminen
- tietoturvatoimintaan liittyvät kustannustavoitteet
- kypsyystason arviointi (laadullisen arvioinnin näkökulma)

Taloudellisena tavoitteena kyseisessä teoksessa mainitaan riskien toteutumisesta toiminnalle aiheutuvien menetyksien vähentyminen. Tähän esimerkkeinä voidaan ajatella vaikka, ettei kauppoja menetetä kilpailijoille tai, etteivät asiakastiedot siirry entisten työntekijöiden mukana toisiin yrityksiin. Negatiiviset seuraukset näiden riskien toteutumisesta voivat olla taloudellisesti hyvinkin pitkäaikaisia.

3.3 Henkilöstön osaaminen

Tietoturvavahinkojen toteutuessa voidaan perimmäisinä syinä usein nähdä uhan tiedostamattomuus käytännön tilanteessa, epätietoisuus oikeista menettelytavoista tai ohjeiden noudattamatta jättäminen. Kuten aikaisemmin on todettu, voidaan ihmistä pitää tärkeimpänä tekijänä tietoturvaan liityvissä asioissa. Tietoturvaa ja siitä huolehtimista tulisi yrityksissä pitää kaikkien vastuuna, jonka toteutuksessa myös kaikilla on vaikutuksensa. Ihmiset käsittelevät suojattavaa tietoa monissa eri muodoissa ja työn vaiheissa. Turvallisuustietoisuus on siten yhä tarpeellisempaa, jolloin myös henkilöstön tietoturvaosaaminen korostuu. (VAHTI 11/2006, 11.)

Tästä voidaan päätellä se, että ehdoton edellytys tietoturvalle on oikeat menettelytavat ja niiden noudattaminen, mutta ilman tarvittavaa perehdytystä, ei tietoturvaratkaisuista saada kaikkea hyötyä irti. Mitä paremmin tietoturvaan liittyvät käytännöt ovat henkilöstön hallussa, sitä paremmin tietoturva toimii. Suositeltavaa olisikin panostaa ennemmin henkilöstön osaamiseen muun muassa ohjeistamalla, perehdyttämällä, kouluttamalla, kehittämällä työmenetelmiä ja asenteisiin vaikuttamalla, kuin laajojen ohjeistuksien laatimiseen (VAHTI 2/2008, 19).

Henkilöstöstä puhuttaessa on syytä tuoda esille myös yrityksen tai organisaation sisältä tulevat riskit, joilla tarkoitetaan lähinnä henkilöstön väärinkäytöksiä. Edellä mainitun henkilöstön osaamiseen panostamisen lisäksi näitä riskejä voidaan minimoida huolellisen rekrytoinnin yhteydessä tehtävillä taustaselvityksillä, tietojen käyttöoikeuksien myöntämisellä työtehtävien mukaisesti, salassapitosopimuksilla, tietojen huolellisella luokittelulla, sisäisellä valvonnalla ja tarkastuksella, kulunhallinnalla ja johdonmukaisella seuraamusmenettelyllä. Lisäksi yrityksen on otettava huomioon, miten se hoitaa irtisanomiset eli työsuhteen päättämisen tietoturvallisesti. (VAHTI 2/2008, 19–20.)

3.4 Lainsäädäntö

Tietoturva elää ja muuttuu voimakkaasti koko ajan, koska toiminnat sekä palvelut sähköistyvät, mitä kautta tekninen riippuvuus kasvaa. Tämä tuo mukanaan uusia uhkia, jotka kohdistuvat erityisesti tietoihin ja niitä käsitteleviin järjestelmiin ja ihmisiin. Tietoturvaa koskevissa asioissa lainsäädäntö on erittäin tärkeässä roolissa jo sen takia, että se asettaa toiminnasta riipuen omat velvoitteensa ja edellytyksensä. Sen keinon pyritään myös vastaamaan näihin uhkiin. (VAHTI 2/2011, 15.)

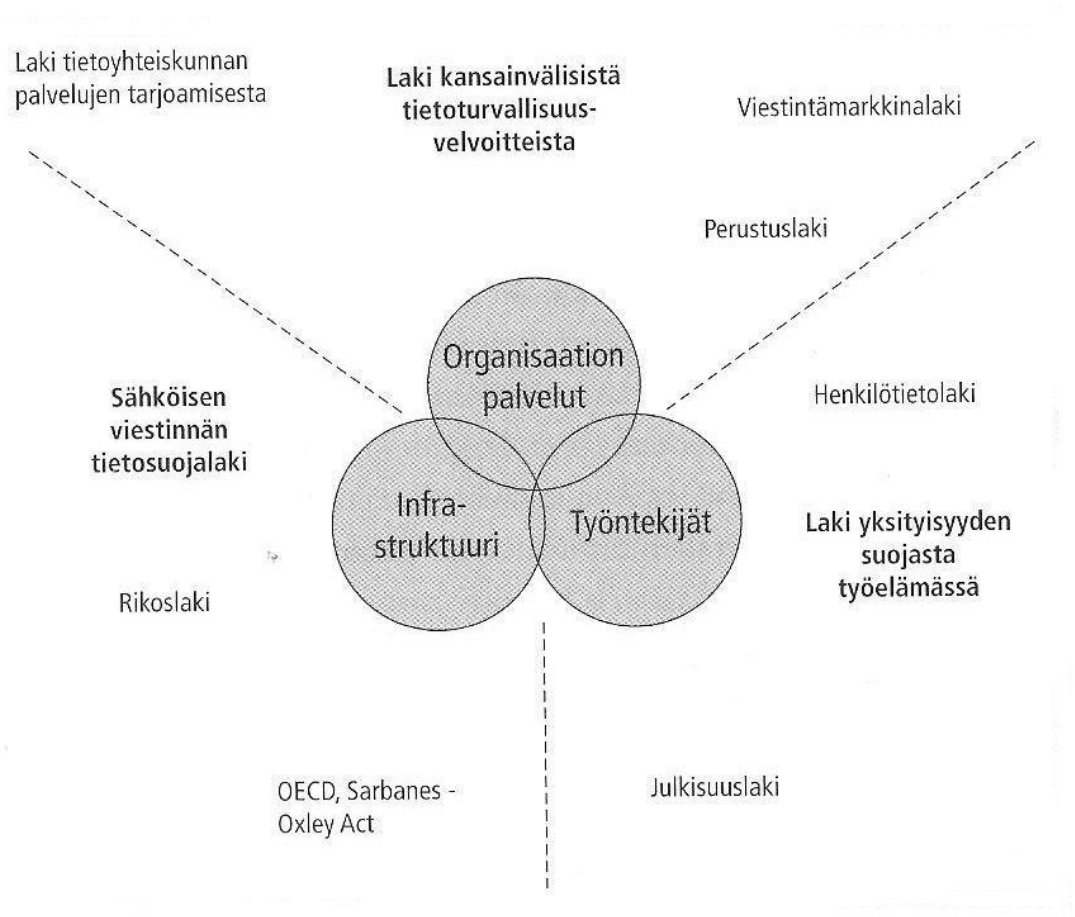
Yrityksissä tuleekin tunnistaa yritystä ja sen toimintaa koskeva lainsäädäntö. Lisäksi tulee varmistua siitä, että toiminta on lainmukaista ja se täyttää sille asetetut velvoitteet. Tietojen suojaamatta jättämisellä voi olla oikeudellisia seuraamuksia, mikä voi olla erittäin haitallista liiketoimintaa ajatellen. Toiminnan lainmukaisuuden lisäksi yritysten vastuulla on myös henkilöstön ohjeistaminen. (VAHTI 2/2011, 15.)

Tietoturvan näkökulmasta lainsäädännössä määritellyt velvoitteet jäävät yleisluontoisiksi kuvauksiksi. Niin tietoturvan toteutus, kuin riittävän tason määrittäminen jäävät yrityksen omalle vastuulle. (Laaksonen, Nevasalo & Tomula 2006, 18.) Tästä johtuen usein johtopäätöksenä tietoturvan kannalta on, ettei pakottavaa tietoturvaa koskevaa lainsäädäntöä ole olemassa, eikä siihen siten tarvitse huomiota kiinnittää. Tähän tekosyyhyn tukeutuvien on kuitenkin huomattava se fakta, että tämän aiheen ympärille rakennettava lainsäädäntö ei pysty millään varautumaan niihin haasteisiin, joita tekniikan tämän hetkinen kehitysvauhti tuo tullessaan.

Siihen on kuitenkin viime vuosina tullut merkittävä määrä uusia säädöksiä, joiden pyrkimyksenä on ollut tietoturvatoimenpiteiden määrittäminen eri tilanteissa. Lainsäädännön ja sen muutoksien tunteminen ja seuraaminen onkin erityisesti kyseessä olevalla alalla kriittisen tärkeää. Laaksosen ym. (2006, 18) mukaan yrityksissä tulisikin kartoittaa pakottavat yksittäiset säädökset, jotka koskevat tietoturvan suunnittelua, ylläpitoa ja kehittämistä. Lisäksi hän nostaa esille sopimuksiin liittyvien tietoturvavelvoitteiden tuntemisen. Erilaisissa hankkeissa, kuten myös turvaurakoissa sopimuksia tehdään eri osapuolten kanssa, minkä takia edellä mainittu seikka on huomioitava.

Tämän opinnäytetyön puitteissa ei ole mahdollista käydä lakeja ja säännöksiä yksityiskohtaisesti läpi. Kuten kuviosta 4 on nähtävissä lainsäädännön kenttä saattaa olla hyvinkin laaja. Sähköinfo Oy ja Turva-alan yrittäjät ovat yhteistyössä (2005) tehneet ohjeen Tietosuoja ja tekniset valvontajärjestelmät, jota näiden asioiden selvittämisessä voidaan hyödyntää. Myös tässä tekstissä lähteenä käytetyssä Laaksosen ym. Yrityksen tietoturvakäsikirjassa (2006) on aihetta käsitelty järkevänä kokonaisuutena. Todettakoon kuitenkin, että tietoturvaa ja tietotuojaa käsitellään Suomen lainsäädännössä muun muassa henkilötieto-, työsopimus-, kilpailu-

ja rikoslaissa. Lisäksi tietoturvarikokset ja -rikkomukset, kuten yrityssalaisuuksien rikkominen, on määritelty laissa kattavasti.



Kuvio 4: Tietoturvaa käsittelevää normistoa (Laaksonen ym. 2006, 23.)

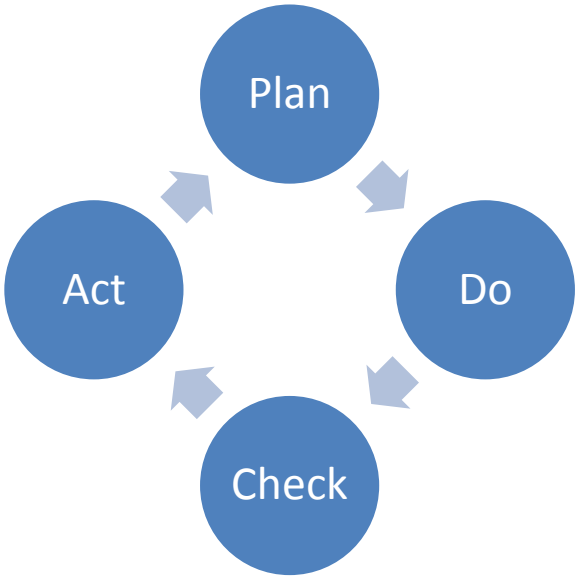
3.5 Toteutus

”Kun tietoturva toimii hyvin, tietojen käsittelytehtävät ja niihin liittyvät toiminnot on etukäteen kartoitettu ja suunniteltu siten, että tiedot on pyritty suojaamaan riittävällä tavalla ja tietoturvariskit on minimoitu” (Yrityksen tietoturvaopas 2012c). Tähän virkkeeseen kiteytyy lyhyesti sanottuna se, kuinka tietoturva toteutetaan. Toki täytyy muistaa se seikka, että korkean turvaluokituksen yrityksillä asia ei ehkä ole näin yksinkertainen, mutta tiivistettynä virke varmasti pätee yritykseen kuin yritykseen.

Yksinkertaisimmillaan tietoturvaa voidaan toteuttaa kuviossa 3 esitellyn portaittaisen toteutusmallin avulla. Toinen tapa organisoidun tietoturvantyön käytännön toteuttamiseksi on luoda sille oma hallintajärjestelmä. Yksi yleistynyt malli on tietoturvastandardi ISO 27001 mukaisen prosessiajattelun PDCA- malli (Plan- Do- Check- Act) (VAHTI 3/2003, 16). Siinä tehtävät ovat jaettu neljään osaan:

- suunnitteluvaiheessa (Plan) prosessi käynnistetään, määritellään suojattavat tiedot ja tehdään riskianalyysit sekä muodostetaan näiden pohjalta jatkuvuusstrategia
- toteutusvaiheessa (Do) suunnitellut ratkaisut toteutetaan ja aloitetaan koulutus
- tarkistusvaiheessa (Check) arvioidaan prosessin tilaa ja toimenpiteiden tehokkuutta
- kehitysvaiheessa (Act) ratkaisuja parannetaan kerättyjen tietojen perusteella

(VAHTI 3/ 2003, 16–18.)



Kuvio 5. PDCA-malli

Hallintajärjestelmiin tai vastaaviin ei tässä työssä sen enempää syvennytä. Ne vaativat suuria linjauksia ja muutosten läpivientiä. Esimerkeillä halutaan lähinnä tuoda esille se fakta, että toimiva tietoturva vaatii suunnittelua ja sitä on ajateltava jatkuvana toimintana.

Vahti- julkaisussa (2/2011) tietoturvallisuuden perustason toteuttamiseksi annetussa asetuksessa (1.7.2010/681 5 §) on tietyt oleelliset kohdat esitetty helpommin lähestyttävästi tarkkojen toimenpiteiden muodossa:

1) toimintaan liittyvät tietoturvariskit kartoitetaan;

2) käytössä on riittävä asiantuntemus tietoturvan varmistamiseksi ja että sen hoitamista koskevat tehtävät ja vastuut määritellään;

3) asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;

4) tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;

5) asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;

6) tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;

7) asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;

8) henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;

9) henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;

10) annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Nämä kohdat tukevat aikaisemmin esitetyn kuvion 3 ajatusta tietoturvan portaittaisesta toteutuksesta. Kuten sanottua, asia on pyritty esittämään mahdollisimman ymmärrettävällä tasolla, jotta saadaan käsitys siitä, kuinka riippuvaisia jokainen vaihe on toisistaan. Vahti- julkaisun asetusta tietoturvan perustason toteuttamisesta tullaan käyttämään sovellettuna opinnäytetyön myöhemmässä vaiheessa sen helpon lähestyttävyyden vuoksi.

Johdon roolia tietoturvaa ja sen toteutusta ajateltaessa ei ehkä ole tarpeeksi vielä korostettu, vaikka se ikään kuin toimii myös tietoturvatyössä suunnan näyttäjänä. Kuten edellä on kertaalleen viitattu, on johdon keskityttävä kokonaisvaltaiseen tietoriskien hallintaan, joka huomioi yrityksen omalle toiminalle keskeiset seikat sekä tärkeimmät sidosryhmät kuten asiakkaat, sopimuskumppanit ja toimeksiannosta toimivat. Tietoriskit ovatkin usein yksi keskeisimmistä riskienhallinnan osa-alueista. (VAHTI 2/2011, 13.)

