

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

ANTTI SULOSAARI

TIETOTURVA-AMMATTILAISEN OSAAMISTARVEKARTOITUS

Diplomityö

Aihe hyväksytty osastoneuvoston kokouksessa

13.10.2004

Tarkastajat: Professori Tommi Mikkonen (TTY)

Lehtori Jukka Koskinen (TTY)

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

Ohjelmistotekniikka

ANTTI, SULOSAARI: Tietoturva-ammattilaisen osaamistarvekartoitus

Diplomityö, 57 sivua, 2 liitesivua

Tarkastajat: professori Tommi Mikkonen ja lehtori Jukka Koskinen

Rahoittaja: ei ulkoista rahoitusta

Elokuu 2005

Avainsanat: yritysturvallisuus, tietoturvallisuus, tietoturva-ammattilainen, BS 7799 ja VAHTI

TIIVISTELMÄ

Liiketoimintaprosessien verkottuessa tiedon suojaamisen tarve on kasvanut, mikä aiheuttaa muutoksia siitä vastuussa olevien osaamistarpeelle. Tämä tutkimus tehtiin osaamistarpeen kartoittamiseksi sekä tietoturvaopetuksen kehittämiseksi Tampereen teknillisen yliopiston Tietoliikennetekniikan laitoksella. Siellä haluttiin tietää, millaisia tietoturva-ammattilaisia teollisuus tarvitsee ja mitä kehityskohteita laitoksen tietoturvaopetuksessa on. Työssä otettiin huomioon kaikki tietoturvallisuuden osa-alueet: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.

Tutkimuksessa tarkasteltiin tietoturva-ammattilaisten toimenkuvia, koulutustaustaa, tietämystä teknisestä ja hallinnollisesta tietoturvasta, tietämyksen kehitystarpeita, tietojen hankintatapoja ja organisaatioiden tietoturvakulttuureita. Lisäksi käsiteltiin BS 7799-tietoturvastandardia ja valtionhallinnon VAHTI-tietoturvaohjeistusta. Henkilöhaastattelujen perusteella muodostettiin tietoturva-asiantuntijan yleinen osaamisprofiili ja lisäksi tietoturvakonsultin, tuotepäällikön ja tietoturvapäällikön osaamisprofiilit. Saatuja osaamisprofiileita verrattiin kirjallisuudessa esiintyneisiin malleihin.

Osaamisprofiileista havaittiin, että on olemassa joitain perusasioita, joita kaikki tarvitsevat. Enimmäkseen tarvittavat asiat määräytyvät kuitenkin ammattilaisen toimenkuvan painopistealueiden perusteella. Yleisiksi huomionarvoisiksi asioiksi opetukseen liittyen katsottiin, että tietoturvaopetuksen pitäisi olla osana muita kursseja ja opettamassa pitäisi olla oikeita ammattilaisia. Tärkeintä opetuksessa olisi saada turvallisuusajattelu esiin ja mukaan ajatusmaailmaan, koska koulutus voi antaa vain valmiuksia ammattilaiseksi kehittymiselle.

TAMPERE UNIVERSITY OF TECHNOLOGY

Department of Information Technology

Institute of Software Systems

ANTTI, SULOSAARI: Survey of Professional Requirements in IT Security

Master of Science Thesis, 57 pages, 2 enclosure pages.

Examiners: Professor Tommi Mikkonen and Lecturer Jukka Koskinen

Funding: no external funding

August 2005

Keywords: corporate security, information security, security professional, BS 7799, VAHTI

ABSTRACT

Today's business processes are extensively networked. The resulting increased need to protect information is bound to alter the requirements set for information security professionals. The purpose of the present study is to survey the specific requirements for security professionals in the industry, and consequently, to further improve the teaching of information security at the Institute of Communications Engineering at the Tampere University of Technology. The scope of the study encompasses all areas of security: administrative and organizational information security, personnel security, physical security, telecommunications security, facilities security, software security, data security, and operations security.

In the study, the job descriptions of security professionals, their educational background, their knowledge of technical and administrative security, the development needs, the methods of data acquisition, and the information security culture in the organisation were surveyed. In addition, the BS 7799 security standard and the VAHTI security directions issued by the Finnish government were discussed. Based on the survey interviews, general knowledge profiles were created for the Security Technician as well as for the Security Consultant, Product Manager, and Chief Information Security Officer respectively. The knowledge profiles were then compared to theoretical models.

The comparison of the knowledge profiles proved that there exist certain basic needs common to all security professionals. In most cases, however, the essential needs were specified by the focal areas in the job descriptions. On the basis of the general observations of the teaching, then, two major targets for development can be formulated: 1) information security ought to be integrated in the contents of other courses, and 2) the teachers of these courses ought to be practising security professionals. In teaching, the key issue would presently be to highlight the general concept of information security and render it an active part of the student's worldview. This is because teaching, even at its best, can only provide a mere framework for becoming a professional.

ALKUSANAT

Olen tehnyt tutkimukseni Tampereen teknillisen yliopiston tietoliikennetekniikan laitokselle tietoturvaopetuksen kehittämiseksi. Toivon, että tästä tutkimuksesta on hyötyä myös muille kuin työn tilaajalle opetuksen suunnittelussa.

Tutkimuksen ohjauksesta ja työn tarkastamisesta kiitän lehtori Jukka Koskista ja professori Tommi Mikkosta. Vanhempiani kiitän tuesta ja oikoluvusta. Kiitän tutkimukseen osallistuneita organisaatioita ja haastattelemani henkilöitä tutkimuksen kannalta arvokkaan tiedon antamista. Lisäksi haluan kiittää Tero Kovasta, Rea-Maria Lehtosta, Manu Setälää, Tommi Tarkiaista sekä muita joilta olen saanut apua tämän tutkimusprojektin toteuttamiseksi.

Tampereella 2.8.2005

Antti Sulosaari

Näyttelijäkatu 21 C 29

33720 Tampere

puh. 040 742 7265

etunimi.sukunimi@iki.fi

SISÄLLYSLUETTELO

| | |
|--|-----------|
| 1. JOHDANTO | 1 |
| 1.1 Tausta | 1 |
| 1.2 Tutkimuksen tavoitteet | 2 |
| 1.3 Työn rakenne | 3 |
| 1.4 Käytetyt tutkimusmenetelmät ja rajaukset..... | 3 |
| 1.5 Tutkimuksen suoritus | 3 |
| 2. KÄSITTEET | 4 |
| 2.1 Tietoturvaluottisuus..... | 4 |
| 2.2 Yritysturvallisuus | 6 |
| 2.3 BS 7799 | 7 |
| 2.4 VAHTI-ohjeet | 9 |
| 2.5 Pätevyysertifikaatit..... | 9 |
| 2.5.1 Certified Information Systems Security Professional (CISSP)..... | 9 |
| 2.5.2 Certified Information Systems Auditor (CISA) ja Certified Information Security Manager (CISM)..... | 10 |
| 2.5.3 Global Information Assurance Certification (GIAC) | 11 |
| 3. TIETOTURVA-AMMATTILAISEN TEHTÄVIÄ KIRJALLISUUDESSA | 13 |
| 3.1 Mieltisen ammattilaisprofiilit..... | 13 |
| 3.2 Mannisen ammattilaisprofiilit | 13 |
| 3.3 Wadlowin ammattilaisprofiilit ja ryhmät | 14 |
| 3.4 Whitmannin & Mattordin ammattilaisprofiilit ja ryhmät | 16 |
| 3.5 BS 7799-1-standardin vaatimukset ja ammattilaisprofiilit..... | 19 |
| 3.6 BS 7799-2-standardin vaatimukset ammattilaisprofiileille..... | 20 |
| 3.7 VAHTI-ohjeiden 7/2003 & 1/2001 ammattilaisprofiilit | 20 |
| 4. HAASTATTELUN KYSYMYKSET..... | 25 |
| 4.1 Kysymysten suunnittelu..... | 25 |

| | | |
|-----------|--|-----------|
| 4.2 | Taustatiedot | 25 |
| 4.3 | Omistajuus ja tietoturvapolitiikka | 27 |
| 4.4 | Tietoturvallisuuden kehittäminen | 30 |
| 4.5 | Osaamisprofiili..... | 31 |
| 4.6 | Mielikuva organisaation tietoturvatietoisuudesta | 32 |
| 4.7 | Tietoturvaopetuksen kehittäminen | 32 |
| 5. | TUTKIMUSTULOKSET | 33 |
| 5.1 | Kyselytutkimuksen suoritus | 33 |
| 5.2 | Kyselyn tulokset..... | 33 |
| 5.2.1 | Taustatiedot | 33 |
| 5.2.2 | Omistajuus ja tietoturvapolitiikka..... | 36 |
| 5.2.3 | Tietoturvallisuuden kehittäminen | 38 |
| 5.2.4 | Osaamisprofiili | 38 |
| 5.2.5 | Mielikuva organisaation tietoturvatietoisuudesta | 41 |
| 5.2.6 | Tietoturvaopetuksen kehittäminen..... | 42 |
| 6. | TULOSTEN TARKASTELU | 44 |
| 6.1 | Erilaisia tietoturva-ammattilaisten profiileita | 44 |
| 6.2 | Tietoturva-ammattilaisten profiili yleisesti | 45 |
| 6.3 | Profiilien vertailu teoriaan..... | 47 |
| 6.4 | Yleisen profiilin vertailu teoriaan | 48 |
| 6.5 | Tavoitteiden saavuttaminen | 49 |
| 7. | YHTEENVETO | 52 |
| 7.1 | Tutkimuksen arviointi..... | 52 |
| 7.2 | Suositus yliopistojen tietoturvaopetukseen | 52 |
| 7.3 | Jatkotutkimuskohteita | 53 |
| | LÄHDELUETTELO | 54 |
| | LIITE: CIAG:N SERTIFIKAATTEJA | 58 |

1. JOHDANTO

1.1 Tausta

Tietoturvan tarpeeseen on organisaatioissa alettu herätä yritysten liiketoimintaprosessien verkottuessa ja tieto-omaisuuden muuttuessa yhä enenevässä määrin sähköiseen muotoon. Sähköinen tieto on hyvin arkaa tahallisille tai tahattomille muutoksille tai katoamiselle, ellei tiedon eheyttä ole mitenkään pyritty varmistamaan. Verkottuvan maailman, erityisesti Internetin sovellusten kuten sähköpostin, roolin noustessa yhä kriittisemmäksi osaksi yritysten välistä viestintää, voidaan havaita, että yritysten järjestelmät eivät ole riittävän turvallisia. Viimeaikaisten erilaisten haittaohjelmien aiheuttamat tilapäiset palvelun katkokset esimerkiksi pankeissa ovat ylittäneet uutiskynnyksen, vaikka ne haluttaisiinkin pitää organisaation omana tietona.

Tietoturva jakaantuu selkeästi kahteen kokonaisuuteen, tekniseen ja hallinnolliseen. Teknistä puolta on yleensä helpompi lähestyä ja sen kustannukset on myös helpompi perustella. Sen sijaan hallinnollista tietoturvaa on vaikeampi lähestyä, koska organisaatioissa ei yleensä ole siihen tarpeeksi asiantuntemusta, resursseja on liian vähän, ja johto ei yleensä ymmärrä tietoriskejä, kuten Kalevi Nikulaisen (11.2.2004) kirjoituksen otsikko ”Johto pihalla tietoriskeissä” antaa ymmärtää.

Yleisesti tietoturva-ammattilaisten toimenkuvat mielletään aika teknisiksi, kuten Parker ja McCray määrittelevät. Don Parkerin artikkelissa (17.5.2004) tietoturva-asiantuntijan tarvittavaksi tietämykseksi esitetään TCP/IP, IDS¹, olennaisen tiedon löytäminen IDS:n tuottamasta datasta, palomuurit, reitittimet, ohjelmointi, käyttöjärjestelmät ja oman verkon heikkouksien testaaminen. Joe McCrayn artikkelissa (2003) asiantuntijan profiiliksi vastaavasti esitetään käyttöjärjestelmätietämys, TCP/IP, ohjelmointia sen verran, että pystyy automatisoimaan asioita scripteillä, ja verkonhallinta, joka koostuu palomuuereista, antivirus-ohjelmistoista, tunnettujen heikkouksien havainnointi-ohjelmistoista, keskitetystä lokin hallinnasta, tunkeutumisen havainnoinnista ja VPN²-tekniikoista. Edistyneen asiantuntijan pitää McCrayn mielestä lisäksi seurata turvallisuus uutisia, osallistua seminaareihin, kokeilla asioita käytännössä testiverkossa, seurata turvallisessa ympäristössä tapahtuvaa oikeaa hyökkäystä esimerkiksi tarkkailemalla hunajapurkkia ja osallistua ”sotapeleihin”. Hunajapurkin eräs toteutus on laittaa organisaation tietoliikenneverkon rajalle suojaamaton palvelin, jolla todellisuudessa ei ole mitään roolia. Suojaamattoman palvelimen tarkoituksena on vetää mahdollisia hyökkääjiä puoleensa

¹ IDS (Intrusion Detection System) on tunkeutumisen havainnointia suorittava tekninen järjestelmä.

² VPN (Virtual Private Network) on yleiskäsite erilaisille yksityisille näennäisverkoille, joiden tarkoitus on mahdollistaa turvalliset suojatut yhteydet esimerkiksi eri toimipaikkojen välillä.

heikon suojauksen houkuttelevuuden vuoksi ja ehkäistä murtoyrityksiä varsinaiseen organisaation tietojärjestelmään. Sotapeleissä tarkoituksena on ratkaista tehtäviä, jotka edellyttävät järjestelmässä olevien aukkojen käyttöä. Nämä näkökulmat tuovat esiin hyvin alan teknisen puolen, mutta molemmat unohtavat standardit ja ohjeet. Näillä kuitenkin selvittää jokapäiväisestä teknisestä tietoturvasta.

Ennakkokäsitykseni mukaan tietoturvan tehtävien jakaantuminen eri toimenkuvilla oleville henkilöille on pirstoutunut eri tavalla eri organisaatioiden sisällä riippumatta organisaatioiden koosta. Ei ole olemassa mitään yleispätevää ratkaisua, joka voitaisiin löytää kaikista organisaatioista. Pienimmissä organisaatioissa koko tietoturvan tehtäväkenttä kuuluu toimivalle johdolle ja tietotekniikasta vastaavalle henkilöstölle. Hieman isommista organisaatioista löytyy jo tietoturvapääällikkö, joka koordinoi ja toimii linkkinä eri yksiköiden välillä tietoturva-asioissa. Tekninen tietoturva on yleensä jotenkin hallinnassa, koska ulkopuolelta ja sisäpuolelta tulevat uhat ja riskit ovat jo realisoituneet hyökkäyksien ja kiristyksien muodossa. On ollut pakko tehdä jo jotain. Sen sijaan hallinnollisella puolella on yleensä tehty vain se, mitä asiakkaat ja mahdollisesti viranomaiset ovat vaatineet tai ei aina edes sitä. Tietoturva on yleensä johdon mielestä vain kustannuserä, koska siitä ei ole suoranaisesti nähtävissä tuloja, vaan pelkästään menoja. Ehkäpä hyvä kannustin johdolle voisi olla kustannusten ennakoitavuus, koska katastrofitilanteiden kustannuksia on mahdotonta ennakoida.

1.2 Tutkimuksen tavoitteet

Tämän diplomityön tavoitteiksi asetettiin selvittää:

- tietoturva-ammattilaisen koulutustausta
- tietoturva-ammattilaisen yleinen tietämyksen taso teknisestä ja hallinnollisesta tietoturvasta
- tietoturva-ammattilaisen ammatissaan tarvitsema osaaminen (tekninen ja hallinnollinen tietoturva)
- organisaation motivaatio ja sitoutuminen tietoturva-asioihin
- tietoturva-ammattilaisen osaamisen puutteet ja kehityskohteet, joiden perusteella organisaation tietoturva-ammattilaisten valmiuksia voitaisiin parantaa
- tietoturva-ammattilaisille tarjottavan ammatillisen peruskoulutuksen ja täydennyskoulutuksen kehityskohteet
- tietoturva-ammattilaisen yleinen profiili ja tehtäväkentät sellaisella tasolla, minkälaisina ne ovat löydettävissä useimmista organisaatioista.

1.3 Työn rakenne

Luvussa 1 käsitellään tietoturvallisuuden nykytilaa organisaatioissa motivaationa tälle työlle, sekä tutkimuksen tavoitteita ja menetelmiä. Luvussa 2 määritellään tietoturvallisuuden ja yritysturvallisuuden käsitteet. Tutustutaan BS 7799-tietoturvastadardiin, VAHTI-ohjeisiin ja erilaisiin pätevyyttä osoittaviin koulutussertifikaatteihin. Luvussa 3 käsitellään kirjallisuudesta löydettyjä ammattilaisprofiileja, niiden muodostamia ryhmiä ja yleisiä vaatimuksia hyvälle ammattilaiselle. Luku 4 käsittelee haastattelukysymysten suunnittelua. Luvussa 5 perehdytään kyselytutkimuksen suoritukseen ja tuloksiin. Luvussa 6 muodostetaan tietoturvakonsultin, tuotepäällikön, tietoturvapäällikön ja tietoturva-ammattilaisen profiilit. Muodostettuja profiileita verrataan tämän jälkeen kirjallisuuteen. Luvun lopuksi pohditaan tavoitteiden saavuttamista. Luvussa 7 arvioidaan tutkimusta, annetaan vinkkejä opetukseen ja jatkotutkimuskohteisiin.

1.4 Käytetyt tutkimusmenetelmät ja rajaukset

Tutkimus suoritettiin henkilöhaastatteluin. Saatuja tuloksia verrattiin BS 7799-standardeihin, VAHTI-ohjeistukseen ja muuhun kirjallisuuteen. Organisaatioissa tietoturva-asiat ovat jakautuneet usealle henkilölle. Tässä keskityttiin vain tärkeimpiin, koska muuten olisi pitänyt haastatella lähes koko organisaation henkilökunta. Haastattelut rajattiin noin kymmeneen haastatteluun, koska jo tällä määrällä uskottiin saatavan riittävän laaja-alainen kokonaiskuva. Haastatteluissa ei auditoitu organisaatioiden tietoturvaa, koska se ei ole tarkoituksenmukaista tämän työn kannalta.

1.5 Tutkimuksen suoritus

Tutkimusta varten laadittiin kysymysrunko, jota käytettiin soveltaen haastatteluiden runkona. Kysymysrunko esitettiin ensin yhdellä tietoturva-ammattilaisella, jonka jälkeen havaitut puutteet ja virheet korjattiin. Tämän jälkeen suoritettiin haastattelut. Haastattelujen tulokset analysoitiin, niistä muodostettiin tietoturvakonsultin, tuotepäällikön, tietoturvapäällikön ja tietoturva-ammattilaisen osaamisprofiilit.

2. KÄSITTEET

2.1 Tietoturvallisuus

Mitä tietoturvallisuus on? Kysymyksen vastaus on moniselitteinen ja yhtä ainoaa vastausta ei ole olemassa. Seuraavassa pohditaan asiaa kirjallisuuden avulla. Olen käyttänyt VAHTI-ohjeiden (7/2003 s.29) mukaista jakoa osakokonaisuuksiin. Muukin jakoperusteet ovat ihan yhtä päteviä, koska jaottelulle ei ole olemassa yhtä ainoaa oikeaa tapaa.

Hallinnollinen tietoturvallisuus on lyhyesti määriteltynä kaikki ne hallinnolliset toimenpiteet, jotka tähtäävät tietoturvallisuuden parantamiseen. Keinoja, joilla tietoturvaa voidaan parantaa hallinnollisin toimenpitein, ovat esimerkiksi organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta. Tietoturvapoliittikka on organisaation johdon kannanotto tietoturvallisuusasioihin. Se sisältää esimerkiksi tietoturvallisuuden yleistavoitteet organisaatiossa, lakeihin ja sopimukseen liittyvät vaatimukset tietoturvalle, organisaation turvallisuuskoulutuksen vaatimukset, liiketoiminnan jatkuvuuden vaatimukset turvallisuudelle, turvallisuuspolitiikan rikkomusten seuraukset, tietoturvallisuuteen liittyvien velvollisuuksien määrittely, poikkeustilanteiden raportointikäytännöt ja viittaukset politiikkaan liittyviin asiakirjoihin, kuten lakeihin ja turvasuunnitelmaan. Tietoturvasuunnitelma sisältää yksityiskohtaisemmat ohjeet kuin politiikka. Se sisältää turvallisuuden kehittämisen aikataulut tietoturvapoliitikassa määriteltyjen tavoitteiden saavuttamiseksi. Lisäksi organisaatioilla on yleensä erillisiä ohjeita, jotka täydentävät tietoturvasuunnitelmaa. Tällaisia ohjeita ovat esimerkiksi tietoturvapoikkeamiin reagoimisen ohje, ylläpitopolitiikka, sähköpostin käytön politiikka ja kuolemantapausohje.

Henkilöstöturvallisuus on organisaation oman tai ulkopuolisten henkilöiden inhimillisestä toiminnasta aiheutuvien tietoturvariskien hallintaa. Henkilöstöriskeihin kuuluvat myös osaamattomuudesta ja erehdyksistä aiheutuvat riskit eikä pelkästään anastuksesta, yritysvakoilusta, petoksesta ja kavalluksesta johtuvat riskit. Henkilöstöturvallisuudessa erityisesti huomioitavia asioita ovat: toimintatavat, rekrytointi, toimenkuvat, käyttöoikeudet, turvallisuuskoulutus ja valvonta. Toimenkuvien tulee olla sellaisia, että riskejä aiheuttavista asioista, esimerkiksi rahan käytöstä, ei vastaa vain yksi henkilö, vaan useampi on tietoinen asioista. Kaikkein kriittisimpien toimintojen toteuttamiseen pitää vaatia vähintään kahden henkilön samanaikainen läsnäolo, jotta toimenpide saadaan suorittaa. Henkilöstöturvallisuudessa pitää huomioida myös avainhenkilöiden sijaiset. Organisaatiossa ei saa muodostua tilannetta, jossa yrityksen toiminta pysähtyy, kun esimerkiksi joku avainhenkilö poistuu organisaation palveluksesta.

Fyysinen turvallisuus kohdistuu laitteistojen ympäristön suojelemaan. Fyysistä turvallisuutta ovat esimerkiksi laitteistojen ulkoinen turvaaminen, lukitus, kulunvalvonta,

vartiointi ja tilojen suojaaminen. Fyysisellä suojautumisella pyritään minimoimaan mahdolliset palo-, vesi-, sähkö-, ilmastointi-, murto- yms. vahingot hidastamalla ja vaikeuttamalla niitä. Esimerkiksi palokuorman minimoinnilla voidaan ehkäistä tulipalon räjähdysmäinen leviäminen, kun vältetään säilyttämästä palavia materiaaleja tarpeettoman suuria määriä samoissa tiloissa. Fyysiseen turvallisuuteen tulee kiinnittää erityistä huomiota silloin, kun omaisuus ei ole organisaation omissa tiloissa, vaan esimerkiksi työntekijän kotona.