3.6 Merkitys

Punaisena lankana tälle kehittämistyölle toiminut ajatus, että urakoitsijalla ja urakointitehtäviä tekevällä on oltava käsitys tietoturvan merkityksestä ja mahdollisista menetelmistä sen hallintaan, antoi aihetta tarkastella sen merkitystä omana kappaleenaan. Merkityksen selvittämisellä, esimerkiksi koulutustilaisuudessa tai tietoturvaohjeistuksessa, voidaan saada aikaan motivoituneempi ja sitoutuneempi työntekijä tietoturvaan liittyvissä asioissa, kun vaikutukset negatiivisten riskien toteutumisesta on tiedossa tai niistä ylipäätään ollaan tietoisia.

Vahti Johdon tietoturvaoppaassa (2/2011, 13) merkitystä on avattu näin: ”Tiedot ja tietoturvallisuus ovat nykypäivän tietokeskeisessä yhteiskunnassa ehdottomia edellytyksiä organisaation toiminnalle. Keskeisten liiketoimintaa ja päätöksiä tukevien tietojen tulee olla saatavilla tarvittaessa. Organisaation toiminta voi lamaantua täysin ilman keskeisiä toimintaympäristön tarvitsemia tietoja, tietojärjestelmiä ja yhteyksiä. Tietojen tulee olla oikeita ja luotettavia. Päätökset, jotka perustuvat virheelliseen tai oikeudettomasti muutettuun tietoon, voivat aiheuttaa vakavia vahinkoja organisaation toiminnalle ja imagolle sekä yhteiskunnan turvallisuudelle. Tietojen asianmukaisesta salassapidosta on huolehdittava tiedon suojaustason edellyttämällä tavalla.”

”Asianmukaisella tietojen suojauksella turvataan organisaation toimintaympäristöä, yhteiskuntaa sekä asiakkaiden ja yhteistyökumppaneiden tietoja. Tietojen luvaton päätyminen sivullisille voi täyttää rikoksen tunnusmerkistön. Se voi myös vaarantaa toimintaympäristön turvallisuuden ja palveluiden jatkuvuuden tai rikkoa yksilöiden perusoikeuksia, yksityisyyden suojaa ja turvallisuutta. Organisaation tulee omaan toimintaan liittyvien tietojen salassapidon lisäksi huolehtia sidosryhmiensä ja erityisesti asiakkaidensa tiedoista. Muun muassa henkilötietoihin ja yritysten liike- ja ammattisalaisuuksiin liittyy salassapitovelvoite.” (VAHTI 2/ 2011, 13.)

Tästä voidaan päätellä, että tiedot ja tietoturva ovat nykyään organisaatiosta tai yrityksestä riippumatta ehdoton toiminnan edellytys. Liiketoimintaa uhkaavien tietoturvariskien toteutuminen voi pahimmillaan keskeyttää yrityksen toiminnan ja vahingoittaa imagoa, mikä puolestaan johtaa taloudellisiin menetyksiin. Hyviä tietoturvakäytäntöjä voidaan taas pitää hyvän maineen ja laadun merkkeinä. On myös tärkeää huomioida, että tietojen vuotaminen voi täyttää jopa rikoksen tunnusmerkistön.

Kuitenkin toimiva tietoturva koetaan usein jäykäksi toteuttaa ja mahdottomaksi valvoa. Tärkeäksi se koetaan vasta, kun sen laiminlyönti aiheuttaa taloudellisia menetyksiä. Tietoturvaa voidaan kuitenkin parantaa hyvin pienellä vaivalla ja kassalla. Turvallisuuskulttuurin edistä-

minen vaikka pelkkien ohjeiden olemassa ololla, koulutusten järjestämisellä tai johdon ilmaisemana tahtotilana voi olla riittävää.

4 Menetelmät sen hallintaan

Tämä luku esittelee yleisesti tietoturvan laajan kokonaisuuden ymmärtämiseksi ja organisoinnin helpottamiseksi jaetut tietoturvan kahdeksan osa-aluetta, joita jo sinänsä voidaan pitää menetelminä tietoturvan hallitsemiseksi. Nämä ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus (VAHTI 3/2007). Samat osa-alueet oli tunnistettu myös hankeyrityksessä, minkä takia ne käydään läpi omana osuutenaan. Osa-alueiden läpikäynnissä on huomioitava, että niihin liittyy laajoja kokonaisuuksia, minkä johdosta niitä kuvataan arviolta hyvin yleisellä tasolla. Esitellyissä osa-alueissa esiintyy myös päällekkäisyyksiä, koska jako ei ole mitenkään yksiselitteinen.

Luvussa on paljon kokonaisuutena lukuun 3 liittyvää, mutta tarkastelukulma on erilainen. Tässä luvussa on pyritty esittelemään varsinaisia menetelmiä kyseisten osa-alueiden kautta. Erilaisia menetelmiä löytyy varmasti monia, mikä johtuu pitkälti siitä, että periaatteessa ne tulisi jokaisessa organisaatiossa ja yrityksessä olla jokaisen omaa toimintaa mahdollisimman hyvin tukevia. (Laaksonen ym. 2006, 116.) Tästä johtuen tekstissä esitellään vain yksi näkemys siitä, mitä ne teoriassa voisivat sisältää.

Aihetta on avattu lähinnä siitä tarkastelukulmasta, mitä turvaurakointiyrityksen tulisi huomioida suojatakseen omaa toimintaansa sekä tietoteknisten turvallisuusjärjestelmien urakointitehtävissä. Periaatteessa osa-alueista luetellaan tärkeimmät asiat ja avataan niitä vain tarvittava määrä, jotta ymmärretään, mistä asiassa on kyse. Pähkinänkuoressa tietoturvan hallintaan ja sen eri osa-alueiden hallintaan sovellettavien menetelmien keskeisimmät kysymykset koostuvat seuraavista kysymyksistä:

- Mitä pitää tehdä suojataksemme tietoa?
- Miten se tehdään?
- Ja kuka sen tekee? (ks. liite 1)

4.1 Hallinnollinen turvallisuus

Hallinnollisella tietoturvallisuudella pyritään luomaan perusteet tietoturvan ylläpidolle ja kehittämiselle muun muassa suunnitelmien ja vastuumäärittelyjen kautta. Sen avulla kootaan muut osa-alueet helpommin lähestyttäväksi kokonaisuudeksi (Miettinen 2002, 131). Usein yrityksissä laaditaan tietoturvapolitiikka, missä on määritelty peruskäsitteet, mihin yritys si-

toutuu tietoturva-asioissa, ylläpidon ja kehittämisen toimet sekä vastuut. (Miettinen 1999, 145.) Suppeimmillaan sillä voidaan tarkoittaa lain vähimmäisvaatimusten täyttämistä. Tietoturvakäytännöt onkin suhteutettava toiminnan luonteen ja liiketoiminnan ja muiden ulkoisten vaatimuksien mukaan. Tärkeintä olisi saada tietoturva osaksi jokaisen työntekijän päivittäisiä toimia. (Laaksonen ym. 2006, 115–116.)

Kysymyksen ”miten se tehdään” vastauksena voidaan palata opinnäytetyössä taaksepäin lukuihin 3.1 ja 3.5. Näissä luvuissa on esitelty kaksi kokonaisvaltaista menetelmämallia hallinnollisen tietoturvan toteuttamiseen: tietoturvan portaittainen toteutus ja PDCA-malli. Erityishuomiota tulee kiinnittää myös lainsäädäntöön, joka omalta osaltaan tarjoaa vastauksia kysymyksiin ja vaatimuksia tietyille toimenpiteille.

Hallinnollisen puolen toteuttaminen on luonnollisesti ylimmän johdon tehtävänä. Ylimmän johdon tuleekin suunnittelussa keskittyä kriittisen tiedon tunnistamiseen, minkä pohjalta muodostetaan käsitys nykytilanteesta. Sen lisäksi, niin johdon, kuin esimiesten ja henkilöstön, on tunnettava lainsäädännön asettamat vaatimukset. Tämän jälkeen on helpompi miettiä tarkemmat suojaustoimenpiteet ja asettaa ne toimintaa parhaiten tukeviksi. Lisäksi tietoturvan perusteita luodessa pitää suunnitella tietoturvakoulutuksen toteuttaminen ja seuranta.

4.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus nousee useissa tietoturvaa käsittelevissä teoksissa merkittävään asemaan. Tässä tapauksessa sillä tarkoitetaan henkilöstön toiminnasta aiheutuvien tietoturvauhkien hallintaa. Käytännössä, kun tietoa halutaan näiltä osin suojata, on huolehdittava monesta asiasta uuden työntekijän palkkaamisesta tai yhteistyökumppanin valinnasta aina työsuhteen tai – sopimuksen päättymiseen. (Laaksonen ym. 2006, 138 – 145.)

Laaksonen ym. (2006, 138–145) ovat sisällyttäneet henkilöstöturvallisuuteen tietoturvan näkökulmasta seuraavat huomioitavat seikat:

- työntekijän palkkaaminen tai yhteistyökumppanin valinta
- taustatarkastukset
- luottotietokyselyt
- sopimukset
- toimenkuvan muutokset
- työtehtävien suorittamisessa huomioitavat asiat
- työsuhteen tai -sopimuksen päättyminen

Raggadin (2010, 16–17) mukaan näistä kohdista ensimmäinen on luonnollisesti se, mikä voi jo itsessään johtaa tietoturvan epäonnistumiseen. Lisäksi hän nostaa esille taustatarkastukset,

käyttöoikeudet ja niistä huolehtimisen työntekijän toimenkuvien muuttuessa sekä koulutuksen ja salassapitosopimukset, mikäli työtehtävä sitä edellyttää. Jos näitä ajatellaan niin sanotulla menetelmätasolla, niin esimerkiksi Internetin hakukoneilla, ja varmistumalla työtodistusten aitoudesta taustatarkistusten yhteydessä, voidaan parantaa tietoturvaa huomattavasti tällä osa-alueella. Työsuhteen päättyessä tulee huolehtia muun muassa yritykselle kriittisistä tiedoista, henkilön tietosuojasta ja muista työsuhteen päättymisen menettelytavoista kuten käyttäjätunnusten poistamisesta. (Laaksonen 139, 144.)

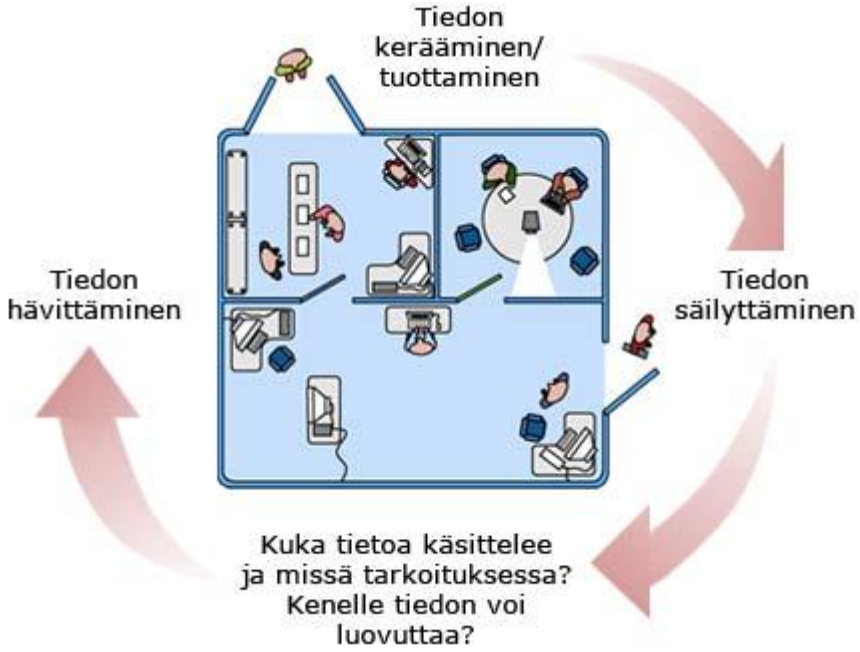
Näiden lisäksi on nostettava esille sopimukset. Laaksosen mukaan (2006, 141) työsopimusta allekirjoitettaessa tietoturvan kannalta on oleellista kirjata ylös, toimenkuva, lähin esimies ja vastuut henkilön koulutuksesta ja perehdytyksestä. Työ- ja liikesuhteissa hän korostaa luottamuksellisten tietojen pysymistä niillä henkilöillä, jotka ovat siihen oikeutettuja. Tätä voidaan edesauttaa salassapitosopimuksilla, joilla suojataan sitä, ettei luottamuksellinen materiaali päädy esimerkiksi yhteistyökumppaneilta eteenpäin. Salassapitosopimusten vaikuttavuuden takaamiseksi tulee niissä määritellä seuraamukset sopimusrikkotilanteissa.

Koulutuksesta ja tietoturvatietoisuuden lisäämisestä on mainittu tekstissä aiemmin ja siihen viitataan myös myöhemmässä vaiheessa. Voidaan sanoa, että se kulkee kaikissa vaiheissa olennaisena osana mukana. Henkilöstölle on tärkeää muodostaa kuva tietoturvaan liittyvistä riskeistä ja tärkeimmistä menetelmistä niiden toteutumisen estämiseksi. Tämän lisäksi tietoturvan merkitystä tulisi korostaa, mitä kautta ymmärrys sen tärkeydestä saattaisi kasvaa.

Kuka tämän tekee? Vastuu yrityksissä on yleensä niillä henkilöillä, jotka vastaavat uusien työntekijöiden palkkaamisesta. Vastaavasti yhteistyökumppanien osalta salassapitosopimukset kirjoitetaan muiden sopimusten solmimisten yhteydessä. Myös koulutuksille ja niiden järjestämiselle tulee löytyä vastaava, joka lisäksi pitää kirjaa siitä, mitä koulutuksia kukin on saanut.

4.3 Tietoaineistoturvallisuus

Tietojen suojaamisessa on varmistuttava, että siitä on huolehdittu koko tiedon elinkaaren ajan. Tieto ei ole ainoastaan tietokoneissa, matkapuhelimissa ynnä muissa, vaan myös paperimuodossa. Tästä johtuen on varmistuttava myös tiedon turvallisesta hävittämisestä. (KATAKRI 2011, 101.)



Kuvio 6: Tiedon elinkaari (Yrityksen tietoturvaopas 2012e.)

Tyypillisesti urakointitehtävissä käsitellään luottamuksellisia tai jopa salaisia tietoja, jolloin ohjeistaminen ja ohjeistukset tiedon käsittelyyn sen elinkaari huomioiden on tärkeää. Yrityksissä yleensä tietoturvasta vastuussa oleva henkilö(t) määrittelee puitteet tietojen suojaamiselle, mutta lopullinen vastuu on käyttäjällä (Miettinen 1999, 187).

Miettinen (2002, 135–136) esittelee kirjassaan turvaluokitusmallin (kuvio 7), josta ilmenee myös käsittelysäännöt tiedon tärkeysluokan mukaan. Käsittelysäännöt on luotu muun muassa tiedon säilytyksestä toimipaikalla, tallentamisesta, luovutuksesta, kuljettamisesta ja hävittämisestä. Myös kansallisen turvallisuusauditointikriteeristön (2011, 90, 98–105, 110) mukaan on kiinnitettävä huomiota tiedon luokittelumenettelyihin (merkintään), säilyttämiseen, suojattavaa tietoa sisältävien liikuteltavien muistien ynnä muiden suojaukseen ja luvattoman pääsyn estämiseen, kopiointiin, tulostukseen, matkatyöhön, etäkäsittelyyn, tiedon postittamiseen ja sähköiseen välittämiseen sekä käytöstä poistoon ja hävittämiseen.

Käsittelysääntö	Julkinen	Sisäinen	Luottamuksellinen	Salainen
Merkintä	ei merkitä pääsääntöisesti	merkintä "sisäinen" dokumentin kansilehteen tai etusivulle	merkintä "luottamuksellinen" dokumentin kansilehteen tai etusivulle	merkintä "salainen" dokumentin kansilehteen tai etusivulle
Käsittelypaikka	ei rajoituksia	käsittelyssä huomioitava, että tieto ei ole sivullisten näh-	sivullisislta eristetty tila, johon ei näe/ kuule tilan ulko-	sivullisislta eristetty tila, johon ei näe/ kuule tilan ulko-

		tävillä tai kuulta-villa	puolelta	puolelta
Säilytys toimi-paikalla	ei rajoituksia	sallittu työtilassa avoimissa hyllyissä	säilytettävä lukitu-ssa tilassa tai kaapissa	säilytettävä lukitu-ssa tilassa ja kaapi-ssa (suosituksena kassakaappi)
Tallennus lähiver-kon palvelimelle, henk.koht. työ-asemalle ja kannet-tavalle	ei rajoituksia. Käytettävä virus-torjuntaa	ei rajoituksia. Käytettävä virus-torjuntaa	voidaan tallentaa, jos suojattu pääsyn-valvonnalla. Käytettävä virus-torjuntaa	voidaan tallentaa, jos suojattu pääsyn-valvonnalla. Käytettävä virus-torjuntaa ja tietojen salausta
Tallennus erilliselle muistivälineelle	ei rajoituksia. Käytettävä virus-torjuntaa	ei rajoituksia. Käytettävä virus-torjuntaa	sallittu, jos käyttö-oikeus vain tietoja tarvitsevilla. Käy-tettävä virustorjuntaa	sallittu, jos käyttö-oikeus vain tietoja tarvitsevilla. Käy-tettävä virustorjun-taa ja tietojen salausta
Tulostus	ei rajoituksia	ei rajoituksia	sallittu yhteisille kir-joittimille,kun tulos-tus valvottu henk.koht.	sallittu ainoastaan henk.koht. kiroitti-melle
Kopiointi	ei rajoituksia	ei rajoituksia	vain tiedon haltijan luvalla	vain tiedon omistajan luvalla
Jakelu yrityksen sisällä	ei rajoituksia	sallittu tiedon haltijan luvalla	sallittu tiedon omista-jan luvalla	sallittu tiedon omis-ta-jan luvalla
Luovutus yrityksen ulkopuolelle	ei rajoituksia. Varmis-tuttava tietojen oi-keel-lisuudesta ennen luo-vuttamista	sallittu tiedon haltijan luvalla	sallittu tiedon omista-jan luvalla, vaadittava salassapitositoumus vastaanottajalta	sallittu tiedon omis-ta-jan luvalla, vaadittava salassapitositoumus vastaanottajalta
Kuljetus matkoilla	ei rajoituksia	ei rajoituksia. Kulje-tettava käsimatka-tavarana	vältettävä kuljetusta. Kuljetettava käsi-matkatavarana	vältettävä kuljetusta. Kuljetettava käsi-matkatavarana
Etäkäsittely tieto-verkon kautta	ei rajoituksia	sallittu käyttäjän vahvalla tunnistuksel-	sallittu käyttäjän vahvalla tunnistuksel-	sallittu käyttäjän vahvalla tunnistuksel-

		la ja todentamisella	la ja todentamisella, salauksen käyttö suositeltavaa	la ja todentamisella, salauksen käyttö pakolllista
Lähettäminen postitse	ei rajoituksia	suljetussa kirjekuoressa	suljetussa kirjekuoressa	suljetussa kirjekuoressa. Toimitus henkilökoht. Vastaanottajalle
Lähettäminen sähköpostilla	ei rajoituksia	ei rajoituksia	vältettävä lähettämistä spostilla, salauksen käyttö suositeltavaa	sallittu ainoastaan salattuna
Käytöstä poisto ja hävittäminen	ei rajoituksia	fyysisesti tuhoamalla (silppuaminen) tai päälle kirjoittamalla	fyysisesti tuhoamalla (silppuaminen) tai päälle kirjoittamalla	fyysisesti tuhoamalla (silppuaminen) tai päälle kirjoittamalla. Saatava tuhoamistodistus

Kuvio 7: Tietojen turvaluokitusmalli (Miettinen 2002, 135–136.)

4.4 Fyysinen turvallisuus

Fyysisen turvallisuuden avulla luodaan edellytykset muille suojaustoimenpiteille tietoturvan ylläpitämiseksi. Fyysisiä suojauskeinoja suunniteltaessa on kuitenkin tarkkaan arvioitava turvallisuustarpeita ja – ratkaisuja: yrityksen koko, toimiala ja henkilöstön määrä asettavat erilaisia vaatimuksia fyysiselle suojaukselle. Tietoturvaa ajateltaessa kaikki ne tilat, joissa merkityksellistä tietoa käsitellään, tulisi olla suojattuina. Tarkoituksena on estää tietojen tuhoutuminen, vahingoittuminen ja joutuminen vääriin käsiin. Tässä apuna voidaan käyttää esimerkiksi tilojen tärkeysluokittelua. (Laaksonen ym. 2006, 125- 126.)

Tekniikan toimivuuden varmistamiseksi tietojärjestelmien sydänten eli palvelimien fyysiseen suojaan tulee erityisesti panostaa. Palvelimet tulee säilyttää lukkojen takana ja pääsyn tilaan pitää olla rajattu. Koska koneet kuumenevat, on ilmastointi palvelintilassa pakollista. Näiden lisäksi riskianalyysi tulee tehdä tulipalon, vesivahingon, pölyhaittojen ja varkauden varalle. (Yrityksen tietoturvaopas 2012f.)

Fyysistä turvallisuutta toteutettaessa suojaustoimenpiteet ovat usein, rakenteellisen suojauksen lisäksi, tietoteknisiä turvallisuusjärjestelmiä, kuten kulunvalvonta-, kameravalvonta-, murtohälytin- ja paloilmaisinjärjestelmät. ”Noudattamalla vakuutusyhtiöiden vakuutuskirjojen vaatimuksia monet tietoturvan kannalta oleelliset kohteet tulee suojattua” (Laaksonen

ym. 2006, 127). Tietoturvan ja järjestelmistä ylipäätään saatavan hyödyn kannalta tärkeään rooliin nousee niiden käytön kouluttaminen. Ohjeistamisella ja ohjeilla eri laitteiden ja tapahtumien hallintaan voidaan vaikuttaa henkilöstön osaamiseen, jolloin suojaus tehostuu. (Kulunvalvonta ja rikosilmoitinjärjestelmät 2007, 109.)

4.5 Käyttöturvallisuus

VAHTI-ohjeessa (3/2007, 65) kerrotaan, että ”käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet”. Sitä toteutetaan huolehtimalla muun muassa:

- toimivuuden valvonnasta
- käyttöoikeuksien hallinnasta
- käytön ja lokien valvonnasta
- ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä
- varmuuskopioinnista
- häiriöraportoinnista

Lisäksi ohjeessa mainitaan, että ”kaikkien tietojärjestelmien suojaaminen haittaohjelmilta (kuten sähköpostiviruksilta tai verkkomadoilta) on osa käyttöturvallisuutta. Järjestelmien käyttöturvallisuuden taso perustuu järjestelmässä olevien tietojen luokitukseen”.

Leppäsen (2006, 303–304) mukaan käyttöturvallisuudella varmistetaan henkilöstön tietoturvan ylläpitämiseen liittyvien toimenpiteiden hallinta. Hän listaa käyttöturvallisuuden koostuvan seuraavista osa-alueista:

- työaseman käyttö
- tietovälineiden käyttö
- tietoaineistojen käyttö
- liitetietojen käyttö
- sähköpostin käyttö
- internetin käyttö
- virustorjunta
- lähiverkko
- käyttöoikeuksien ja salasanojen hallinta
- varmuuskopiointi
- tilojen lukitus ja kulunvalvonta

Näistä tarkempaan tarkasteluun on nostettu työaseman käyttö, virustorjunta, käyttöoikeuksien ja salasanojen hallinta sekä varmuuskopiointi. Työasema on usein tärkein työväline matkapuhelimien ohella työtehtävästä riippumatta. Loppukäyttäjän vastuu työasemansa suojaamisesta on suuri. Tästä johtuen hänen on tunnettava työasemien suojauksen periaatteet esimerkiksi koulutuksen ja ohjeiden avulla. (Miettinen 2002, 137–139.)

Työasemaa voidaan suojata luvattomalta käytöltä muun muassa käyttöoikeuksien ja salasanojen avulla. Käytännössä kaikki käyttäjät tulisi yksilöllisesti tunnistaa ja todentaa henkilökohtaisilla käyttäjätunnisteilla ja salasanalla ennen pääsyn sallimista tietoverkkoihin tai -järjestelmiin. Salasanan merkitys tulisi olla korostettua ja sen vaihto pakotettua määräajoin. Päivittäisessä toiminnassa on huomioitava muun muassa työasemalta poistuminen väliaikaisesti ja päivän päätyttyä, jolloin tietokoneen sammuttamisella voidaan estää luvaton tunkeutuminen tietoverkkojen kautta. Lisäksi niin sanottu puhtaan pöydän ja näytön politiikka tulisi olla osa työaseman suojausta (KATAKRI 2011, 85, 114- 115).

Lisäksi työasemat ja matkapuhelimet tulee suojata virusten torjuntaohjelmistolla. Olennaisinta on, että torjuntaohjelma on ajantasainen ja kattaa kaikki tietokoneet kannettavista kiinteisiin. Lisäksi tiedostojen vastaanottajan ja lähettäjän tulee tehdä virustarkastus kaikille tiedostoille. Käytännössä on oltava sovittuna ja ohjeistettuna virustorjunnan tavoitteet, toteutus, vastuut ja toiminta virusepäilyissä. (Miettinen 2002, 139–140.) Virustorjunnan lisäksi internetiin liitetyt tietokoneet vaativat palomuuria, jonka avulla suoja ulkopuolisia tunkeilijoita (vakoiluohjelmat ja virukset) vastaan paranee (Yrityksen tietoturvaopas 2012g).

Varmuuskopioinnin avulla varmistetaan liiketoiminnan jatkuvuus mahdollisissa ongelmatilanteissa. Sillä varmistetaan, että ajan tasalla olevat tiedot ja ohjelmat on käytettävissä kaikissa tilanteissa. Varmuuskopiointi on hyvä järjestää tiedoille ja ohjelmille automaattiseksi, jolloin työntekijän vastuu pienenee henkilökohtaisten tietojen varmuuskopioinnista huolehtimiseen. Kopioiden säilyttäminen on oleellinen osa myös tätä prosessia, mikä jää yleensä liian vähälle huomiolle. Ihannetilanne olisi se, jos varmuuskopiot voitaisiin sijoittaa fyysisesti eri tilaan, kuin missä alkuperäiset tiedot sekä ohjelmat sijaitsevat. Näin pysytystään paremmin suojautumaan esimerkiksi tulipaloa ja varkauksia vastaan. (Miettinen 2002, 239–240; KATAKRI 2011, 117.)

4.6 Laitteistoturvallisuus

Laitteistoturvallisuus on käsitteenä laaja, koska kaikki yrityksen tekniset laitteet voidaan lukea sen piiriin. Lähtökohtana sille voidaan kuitenkin pitää sitä, että jo hankittaessa laitteita, niiden tietoturvaominaisuudet ovat sitä luokkaa, että ne vastaavat yrityksen liiketoiminnan tarpeita myös turvaominaisuuksien osalta. (Miettinen 1999, 221–222.)

Miettinen (1999, 222) lähestyy laitteistoturvallisuuden perussuojausmenetelmiä seuraavasti:

- pääsynvalvonta laitteeseen
- laitteiston lokitietietojen kerääminen
- luotettava varaosien saanti
- laitteiden varmentaminen kriittisissä kohteissa
- laitteiden energian saannin varmistaminen
- asianmukainen laitteistodokumentaatio
- asianmukaisesti laaditut ylläpito- ja huoltosopimukset.

Yhtenä tärkeimmistä hän pitää pääsynvalvontaa laitteisiin, jonka avulla pyritään estämään pääsy laitteen sisälle oikeudetta suoraan laitteeseen kytkeytymällä tai etäyhteydellä. Tällä tarkoitetaan käyttäjätunnusten ja salasanojen kysymistä ennen laitteeseen pääsyä, mitä jo käyttöturvallisuuden kohdalla on käyty läpi. Tästä johtuen mielenkiinto kohdistuukin jäljellä oleviin kohtiin, joita tässä yhteydessä lähestytään erityisesti tietoteknisten turvallisuusjärjestelmien urakointitehtävien näkökulmasta, vaikka käytännöt pätevät yrityksien omaankin toimintaan.

Lokitietojen eli laitteistojen tapahtumatietojen keräämisellä pyritään esimerkiksi vikatilanteiden sattuessa siihen, että ne pystytään paikallistamaan ja selvittämään. Myös väärinkäyttötilanteissa poikkeustilanteen todentaminen jälkikäteen on tärkeää. Näin vian korjaaminen tai väärinkäytön todentaminen helpottuu. Lokitietojen asianmukainen käsittely tulee myös olla järjestetty. (KATAKRI 2011, 89.)

Kun jokainen laite jossain vaiheessa vikaantuu, tulee varaosien saatavuus olla taattuna. Jo laitetta hankittaessa tulee varmistua esimerkiksi sopimusten avulla, että toimittaja pystyy takaamaan varaosien saannin kaikissa tapauksissa. Ongelmatilanteiden selvittelyä helpottaa myös asianmukainen laitteistodokumentaatio ja – rekisteri (KATAKRI 2011, 92). Sen tulee sisältää ainakin laitteiston teknisen rakenteen kuvaus ja käyttöohjeet joko kirjallisessa tai sähköisessä muodossa. (Miettinen 1999, 223.) Huoltotoimenpiteiden tai käytöstä poiston yhteydessä on varmistuttava, etteivät ne mahdollista tietojen joutumista kolmansille osapuolille. Lisäksi on mietittävä, että havaitaanko ylipäätänsä, jos laite viedään luvatta yrityksen tiloista. (KATAKRI 2011, 91–92).