Tietoliikenneturvallisuudella pyritään varmistamaan siirrettävän tiedon muuttumattomuus, luottamuksellisuus, tietoliikennelaitteistojen fyysinen turvallisuus, estämään tiedon kulkeutuminen väärään paikkaan sekä todentamaan vastaanottaja että lähettäjä. Tietoliikenneturvallisuuteen kuluvat kaikki televerkot, liityntäpisteet ja liitettujen päätelaitteiden rajapinnat. Voidaan siis puhua suojauksesta päästä päähän eli lähettäjältä vastaanottajalle. Tietoliikenneturvallisuudessa tarkastellaan tiedonsiirtovälineitä, tiedonsiirtoprotokollia, verkkotopologioita, tietoturvaluotteita ja salausalgoritmeja. Tietoliikenneverkkojen turvallisuudessa erityshuomion saavat organisaatioiden verkkojen väliset liityntäpisteet, koska organisaatioiden osaamistasot, politiikat ja kiinnostus turvallisuutta kohtaan vaihtelevat suuresti. Lisäksi pitää kiinnittää huomiota tietoliikennetuotteiden nopeaan uudistumiseen, joka aiheuttaa sen, että verkossa saattaa olla hyvin eri-ikäisiä, standardien eri versioita noudattavia laitteita. Aina kaikki laitevalmistajat eivät noudata kaikkia standardien vaatimuksia viimeiseen asti ehtiäkseen riittävän ajoissa markkinoille. Lisäksi standardien ohjeet saattavat olla liian väljät. Näiden seurauksena pitää varautua siihen, että kaikki laitteiden ominaisuudet eivät ole käytettävissä kaikkien laiteyhdistelmien yhteydessä.

Laitteistoturvallisuuden piiriin kuuluvat laitteet ja laitteisiin liittyvät laitteiden omat ohjelmistot eli laitekohtaiset käyttöjärjestelmät. Laitteistoihin liittyviä turvallisuusominaisuuksia ovat tunnistaminen, todentaminen, osastointi, pääsynvalvonta, itsetarkkailu, tiedon luokittelu ja valmistajan laaduntarkkailu. Laitteistojen turvaaminen käytöstä poistamisen yhteydessä on syytä tehdä suunnitelmat. Laitteistoturvallisuuden tietokonearkkitehtuuri muodostaa rajapinnan ohjelmistoturvallisuudelle.

Ohjelmistoturvallisuus kattaa käyttöjärjestelmän ja sovellukset. Käyttöjärjestelmät kuuluvat pääosin ohjelmistoturvallisuuteen, mutta rajanveto laitteistoturvallisuuteen on yhtä hankalaa kuin rajata käyttöjärjestelmään kuuluvat ohjelmat ja erilliset sovellukset. Ohjelmistoturvallisuuteen vaikuttavat keskeisesti tietokonearkkitehtuurit, käyttöjärjestelmät, kääntäjät, sovellukset, haittaohjelmat, ohjelmistojen virheet ja näihin liittyvät tietoturvaominaisuudet. Ohjelmistoturvallisuus toimii rajapintana laitteistoturvallisuuden ja henkilöstö- tai hallinnollisen tietoturvan välissä. Juhani Paavilaisen (1998) mukaan korkeantason kääntäjän käyttäminen on riskitekijä, jos ohjelman tietoturvatason on oltava erittäin korkea; kääntäjät itsessäänkin sisältävät virheitä. Mitä monimutkaisemmiksi ohjelmistot muodostuvat, sitä vaikeammin ne ovat

yhden ihmisen käsitettävissä, jolloin kääntäjän lähdekoodiin jääneiden virheiden todennäköisyys kasvaa. Ohjelmistojen turvallisuusvaatimukset tulee päättää suunniteltaessa, koska myöhemmin turvallisuutta on lähes mahdotonta lisätä tai se tulee ainakin huomattavasti kalliimmaksi. Tästä syystä useimmat saatavissa olevat valmiit ohjelmistot eivät ole kelvöllisiä kaikkeen käyttöön, koska niitä suunniteltaessa ei ole riittävästi huomioitu turvallisuutta.

Tietoaineistoturvallisuus eroaa muista turvallisuuden osa-alueista siten, että se kohdistuu pelkästään tietoihin, olivat ne sitten missä muodossa tahansa. Muut osa-alueethan ovat kohdistuneet toimintaan tai materiaan tiedonkäsittelyssä tai sen ympäristössä. Tietoaineistoturvallisuus on tietojen ja tietovälineiden tunnistamista, turvallisuusluokitusta, säilytystä, varmistamista, käsittelyä ja tarpeettoman tiedon tuhoamista. Tarkoituksena on turvata tietojen eheys, muuttumattomuus, aitous, saatavuus ja luottamuksellisuus. Tiedon turvaluokittelu on tärkeä osa tietoaineistoturvallisuutta. Tiedon luokittelussa on erityisesti muistettava, että tiedon turvaluokka todennäköisesti muuttuu ajan kuluessa, esimerkiksi salainen tieto muuttuu julkiseksi. Tiedon eheyden kannalta on tärkeää, että vanhat versiot tiedosta on erotettavissa ajan tasalla olevista tiedoista, esimerkiksi lait ja asetukset.

Käyttöturvallisuus on turvallisen käyttötavan, turvallisen käyttöympäristön, tapahtumien valvonnan ja toiminnan jatkuvuuden muodostama kokonaisuus. Turvallinen käyttötapa edellyttää järjestelmän asennukselta ja ylläpidolta organisaation tietoturvasuunnitelman mukaista toimintaa. Turvallinen käyttöympäristö muodostuu järjestelmän fyysisen- ja laitteistoturvallisuuden ylläpidosta. Tapahtumien valvonnalla tarkoitetaan sitä, että tapahtumat ja niiden aiheuttajat ovat tarvittaessa jäljitettävissä esimerkiksi järjestelmän lokeista. Jatkuvuus varmistetaan dokumentoidulla jatkuvuussuunnitelmalla, joka sisältää tai siinä on viittaukset dokumentteihin, joista löytyvät toipumissuunnitelma, pääsynvalvonnan toteutus, järjestelmän mahdolliset lokitiedostot ja muu suojaus. Juhani Paavilaisen (1998) mukaan: "Käyttöturvallisuus yhdistää fyysisestä-, laitteisto-, ja ohjelmistoturvallisuudesta muodostuvan kokonaisuuden niin, että se vastaa hallinnollisessa turvallisuudessa määritettyä tasoa."

2.2 Yritysturvallisuus

Yritysturvallisuus on laajempi kokonaisuus kuin tietoturvallisuus. Juha E. Miettinen (2002) jakaa yritysturvallisuuden seuraaviin kokonaisuuksiin mukaillen Yritysturvallisuuden neuvottelukunnan tekemää jaottelua. Suluissa VAHTI-ohjeiden mukainen tietoturvallisuuden jaottelu sijoitettuna siten, mihin ne sisällön mukaan sopisivat.

- Yritysturvallisuuden johtaminen (hallinnollinen turvallisuus)

- kiinteistö- ja toimitilaturvallisuus (fyysinen turvallisuus)
- henkilöturvallisuus (henkilöstöturvallisuus)
- vakuuttaminen (käyttöturvallisuus)
- tietoturvallisuus (tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus)
- poikkeusoloihin varautuminen (käyttöturvallisuus)
- paloturvallisuus ja pelastustoiminta (fyysinen turvallisuus)
- ympäristönsuojelu
- ulkomaan toimintojen yritysturvallisuus (hallinnollinen turvallisuus)
- matkustusturvallisuus (hallinnollinen turvallisuus)
- rikosturvallisuus (fyysinen turvallisuus)
- työsuojelu
- tuotannon ja muun toiminnan yritysturvallisuus (käyttöturvallisuus).

Kun verrataan oheista jakoa VAHTI-ohjeiden mukaiseen tietoturvan jaotteluun, huomataan, että tietoturvaluuteen ahtaasti tulkittuna kuuluvat vain tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus. Hallinnollinen ja käyttöturvallisuus saavat suuremman painoarvon yritysturvaluudessa kuin pelkässä tietoturvaluudessa. Yritysturvaluuden näkökulma painottuu riskienhallintaan, lakien ja asetusten noudattamiseen ja erityisesti yrityksen toiminnan jatkuvuuden turvaamiseen. Lisäksi yritysturvaluuteen liittyy ympäristönsuojelu ja työsuojelu, jotka eivät liity mitenkään tietoturvaluuteen, mutta ovat osa yrityksen toimintaa, jota säädellään laeilla ja asetuksilla. Asioiden painottuminen yritysturvaluudessa eri tavalla kuin tietoturvaluudessa on luonnollista. Yritysturvaluuden tehtävänä on palvella yrityksen varsinaista liiketoimintaa. Tietoturvaluuden tehtävänä on turvata tietojen eheys, muuttumattomuus, aitous, saatavuus ja luottamuksellisuus. Yritysturvaluudessa vaatimukset tulevat asiakkailta ja yhteiskunnalta. Sen sijaan tietoturvaluuden käsite ei sisällä vaatimusta ottaa kaikkia yritystoiminnan velvollisuuksia ja vastuuta huomioon.

2.3 BS 7799

BS 7799-tietoturvastandardin juuret ovat Iso-Britannian Kauppa- ja Teollisuusministeriön DTI:n tietoturvatyöryhmän vuonna 1993 julkaistussa tietoturvan hallintaa koskevassa menettelytapaohjeessa (Code of Practice for Information Security Management). Gamma Secure Systems Limited:n (2004a) mukaan vuonna 1995 julkaistu ensimmäinen versio ei

sisältänyt tarkkoja vaatimuksia siitä kuinka organisaatioiden tietoturva tulisi toteuttaa. Standardiin lisättiin vuonna 1998 toinen osa, joka asetti vaatimukset standardin noudattamisesta. Vuonna 1999 standardi päivitettiin ja siihen lisättiin uusia ohjeistuksia, jotka huomioivat informaatioalan uusimmat kehityssuunnat esimerkiksi e-kaupan sekä langattoman tietoliikenteen. ISO hyväksyi standardin ensimmäisen osan joulukuussa 2000 julkaistavaksi pienin muutoksin kansainvälisenä standardina BS ISO/IEC 17799:2000. Edellä mainitusta ISO-standardista on 15.6.2005 tullut uusi versio. Vuonna 2002 standardin toisesta osasta tuli uusi versio. Uudistuksessa keskityttiin yhtenäistämään standardia muiden ISO-standardien kanssa. Gamma Secure Systems Limited on yksi standardin valmistelusta vastaavan työryhmän jäsenyrityksistä.

BS 7799-standardi sisältää valvontatoimenpiteitä, jotka toteuttamalla organisaatio pystyy nostamaan tietoturvasa tasoa. Valvontatoimenpiteet on jaoteltu alla oleviin aihealueisiin:

- tietoturvapoliittika
- organisaation jako turvallisuuden vastualueisiin
- tietojen luokittelu, arvostaminen ja suojaus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenteen turvaaminen
- pääsyoikeuksien valvonta
- järjestelmien kehittäminen ja ylläpito
- liiketoiminnan jatkuvuuden hallinta
- vaatimustenmukaisuus (lainsäädäntö, sopimukset).