Kaikista kriittisimmissä urakointikohteissa laitteiden varmentamisesta tulee huolehtia toiminnan jatkuvuuden takaamiseksi. Laitteiden varmentamisella tarkoitetaan sitä, että vioittuneen laitteen tilalle on saatavilla vastaava laite, joka hoitaa vioittuneen tehtävät. Samassa yhteydessä tulee varmistua laitteen sähkönsaannista. Sähkökatkosten varalle yleisin suojauskeinoa on ottaa käyttöön joko laite- tai kiinteistökohtainen virransyöttöjärjestelmä, kuten akkuihin perustuvat UPS-laitteet tai varavoimageneraattorit. (Miettinen 1999, 223–224.)

Turvaurakkaan voi kuulua myös laitteiden ylläpidosta huolehtiminen. Laitteiden häiriöttömästä toiminnasta voidaan osaltaan varmistua laatimalla asianmukaiset ylläpito- ja huoltosopimukset. ”Sopimuksissa on määriteltävä yksityiskohtaisesti, mitkä asiat kuuluvat sopimukseen, miten nopeasti huollot suoritetaan ja kuka toimet suorittaa.” (Miettinen 1999, 224.)

4.7 Ohjelmistoturvallisuus

Ohjelmistojen ja eri lisenssien hallinta ei välttämättä lukeudu aina niihin kaikista tärkeisimpiin tietoturvallisuuden osa-alueisiin, mutta ohjelmistoturvallisuuden laiminlyönti voi johtaa vakaviin tietoturvaloukkauksiin. Esimerkkinä mainittakoon virustorjuntaohjelmistot, joissa lisenssin käyttöoikeuden loppuminen saattaa lopettaa myös itse ohjelman toimimisen. Täten myös ohjelmistojen hallinnasta ja niiden ajantasaisuudesta esimerkiksi rekisterin avulla on huolehdittava. Lisäksi tulisi varmistua siitä, että luvattomat ohjelmistoasennukset havaitaan. (KATAKRI 2011, 92.)

Ohjelmistoturvallisuuden perussuojausmenetelmät myötäilevät hyvin pitkälti laitteistoturvallisuuden vastaavia. Aivan kuten laitteistoihin, myös ohjelmistoihin tarvitaan asianmukainen pääsynvalvonta. Ohjelmistojen tapahtumia seurataan, huolehditaan tietojen ja ohjelmistojen varmuuskopioinnista ja ohjelmistodokumentaatiosta sekä ylläpito- ja huoltosopimuksista. Ohjelmistoihin liittyvissä ongelmatilanteissa tapahtumatietojen kirjaaminen muistiin sekä viimeiseksi mainitut sopimukset ovat erityisen tärkeitä.

Näiden lisäksi on syytä varmistua, että ohjelmat ovat hankittu ja asennettu vain luotettavista lähteistä (KATAKRI 2011, 97). Niin laitteiden, kuin ohjelmistojen hankinnassa on syytä varmistua niiden laadusta ja tietoturvasta. Hyvä pääsynvalvontakaan ei välttämättä pysty estämään luvatonta käyttöä, jos todennusmekanismit voidaan muuta kautta ohittaa.

Ohjelmistoturvallisuuden yhteydessä on varmistuttava jälleen myös siitä, että henkilöstö on ohjeistettu ohjelmistojen turvallisesta käytöstä. Tähän kuuluu lisäksi sallittujen ja kiellettyjen ohjelmistojen määrittäminen sekä käytännöt. Henkilöstölle on oltava selvää, mitä omia ohjelmistoja työasemille saa asentaa vai saako niitä ylipäätään asentaa ollenkaan.

4.8 Tietoliikenneturvallisuus

Ne toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus, on jälleen laaja kokonaisuus ja sen tekniseen tarkasteluun vaaditaan asiantuntijuutta ja kokemusta. Tämän kehittämistyön kannalta ei ole olennaista käydä läpi kaikkia teknisiä menetelmiä tietoliikenteen teknisistä suojausmenetelmistä. Se ei kuitenkaan poista sitä tosiasiaa, että tietotekniset tur-

vallisuusjärjestelmät toimivat erilaisissa tietoliikenneverkoissa, ja niiden turvallinen käyttö on hallittava.

VAHTI- julkaisussa (5/2004) tietoliikenneturvallisuuden suojauskeinoiksi luetellaan muun muassa laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. Asennus-, ja miksi ei myös ylläpitotehtäviä ajatellessa, korostuu ajan tasalla oleva dokumentaatio ja sen hallinta tietoliikenteen turvaamiseksi. Lisäksi kaapeloinnin suojaus fyysisiltä uhilta kuten katkaiseminen, häirintä ja kiinnittyminen on käytössä olevien resurssien mukaan huomioitava tietoliikenteen kannalta ja riskit minimoitava ainakin hyvällä suunnittelulla. Suunnittelussa on huomioitava fyysisen suojauksen lisäksi, etteivät yhteydet ja varayhteydet ole riippuvaisia yhdestä yksittäisestä toimivasta komponentista.

Kansallisessa turvallisuusauditointikriteeristössä (KATAKRI 2011, 75–84) tietoliikenneturvallisuus on yksi neljästä tietoturvaan liitetystä osa-alueesta. Siinä lähdetään liikkeelle siitä, että tietoliikenneverkon rakenne tulee olla lähtökohtaisesti turvallinen. Kriteeristössä painotetaan muun muassa palomuurien ja vastaavien tärkeyttä ja toimivuutta, joilla osaltaan pyritään suojaamaan tietoliikennettä ja varautumaan yleisimpiin verkkohyökkäyksiin.

Kuten luvun alussa mainittiin turvallisuusjärjestelmien yhteys verkkoon, tulee hallintayhteydet täten suojata asianmukaisesti. Lisäksi asiakkaita tulisi urakointikohteissa neuvoa aktiivilaitteiden koventamisesta, johon käytännössä suositellaan vähintään muun muassa oletussalasanojen vaihtamista. Niin KATAKRI:ssa kuin yllä mainitussa Vahti-julkaisussa verkkoa, järjestelmiä ja niiden käytön valvomista pidetään oikein mitoitettuina olennaisena seikkana. (KATAKRI 2011, 80, 83.)

5 Turvaurakoitsijan tietoturvan hallinta

Tässä luvussa käydään läpi olennaisimpia tietoturvan hallinnan seikkoja hankeyrityksen turvaurakointiprosessimallin kautta. Se on yksi olennaisimmista luvuista, kun ajatellaan esimerkiksi TU-yritystssertifikaatin myöntämistä turvaurakointiyrityksille. Luvussa on yhdistelty työssä saavutettuja tuloksia edellä käydyn yleisluontoisen kuvauksen kautta.

Tietoa liikkuu koko turvaurakointiprosessin aikana. Tiedon suojaaminen (käytettävyys, eheys, luottamuksellisuus, kiistämättömyys ja todentaminen) koko prosessin aikana ja sen jälkeen toimii perusajatuksena tietoturvan hallinnalle tietoteknisten turvallisuusjärjestelmien urakointitehtävissä. Tästä johtuen tietoturvan hallinta tuleekin olla jatkuvaa toimintaa, mistä

esimerkkinä aikaisemmin tekstissä esitelty tietoturvan toteutus. Urakointitehtävissä on myös kriittisen tärkeää olla tietoinen siitä, että lainsäädäntö ohjaa hyvin pitkälle koko toimintaa.

Tietoturvan yhtenä tavoitteena kyseisessä prosessissa on estää myös niin sanotuista kaupallisista syistä tietojen, kuten liikesalaisuuksien, kaupallisten sopimusten ja immateriaaliarvojen, joutuminen väärille tahoille. Hyvin hallitulla ja toteutetulla tietoturvalla voidaan edistää lisäksi urakan kustannustehokkuutta. Tietoturvan kannalta onkin huomioitava kytkökset urakkaa edeltäneisiin ja seuraaviin vaiheisiin, jolla tässä tarkoitetaan ylläpitovaihetta. (VAHTI 9/2008, 15.)

Turvaurakoinnissa käsitellään tietoja useissa vaiheissa ja eri muodoissa. Näitä urakoinnissa tyypillisiä tietoja voi olla dokumentteina esimerkiksi pohjapiirustuksina, suunnittelussa ja työssä tuotettuina dokumentteina, suullisessa muodossa muun muassa kokouksissa tuotettuina sekä tulosdokumenteissa. Tyypillistä hankkeille ja urakoille on myös se, että tiedon tuottamiseen ja käsittelyyn osallistuvat useat osapuolet vaihtelevilla tietoturvatavoilla sekä -tasoilla. (VAHTI 9/2008, 15.)

Vahti-ohjeistossa (9/2008, 15–16) urakan perusajatusta tiedon suojaamisesta on avattu seuraavasti:

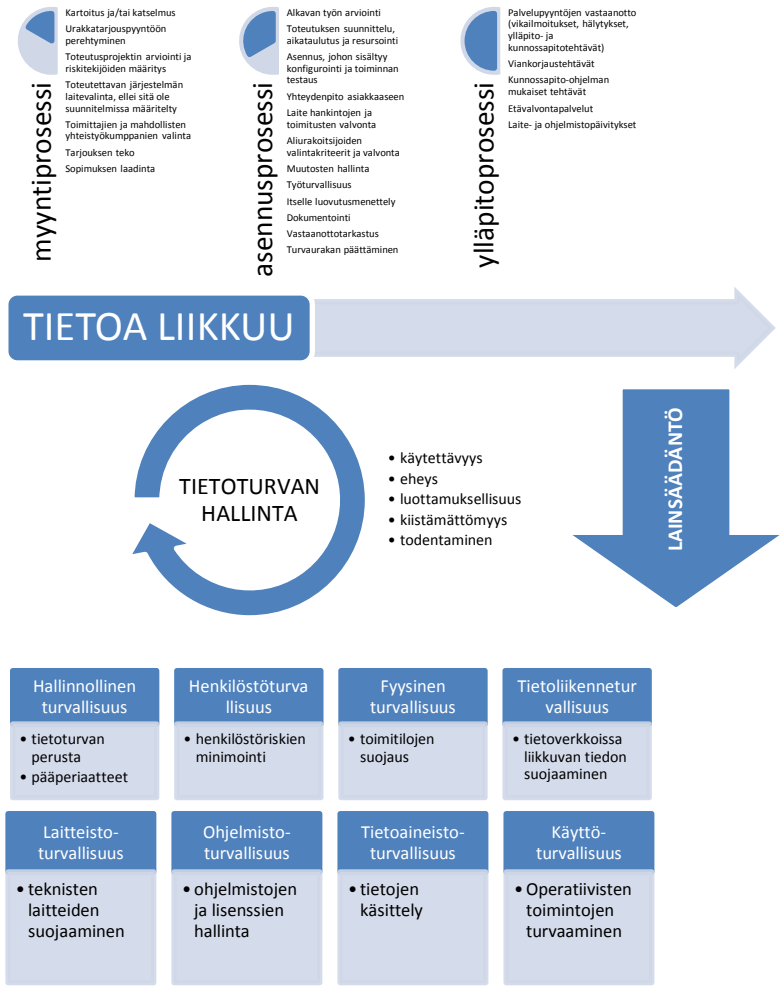
- Luottamuksellisuuden turvaamisella varmistetaan, että urakoitsijalla on mahdollisuus saada tietoturvaluokasta riippumatta tarvittavat tiedot käyttöönsä. Sillä varmistetaan myös se, että tiedot eivät joudu urakan kautta muiden tietoon vastoin tiedon omistajan tahtoa.

- Eheyden turvaamisella varmistetaan muun muassa dokumenttien ja niiden käytön välinen oikea yhteys, dokumenttien versioiden yhdenmukaisuus sekä hyväksyttyjen dokumenttien muuttumattomuus.

- Kiistämättömyyden turvaamisella varmistetaan, että urakoitsija on saanut haltuunsa työn kannalta keskeisiä dokumentteja. Sillä varmistetaan myös, että kommentoitavaksi, noudatettavaksi tai muuten käsiteltäväksi toimitetut urakan dokumentit on saatettu asianomaisten tahojen käyttöön.

- Käytettävyyden turvaamisella varmistetaan työprosessien tehokas läpivienti takaamalla muun muassa dokumenttien ja tietojen saatavuus työn asettamien vaatimusten mukaisesti.

Turvaurakointiprosessin ja tietoturvan välisiä suhteita on pyritty kuvaamaan seuraavassa kuvi-ossa:



Kuvio 8. Tietoturvan hallinta turvaurakointiprosessissa

5.1 Myyntiprosessi

Turvaurakan tietoturvan hallinnalla on kaksi tarkoitusta: varmistaa käyttöön saatujen ja tuotettujen tietojen tietoturvallisuus sekä tietoisten päätösten teon käyttöön hyväksyttävien ja tuotettavien tietojen ja dokumenttien luottamuksellisuuden taso. Näiden tarkoitusten täyttämiseksi urakkaan liittyvien tietojen käsittelylle ja turvallisuusluokittelulle tulee määritellä riittävän yksityiskohtaiset periaatteet, jotka kukin osallistuva taho voi rinnastaa omaan toimintaansa, kuten asianhallintaan liittyviin periaatteisiinsa. (VAHTI 9/2008, 16.)

Turvaurakointiprosessin näkökulmasta hallinnollinen tietoturva sijoittuu luonnollisesti aivan alkuun eli myyntiprosessivaiheeseen, jossa yhtenä vaatimuksena on riskitekijöiden määritys. Jos tämä ajattelu yhdistetään aikaisemmin esiteltyyn VAHTI- julkaisun (2/2011) tietoturvan

perustason toteuttamiseen, niin kohdat 1) ja 2) voidaan liittää osaksi myyntiprosessissa huomioitavia seikkoja. Kohdassa 1) painotetaan toimintaan liittyvien tietoturvariskien kartoitusta. Näihin riskeihin on voitu varautua erilaisten ohjeiden ja hyvien käytäntöjen mukaisilla perusmenettelyillä (VAHTI 9/2008).

Kohdassa 2) vaaditaan tietoturvan hoitamista koskevien tehtävien ja vastuiden määrittelyä. Voidaan puhua myös tietoturvan organisoinnista, josta yksi esimerkki löytyy liitteestä 1. Näiden määrittely ei koske ainoastaan omaa henkilöstöä vaan niin ikään toimittajia ja muita mahdollisia yhteistyökumppaneita. Toimittajien ja yhteistyökumppaneiden valinnassa on syytä kiinnittää huomiota siihen, että myös heidän toiminnassaan on huomioitu tietoturvatekijät, kuten tietojen käsittelijöiden luotettavuus ja tietojen käsittelyn ohjeistus ja koulutus.

Tapahtumien dokumentointi on myös erityisen tärkeää (VAHTI 9/2008, 24). Lisäksi dokumentoinnin yhteydessä voidaan korostaa sopimusten laadinnan merkitystä, joka on kaikissa tapauksissa tehtävä huolella. Tämä johtuu siitä, että tapauksia saatetaan joutua myöhemmin käsittelemään oikeudessa, jos lopputulos ei vastaa alussa sovittua tai, jos urakka viivästyy. Tämä on huomioitava myös asennusprossissa, kun aliurakoitsijoista päätetään. Edellisten lisäksi on varmistuttava lainsäädännön vaikutuksista toimintaan.

Tietoturvavuotojen ja – varkauksien ollessa mahdollisia tietoturvariskejä (Kulunvalvonta ja rikosilmoitinjärjestelmät 2007, 66) on kiinnitettävä huomiota myös henkilöstöturvallisuuteen. Se johtuu siitä, että henkilöstöön liittyviä luotettavuusriskejä pystytään minimoimaan muun muassa rekrytoinnin, toimenkuvien, käyttöoikeuksien määrittelyn, koulutuksen ja valvonnan sekä tausta- ja turvallisuusselvitysten avulla. Myös tässä yhteydessä on huomioitava lainsäädännön asettamat vaatimukset joidenkin tarkastuksien ja tehtävien osalta. (VAHTI 2/2008, 21.)

Henkilöstöturvallisuudessa tulisi kattaa ainakin VAHTI- julkaisussa (2/2011) annetussa tietoturvallisuuden perustason toteutuksen asetuksessa mainitut kohdat 8) ja 9) joissa toimenpiteinä on lueteltu henkilöstön luotettavuuden varmistaminen asiakirjojen käsittelyyn liittyvissä tehtävissä sekä ohjeiden ja koulutuksen antaminen tietojen asianmukaisesta käsittelystä. Yksi tapa tähän voisi olla urakkakohtaiset vaitiolositoumukset, joilla vahvistettaisiin henkilöiden velvollisuuksien tietäminen ja tietoturvakäytäntöjen tunteminen. Urakkaan sisältyvien luottamuksellisten tietojen asianmukaista käsittelyä voitaisiin puolestaan ohjeistaa kuviossa 7 esitetyllä tavalla.

Tietoaineistoturvallisuus, jonka päämääränä on tietojen suojaaminen, koskee koko prosessia, mutta toimenpiteet ja muu ohjeistus on oltava valmiiksi luotuna jokaista urakkaa sekä yritystä itseään varten. ”Tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmistami-

seen ja palauttamiseen sekä tuhoamiseen liittyvät toimet. Aineistoihin kuuluvat myös manuaalisen tietojenkäsittelyn asiakirjat sekä automaattisen tietojenkäsittelyn tulosteet" (Hakala, Vainio & Vuorinen 2006, 11). Tässä korostuu tiedon turvaaminen koko sen elinkaaren ajan. Jälleen myös käsittelysäännöt nousevat suureen rooliin. Tietoaineistoturvallisuudella voidaan kattaa tietoturvan perustason toteuttamisessa kohta 3) eli asiakirjojen käsittelyä koskevat tehtävät ja vastuut. Suojausmenetelmiä ja – toimenpiteitä on käyty aikaisemmin läpi luvussa 4.3.

Yhteenvetona voidaan sanoa, että heti myyntiprosessivaiheessa, periaatteessa jo ennen urakan varsinaista aloittamista, joudutaan miettimään suurin osa tietoturvaan liittyvistä kysymyksistä. Tässä vaiheessa tehdyt tietoturvaratkaisut määrittävät hyvin pitkälle urakan tietoturvallisen onnistumisen. Kuitenkin jokaista kohtaa ei välttämättä tarvitse urakkakohtaisesti tehdä: tietoturvan hoitamista ja asiakirjojen käsittelyä koskevat tehtävät ja vastuut on voitu määritellä sekä niiden käsittelyyn liittyvien henkilöiden luotettavuudesta ja koulutuksesta varmistuttu turvaurakointiyrityksessä valmiiksi. Siten jäljelle jää tietoturvariskien kartoitus ja laitejärjestelmistä, - toimittajista ja muista mahdollisista yhteistyökumppaneista huolehtiminen.

5.2 Asennusprosessi

Fyysinen turvallisuus, jolla siis tarkoitetaan toimitilojen ja niihin sijoitettujen laitteiden suojaamista, sijoittuu tietoteknisten turvallisuusjärjestelmien asennusprosessi vaiheeseen. Esimerkiksi palvelimien suojaaminen fyysisiltä uhilta (palo-, vesi-, sähkövahingot, varkaus ja ilkivalta) on oleellista turvaurakan toteutuksen suunnittelussa. (Hakala ym. 2006, 11.) Suunnitteluvaihe on tietoturvan kannalta yksi tärkeimmistä vaiheista, koska sen tavoitteena on estää mahdollisten tietoturvauhkien toteutuminen. Fyysinen turvallisuus VAHTI-julkaisun (2/2011) tietoturvallisuuden toimenpiteisiin liittyy kohtiin 4), 6) ja 7): tietojen saannin ja käytettävyyden turvaaminen, tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman käsittelyn estäminen riittävillä (tietoteknisillä) turvallisuusjärjestelyillä ja muilla toimenpiteillä ja tietojenkäsittely- ja säilytystilojen riittävä valvominen ja suojaaminen.

Käyttöturvallisuus liitetään yleisesti yrityksen operatiivisten eli päivittäisten toimintojen turvaamiseen. Kyseinen osa-alue voidaan sisällyttää ohjelmistoturvallisuuteen dokumentoinnin vähentämiseksi tai kaikkiin tietoturvan osa-alueisiin niiden käytöstä aiheutuvien riskien pienentämiseksi, mutta asennusprosessissa päivittäisten rutiinien turvaaminen voidaan nähdä niin olennaisena, että sitä tulisi käsitellä omana kokonaisuutenaan. (Miettinen 2002, 158–159; Hakala ym. 2006, 12.)

Käyttöturvallisuudella pyritään täyttämään kohta 6) VAHTI-julkaisussa annetussa tietoturvallisuuden perustason toteutuksen asetuksessa eli tietojen luvaton muuttaminen ja muun luvattoman tai asiattoman käsittelyn estäminen käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä. Sen lisäksi muun muassa varmuuskopioinnilla voidaan varmistaa tietojen saatavuus ja käytettävyys myös muuttuneissa olosuhteissa (kohta 4).

Laitteistoturvallisuus, jolla tarkoitetaan kaikkien teknisten laitteiden suojaamista, pyrkii osaltaan huolehtimaan niin ikään kohdista 4) ja 6). Tällä tarkoitetaan sitä, että riittävällä teknisten laitteiden suojauksella voidaan vaikuttaa tietojen saannin ja käytettävyyden turvaamiseen, kun tekniset laitteet ovat niiltä määrin suojattuina, etteivät ne pääse vahingoittumaan. Lisäksi sillä voidaan vaikuttaa siihen, että tietojen luvatonta muuttamista ja muuta luvatonta tai asiatonta käsittelyä pystytään estämään. Keinoja tähän on lueteltu luvussa 4.6.

5.3 Ylläpitoprosessi

Ohjelmistoturvallisuuteen kuuluu Hakalan ym. (2006, 11) mukaan ohjelmistoturvallisuuteen luetaan kaikki ohjelmistoihin liittyvät seikat. Esimerkiksi he mainitsevat ohjelmistojen testauksen, jolla pyritään varmistamaan sovellusten sopivuutta, ohjelmistojen keskinäistä yhteensopivuutta ja toiminnan luotettavuutta ja virheettömyyttä. Siihen kuuluu myös ohjelmistoversioiden ja lisenssien hallinta. Näistä seikoista on tietenkin hyvä varmistua jo ennen asennusprosessin aloittamista, mutta, jos turvaurakassa on sopimuksen mukaan sitouduttu ylläpitoon liittyviin tehtäviin, korostuu toimivan tietoturvan ylläpidossa muun muassa laite- ja ohjelmistopäivityksistä huolehtiminen.

Kuten kuviossa 8 on kuvattu, tarkoitetaan tietoliikenneturvallisuudella tietoverkoissa liikkuvan tiedon suojaamista (Hakala ym. 2006, 12). Tietoliikenneturvallisuus on jätetty ylläpitoprosessi vaiheeseen vain siksi, että mahdolliset verkon huolto- ja ylläpitosopimukset on laadittavat huolella ongelmatilanteita varten. Muutoin se tulee huomioida koko prosessin ajan, jos ajatellaan yksinkertaisesti esimerkiksi luottamukselliseksi luokitellun tiedon välittämistä sähköpostitse, jolloin salauksen käyttö on suositeltavaa.

Ylläpitoprosessiin on listattu kuuluvaksi palvelupyyntöjen vastaanotto, kuten vikailmoitukset, hälytykset, ylläpito- ja kunnossapitotehtävät, viankorjaustehtävät, kunnossapito-ohjelman mukaiset tehtävät, etävalvontapalvelut ja aiemmin mainitut laite- ja ohjelmistopäivitykset. Tästä johtuen ylläpitoon liittyvät tehtävät ja niistä huolehtiminen ovat tärkeitä niin liiketoiminnan kuin toimivan tietoturvan kannalta. Jälleen kerran sopimusten rooli on mainitsemisen arvoinen seikka, kun puhutaan ylläpitoprosessista, joka on muihin prosessin kohtiin verrattuna pitkäaikaisin.

Aiemmin mainitun ohjelmisto- ja tietoliikenneturvallisuuden lisäksi ylläpitoprosessiin kuuluu olennaisena osana laitteistoturvallisuus. Asianmukaisella laitteistojen tapahtumatietojen (lokitiedot) kerääminen helpottaa esimerkiksi vikatilanteiden selvittämistä ja korjaamista. Lisäksi laitteistorekisteri tulee olla luotuna juuri ongelmatilanteiden selvittelyä varten. Tekstissä on aikaisemmin mainittu myös siitä, että huoltotoimenpiteiden tai käytöstä poiston yhteydessä on varmistuttava, etteivät ne mahdollista tietojen joutumista kolmansille osapuolille.

6 Kyselyn toteutus, rakenne ja analysointi

Kuten opinnäytetyön alussa on mainittu, toteutettiin siihen liittyen kysely sähkö- ja turvaurakoitsijoiden keskuudessa. Sen tarkoituksena oli kerätä tarvittavaa tutkimusaineistoa aiheesta ja tuottaa myös hankeyritykselle tietoa urakoitsijoiden tietoturvan hallintaan liittyvistä asioista. Kyselyn analysoinnin avulla on pyritty tekemään tulkintoja muun muassa turvaurakoitsijoiden tietoturvan hallinnasta ja liittämään ne osaksi pohdintaosuutta.

Suhteessa kehittämistyön tutkimuksellisiin tavoitteisiin sekä toteutusaikatauluun kysely oli ehdoton valinta tutkimusmenetelmäksi. Kyselytutkimuksen etuihin lukeutuu se, että sen avulla voidaan periaatteessa kerätä laaja tutkimusaineisto suurelta määrältä ihmisiä ja se on menetelmänä nopea ja tehokas (Ojasalo ym. 2009, 108). Tämä johtui osaksi myös siitä, että hankeyrityksessä oli aikaisemminkin toteutettu vastaavanlaisia kyselyitä ja heillä oli käytössään laaja verkosto, joille kysely voitiin lähettää. Sen avulla voitiin vahvistaa sitä käsitystä, mikä kirjoittajalle oli muun muassa kirjalliseen aineistoon perehtymisen yhteydessä ja sen jälkeen urakoitsijoiden tietoturvan hallinnasta muodostunut.

Alaluvuissa käydään ensiksi läpi kyselyn toteutusta lyhyesti. Siinä tuodaan esille lähinnä toteutustapaa sekä sitä kenelle kysely lähetettiin. Tämän jälkeen käydään läpi kyselyn rakennetta ja tuodaan esille miksi kyseisiä asioita on kysytty ja miten ne palvelevat tutkimustavoitteita. Lopussa analysoinnin yhteydessä on tarkoitus käsitellä vastauksia ja miettiä alustavia johtopäätöksiä. Itse kyselyä ei ole tekstiin liitetty sen ollessa tutkimusaineistoa.

6.1 Kyselyn toteutus

Kehittämistyöhön kysely toteutettiin internet-pohjaisena kyselynä Webropolin avulla, jolloin vastaaja itse täytti vastauskohdat. Se lähetettiin sähköpostin kautta 484 sähkö- ja/tai turvaurakoitsijalle. Mukana olivat Turva-alan yrittäjät ry:n noin 100 jäsenyritystä ja noin 400 STUL ry:n isohkoa jäsenyritystä. Kyselyn kohdeyritykset valittiin hankeyrityksen olemassa olevia yhteystietoja hyväksikäyttäen. Siitä syystä havaintoyksiköillä, jotka tässä tapauksessa on valittu harkinnanvaraisesti, tarkoitetaan niin sanottua näytettä. Internetkyselyiden haasteena

on perusjoukon ja otantakehikon määritteleminen, koska kattavaa listaa hankeyrityksen sähköpostiosoitteista on mahdotonta löytää (Ojasalo ym. 2009, 111).

Vastauksien vähäisen määrän takia yrityksille lähetettiin uusintapyyntö, jonka jälkeen vastausajan umpeuduttua 484 sähkö- ja/tai turvaurakoitsijasta noin 34 (7 %) vastasivat strukturoituihin kysymyksiin ja noin 10 (2 %) avoimiin kysymyksiin. Vastaajien määrä on edellä esitetty noin muodossa, koska eri kysymyskohtien vastaajien määrässä oli vaihteluita. Vastausprosentti on erittäin huono, mutta tarkoituksena ei ollut täyttää kyselyihin yleisesti päteviä tutkimuksellisia määreitä, vaan antaa suuntaviivoja aiheen pohdiskelulle sekä tietoa yrityksen käyttöön. Vastausmäärien takia ei sähkö- ja turvaurakoitsijoita koskevia yleistyksiä tehdä, mitä normaalisti määrällisessä tutkimuksessa tavoitellaan, koska näytteestä tällaisia yleistyksiä ei voida tehdä (Ojasalo 2009, 110).

Kysely käynnistyi 23.10.2012 ja vastausaikaa annettiin 31.10.2012 asti. Näin vastaajilla oli reilu viikko aikaa vastata siihen. Kyselyyn osallistujat vastasivat kyselyyn nimettömästi ja täysin luottamuksellisesti.

6.2 Kyselyn rakenne

Kyselyn teko aloitettiin tutustumalla aihetta käsittelevään kirjallisuuteen ja vastaavanlaisiin tutkimuksiin tarvittavan tietoperustan luomiseksi ja kohdeilmiöön perehtymiseksi. Turvaurakoinnin näkökulmasta tietoturvan hallintaan liittyvää aineistoa ei pahemmin ollut saatavilla. Itse lomakkeen suunnittelussa kiinnitettiin erityisesti huomiota kehittämistyön tavoitteisiin. Siihen pyrittiin sisällyttämään vain ja ainoastaan sellaiset kysymykset, jotka ovat olennaisia näiden tavoitteiden saavuttamiseksi. (Ojasalo ym. 2009, 115–116.) Tämän lisäksi kysely sisälsi saatesanat, joiden avulla pyrittiin muun muassa herättämään mielenkiinto ja luoda lyhyt katsaus opinnäytetyön aiheeseen sekä antamaan tarvittavat tiedot vastaamiseen.