Standardin ensimmäinen osa sisältää valvontatoimenpiteiden kuvauksen ja tarkoituksen sekä ehdotuksia hyviksi havaituista tavoista toteuttaa ne. Standardin toisessa osassa taas määritellään tarkemmin se, mitä organisaation tulisi toimenpiteillä saavuttaa. Standardin noudattamisen vahvuus on siinä, että se vaihe vaiheelta auttaa organisaatiota rakentamaan toimivan tietoturvaa parantavan järjestelmän. Standardia seuraamalla organisaatio pystyy paremmin tunnistamaan liiketoimintaprosessiensa kannalta kriittisimmät tietoturvaohat, varautumaan niihin, ja tätä kautta paremmin ymmärtämään tietoturvan merkityksen organisaation liiketoiminnan jatkuvuuden kannalta. Standardin käytön suurin hyöty on siinä, että sen voi sertifioida. Sertifioidulla yrityksellä on näin mahdollisuus esittää asiakkailleen riippumattoman tahon suorittaman tarkastuksen tulos. Täytyy kuitenkin muistaa, että standardin toteuttaminen ei takaa lakisääteisten velvoitteiden täyttymistä, koska standardi ei ota huomioon maakohtaista lainsäädäntöä.

Gamma Secure Systems Limited:n (2004b) mukaan organisaation tietoturvallisuuden hallintajärjestelmä tullaan tarkistamaan valtuutetun BS 7799-asessorin toimesta, jos organisaatio haluaa sertifioida itsensä standardia vasten. Saatu sertifikaatti sisältää tiedon

siitä, mitkä organisaation toiminnot sertifioitiin sekä muita olennaisia tietoja, kuten soveltamissuunnitelman. Asessori palaa tietyin väliajoin tarkistamaan, että organisaation tietoturvallisuuden hallintajärjestelmä toimii tarkoituksenmukaisesti. Organisaation tulee sertifioida hallintajärjestelmänsä uudelleen kolmen vuoden välein. Myönnettyjä sertifikaatteja Suomessa voi tarkastella SFS:n (2004) WWW-sivulta. Standardi sanoo, että se ei ole kaiken kattava. Tämän vuoksi täytyy muistaa, että jos organisaatio hakee sertifikaatin pelkästään sertifikaatin vuoksi, niin standardin ohjeet ja määräykset tulevat täytetyksi, vaikka organisaatio ei sitoutuisi turvallisuuden kehittämiseen. Pelkän sertifikaatin saamiseksi riittää asioiden dokumentointi ja organisaation johdon hyväksyntä jättää löydetty riskit olemassa olevalle tasolle. Siis tällainenkin toteutus saattaa tulla hyväksytyksi, koska sertifikaatin myöntäjät ovat kaupallisia yrityksiä, ja sertifikaatin hankinnan perimmäinen syy saattaa olla liikekumppanin vaatimus asiakassuhteen jatkamiselle.

2.4 VAHTI-ohjeet

Suomessa Valtiovarainministeriö (VM) ohjaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Ohjeita kehittää VM:n asettama valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). Ohjeistus kattaa kaikki tietoturvallisuuden osa-alueet, joista on kerrottu tarkemmin jo kohdassa 2.1. Tätä jakoa on käytetty myös tässä työssä. VAHTI-ohjeistuksen tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta tietoturvallisuutta kehittämällä. VAHTI-ohjeet käsittelevät asiaa konkreettisemmalla tasolla kuin edellä mainitut BS 7799-standardit. Ne ottavat huomioon lisäksi myös Suomen lainsäädännön ja erityisesti viranomaisten tietojärjestelmien toiminnan. Tosin näistä ohjeista ei löydy tarkkaa järjestelmäkuvausta. Sen sijaan sieltä löytyy suoria tarkistuslistoja, joita läpikäymällä voi helposti huomata, mihin asioihin pitäisi puuttua.

2.5 Pätevyyssertifikaatit

Oheessa kerrotaan muutamasta myöhemmin esiin tulevasta sertifikaatista, jolla voi osoittaa pätevyytensä tietoturvatehtäviin. Sertifikaatteja on myös muita samantapaisia kuin alla olevat turvallisuuden johtamiseen liittyvät. Yleensä sertifikaatit keskittyvät kuitenkin johonkin tuotteeseen, jolloin ne sopivat lähinnä yhteen tuotteeseen keskittyvälle tekniselle asiantuntijalle.

2.5.1 Certified Information Systems Security Professional (CISSP)

Certified Information Systems Security Professional (CISSP) sertifikaatteja myöntää International Information Systems Security Certification Consortium, Inc eli (ISC)² (2005a), joka on voittoa tavoittelematon organisaatio. Suomessa CISSP-tutkintoja järjestää Tietoturva ry (2005). CISSP-sertifikaatin koe kestää kuusi tuntia, ja se sisältää 250 monivalintakysymystä oheisista aihealueista. Jotta kokeeseen on mahdollista

osallistua, osallistujalla täytyy olla vähintään kolmen vuoden yhtäjaksoinen työkokemus yhdestä tai useammasta alla olevasta aihealueesta välittömästi koetta edeltävältä ajalta ((ISC)² 2005b):

- pääsynvalvonta (Access Control Systems and Methodology)
- sovellusten ja järjestelmien turvallisuuskehitys (Applications and Systems Development Security)
- jatkuvuus ja toipumissuunnittelu (Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP))
- kryptologia (Cryptography)
- lainsäädäntö ja etiikka (Law, Investigation and Ethics)
- operatiivinen turvallisuus (Operations Security)
- fyysinen turvallisuus (Physical Security)
- turvallisuusarkkitehtuurit ja mallit (Security Architecture and Models)
- turvallisuusjohtamisen käytännöt (Security Management Practices)
- tietoliikenne ja verkkoturvallisuus (Telecommunications and Network Security).

Jotta CISSP-sertifikaatti pysyy voimassa, on kolmen vuoden aikana hankittava tarpeeksi täydennyskoulutuspisteitä. Sertifikaattiin on mahdollista liittää myös valinnaisia osia. Tällöin on mahdollista saavuttaa Information Systems Security Engineering Professional (ISSEP), Information Systems Security Architecture Professional (ISSAP) tai Information Systems Security Management Professional-sertifikaatti (ISSMP).

2.5.2 Certified Information Systems Auditor (CISA) ja Certified Information Security Manager (CISM)

CISA ja CISM ovat sertifikaatteja, joita myöntää ISACA (Information Systems Audit and Control Association). Lyhenteet tulevat sanoista Certified Information Systems Auditor ja Certified Information Security Manager. Suomessa ISACA:a edustaa jäsenyhdistys Tietojärjestelmien tarkastus ja valvonta ry (2005). Sertifikaateilla on seuraavat yhteiset vaatimukset:

- Vähintään viiden vuoden työkokemus tietojärjestelmien auditoinnista.
- Hakija hyväksyy ISACA:n eettiset säännöt (ISACA 2005a Code Of Professional Ethics).
- Jotta sertifikaatti pysyy voimassa, tarvitaan vähintään 120 tuntia hyväksytyä jatkokoulutusta kolmen vuoden aikana, josta vähintään 20 tuntia joka vuosi.

CISA-kokeen aihealueet ja painoarvot ovat (ISACA 2005b):

- tietojärjestelmän auditointi (The IS audit process) 10%
- tietojärjestelmän ylläpito, suunnittelu ja organisointi (Management, planning, and organization of IS) 11%
- tekninen infrastruktuuri ja sen toteutus (Technical infrastructure and operational practices) 13%
- tietojen turvaaminen (Protection of information assets) 25%
- toipumis- ja jatkuvuussuunnittelu (Disaster recovery and business continuity) 10%
- liiketoimintajärjestelmän kehitys, hankinta, implementointi ja ylläpito (Business application system development, acquisition, implementation and maintenance) 16%
- liiketoimintaprosessin evaluointi ja riskinhallinta (Business process evaluation and risk management) 15%.

CISM-kokeen aihealueet ja painoarvot ovat (ISACA 2005c):

- hallinnollinen tietoturva (Information Security Governance) 21%
- riskienhallinta (Risk Management) 21%
- tietoturvan kehittäminen (Information Security Program(me) Management) 21%
- tietoturvan johtaminen (Information Security Management) 24%
- vastesuunnittelu (Response Management) 13%.

2.5.3 Global Information Assurance Certification (GIAC)

Global Information Assurance Certification (GIAC) on System Administration, Networking, and Security Organization (SANS):n sertifikaattiperhe, joka koostuu yksittäisistä sertifikaateista ja yksittäisten sertifikaattien muodostamista kokonaisuuksista. GIAC:n (2005a) mukaan sertifikaatteja on kahta tasoa, hopea (Silver) ja kulta (Gold). Hopeatasoon riittää pelkän kokeen suorittaminen. Kultatasoon vaaditaan lisäksi kirjallinen raportti, jonka sisällön pitää olla hyödyllinen yhteisölle. Vaativin sertifikaateista CIAC:n (2005b) mukaan on GIAC Security Expert (GSE). Se edellyttää esitietoina seuraavat sertifikaatit:

- GIAC Certified Firewall Analyst (GCFW)

- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Certified UNIX Security Administrator (GCUX)

Sertifikaateista yhden suorituksen on oltava hyväksytty vähintään 90%:lla pisteistä. GIAC (2005b) koe sisältää kirjallisia ja laboratorio-osuuksia. Laboratorio-osuudessa analysoidaan verkkoliikenteestä merkkejä tunkeutumisista, hyökkäyksistä ja epätavallisista ohjelmista. Lisäksi verkkoliikenteen perusteella yritetään päätellä verkon arkkitehtuuri, koko, palomuurin sijainti ja suoritetaan verkon haavoittuvuuksien arviointi. Kirjallinen osuus muodostuu monivalintakysymyksistä (20%) ja esseistä (80%). Lisäksi sertifikaatin vaatimuksena on suullinen esitys omavalintaisesta aiheesta. Muita CIAG:n (2005c) tarjoamia sertifikaatteja löytyy liitteestä.

3. TIETOTURVA–AMMATTILAISEN TEHTÄVIÄ KIRJALLISUUDESSA

3.1 *Miettisen ammattilaisprofiilit*

Juha E. Miettinen (2002) on muodostanut seuraavanlaiset yritysturvallisuuden asiantuntijaprofiilit: johtaja, esimies tai päällikkö, tutkija, erikoisasiantuntija ja suoritetyöntekijä. **Johtajalla** on yleensä pitkä työkokemus omalta ammattialaltaan, johtamistaitoa ja korkea peruskoulutus. Johtaja on yleensä ylin päättäjä ja hänen vastuullaan on turvallisuusyksikön tai sen osan johtaminen. Tyypillisiä tehtävänimikkeitä ovat turvallisuusjohtaja, yritysturvallisuusjohtaja, ympäristöjohtaja, pelastusjohtaja, riskienhallintajohtaja ja vakuutusjohtaja. **Esimies tai päällikkö** voi olla koulutustaustaltaan melkein mitä tahansa, mutta mitä vaativammassa asemassa hän on sitä korkeampaa koulutusta ja työkokemusta vaaditaan. Työssään hän on vastuullinen johtamansa yritysturvallisuuden ryhmän esimiehenä ja vastaa myös sen toiminnan ohjauksesta. Esimerkkejä tämän tason tehtävänimikkeistä ovat turvallisuuspäällikkö, tietoturvallisuuspäällikkö, ympäristöpäällikkö ja vakuutuspäällikkö. **Yritysturvallisuusalan tutkijalla** on yleensä suoritettuna ylempi korkeakoulututkinto opiskelemassaan pääaineessa ja hän on jo suorittanut tai mahdollisesti aikoo suorittaa jatkotutkinnon. Toimenkuvana tutkijalla on yritysturvallisuuden tutkimustyö. **Erikoisasiantuntijalla** on alan korkea peruskoulutus ja jonkin yritysturvallisuuden erikoisalueen osaaminen. Koulutukseltaan hän on esimerkiksi insinööri. Toimenkuvassaan hän keskittyy yhteen tai muutamaankin kohdassa 2.2 mainittuihin yritysturvallisuuden osa-alueisiin, esim. rikosturvallisuus. Omalla osaamisalueellaan hänellä on laaja ammatillinen osaaminen. **Suoritetyöntekijä** on yritysturvallisuuden ammattilainen, jolla on alan peruskoulutus, mutta ei omia alaisia. Tyypillisiä työtehtäviä ovat vahtimestari, vartija ja henkivartija. Suoritetyöntekijä ei kuulu tämän työn tarkastelun piiriin.