Lomakkeen pituus haluttiin pitää mahdollisimman lyhyenä ja ulkoasu selkeänä, jotta vastaamishalukkuus ei ainakaan siitä johtuen kärsisi. Näin ollen myös tietojen tulkitseminen oli helpompaa. Kyselyn keskimääräiseksi vastausajaksi arvioitiin maksimissaan 10 minuuttia, jota voidaan pitää sopivana aikana. Kysymystenasettelu tehtiin arvion mukaan yksinkertaiseksi ja helppotajuiseksi, koska aihealue ja jotkin käsitteet saattoivat osalle olla vaikeita tai muuten haasteellisia. Vastausvaihtoehdoiksi valittiin kyllä tai ei, jotta vastaaminen olisi nopeaa ja helppoa, ja vastaukset sitä kautta tarkkoja, kun esimerkiksi ”en osaa sanoa” vaihtoehto oli suljettu pois. Näin siitä huolimatta, että kyseistä vaihtoehtoa suositellaan eri ohjeissa käytettäväksi. Näiden uskottiin vaikuttavan myös siihen, että mahdolliset vastaajat jaksavat ja osaavat vastata kyselyyn. (Ojasalo ym. 2009, 116.)

Kyselyn suunnittelussa haluttiin edellisten lisäksi keskittyä siihen, että kysymyskohdat ymmärrettäisiin samalla tavalla, eivätkä ne olisi niin sanottuja johdattelevia kysymyksiä. Tähän päämäärään päästäkseen kysymykset oli muotoiltu järkevä pituisiksi ja mahdollisimman tarkoiksi. Lisäksi kysymysmäärä haluttiin pitää suhteellisen pienenä ja niiden järjestys johdonmukaisena kulkien isoista kokonaisuuksista pienempiin yksityiskohtiin.

Kysely sisälsi yhteensä 18 strukturoitua kysymystä ja lisäksi 2 avointa kysymystä. Ensimmäisillä strukturoiduilla kysymyksillä pyrittiin selvittämään enemmän tietoturvan hallinnollista puolta yrityksissä sekä tietoturvan toteutukseen yleisesti liitettyjä seikkoja, joihin on suhteellisen helppo lähtökohtaisesti vastata. Näitä niin sanottuja isojen kokonaisuuksien hahmottamiseen tarkoitettuja kysymyksiä oli ensimmäiset kahdeksan kysymystä. Kysymysten avulla haluttiin selvittää onko puitteet toimivalle ja jatkuvalle tietoturvatyölle olemassa ja miten sen kannalta olennaisimpia asioita on vastaajien keskuudessa huomioitu. Onko tekstissäkin aikaisemmin käsitellyt tiedon turvaamisen lähtökohdat kunnossa?

Tämän jälkeen kysymykset (9-15) kohdistuivat tarkemmin juuri turvaurakoinnissa huomioitaviin tietoturvaperiaatteisiin ja siihen miten niistä on huolehdittu. Yhtenä päämääränä oli näiden kysymysten kautta saada selville tavallaan koko tietoturvan merkitystä urakoitsijoille. Tämän takia kysymykset muodostuivat hyvin perusasioista, kuten esimerkiksi käyttöturvallisuudessa huomioitavista seikoista. Näiden kysymysten tarkoituksena oli ylipäätään tuottaa tietoa siitä, millä tasolla tietoturva urakoitsijoiden keskuudessa on.

Strukturoitujen kysymysten viimeiset kysymykset 16–18 olivat nimenomaan hankeyritystä kiinnostavia kysymyksiä, jotka samalla palvelivat myös työn tavoitteita. Niiden avulla hankeyritys sai tietoonsa, missä yrityksissä on käytössä turvaurakointitehtävät kattava toiminnanohjaus- tai laatujärjestelmä ja onko heidän tarjoama yrityssertifiointipalvelu tuttu. Lisäksi haluttiin selvittää rakennuttajien osuutta tietoturvavaatimuksissa, koska usein turvaurakoitsijalta edellytetään luotettavuutta ja tietoturvaohjeistuksen ja – toimintamenetelmien olemassaolon osoittamista esimerkiksi sertifiointitodistuksella.

Kyselyn kahteen viimeiseen kysymykseen, jotka olivat avoimia ja järjestyksessään siis kohdat 19 ja 20, osallistujat saivat kertoa näkemyksiään tietoturvariskeistä sekä mielipiteitään turvaurakoinnissa huomioitavista tietoturva-asioista. Vähäisistä vastausmääristä huolimatta avointen kysymysten kohdalla saatiin arvokkaita näkemyksiä koottua yhteen. Samalla avoimet kysymykset antoivat hyvää kuvaa siitä tietoturvan tasosta, joka turvaurakointikohteissa vallitsee.

6.3 Kyselyn analysointi

Vähäisen kyselyyn vastanneiden määrästä huolimatta voidaan sitä pitää oikeana menetelmänä suhteessa tutkimustavoitteisiin. Analysoinnin yhteydessä on tarkoituksena tuoda esille joitain huomiota herättäviä kohtia ja yhdistää ne tulkinnan avulla osaksi pohdintaa. Aineistoa esitellään suurimmaksi osaksi prosenttiosuuksien muodossa.

Kyselyyn vastanneista 85 % on tunnistanut toiminnalleen kriittiset tai luottamukselliset tiedot. Tämä on sinänsä erittäin tärkeää, että ylipäätänsä tiedetään mitä tietoja tulee suojata. Lähtökohtaisesti kyselyyn vastanneiden keskuudessa oltiin siis ainakin tämän suhteen oikeilla jäljillä. Kuitenkin tarkempi riskianalyysi oli noin kahdella kolmasosalla tekemättä. Riskianalyysi mahdollistaisi tietoturvan toimenpiteiden tehokkaamman kohdistamisen. Muutenkin tietoturvatoimenpiteiden tulisi yleisesti perustua riskienarviointiin.

Tietoturvapolitiikka oli luotu puolessa vastanneissa yrityksissä, mutta seuraava askel kohti toimivaa tietoturvaa tietoturvasuunnitelman muodossa, jossa tavoitteet, vastuut ja toimenpiteet on yksityiskohtaisemmin kuvattu, oli suurimmalla osalla eli noin 68 % tekemättä. Sen avulla voitaisiin helpottaa tunnistamaan tietoa uhkaavat riskit ja kohdistamaan suojaus riittävällä tasolla sekä tehokkaasti oikeisiin kohteisiin.

Yhteiset pelisäännöt tietoturvan käytäntöihin ja menetelmiin oli suurimassa osassa (noin 65 %) yrityksistä luotu ja sen myötä henkilöstön toiminta eri tilanteissa kyselyn mukaan selvää. Tästä voitaisiinkin päätellä, että tietoturvasuunnitelman luomiseksi vastanneiden urakointiyritysten keskuudessa tarvitsisi enää miettiä tietoturvan tavoitteiden ja vastuiden yksityiskohtaisempaa kuvaamista. On kuitenkin huomioitava se seikka, että tietoturvan käytäntöjen ja menetelmien luominen kyseisissä tehtävissä, joissa on kiinnitettävä erityistä huomiota tietoturva- ja salassapitomenetelmiin, tulisi olla kaikilla tehtynä. Siten yksi kolmasosa kieltäviä vastauksia oli tässä kohtaa liikaa.

Toiminnan jatkuvuuteen oli vain yli 60 % kiinnittänyt huomiota, joten hälyttävän suuressa osassa tämä liiketoiminnan ehdoton edellytys oli jäänyt turvaamatta. Kuitenkin 85 % kertoi huolehtineensa riittävästä varmuuskopioinnista. Tässä kohdassa kysymysten voidaan sanoa olleen arviolta hieman johdattelevia, mutta ehkä vastaajien keskuudessa varmuuskopiointia ei mielletty osaksi toiminnan jatkuvuuden turvaamista, jota se omalta osaltaan on. Tästä johtuen voidaan päätellä, että toiminnan jatkuvuuteen on ainakin joissain määrin kiinnitetty huomiota, vaikka se vaatii osakseen suunnitelmia ja niiden toimivuuden testaamista.

Edellisten lisäksi reilu 40 % ei pitänyt tämän hetkistä tietoturvatasoa tyydyttävänä. Tämä oikeastaan kuvaa hyvin sitä, mitä edeltävät vastaukset antoivat ymmärtää eli joitain asioita on

vaihtelevalla tavalla tietoturvan eteen tehty, mutta järjestelmällinen tapa toimia puuttuu. Tietoturvaan liittyviin kokonaisuuksiin ei tarvittavissa määrin olla monessakaan urakointiyrityksissä paneuduttu sen vaativalla tavalla.

Vaikka suurin osa kyselyyn vastanneista yrityksistä oli tunnistanut kriittisimmät tiedot, niin huomion arvoista oli se, että lähes yksi kolmasosa ei ollut tietoisia toimintaansa liittyvistä laeista ja niiden asettamista velvollisuuksista ja vaatimuksista. Kyseistä seikkaa on tässäkin työssä teoriasta nousseen merkityksen takia useaan otteeseen painotettu. Osa urakointiyrityksille kriittisimmistä tiedoista kun määritellään jo laissa.

Pieni ristiriita oli kyselyssä myös siinä, että lähes kaikissa yrityksissä (85 %) oli huolehdittu dokumenttien ja asiakirjojen turvallisesta säilyttämisestä ja hävittämisestä, mutta tietojen käsittelystä ei ollut 69 % vastanneista laatineet toimintaohjeita. Tietojen säilyttäminen ja hävittäminen kuuluu olennaisena osana tietojen käsittelyn ohjeistukseen ja osaltaan jatkuvuuden turvaamiseen. Tämä ehkä kuvastaa osaltaan lisäksi sitä, että yli puolet vastanneista kertoi, etteivät etä- ja matkatyön tietoturvaperiaatteet olleet käytössä. Oli vika sitten kysymystenasettelussa tai muussa, tulisi muun muassa luvussa 4.3 esiteltyyn tietoaineistoturvallisuuteen kiinnittää huomiota. Siinä esitellyt käsittelysäännöt yksinkertaisuudessaan voisi tarjota apua tähän.

Sopimusten, ja eritoten salassapitosopimusten avulla, voidaan alihankkijoita ja muita yhteistyökumppaneita sitouttaa tietoturvaan. Lähes puolet vastanneista ei kuitenkaan ollut huolehtinut näistä seikoista. Tämä osaltaan johtuu myös siitä, ettei lain vaatimuksista olla kovin tietoisia. Tietoturvaan liittyvän lainsäädännön lisäksi ei olisi haittaa tuntea sopimuksiin liittyviä tietoturvavelvoitteita, koska ainakin sähkö- ja teleurakoinnissa on käytössä yleisiä sopimusehtoja, jotka tulisi tuntea.

Kyselyn perusteella ei voida sanoa, että henkilöstön tietoturvatietoisuus olisi huipussaan, kun noin 35 % vastanneista ei ollut perehdyttäneet henkilökuntaansa tietoturvan käytäntöihin. Perehdyttämisen, kouluttamisen ja ohjeistamisen tärkeyttä toimivan tietoturvan kannalta on pyritty tämän työn yhteydessä tuomaan esille. Usein turvaurakoissa, etenkin tietoteknisten turvallisuusjärjestelmien osalta, edellytetään niiden käytön perehdyttämistä myös tuleville käyttäjille. Onko tämä mahdollista, jos oma henkilöstö ei ole tietoinen tietoturvan käytännöistä?

Vastauksista tuli selvästi esille myös se, että myöskään rakennuttajat eivät huomio tietoturvavaatimuksia riittävästi hankintavaatimuksissa. Tätä mieltä oli noin 73 % vastanneista. Tämän voisi osaltaan kuvitella vaikuttavan löyhään tietoturvavaatimuksien huomiointiin hankinnoissa, joka on kuitenkin ensisijaisen tärkeää, jos ajatellaan esimerkiksi laitteiden ylläpitoa.

Ensimmäisestä avoimesta kysymyksestä, jossa pyydettiin vastaajilta näkemyksiä turvaurakointitehtävien suurimmista tietoturvariskeistä, esiin nousi muun muassa tiedon turvallinen käsittely sen eri muodoissa ja vaiheissa sekä ihmiset ja henkilöstö. Niin sanottu liikkuva käyttö koettiin myös suureksi riskiksi. Nämä tukevat erittäin hyvin niitä ongelma-alueita joita nousi suljettujen kysymystenkin kohdalla. Muun muassa nämä olivat kohtia, joihin kyselyyn annetuiden vastausten perusteella oli heikoiten huomioitu.

Toisessa avoimessa pyydettiin mielipiteitä niistä seikoista, joita tietoturvan kannalta tulisi kyseisissä tehtävissä ottaa huomioon. Vastaukset myötäilivät hyvin pitkälle toisessa avoimessa kysymyksessä mainittuja kohtia. Turvallisen tietojen käsittelyn ohjeistus ja niiden noudattaminen koettiin tärkeäksi. Mielenkiintoista tässä onkin se, että miksi nämä asiat on luvalla sanoen huonosti hoidettu, jos ne samalla koetaan tärkeiksi. Tähän tuotiin esille muun muassa pakottavan lainsäädännön puuttuminen. Tämä on vielä tällä hetkellä totta, mutta, jos urakointiyrityksissä oltaisiin paremmin selvillä lain velvoitteista ja vaatimuksista heidän toimintaan, ei pakottavan lainsäädännön puuttuminen ehkä olisikaan niin suuri este ”riittävän” tietoturvan ja – tason toteuttamiselle.

Lyhyenä yhteenvetona kyselyn pohjalta voidaan todeta, että kyseisissä yrityksissä tietoturvaan liittyvässä suunnittelussa, toteutuksessa, seurannassa on vielä paljon kehitettävää. Suhteutettuna siihen, kuinka turvallisuusorientoitunut ala on kysymyksessä, tulisi myös tietoturvaan kiinnittää enemmän huomiota. Sen tulisi lähteä järkevästi suhteutetun kokonaisuuden hallinnasta yksittäisempiin periaatteisiin ja ohjeistuksiin. Tietoturvapolitiikan ja – suunnitelman laatimisella pystyttäisiin paremmin vastaamaan näihin haasteisiin. Niiden avulla voitaisiin saada eri asiat sovitettua paremmin yhteen ja luotua järjestelmällinen tapa toimia, kun tällä hetkellä tietoturvaa on huomioitu vähän sieltä täältä. Edellisten lisäksi tulisi erityisesti panostaa muun muassa tietoturvallisten toimintatapojen iskostamiseen yrityksissä ja sen työntekijöille koulutuksen ja perehdyttämisen sekä saatavilla olevien ohjeiden, kuten käsittelysääntöjen, avulla.

7 Pohdinta

Tietoturvavahingoissa yleisesti ottaen tuntuu suurimmaksi osaksi olevan syynä se, ettei uhkasta olla käytännön työtilanteessa oltu tietoisia, oikeat menettelytavat ovat puuttuneet tai niitä ei ole noudatettu. Ihminen ja henkilöstö nousevat usein tärkeimmäksi tekijäksi tällä saralla. Yrityksessä jokaisen tulisi omalta osaltaan olla vastuussa tietoturvasta ja sen toteuttamisesta. Turvallisuustietoisuuden lisääminen esimerkiksi henkilöstön koulutuksella on tässä avainasemassa. (VAHTI 11/2006, 21.)

Tietoturvan hallinnan kannalta tietoteknisten turvallisuusjärjestelmien urakointitehtävissä olisi tärkeää tunnistaa ja tuoda esiin luottamuksellisten tietojen merkitystä ja sovittaa yhteen luokitusta vastaavat käsittelysäännöt. Luottamuksellista tietoa varten luodut käsittelysäännöt sekä niiden noudattaminen voitaisiin ajatella muodostavan työn edellyttämän tietoturvallisuuden ja luottamussuhteen toimijoiden välillä.

Urakointitehtävissä, samoin kuin niitä toteuttavissa yrityksissä, tulisi muodostaa tietoturvallinen tapa toimia, jota koko henkilöstö noudattaisi. Tarvittavan tietoturvatason määrittäminen omaa toimintaa mahdollisimman hyvin tukevaksi ja sen johdonmukainen hallinta edesauttavat toimivan tietoturvan toteutusta. Liian tiukat tietoturvaperiaatteet voivat vaikeuttaa työtä, lisätä kustannuksia ja johtaa ohjeiden noudattamatta jättämiseen, mikä taas johtaa uusiin tietoturvariskeihin. Liian löyhä tietoturvataso puolestaan nostaa riskitasoa ja voi pahimmillaan estää tiedon saamisen luottamuksen puuttuessa tai aiheuttaa tietoriskien toteutumisen. (VAHTI 9/2008, 21.)

Pohdinnan yhteydessä voidaan myös tehdä tilaa ajatukselle, tulisiko rakennuttajia jotain kautta perehdyttää tietoturva-asioihin, koska he eivät kyselyn vastauksien perusteella huomio riittävästi tietoturvaseikkoja. Tätä ajatusta tukee myös allekirjoittaneelle työtä tehdessä muodostunut käsitys muun muassa siitä, millä tasolla rakennuttajien dokumenttien käsittely ja suojaaminen joissain tapauksissa tällä hetkellä on. Vaatimusten lisääminen aiheuttaisi myös tietoturvaan liittyvien seikkojen tarkemman huomioinnin. Toinen kysymys on herännyt siihen liittyen, miten tietoturvaan liittyvien turvallisuustekijöiden noudattamista voidaan valvoa tai edes edistää. Vielä tällä hetkellä sen tulisi lähteä yrityksistä itsestään.

7.1 Turvaurakoitsijan tietoturvan menetelmäohjeiston tarpeet

Turvaurakoitsijan tietoturvan menetelmäohjeiston tarpeita on ehkä helpoin lähestyä kahdesta eri tarkastelukulmasta, joita myös tässä opinnäytetyössä on hyvin pitkälti käytetty: yrityksien ja niiden toiminnan sekä turvaurakointiprosessin tarkastelukulmista. Lisäksi nämä tulisi liittää osaksi työn perimmäistä tarkoitusta eli kohdeyrityksen palvelutoimintaa eli koulutusta ja tietoturvaohjeistusta sekä sertifiointia tukeviksi. Perusteet näille muodostuvat tekstissä esiteltyjen seikkojen ja kirjoittajan sitä kautta tehtyjen päätelmien pohjalta.

Hankeyrityksen palvelutoimintaa tukee parhaiten työn alkupuoli, jossa olemassa olevaa teoriaa on lähestytty turvaurakoinnille olennaisia tekijöitä ja menetelmiä silmällä pitäen. Siinä on pyritty muodostamaan kuvaa siitä, mitä kokonaisvaltainen tietoturvan hallinta pääasiassa voisi sisältää. Itse koulutukseen ei tämän työn kannalta ole ollut tarpeellista ottaa kantaa. Tarkoituksena olisi, että tehtyä selvitystä vallitsevista tietoturvateorioista voitaisiin hyödyntää hankeyrityksessä heidän parhaaksi katsomalla tavalla.

Urakointiprosessin tarkastelukulmaa on käsitelty omana kappaleenaan luvussa viisi. Niin ikään kyseessä on eräänlainen selvitys, mitä osaksi teorian ja osaksi opinnäytetyön yhteydessä saatujen tulosten pohjalta tietoturvan hallinnassa tulisi ottaa huomioon sertifiointeja myönnettäessä. Esimerkkikuvauksia menetelmäohjeista on siis luotu kaksi, joissa molemmissa on hyödynnetty teorian lisäksi kyselyn analysointia. Kaiken edellä mainitun pohjalta on vielä luvussa 7.3. kerätty yhteen, mitä tietoturvapolitiikka tulisi turvaurakointiyrityksessä sisältää.

7.2 Esimerkkikuvaus turvaurakoitsijan tietoturvan menetelmäohjeesta

Hankeyritys toivoi lopputuotoksena esimerkkikuvausta menetelmäohjeesta turvaurakoitsijoille. Nämä kaksi menetelmäohjetta toimivat esimerkkikuvauksena turvaurakoitsijoille yritysten omaa toimintaa sekä urakkaprosessia varten. Lähinnä asiakokonaisuuksien muotoon kerätyt kohdat on muodostettu tekstissä aikaisemmin huomioiduista kohdista. Lisäksi niihin on sisällytetty kyselyssä esiin nousseita seikkoja.

Ohjeiden tarkoituksena on tiivistää keskeisimmät tietoturvaperiaatteet ja antaa käytännön neuvoja tietoturvan toteuttamiseen. Sitä ei ole muokattu millään tavoin visuaaliseen muotoon tai esitelty tarkempia asiasisältöjä, koska tarkoituksena oli tehdä esimerkkikuvaus, jonka sisältö voidaan tapauskohtaisesti tarkemmin määritellä.

Urakointiyritysten tietoturva (koulutusta ja tietoturvaohjeistusta tukeva):

Lähtökohtana yrityksillä tulisi olla se, että kaikilla on tietoja, jotka tulee turvata. Tietoturvasta huolehtiminen tulisi nähdä liiketoimintaa edistävänä tekijänä laadukkaana toimijana.

- varmistuminen lainsäädännön vaikutuksista toimintaan

  Yrityksissä tulisi kartoittaa vähintään pakottavat yksittäiset säädökset, jotka koskevat tietoturvan suunnittelua, ylläpitoa ja kehittämistä. Lisäksi sopimuksiin liittyvien tietoturvavelvoitteiden tunteminen on tärkeää turhien kustannusten minimoimiseksi. Yritykset vastaavat itse toimintansa lainmukaisuudesta, johon muun muassa henkilöstön ohjeistaminen tietoturva-asioissa kuuluu. Lainsäädäntö on yksi keino varautua tietoturvauhkiin.

- tietoturvakartoitus

  Lainsäädännön ohella tietoturvakartoitus on ehdoton lähtökohta tietoturvan hallinnan kannalta. Se alkaa suojattavien kohteiden kartoituksella, missä tunnistetaan toiminalle kriittiset tiedot. Näin saadaan selville, mitä tietoja suojataan. Riskianalyysin avulla

varmistetaan tietoturvaan liittyvien suojaustoimenpiteiden tehokas kohdistaminen. Näin tiedetään myös, mitä ohjeita tietojen turvaamiseksi tarvitaan. Tietoturvariskien kartoittamisella on ehkäisevä vaikutus niiden toteutumiseen, mikä puolestaan tukee liiketoiminnan jatkuvuutta.

- organisointi ja vastuut

  Tietoturvan organisoinnin ja vastuuttamisen kautta yrityksissä tiedetään kuka tekee ja mitä tekee. Pelkkä tieto siitä, mikä omalle vastuulle kuuluu auttaa henkilöstöä sitoutumaan asetettuihin tietoturvavelvoitteisiin. Muun muassa yrityksen toimintaa koskevien lakien tunteminen kuuluu kaikkien työntekijöiden vastuulle.

- tietoturvapolitiikka ja – suunnitelma

  Tietoturvapolitiikan ja – suunnitelman tarkoituksena on vastata kysymyksiin mitä, miksi, miten. Politiikassa esitetään yleisluontoinen kuvaus tietoturvan tavoitteista, vastuista ja toimenpiteistä, kun suunnitelmassa näiden kohtien määrittely on yksityiskohtaista. Suunnitelma sisältää tietoturvan osa-alueet, joiden avulla on tarkoitus vastata kokonaisvaltaisesti tietoturvaan liittyviin seikkoihin:

  - Hallinnollinen tietoturva (mm. tietoturvaperiaatteet, tietoturvaohjeistus, seuranta ja kehittäminen)

  - Henkilöstöturvallisuus (mm. rekrytointi: palkkaaminen, toimenkuvat, käyttöoikeudet, työsuhteen päättäminen, sopimukset, koulutus)

  - Tietoaineistoturvallisuus (mm. käsittelysäännöt: tiedon säilytys, luovutus, hävitys)

  - Fyysinen turvallisuus

  - Käyttöturvallisuus (mm. työaseman käyttö, virustorjunta, käyttöoikeuksien ja salasanojen hallinta sekä varmuuskopiointi)

  - Tietotekninen turvallisuus (mm. laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus)

- Käyttöönotto

  Tietoturva ei synny itsestään, vaan sanoista on siirryttävä tekoihin. Ohjeistusten ja muiden käyttöönotto vaatii perehdytystä ja tietoa tietoturvan merkityksestä. Tekniikan lisäksi myös ihmisten on toimittava oikein.

- Tarkistus ja jatkuvuus

  Valittujen suojaustoimenpiteiden ja – tason tarkastaminen sekä sen kautta tehdyt muutokset tehostavat toimintaa edelleen. Lisäksi toiminnan jatkuvuuden turvaaminen toimintaan nähden riittävien suunnitelmien avulla ja niiden testaus mahdollisten poikkeustilanteiden, kuten tietoteknisten laitteiden vikaantuminen, on liiketoiminnan ehdoton edellytys. Toimiva tietoturva on jatkuvaa kehittämistä.

Turvaurakointiprosessin tietoturva (sertifiointia tukeva):

Turvaurakointiprosessi on jaettu kolmeen vaiheeseen: myynti-, asennus- ja ylläpito. Samaa jakoa on käytetty myös tietoturvan menetelmäohjeen esimerkkikuvauksessa.

Myyntiprosessi:

- riskitekijöiden määritys

  Riskitekijöiden määritys tulee tehdä urakkakohtaisesti ennen varsinaisten työn aloittamista ja mahdollisesti tarkentaa niitä urakan edetessä. Siten sen yhteydessä on huomioitava kaikki kolme prosessin vaihetta. Tietoturvan osalta niihin varautuminen voi tapahtua esimerkiksi erilaisten ohjeiden ja hyvien käytäntöjen mukaisilla perusmenettelyillä. Lisäksi tietoturvan kannalta toteutettavan järjestelmän laitevalinnassa tulee varmistua siitä, että ne ovat lähtökohtaisesti tietoturvallisia. Ennen urakan aloittamista tulee myös varmistua henkilöstön luotettavuudesta asiakirjojen käsittelyyn liittyvissä tehtävissä. Riskien ehkäiseminen mahdollistaa urakan onnistumisen.

- tehtävien ja vastuiden määrittely

  Voidaan puhua myös tietoturvan organisoinnista. Tehtävät ja vastuut tulisi pääperiaatteiltaan olla määriteltyinä jo työtehtävään palkattaessa. Kuitenkin nämä voivat vaihdella urakkakohtaisesti, joten silloin ne on saatettava työntekijöiden tietoon. Näiden määrittely ei koske ainoastaan omaa henkilöstöä vaan niin ikään mahdollisia laitetoimittajia ja muita mahdollisia yhteistyökumppaneita. Toimittajien ja yhteistyö-

kumppaneiden valinnassa on syytä kiinnittää huomiota siihen, että myös heidän toiminnassaan on huomioitu tietoturvatekijät, kuten tietojen käsittelijöiden luotettavuus ja tietojen käsittelyn ohjeistus sekä koulutus.

- Sopimusten laadinta

  Sopimuksien laatimiseen liittyy joitakin epävarmuustekijöitä tietoturvaan liittyen. Niiden ehkäisemiseksi tulee tuntea sopimuksiin liittyvät tietoturvavelvoitteet. Sopimuksissa on määriteltävä yksityiskohtaisesti, mitkä asiat kuuluvat sopimukseen, miten nopeasti huollot suoritetaan ja kuka toimet suorittaa. Sopimuksiin liittyen tapahtumien dokumentointi on myös erityisen tärkeää, jos asioita joudutaan jälkikäteen yrittää todistella. Dokumentointi koskee koko prosessia alusta loppuun. Sopimusten avulla on lisäksi mahdollista sitouttaa yhteistyökumppaneita tietoturvaan liittyviin asioihin.

Asennusprosessi:

- toteutuksen suunnittelu

  Toteutuksen suunnitellussa on huomioitava se, että lähtökohtaisesti kyse on asiakkaan tietojen saannin ja käytettävyyden turvaamisesta, tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman käsittelyn estämisestä riittävillä (tietoteknisillä) turvallisuusjärjestelyillä ja muilla toimenpiteillä. Lisäksi tulee kiinnittää huomiota tietojenkäsittely- ja säilytystilojen riittävään valvomiseen ja suojaamiseen. Teknisten laitteiden riittävällä suojaamisella pyritään siihen, etteivät ne pääse vahingoittumaan. Myös kaapeloinnin suojaus fyysisiltä uhilta kuten katkaiseminen, häirintä ja kiinnittyminen on käytössä olevien resurssien mukaan huomioitava ja riskit minimoitava ainakin hyvällä suunnittelulla. Suunnittelussa on huomioitava myös, etteivät yhteydet ja varayhteydet ole riippuvaisia yhdestä yksittäisestä toimivasta komponentista. Suunnittelun päätavoitteena on estää tietoturvauhkien toteutuminen.

- tietojen käsittelysäännöt

  Tietoteknisten turvallisuusjärjestelmien urakointitehtävissä haltuun uskotaan yrityksiin liittyvää toiminnalle kriittistä tietoa, jolloin käyttöön saatujen ja tuotettujen tietojen tietoturvallisuuden ja luottamuksellisuuden tasosta tulee varmistua. Näiden tarkoitusten täyttämiseksi urakkaan liittyvien tietojen käsittelylle ja turvallisuusluokittelulle tulee määritellä riittävän yksityiskohtaiset periaatteet, toisin sanoen käsittelysäännöt, jotka kukin osallistuva taho voi rinnastaa omaan toimintaansa. Käsittelysääntöihin tulisi vähintään kuulua tietojen säilyttämiseen, varmistamiseen ja pa-

lauttamiseen sekä tuhoamiseen liittyvät toimet. Ohjeet ja koulutus korostuu tässä yhteydessä.

- valvonta

  Urakoissa voi olla useita toimijoita samaan aikaan, joilla tietoturvaseikat on huomioitu vaihtelevalla tasolla. Kuitenkin tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely tulisi pyrkiä estämään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä.

- laitteiden varmentaminen

  Kaikista kriittisimmissä urakointikohteissa laitteiden varmentamisesta tulee olla huomioituna. Laitteiden varmentamisella tarkoitetaan sitä, että vioittuneen laitteen tilalle on saatavilla vastaava laite, joka hoitaa vioittuneen tehtävät. Samassa yhteydessä tulee varmistua laitteen sähkönsaannista.