3.2 *Mannisen ammattilaisprofiilit*

Tampereen yliopiston tietoturvapäällikkö Minna Manninen on seminaariesityksessään Suuren organisaation tietoturva (16.3.2004) nimennyt organisaatiosta seuraavat tietoturva-ammattilaisprofiilit: ylin johto, tietoturvallisuuden johto, tietoturvapäällikkö, atk-yksikkö yleensä, tietotekninen asiantuntija, osaston johtaja, tietojärjestelmän omistaja ja järjestelmän pääkäyttäjä. **Ylimmän johdon** tehtävänä on viime kädessä vastata tietoturvallisuudesta, ellei johto ole delegoinut vastuutaan. Ylimmän johdon tehtävänä on tietoturvallisuuden osalta taata tietoturvallisuuden tarvitseman resurssit, organisoida tietoturva, huomioida tietoturva riskienhallinnassa, hyväksyä tietoturvapolitiikka, asettaa vaatimukset raportoinnille tietoturvan toteutumisesta ja määritellä organisaation

tietoturvan tavoitetaso. **Tietoturvallisuuden johdon** tehtävänä on valmistella ja ohjata tietoturvallisuuden käytännön toteutusta, kehittää tietoturvaa tietoturvapolitiikan mukaisesti, olla asiantuntijaryhmänä tietoturvapolitiikan määrittelyssä, huolehtia henkilöstön tietoturvakoulutuksesta, valvoa turvallisuutta ulkoistetuissa atk-palveluissa, raportoida ja tehdä aloitteita tietoturvallisuudesta ylimmälle johdolle. **Tietoturvapääällikkö** valmistelee tietoturvan kehittämishankkeita yhdessä tietoturvan johtoryhmän kanssa, on päävastuullinen tietoturvallisuuden johtoryhmässä, tiedottaa tietoturva-asioista, avustaa tietoturvallisuuden toimeenpanossa, järjestää tietoturvallisuutta koskevan seurannan ja informoi johtoa. **Atk-yksikön** tehtävänä on huolehtia teknisestä tietoturvasta, vastata tietoliikenneverkon turvallisuudesta, huolehtia käyttäjähallinnasta, huolehtia varmuuskopioinnista, järjestää tekniseen tietoturvaan liittyvä koulutus organisaatiolle ja neuvoa tekniseen tietoturvaan liittyvissä kysymyksissä. **Tietoteknisiin asiantuntijoihin** kuuluvat ylläpitäjä, suunnittelija, ohjelmoija ja atk-tuki. Näiden tehtävänä on soveltaa ja toteuttaa organisaation tietoturvaperaatteita oman erikoisasiantuntemuksensa mukaisesti, vastata tietoturvatyömenpiteistä omalla vastuualueellaan sekä raportoida tietoturvallisuudesta ja häiriöistä esimiehilleen. **Osaston johtajan** tehtävänä on resursoida ja toimeenpanna osaston tietoturvallisuus ja siihen liittyvät kehitystoimenpiteet asetettujen tavoitteiden mukaisesti, seurata kuinka henkilökunta noudattaa tietoturvaohjeistusta, toimia osastonsa tietoturvallisuuden yhteyshenkilönä, nimetä yksikkönsä tietojärjestelmien omistajat sekä raportoida tietoturvallisuudesta ja häiriöistä esimiehilleen. **Tietojärjestelmän omistajan** tehtävänä on vastata henkilörekisteri-, tietojärjestelmäselosteista, tietojärjestelmäkuvauksista, tietojen suojauksesta, varmuuskopioinnista, toimeenpanna tietojärjestelmänsä turvallisuustoimenpiteet, kehittää tietojärjestelmän turvallisuutta, seurata tietojärjestelmänsä tietoturvallisuuden tilaa sekä raportoida tietoturvallisuudesta ja häiriöistä esimiehilleen. **Järjestelmän pääkäyttäjän** tehtävänä on ylläpitää tietojärjestelmän turvallisuusmenettelyt, seurata järjestelmän tietoturvallisuuden tilaa, varautua poikkeaviin tapahtumiin ja niistä aiheutuviin toimenpiteisiin, raportoida tietoturvallisuudesta ja häiriöistä esimiehilleen.

3.3 Wadlowin ammattilaisprofiilit ja ryhmät

Thomas A. Wadlow:n (2001) mukaan paras valinta verkkoturvallisuusasiantuntijaksi on ohjelmoija, jolla on kykyä ja kokemusta ajatella kuin krakkeri, mutta jolla on tarpeeksi itsehillintää olla muuttumatta itse krakkeriksi. Turvallisuusorganisaatiosta hän löytää seuraavanlaisia tehtäviä, joiden pitäisi löytyä useimmista organisaatioista. Samalla henkilöllä voi olla useampia tehtäviä tai sama tehtävä voi olla jakautuneena useammalle. Yleensä tietoturvakäytännössä henkilöitä ei ole alla olevien tehtävien määrää, vaan vähemmän. Tehtävien nimet on Jukka Koskisen Verkon tietoturva kurssilla (2004) suomennettu nimistä mukailtu, suluissa alkuperäinen nimitys. **Turva-arkkitehti** (Security Architect) toimii kaikkien turva-asioiden koordinaattorina ja kehittää uusia

politiikkoja. **Sisäinen auditoija** (Internal Auditor) tarkkailee, että organisaation järjestelmät ovat käytännössä organisaation suunnitelmien mukaiset. Hän on mukana suunnittelemassa organisaation järjestelmäspesifikaatioita ja johtaa järjestelmäpäivityksiä ja -korjauksia tietoverkkoasiantuntijoiden kanssa.

Operointiryhmä koostuu turvaoperaatioiden päälliköstä (Security Operations Manager) ja turvaoperaattoreista (Security Operations). **Turvaoperaatioiden päällikkö** on vastuussa korjauspartioiden vaste-ajasta ja raportoi tietohallintoon ongelmien korjauksista ja niihin käytetystä ajasta. **Turvaoperaattori** huolehtii päivittäistoimintojen käytännön toteuttamisesta, kuten käyttö-oikeuksien lisäyksistä ja poistoista järjestelmiin.

Kehitysryhmä koostuu kehityspäälliköstä (Development Engineering Manager), kehitysinsinööreistä (Development Engineer), Autentikoinnin järjestelyistä vastaavista (Authentication) ja lokitietojen keräämisen järjestelystä (Logging). **Kehityspäällikkö** vastaa kehitysprojektien aikataulutuksesta ja koordinoi kehitysprojekteja turva-arkkitehdin kanssa. **Kehitysinsinööri** integroi tuotteet ja kirjoittaa omaakin koodia implementoidakseen uusia palveluita ja parantaakseen vanhoja. **Autentikoinnin järjestelyistä vastaava** hoitaa käyttäjien hallinnan toteutuksen ja suunnittelun organisaation järjestelmissä. **Lokitietojen keräämisen järjestelyissä** päätetään, mitä lokitietoja on tarpeellista kerätä ja tarkkaillaan, että lokitiedot ovat virheettömiä. Havaittaessa puutteita ne korjataan välittömästi.

Turvaryhmä koostuu isäntäkoneiden turvaajista (Host Security), verkon turvaajista (Network Security) ja fyysisistä turvaajista (Physical Security). **Isäntäkoneiden turvaaja** vastaa organisaation työasemien ja palvelimien turvallisuuden suunnittelusta ja toteutuksesta yhteistyössä yleisen tason ylläpitäjien kanssa. **Verkon turvaaja** on vastuussa verkkoturvan suunnittelusta ja sen konfiguroinnista verkkolaitteisiin. Hän raportoi verkonhallintaryhmälle toiminnastaan. **Fyysinen turvaaja** vastaa organisaation avaimista, kulkuluvista, henkilökorteista, käyttö-oikeuksista, käyttämisen lokitiedoista ja lokitietojen käytön valvonnasta.

Vasteryhmä koostuu vastepäälliköstä (Response Team Manager), vartija-tarkkailijoista (Watchstander), dogfightereista (Dogfighter), tason yksi vasteista (Incident Response-Level 1), tason kaksi vasteista (Incident Response-Level 2) ja vahinkojen arvioinnista ja korjauksesta (Damage Control). **Vastepäällikkö** johtaa vasteryhmiä. **Vartija-tarkkailija** tarkkailee mahdollisia häiriöitä järjestelmissä ja korjaa pienet häiriöt itse. Kutsutaan myös standardivasteeksi. **Dogfighter** tarkkailee jatkuvasti hyökkäyksiä ja tekee ensivaiheen vahinkoraportin. Päätehtävänä on hyökkäyksistä aiheutuvien häiriöiden minimointi. **Tason yksi vaste** on ensimmäisenä hälytyksen vastaanottava korjauspartio, jonka tehtävä on ratkaista ongelma tai vakavuuden mukaan kutsua apuvoimia. Se keskittyy ongelmamäärän pienentämiseen. **Tason kaksi vaste** hälytetään ensimmäisen tason vasteen pyynnöstä ratkaisemaan ongelmia, joista ensimmäisen taso ei yksinään selviä. Se keskittyy ratkaisemaan harvoja ongelmia tai pitkäkestoisia ongelmia laadukkaasti.

Vahinkojen arviointi ja korjaus aktivoituu tehtäväänsä, kun kyse on pitempään kestävästä ja vakavammasta loukkausten käsittelystä, jolloin tason yksi vaste ei enää riitä.

Jäljitysryhmä koostuu jäljityspäälliköstä (Forensics Team Manager), jäljitysanalyytikoista (Forensic Analyst) ja lainvalvojista (Law Enforcement). **Jäljityspäällikkö** johtaa jäljitysanalyytikkoja. **Jäljitysanalyytikko** selvittää ja tutkii tunkeutumisten menetelmiä. Hän kehittää muiden asiantuntijoiden kanssa tunkeutumisen varoitus- ja havainnointimenetelmiä. **Lainvalvoja** pitää yllä organisaation uskottavuutta toimia lain mukaisesti olemalla yhteydessä viranomaisiin.

Dokumentointiryhmä koostuu dokumentointipäälliköstä (Documentation Manager), dokumentoijista (Documentation) ja politiikan ja käytäntöjen hallinnasta (Policies and Procedures). **Dokumentointipäällikkö** johtaa turvallisuuskäytäntöjä. **Dokumentoija** kirjoittaa turvallisuuskäytäntöjä ja käyttöohjeita. **Politiikan ja käytäntöjen hallinta** huolehtii, että turvallisuuspolitiikka on ajan tasalla. Se vastaa yhdessä henkilöstöhallinnon kanssa, että kaikki työntekijät ovat lukeneet turvallisuuspolitiikan viimeisimmän version.

Tiedotusryhmä koostuu sisäisistä (Communications) ja ulkoisista tiedottajista (Press Liaison). **Sisäinen tiedottaja** huolehtii, että tieto kulkee turvallisuusorganisaation sisällä ja toimii turvallisuusorganisaation tiedottajana organisaation ulkopuolelle. **Ulkoisen tiedottaja** toimii turvallisuusosaston yhteyshenkilönä medioille ja valvoo yrityksen ulkoista tiedottamista turvallisuusnäkökulmasta.