- toiminnan testaus

  Asennukseen kuuluu laitteistojen, ohjelmistojen jne. konfigurointi ja niiden toimivuuden testaus. Sillä pyritään varmistamaan niiden sopivuutta, esimerkiksi ohjelmistojen keskinäistä yhteensopivuutta ja toiminnan luotettavuutta sekä virheettömyyttä, joka on tietoturvan kannalta erittäin oleellista. Vaikka tämä vaihe on liitetty osaksi asennusprosessia, olisi toimivuudesta luonnollisesti hyvä varmistua ennen hankintaa kustannusten ja tietoturvariskien minimoimiseksi.

Ylläpitoprosessi:

- palvelupyyntöjen vastaanotto

  Palvelupyyntöjen vastaanotolla tarkoitetaan vikailmoituksia, hälytyksiä, ylläpito- ja kunnossapitotehtäviä siinä määrin kun niistä on sopimuksissa sovittu. Esimerkiksi vikatilanteissa laitteistojen tapahtumatietojen kerääminen auttaa paikallistamaan ja selvittämään niitä. Lisäksi väärinkäyttötilanteissa poikkeustilanteen todentaminen jälkikäteen on tärkeää. Näin vian korjaaminen tai väärinkäytön todentaminen helpottuu. Lokitietojen asianmukainen käsittely tulee myös olla järjestetty.

- viankorjaustehtävät

  Viankorjaustehtävien yhteydessä on oltava varmistuttu varaosien saatavuudesta. Lisäksi hyvin ylläpidetty laitteistodokumentaatio ja – rekisteri helpottaa viankorjaustehtäviä. Huoltotoimenpiteiden tai käytöstä poiston yhteydessä on varmistuttava, etteivät ne mahdollista tietojen joutumista kolmansille osapuolille.

- etävalvonta

  Mahdollisessa etävalvontapalvelussa tietoliikenteen tietoturva sekä turvallinen käyttö tulee olla taattuna. Tietoliikenneturvallisuuden suojauskeinoiksi on aikaisemmin työssä mainittu muun muassa laitteistojen ja siirtoyhteyksien ylläpito sekä niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

- laite- ja ohjelmistopäivitykset

  Laitteistojen ja ohjelmistojen hallinnasta ja niiden ajantasaisuudesta on tietoturvan kannalta erittäin olennaista huolehtia, jos urakassa näin on sovittu. Lisäksi tulisi varmistua siitä, että luvattomat ohjelmistoasennukset voidaan havaita.

7.3 Turvaurakointiyrityksen tietoturvapolitiikan sisältö

Edellä listatut kohdat ja kyselyn analysointi antoi aihetta tarkastella tarkemmin sitä, mitä tietoturvapolitiikka tulisi sisältää. Sen avulla saadaan hieman konkretisoitua sitä, miten turvaurakointiyrityksissä tietoturvaa tulisi hoitaa. Tässä on esitetty yksi ehdotus sen sisällöstä.

Kirjalliseen muotoon laaditussa dokumentissa yrityksen tietoturvapolitiikassa lähdetään liikkeelle siitä, mitä sillä juuri kyseisessä yrityksessä tarkoitetaan ja mikä siitä tekee yritykselle tärkeän. Turvaurakoinnin näkökulmasta näitä seikkoja voisi olla esimerkiksi lainsäädännön vaikutukset sekä asiakkaiden tietojen turvaaminen. Näin saadaan luotua tietoturvalle määritelmä, josta huokuu sen tärkeys koko toimintaa ajatellen sekä hahmotettua osaltaan myös suojattavat kohteet. Nämä kohdat toimivat myös eräänlaisena johdon tahdonilmaisuna tietoturvaan sitoutumiselle.

Politiikassa ilmaistaan myös tietoturvan organisointi tai toisin sanoen siihen liittyvät vastuut raportointia ja seurauksia myöten. Määritelmien ja kannanoton jälkeen kuvataan menetelmät, joilla tietoturva pyritään varmistamaan. Menetelmiin kuuluu riskien tunnistamisen ja

hallinnan lisäksi kannanotto siihen, kuinka sitä valvotaan, koulutetaan ja mitä tietoturvaseikkoja esimerkiksi sopimuksia laadittaessa painotetaan. Lisäksi on hyvä tuoda esille yhteenveto yleisperiaatteista ja siitä, mitä muita tietoturvakäytänteitä on sekä mihin standardeihin tai sertifiointeihin on yrityksessä sitouduttu. Luettelo mahdollisista tietoturvaohjeista voidaan liittää politiikan yhteyteen.

Yhteenvetoa tulee esitellä myös siitä, kuinka huolehditaan jatkuvasta tietoturvan kehittämisestä ja sen edistämisestä. Tämän yhteydessä on myös syytä kuvata turvaurakointiyrityksen jatkuvuuden hallinta sekä mikä rooli tietoturvalla on tällä saralla. Sisällöltään koko tietoturvapolitiikka tulee olla kaikkien ymmärrettävissä. Lisäksi se on julkinen dokumentti, johon voi vaivatta tutustua ja, jonka voi esimerkiksi yhteistyöyrityksille ojentaa merkkinä tietoturvallisesta tavasta toimia. Se ei kuitenkaan saa sisältää mitään, mitä voidaan käyttää yritystä itseään vastaan.

Kun perusta tietoturvalle on politiikan avulla luotu, tulee siitä tiedottaa henkilöstölle ja varmistua käyttöönotosta. Tiedottamisen yhteydessä pitää korostaa sen merkitystä yrityksen toiminnalle. Lisäksi on hyvä painottaa linjausten mukaisesti, että tietoturvan toteuttaminen, vastuu ja kehittämien koskee kaikkia yrityksessä työskenteleviä.

8 Yhteenveto

Kyseisessä opinnäytetyössä on pyritty esittämään tietoturvan hallintaan liittyviä toimia, niin yleisellä tasolla, kuin turvaurakoinnin ja tietoteknisten turvallisuusjärjestelmien urakointitehtävien tarkastelukulmasta. Siihen on lähtökohtaisesti pyritty keräämään niitä asioita, joiden avulla tietoturvan hallintaa voitaisiin lähteä viemään eteenpäin ja kehittämään sitä. Läpi työn on lisäksi kulkenut ajatus siitä, että sen on loppupeleissä tarkoitus tukea hankeyrityksen palvelutoimintaa ja heidän yrityssertifiointia.

Yhteenvetona työn alussa lähdettiin liikkeelle avaamalla tutkimuksellista kehittämistyötä sen taustojen ja tavoitteiden, keskeisten käsitteiden, hankeyrityksen esittelyn sekä menetelmällisen perustan kautta. Tämän jälkeen pyrittiin tuomaan tietoturvaan liitetty yleiskäsitys menetelmätasolle painottaen yhä enemmän turvaurakoinnin näkökulmaa. Seuraavaksi syvennyttiinkin edellä käydyn avulla puhtaasti hankeyrityksen turvaurakointiprosessin ajattelumallissa tietoturvan osalta huomioitaviin tekijöihin. Työtä varten teetetyn kyselyn analysointia tekstin loppupuolella hyödynnettiin pohdintaosuudessa, jonka yhteydessä muodostettiin yksi työn keskeisimmistä lopputuotoksista eli esimerkkikuvaukset tietoturvan menetelmäohjeista. Menetelmäohjeissa on koottu kaikki tärkeimmät asiat järkeväksi kokonaisuudeksi.

Kaiken kaikkiaan esille nousi hyvin tärkeinä seikkoina muun muassa lainsäädännön vaikutusten tunteminen sekä tiedon turvallinen käsittely, kun kyseisissä urakointitehtävissä paljon yrityksille luottamuksellisia tietoja liikkuu. Myös se, että toimivan tietoturvan takaamiseksi ei riitä vain esimerkiksi yhden tietoturvan osa-alueen huomioiminen, vaan se vaatii osaksi kokonaisvaltaista hallintaa, johon kuitenkin voidaan päästä ilman kohtuuttomia investointeja. Lähinnä kunnollisella suunnittelulla, esimerkiksi laitehankintoja tehdessä ja käsittelysäännöillä voidaan merkittävästi edistää tietoturvaa. Monin paikoin ei välttämättä ole kyse teknisen tietoturvan toteutuksesta, vaan liikkeelle tulisi lähteä niin sanotuista perusasioista.

Monille sähkö- ja turvaurakointiyritykselle olisi tärkeää tunnistaa tietoturvan kunnollisen hallinnan tarve nyt ja eritoten korostuen lähitulevaisuudessa. Pienten toimien kautta voitaisiin liikkua kohti systemaattista tietoturvan kehittämistä. Vähimmillään sillä voitaisiin tarkoittaa sitä, että turvaurakoitsijoilla olisi käsitys tietoturvan merkityksestä ja mahdollisista menetelmistä sen hallintaan, jota myös hankeyrityksen sertifiointi edellyttää. Sitä kautta niitä voitaisiin yrittää tuoda osaksi jokapäiväistä toimintaa.

Lähteet

Bloomberg 2012. Tietomurto tärveli Coca-Colan miljardibisnekset. Viitattu 9.11.2012. http://www.itviikko.fi/tietoturva/2012/11/06/tietomurto-tarveli-coca-colan-miljardibisnekset/201241433/7

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

Halmevuo, J., Kyrölä, T. & Vuori M. 2004. Tietotriskien tärkeitä näkökohtia. Viitattu 2.10.2012. http://pk-rh.com/pdf/tietoriskien-tarkeita-nakokohtia-tietokortti.pdf

Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen, P. Yrityksen turvallisuusopas. 2008. 1. painos. Helsinki: Gummerus Kirjapaino.

Henkilö- ja Yritysarviointi Seti Oy. 2012. Viitattu 19.9.2012. http://www.seti.fi/

KATAKRI. 2011. Kansallinen turvallisuusauditiointikriteeristö, 2. versio. Helsinki: Puolustusministeriö.

Kulunvalvonta- ja rikosilmoitinjärjestelmät. 2007. 4. painos. Tampere: Tammer-Paino.

Laaksonen, M.; Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing.

Leppänen, J. Yritysturvallisuus käytännössä. 2006. Helsinki: Talentum.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen - näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOY.

PK-RH. 2009. Pk- yrityksen riskienhallinta. Viitattu 2.10.2012. http://pk-rh.fi/riskilajit/tietoriskit/tietoriskien-tunnistaminen-ja-hallinta.html

Raggad, B. G. 2010. Information Security Management: concepts and practice. Boca Raton: CRC Press.

Ruohonen, M. Tietoturva. 2002. Porvoo: WS Bookwell.

Sähköinfo. 2012. Viitattu 5.12.2012. http://www.sahkoinfo.fi/Default.aspx?id=1279

VAHTI 3/2003. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. Valtiovarainministeriö.

VAHTI 5/2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Valtiovarainministeriö.

VAHTI 6/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. Valtiovarainministeriö.

VAHTI 11/2006. Tietoturvakouluttajan opas. Valtiovarainministeriö.

VAHTI 3/2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Valtiovarainministeriö.

VAHTI 2/2008. Tärkein tekijä on ihminen.Valtiovarainministeriö.

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. 2008. Valtiovarainministeriö.

VAHTI 9/2008. Hankkeen tietoturvaohje. Valtiovarainministeriö.

VAHTI 2/2011. Johdon tietoturvaopas. Valtiovarainminiseriö.

Viestintävirasto. 2012. Tietoturvalliseen yhteiskuntaan. Viitattu 23.11.2012.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Yrityksen tietoturvaopas. 2012a. Viitattu 2.10.2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/toimiva_tietoturva.html

Yrityksen tietoturvaopas. 2012b. Viitattu 3.10.2012
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/portaittain_eteenpain.html

Yrityksen tietoturvaopas. 2012c. Viitattu 4.12.2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/hyvin_toteutettu_tietoturva.html

Yrityksen tietoturvaopas. 2012d. Viitattu 18.10. 2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/toimiva_tietoturva_1.html

Yrityksen tietoturvaopas. 2012e. Viitattu 18.10. 2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tiedon_elinkaari.html

Yrityksen tietoturvaopas. 2012f. Viitattu 14.11. 2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tekniikan_toimivuus_palvelimet.html

Yrityksen tietoturvaopas. 2012g. Viitattu 15.11.2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tekniikan_toimivuus_palomuuri.html

Kuviot

Liitteet

Liite 1 Tietoturvan organisointi ja vastuut

Koko henkilöstö

- Tietoturvatoiminnan tavoitteet
- Tietoturvatoiminnan organisointi, vastuut ja tehtäväjako
- Noudatettava ohjeisto ja sen sijainti
- Peruskäsitteet
- Toiminnan julkisuus ja salassapitovelvoitteet
- Asianhallinnan turvallisuus
- Asiakirjojen luokittelu ja käsittely
- Henkilötietojen käsittely
- Tietokoneen käyttö
- Internetin ja sähköpostin käyttö
- Toimitilaturvallisuuden perusteet
- Vierailijakäytäntö
- Etätyö ja etäkäyttö
- Matkatyö ja mobiililaitteiden käyttö
- Aloitetoiminta
- Toiminta ongelmatilanteissa ja ilmoitusvelvollisuus
- Seuraamukset

Organisaation johto ja esimiehet

- Tietoturvallisuuden hallintajärjestelmä
- Tietoturvapolitiikka ohjauskeinona
- Suojattavien kohteiden määrittely
- Riskien arviointi ja hallinta
- Resurssien hallinta
- Henkilöstöturvallisuus (palvelussuhteen alkaminen, henkilöstön valvonta, palvelussuhteen päättyminen)
- Työturvallisuus ja työsuojelu
- Tiedottaminen
- Hankinnat ja tietoturvallisuus
- Palvelujen valvonta
- (Liike)toiminnan jatkuvuussuunnittelu
- Arviointien ja auditointien hyödyntäminen
- Mittarit ja jatkuva parantaminen

- Johdon katselmus

Tietotekniikkahenkilöstö (toimenkuvien mukaan kohdentaen)

- Tekninen tietoturvallisuus (laitteisto, varusohjelmisto, tietoliikenne)
- Tietoturvatuotteet
- Tekninen valvonta ja auditointi (huom. säädökset)
- Lokien seuranta ja hallinta (huom. säädökset)
- Toipumissuunnittelu
- Erikoistumisalueen mukainen lisäkoulutus

Tietojärjestelmien omistajat ja pääkäyttäjät sekä tietojärjestelmien kehittäjät ja ylläpitäjät

- Tietoturvavaatimusten määrittely
- Projektityö
- Systeemityö
- Riskien arviointi ja hallinta
- Muutosten hallinta
- Järjestelmäkohtainen jatkuvuus- ja toipumissuunnittelu
- Henkilörekisteriselosteet
- Tietojärjestelmäselosteet

Tietoturva-asiantuntijat ja tietoturvaryhmän jäsenet

- Tietoturvallisuuden hallintajärjestelmä
- Tietoturvasuunnittelu
- Jatkuvuus- ja toipumissuunnittelu
- Vakavien häiriötilanteiden ja poikkeusolojen varautumissuunnittelu
- Toiminta ongelmatilanteissa
- Erikoistumisalueen mukainen lisäkoulutus

(VAHTI 11/2006, 21–23.)