Tutkija (Researcher) pitää itsensä ajan tasalla viimeisimmistä turvallisuusongelmista ja korjauksista. Hän kouluttaa organisaatiossa edellä mainituista asioista organisaation henkilökuntaa. **Ylläpitäjä** (Systems Administrator) toimii ylläpitäjänä turvatiimin omille järjestelmille. Erillinen tehtävä yleiseen ylläpitäjään verrattuna, koska turvajärjestelmien omat turvavaatimukset ovat suuremmat kuin yleiset.

3.4 Whitmannin & Mattordin ammattilaisprofiilit ja ryhmät

Tietoturva-asiantuntijoiden pohjakoulutuksena on havaittavissa kolme erilaista ryhmää. Ensimmäiseen ryhmään kuuluvat poliisin tai puolustusvoimien ammateissa työskennelleet. Toisen ryhmän muodostavat erilaisissa IT-ammateissa työskennelleet. Kolmanteen ryhmään kuuluvat yliopistoissa asiaa opiskelleet. Kuitenkin viime mainitut ovat tänä päivänä vielä selvä vähemmistö. Tällä hetkellä tietoturva-ammattilaisten suurin enemmistö tulee ryhmästä kaksi.

Yleiset vaatimukset tietoturva-asiantuntijalle (Security professionals) on lueteltu seuraavassa:

- Ymmärtää organisaation toiminnan kaikilla tasoilla johdosta valmistukseen.
- Ymmärtää, että useimmiten tietoturvasuhteellisuus on hallinnollinen ongelma ja erittäin harvoin pelkästään tekninen ongelma.

- Omaa hyvät viestintätaidot sekä suullisesti että kirjallisesti ja osaa ratkoa loppukäyttäjien ongelmia yhteistyössä heidän kanssaan.
- Toimii turvallisuuspolitiikan esikuvana siten, että organisaation muu henkilökuntakin innostuu näkemään turvallisuusasiat hyödyllisinä eikä pelkästään rasitteena.
- Tuntee ja osaa soveltaa yleisimpiä IT-teknologioita. Hänen ei kuitenkaan tarvitse olla näiden alueiden ekspertti.
- Tietää mitä IT- ja tietoturva-termit merkitsevät.
- Osaa suhtautua sopivalla vakavuudella organisaatioon kohdistuviin turvallisuusriskeihin ja pyrkii estämään niiden realisoitumisen.
- Osaa soveltaa tekniikoita ja teknologioita ratkaistessaan turvallisuusongelmia.

Tietohallintojohtaja (Chief Information Officer) suunnittelee yhdessä organisaation ylimmän johdon kanssa tiedonhallintastrategian. **Tietoturvapäällikkö** (Chief Information Security Officer) vastaa tietoturvan johtamisesta tietoturvaosaston ylimpänä päällikkönä. Tietoturvapäälliköt ovat vastuussa tietoturva projektien suunnittelusta ja toteutuksesta. Eensisijaisesti he ovat hallinnollisesti suuntautuneita. Tekniikka tulee vasta toisella sijalla. Yleensä tietoturvapäälliköt tekevät hallinnolliseen turvallisuuteen kuuluvien ohjeistusten, esim. tietoturvapolitiikan, valmistelun. He työstävät ne valmiiksi organisaation asiantuntijoiden kanssa tai hyväksyvät muiden valmistelemat ohjeistukset. He laativat ja vastaavat tietoturva-organisaation budjetista johdolta saamiensa resurssien puitteissa. Tietoturvapäälliköt päättävät myös omien osastojensa rekrytoinneista. Yleisin ammatillinen pätevyysvaatimus on Certified Information Systems Security Professional (CISSP) sertifikaatti. Lisäksi vaaditaan yleensä myös akateeminen loppututkinto, joka voi olla IT-alalta, oikeustieteestä, taloudesta tai joltain muulta alueelta, joka liittyy jollakin tavoin turvallisuuteen. Kyvykkyys tämän tason tehtävään osoitetaan kuitenkin työkokemuksella. **Tietoturvajohdajien** (Security Manager) tehtävänä on avustaa tietoturvapäällikköä ja ylläpitäjiä. He hankkivat tietoa ja kehittävät organisaation tietoturvaohjeistusta ja riskienhallintaa. He vastaavat myös päivittäisten turvallisuusrutiinien toteutumisesta, hyväksyttävästä riskitasosta ja toiminnan tuloksellisuudesta. Pätevyysvaatimuksena saattaa olla jokin seuraavista sertifikaateista CISSP tai Certified Information Security Manager (CISM) tai Global Information Assurance Certification (GIAC). Heidän tulee osata suunnitella politiikkoja ja ohjeita. Lisäksi heillä täytyy olla kokemusta kaikille johtajille kuuluvista talousasioista, esimerkiksi budjetoinnista ja projektien johtamisesta. **Tietoturva-asiantuntijat** (Security Technician) ovat teknisiä asiantuntijoita, joiden tehtäviin kuuluu esimerkiksi palomuurien asentaminen, IDS:n eli tunkeutumisen havainnoinnin järjestäminen, päivittäisten teknisten

ongelmien ratkaiseminen ja verkonhallinta. Pätevyysvaatimuksena on yleensä jonkin teknisen osa-alueen hallinta, esimerkiksi tietyn valmistajan palomuuriohjelmiston sertifikaatti.

Tietoturvaprojektiryhmä koostuu projektiryhmien päälliköstä (Champion), projektiryhmien johtajista (Team leader), tietoturva politiikan suunnittelijoista (Security policy developers), riskien hallinnan asiantuntijoista (Risk assessment specialists), tietoturva-asiantuntijoista (Security professionals), ylläpitäjistä (Systems administrators) ja loppukäyttäjistä (End users). **Projektiryhmien päällikkö** suunnittelee projektit, aikataulut ja resurssit. **Projektiryhmän johtajalla** on tietämystä projektin johtamisesta ja teknisestä tietoturvasta. **Tietoturva politiikan suunnittelijat** ymmärtävät organisaation tietoturvakulttuurin, tietoturva politiikan ja vaatimukset poliitikoille. **Riskienhallinnan asiantuntijat** ymmärtävät riskienhallinnan, organisaation omaisuuden arvostamisen ja riskienhallinnan menetelmät omaisuuden suojaamiseksi. **Tietoturva-asiantuntijat** ymmärtävät tietoturvan sekä tekniseltä että hallinnolliselta kannalta. **Ylläpitäjät** ylläpitävät organisaation tietojärjestelmiä. **Loppukäyttäjät** ovat eri tietojärjestelmien käyttäjiä, joilla on tietämys omasta osaamisalueestaan ja useinkin hyvin eritasoiset tietotekniset valmiudet niiden päivittäiseen käyttöön.

Tiedon omistajiin kuuluvat tietojärjestelmän omistajat (Data owners), tietojärjestelmäoperaattorit (Data custodians) ja käyttäjät (Data users). **Tietojärjestelmän omistajat** vastaavat omistamiensa tietojen turvallisuuden hankkimisesta, turvaamisen tasosta ja turvaluokituksen ajan tasalla pitämisestä. **Tietojärjestelmäoperaattorit** vastaavat tietojen tallentamisesta, ylläpidosta ja päivittäisestä teknisestä turvaamisesta. **Käyttäjät** vastaavat käsittelemiensä tietojen turvallisesta käyttämisestä omalta osaltaan päivittäisissä työtehtävissään.

Jatkuvuussuunnitteluryhmä koostuu projektiryhmien päälliköstä (Champion), projektiryhmien johtajista (Team leader) ja projektiryhmien muista jäsenistä (Team members). **Projektiryhmien päällikkö** suunnittelee jatkuvuussuunnitelmaprojektin, aikataulun ja resurssit. **Projektiryhmän johtaja** toteuttaa projektiryhmien päällikön strategisen suunnitelman ja jakaa tehtävät organisaation henkilöille. **Projektiryhmän muut jäsenet** koostuvat organisaation useiden eri osastojen johtajista (Managers). Johtajat ovat oman alueensa asiantuntijoita, esimerkiksi talousjohtaja (Business manager), tietohallintojohtaja (Information technology manager) ja tietoturva johtaja (Information security manager). Talousjohtajan asiantuntemus liittyy liiketoimintaprosesseihin, asiakasvaatimuksiin ja liiketoimintaprosessien viranomaisvaatimuksiin. Tietohallintojohtajan asiantuntemuksen piiriin kuuluu tietojärjestelmiin liittyvät riskit ja järjestelmien teknisten ominaisuuksien tunteminen. Tietoturva johtaja valvoo projektia ja toimii asiantuntijana tietoturva uhkien, haavoittuvuuksien ja hyökkäyksen ehkäisemisessä.

3.5 BS 7799-1-standardin vaatimukset ja ammattilaisprofiilit

BS 7799-standardin ohjeet vastuunjaosta ovat viitteellisiä. Standardin sertifiointin vaatimuksien toteuttamiseksi riittää vastuukysymyksissä toisessa osassa määriteltyjen vastuiden jakaminen dokumentoidusti organisaation haluamalla tavalla. Standardin vaatimusten toteuttaminen ei takaa lakisääteisten velvoitteiden toteutumista. Alla olevat vastuunjaot ovat standardin esittämiä suosituksia. Vastuunjaossa on lueteltu vain ne alueet, jotka olivat standardissa nimettyinä jollekin tietylle vastuunkantajalle. Standardi sisältää myös muita vastuutettavia asioita, joille ei ole nimetty vastuunkantajaa. Jos vastuunkantajaa ei ole nimetty, viime kädessä kaikesta vastaa organisaation toimitusjohtaja, ellei hän ole muuta määrännyt.

BS 7799-standardin ensimmäisessä osassa määrätään organisaation johto luomaan työryhmä(t) tietoturvapoliittikan hyväksymistä, turvatehtävien määräämistä ja turvallisuuden koordinoimista varten. Standardin mukaan: ”Työryhmän tulee edistää tietoturvaluutta organisaatiossa osoittamalla asiankuuluvaa sitoutumista ja myöntämällä riittävät resurssit.” Standardissa esitetään turvallisuuden koordinoimisesta vastaavalle työryhmälle seuraavat tehtävät:

- tietoturvaluutta koskevien erityisten tehtävien ja velvollisuuksien hyväksyminen koko organisaatiota varten
- tietoturvaluutta koskevien erityisten menetelmien ja prosessien, kuten riskien arvioinnin ja turvallisuuden luokitusjärjestelmien, hyväksyntä
- koko organisaation käsittävien tietoturvaluusaloitteiden, kuten turvallisuustietoisuutta lisäävän ohjelman, hyväksyntä
- sen varmistaminen, että turvallisuus kuuluu osana tietojärjestelmien suunnitteluprosessiin
- uusien järjestelmien ja palvelujen erityisten tietoturvaluusmekanismien toteuttamisen asianmukaisuuden arvioiminen ja koordinointi
- turvallisuuteen liittyvien poikkeustilanteiden arvioiminen
- liikkeenjohdon tietoturvaluudelle osoittamasta näkyvästä tuesta tiedottaminen koko organisaatiolle.

Tietoturvapäälliköllä on päävastuu turvallisuuden kehittämisestä ja toteuttamisesta sekä suojaimekanismien määrittelyn tukemisesta. **Tietoturvaluusneuvoja** koordinoi ja yhdenmukaistaa organisaation sisäistä tietoutta ja kokemuksia sekä tarjoaa apua turvallisuuteen liittyvien päätösten tekemisessä. **Suojeltavan kohteen omistaja** on vastuussa kohteen jokapäiväisestä turvallisuudesta. **Järjestelmän pääkäyttjä** toteuttaa järjestelmän käyttöoikeuksien hallinnan. **Esimehillä** on vastuu resurssien jaosta ja

turvamekanismien toteuttamisesta. **Tietojenkäsittelypalvelujen käyttäjien** tulee kiinnittää huomiota ja raportoida esimiehilleen kaikista järjestelmissä tai palveluissa havaituista tai epäilyistä suojauksen heikkouksista tai niihin kohdistuvista uhkista.

3.6 BS 7799-2-standardin vaatimukset ammattilaisprofiileille

BS 7799-standardin toisessa osassa tarkennetaan ensimmäisen osan vastuunjakoa seuraavasti. ”Johdon tulee osoittaa sitoutumisensa tietoturvallisuuden hallintajärjestelmän luomiseen, käyttöönottoon, käyttöön, valvontaan, katselmointiin, ylläpitoon ja parantamiseen.” Standardin mukaan johto toteuttaa yllämainitut vaatimukset

- määrittelemällä tietoturvallisuuspolitiikan
- varmistamalla, että tietoturvallisuustavoitteet asetetaan ja -suunnitelmat laaditaan
- määrittelemällä tietoturvallisuuteen liittyvät roolit ja vastuut
- viestimällä organisaatiolle tietoturvallisuustavoitteiden ja tietoturvallisuuspolitiikan noudattamisen, niihin liittyvien lakisääteisten velvoitteiden noudattamisen ja jatkuvan parantamisen tärkeydestä
- huolehtimalla, että käytettävissä on riittävät resurssit tietoturvallisuuden hallintajärjestelmän kehittämiseen, toteuttamiseen, käyttöön ja ylläpitoon
- päättämällä hyväksyttävästä riskitasosta
- suorittamalla tietoturvallisuuden hallintajärjestelmän johdon katselmuksia.

”Johdon tulee katselmoida organisaation tietoturvallisuuden hallintajärjestelmä ennalta suunnitelluin väliajoin varmistaakseen sen jatkuva soveltuvuus, asianmukaisuus ja vaikuttavuus. Katselmukseen tulee sisältyä tietoturvallisuuden hallintajärjestelmän arviointi, mukaan lukien tietoturvallisuuspolitiikka ja tietoturvallisuustavoitteet, parannusmahdollisuudet ja muutostarpeet. Katselmuksen tulokset tulee dokumentoida selkeästi ja niistä tulee ylläpitää tallenteita.” Näin alkaa BS 7799-2-standardin (23.3.2003) 6. luku.

3.7 VAHTI-ohjeiden 7/2003 & 1/2001 ammattilaisprofiilit

Taulukko 3.1 on muodostettu ottamalla VAHTI-ohjeesta 7/2003 taulukko1: Tietoturvallisuusriskien arvioinnin tehtäviä ja vastuita, jota on muokattu ja täydennetty VAHTI-ohjeesta 1/2001 kohdasta 2.4 löytyvällä vastaavan sisältöisellä luettelolla. Lihavoidut vastuulliset löytyvät vain VAHTI-ohjeesta 1/2001. Taulukon lopussa käyttäjien jälkeen olevat ryhmät kuuluvat pääsääntöisesti pelkästään valtionhallintoon, joten niitä ei tulla käsittelemään tässä työssä tarkemmin.

Taulukko 3.1: Tietoturvaluusriskien arvioinnin tehtäviä ja vastuita.

| | |
|---|--|
| <p>Ylin johto</p> | <ul style="list-style-type: none"> • Vastaa kokonaisvastuun osana tietoturvaluisuuden toteutumisesta. • Sisällyttää tietoturvaluisuuden osaksi riskienhallintaa. • Luo edellytykset ja takaa tietoturvaluisuuden toteuttamiseksi tarvittavat resurssit. • Vahvistaa tietoturvaluisuuden päälinjaukset. • Hyväksyy tietoturvaluuspolitiikan ja siihen liittyvät periaatteet. • Edellyttää toimintojen tietoturvaluuspriorisointia. • Asettaa vaatimukset raportoinnille. • Asettaa vaatimukset tietoturvaluisuuden huomioon ottamisesta toiminnoissa. |
| <p>Turvallisuusjohto</p> | <ul style="list-style-type: none"> • Osallistuu turvallisuuspolitiikan ja –periaatteiden määrittelyyn. • Turvallisuuspolitiikan mukaisesti kehittää turvallisuuden kokonaistoimintoa. • Ohjaa turvallisuuden käytännön toteutusta henkilöstön, toiminnan ja omaisuuden turvaamiseksi ja niihin kohdistuvien riskien hallitsemiseksi. • Raportoii ylimmälle johdolle turvallisuudesta. |
| <p>Tietojärjestelmän omistajat</p> | <ul style="list-style-type: none"> • Ylläpitävät tietojärjestelmäkuvaukset. • Toimeenpanevat tietojärjestelmäänsä liittyvät turvallisuustoimenpiteet. • Seuraavat tietoturvaluusua omistamassaan tietojärjestelmässä. • Raportoivat tietoturvaluusua ja siihen kohdistuvista häiriöistä. |

| | |
|------------------------|--|
| Tietohallintojohto | <ul style="list-style-type: none"> • Valmistelelee tietohallintoon ja tietotekniikkaan liittyvän tietoturvapoliitiikan. • Ohjaa organisaation tietoturvallisuuden kehittämistoimenpiteitä. • Tietohallinnon tietoturvallisuuden tulosohjaus. • Varmistaa tietoturvallisuuden toteutumisen tietohallinnossa. • Tietoturvallisuuden toteutumisen valvonta ostetuissa atk-palveluissa. • Huolehtii riskien arvioinnista tietojärjestelmäkehityksessä ja tietotekniikkahankkeissa. • Arvioi elintärkeiden tietojärjestelmien haavoittuvuutta. • Käynnistää arvioinnin esiintuomat kehittämistoimenpiteet. |
| Tietoturvallisuusjohto | <ul style="list-style-type: none"> • Osallistuu tietoturvapoliitiikan ja –periaatteiden määrittelyyn. • Kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti. • Huolehtii henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvallisuuskoulutuksen järjestämisestä. • Ohjaa tietoturvallisuuden käytännön toteutusta ja siihen liittyvää riskienhallintaa. • Raportoi ylimmälle johdolle tietoturvallisuudesta. • Luo ja valitsee menettelyt tietoriskien arvioimiseksi. • Hankkii arvioinnissa tarvittavan asiantuntemuksen. • Kouluttaa toiminnasta vastaavan henkilöstön käyttämään arviointimenetelmiä. • Osallistuu asiantuntijana riskien arviointiin. |
| Operatiivinen johto | <ul style="list-style-type: none"> • Vastaa toimialansa tietoturvallisuuden kehittämistoimenpiteiden toteuttamisesta. • Tietojärjestelmän omistajien nimeäminen ja toimialansa tietoturvallisuuden tulosohjaus. • Ottaa huomioon tietoturvavaatimukset johtaessaan toimialaansa. |

| | |
|--|--|
| Esimiehet | <ul style="list-style-type: none"> • Toteuttavat tietoturvatyömenpiteitä asetettujen tavoitteiden mukaisesti. • Seuraavat valtionhallinnon ja omien tietoturvallisuuden ohjeiden noudattamista. • Raportoivat tietoturvallisuudesta ja siihen kohdistuvista uhkista ja häiriöistä. |
| Tietoturva-asiantuntijat | <ul style="list-style-type: none"> • Avustavat johtoa ja yksiköitä tietoturvallisuuden edellyttämien toimenpiteiden kehittämisessä, toimeenpanossa ja päätöksenteossa. • Tulohjaustavoitteiden mukaisesti seuraavat ja kehittävät ehdotuksin tietoturvallisuutta. • Järjestävät tietoturvallisuutta koskevan seurannan ja johdon informaation. • Toteuttavat osaltaan päätetyt tietoturvatyömenpiteet. • Toimivat asiantuntijoina riskien arvioinnissa. |
| Tietopalveluista ja asiakirjahallinnosta vastaavat | <ul style="list-style-type: none"> • Toimeenpaneuvat tietoturvallisuuden tietopalveluissa ja asiakirjahallinnossa hyvän tiedonhallintatavan ja tietoturvallisuustavan mukaisesti. • Raportoivat havaitsemistaan uhkista ja häiriöistä. • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin. |
| Tietojärjestelmän pääkäyttäjät | <ul style="list-style-type: none"> • Ylläpitävät turvallisuusmenettelyt tietojärjestelmässä. • Seuraavat tietojärjestelmien toimintaa tietoturvallisuuden kannalta. • Varautuvat poikkeaviin tapahtumiin ja niiden vaatimiin vastatoimenpiteisiin. • Raportoivat tietoturvallisuutta vaarantavista uhkista ja häiriöistä. • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin. |
| Tietotekniset asiantuntijat | <ul style="list-style-type: none"> • Soveltavat ja toteuttavat viraston tietoturvallisuuspolitiikkaa omaa erikoisasiantuntemustaan hyödyntäen. • Vastaavat tietoturvallisuustyömenpiteiden huomioon ottamisesta omalla vastualueellaan. • Noudattavat hyvää tietoturvallisuustapaa. • Raportoivat tietoturvallisuudesta. |

| | |
|--------------------------------------|--|
| Käyttäjät | <ul style="list-style-type: none"> • Tuntevat tietoturvallisuudesta annetut ohjeet ja noudattavat niitä. • Raportoivat tietoturvallisuutta vaarantavista uhkista, häiriöistä ja ohjeiden vastaisista menettelyistä. • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin. |
| Ministeriön valmiuspäällikkö | <ul style="list-style-type: none"> • Ottaa huomioon varautumistoimenpiteet toiminnassa. • Kehittää ja selvittää hallinnonalan poikkeusoloissa turvattavia toimintoja. • Kehittää elintärkeiden järjestelmien valmiutta yhdessä tietohallintojohdon kanssa. |
| Sisäinen tarkastaja | <ul style="list-style-type: none"> • Seuraa hyväksytyjen periaatteiden ja suunnitelmien toteutumista. • Tarkastaa tietoturvallisuutta. • Arvioi tietoturvaluustoimenpiteiden riittävyyttä suhteessa organisaation vastuisiin ja velvoitteisiin. • Raportoi johdolle tarkastustulokset. |
| Tietoturvallisuusryhmä | <ul style="list-style-type: none"> • Yhteistyöryhmä hallinnonalan sisäiseen ja ulkopuoliseen tietoturvallisuusrajapintojen sovittamiseen ja turvallisuuden seuraamiseen. • Edustaa organisaation eri tahojen tietoturvallisuusnäkemyksiä. • Sovittaa yhteen tietoturvaluustoimenpiteet ja turvallisuustason. • Ohjaa tietoturvaluustoimenpiteitä organisaatioiden ja niiden tuottamien palvelujen rajapinnoissa. |
| Konsultit ja palveluyritykset | <ul style="list-style-type: none"> • Noudattavat hyvää tietojenkäsittely- ja tietoturvaluustapaa. • Ylläpitävät ja valvovat toiminnassaan valtionhallinnon tietoturvaluuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvaluutta. • Raportoivat tietoturvaluudesta ja siihen vaikuttavista tekijöistä. |

4. HAASTATTELUN KYSYMYKSET

4.1 Kysymysten suunnittelu

Tässä luvussa esitellään tutkimuksessa käytetyt kysymykset ja niiden suunnittelu. Kysely on jaettu osakokonaisuuksiin, joka noudattaa kohtien 4.2–4.7 otsikointia. Kysymysten muodostamisessa on käytetty apuna seuraavia lähteitä:

- Tampereen teknillisen yliopiston (TTY) kurssin Tietoturvallisuuden johtaminen (2004) harjoitustyöhön liittyneitä tietoturva-auditointikysymyksiä
- TTY:n Ohjelmistotekniikan ammattilaisten osaamistarvekartoituksen kysymyslomaketta (2004)
- Yliopistojen tietoturvasivustolta löytyviä VAHTI-tietoturva CD:n Tietoturvallisuuden perustason testiä (2004)
- VAHTI-ohjeen 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa liitettä 2.
- Tilastokeskuksen 2/2002 Kysymisen taito-julkaisua.

4.2 Taustatiedot

Taustatietojen kysymykset taulukossa 4.1 käsittelevät yleistä tietoa organisaatiosta ja henkilöstä.

Taulukko 4.1: Organisaatiota ja henkilöstöä käsittelevät kysymykset

| | |
|--|---|
| <p>Nykyisen toimenkuvan ja entisten toimenkuvien lyhyt kuvaus?</p> <p>Koulutus, mahdolliset kurssit ja mahdollinen suunniteltu jatkokoulutus?</p> <p>Mitä tietoja opinnoistasi olet tarvinnut eniten ja mitä vähiten?</p> <p>Oliko opinnoissasi tietoturvallisuutta ja kuinka paljon (mahdolliset kurssinimet ja sisällöt lyhyesti)?</p> <p>Mitä tietoja tietoturvallisuusopinnoistasi olet tarvinnut eniten/vähiten?</p> <p>Työkokemuksesi vuosina ja tietoturvatehtävien osuus siitä?</p> <p>Miten ja mistä olet hankkinut lisää tietoa opiskelun jälkeen?</p> | <p>Oheisia tietoja käytetään luotaessa osaamisprofiileita. Esimerkiksi, jos vastaaja on tietohallintopäällikkö, ja jos saadaan vastauksia useammalta tietohallintopäälliköltä, niin vastauksia voitaisiin verrata keskenään ja yrittää löytää yhteneväisyyksiä. Toisaalta saattaa olla, että löydetään lähes identtisiä profiileita, mutta tittelit eivät korreloi keskenään.</p> |
| <p>Yrityksen toiminnan lyhyt kuvaus (toimiala, asiakkaat, toimittajat)</p> <p>Työntekijöiden määrä yrityksessä (suuruusluokka)?</p> | <p>Jos vastauksia saadaan erilaisilta toimialoilta, niin on mielenkiintoista nähdä, vaikuttaako toimiala toimenkuviiin. Pienemmissä organisaatioissa tehtävät ovat pienemmän ihmisryhmän vastuulla kuin suurissa. Jos saadaan vastaajia eri kokoisista organisaatioista, niin voidaan havaita, mitkä tehtävät hajaantuvat suurissa organisaatioissa eri henkilöille.</p> |
| <p>Minkälaista tietoa yrityksessä käsitellään?</p> | <p>Tietojenkäsittelykysymyksellä yritetään selvittää, miten esimerkiksi pankeissa henkilötietolain vaatimukset on otettu paremmin huomioon kuin jossain pienissä ATK-liikkeissä.</p> |

| | |
|--|--|
| <p>Mitkä tunnistat oheisista sertifikaateista (ISO 9001, ISO 17799, SAS 70, CMM, BSI, WebTrust)?</p> <p>Tiedätkö muita tietoturvasertifikaatteja, jos niin mitä?</p> <p>Mitä sertifikaatteja on organisaatiolla?</p> <p>Onko organisaatiossa suoritettu auditointeja, itsearviointeja tai riskikartoituksia?</p> | <p>Sertifikaattikysymyksellä on tarkoitus selvittää, onko vastaaja kuullut yleensäkin näistä. Jos on, niin onko niitä sovellettu mitenkään ja vaikuttaako vastaajan organisaatioiden hankkimat sertifikaatit mitenkään verrattuna muihin organisaatioihin, jotka eivät ole hankkineet ko. sertifikaatteja.</p> |
|--|--|

4.3 Omistajuus ja tietoturvapoliittikka

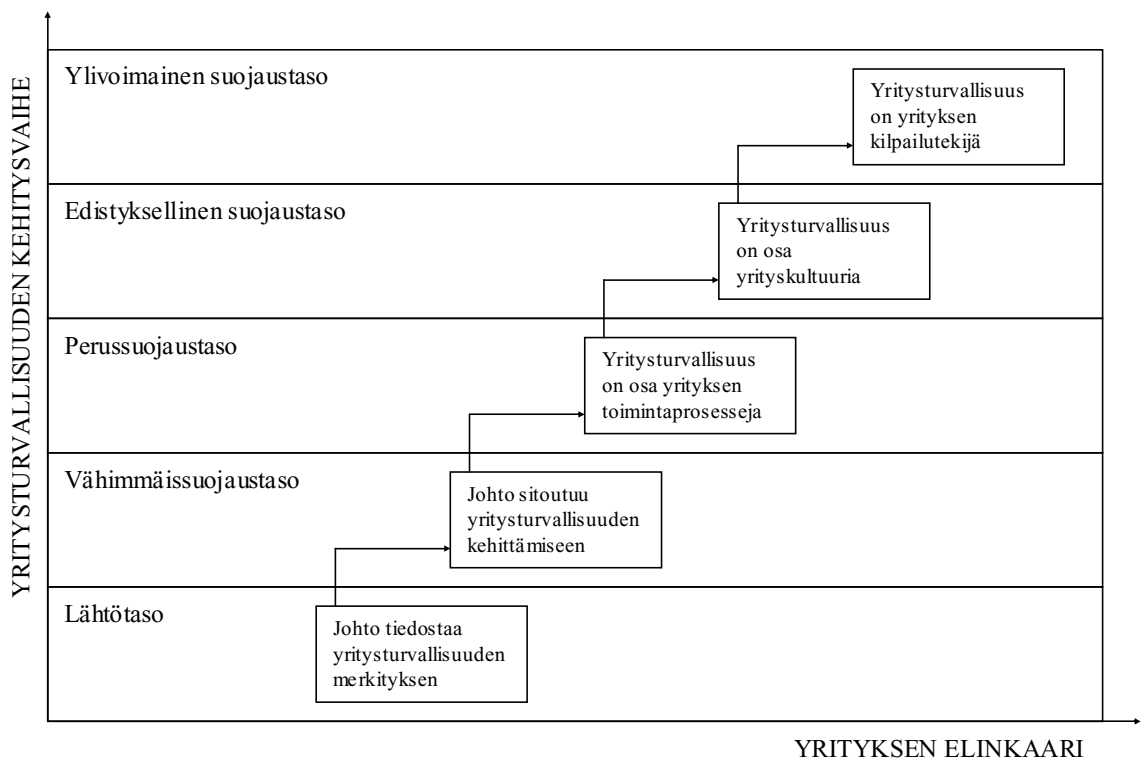
Omistajuutta ja tietoturvapoliittikkaa käsittelevissä kysymyksissä taulukossa 4.2 pyritään selvittämään organisaation yleistä hallinnollisen tietoturvan tasoa ja samalla kartoittamaan mahdollisia puutteita. Lisäksi selvitetään myös haastateltavan yleistä tietoturva-osaamisen tasoa.

Taulukko 4.2: Omistajuutta ja tietoturvapoliittikkaa käsittelevät kysymykset.

| | |
|---|---|
| <p>Onko henkilöitä nimetty tietojen tai tietojärjestelmien vastuuhenkilöiksi (tiedon/järjestelmän omistaja)?</p> <p>Jos on, niin kerro, minkälaisen tietojen/järjestelmien ja mitä toimenpiteitä vastuu edellyttää vastuuhenkilöiltä?</p> <p>Jos ei ole, niin miten tietojen/järjestelmien vastuunjako on toteutettu?</p> | <p>Tiedon omistajan määrittelevä kysymys pohjautuu BS 7799-standardin vaatimuksiin. Standardin mukaisesti sertifioidun yrityksen on määriteltävä omistajat. BS 7799-standardissa ei määritellä, miten omistajuus jaetaan tai mitä omistajan tehtäviin kuuluu. Onkin mielenkiintoista tarkastella tämän kysymyksen vastauksia, koska määrämuotoista soveltamisohjetta ei ole olemassa. Jos omistajuutta koskeviin kysymyksiin saadaan kielteiset vastaukset, niin on todennäköistä, että vastuukysymyksissä on puutteita. Ehkä on myös löydettävissä jokin muu hyvä tapa organisoida vastuukysymykset.</p> |
|---|---|

| | |
|--|--|
| <p>Kuvaile tietoturvallisuuspolitiikkaanne (tavoitteet, onko tavoitteet aikataulutettu, laajuus, onko dokumentoitu?).</p> <p>Onko johto sitoutunut tietoturvapolitiikkaan ja miten sitoutuminen ilmenee?</p> <p>Onko tietoturvapolitiikalla vastuuhenkilöä tai -henkilöitä?</p> <p>Miten valvotaan tietoturvapolitiikan noudattamista?</p> | <p>Tietoturvapolitiikka on johdon kannanotto tietoturvan hoitamiseksi. Siitä ilmenee mm. tiedon omistajat vähintään karkealla tasolla. Poliitikasta eivät ilmene tekniset suojauskeinot, vaan ainoastaan hyväksyty toimintatapa, koska johto ei ole tietoturvan asiantuntija. Muussa tapauksessa tietoturvapolitiikka on tarpeettoman laaja, tärkeät vastuukysymykset hukkuvat nippelitiedon joukkoon, eikä kukaan jaksa lukea nippelitiedon sekamelskaa. Jos johto ei ole sitoutunut laatimaansa politiikkaan, niin voidaan päätellä, että politiikkaa ei monikaan käytännössä noudata. Tällainen politiikka on todennäköisesti laadittu sen vuoksi, että jokin sidosryhmä on sellaista vaatinut. Jos organisaatiossa on tietojen omistaminen jaettu, niin pitää myös muistaa määritellä tietoturvapolitiikan omistaja. Muutoin politiikka jää tulevaisuudessa päivittämättä, jos kukaan ei huolehdi siitä. Johdon on valvottava tietoturvapolitiikan noudattamista ja noudatettava itse sitä. Ellei johto noudata esimerkinomaisesti politiikkaa, viestittää johto käytöksellään tietoturvapolitiikan olevan vain paperi, jolla ei ole sen kummempaa merkitystä.</p> |
| <p>Miksi tietoturvallisuus on tärkeää yrityksessäsi?</p> <p>Miten tietoturvallisuus ilmenee työtehtävissäsi?</p> | <p>Tässä yritetään selvittää millainen mielikuva vastaajalla on organisaation suhtautumisesta tietoturvaan. Ennalta ei voi sanoa, millaisia vastauksia voisi odottaa saavansa, mutta kysymyksen vastauksista voi päätellä, korreloiko organisaation tietoturvamyynteisyys muiden vastauksien kanssa.</p> |
| <p>Miten tietoturvan tekninen ja hallinnollinen näkökulma näkyy organisaatiossasi?</p> <p>Miten tietoturvan tekninen ja hallinnollinen näkökulma näkyy toimenkuvassasi?</p> | <p>Hallinnollisen ja teknisen tietoturvan jaottelukysymyksellä pyritään selvittämään, minkälainen käsitys vastaajalla on näistä kahdesta osa-alueesta ja onko asiaa ajateltu kahtena eri osa-alueena, jotka tosin menevät osittain päällekkäinkin. Vastauksista voisikin ehkä päätellä kumman vastaaja näkee suurempana osa-alueena. Suurempi osa-alue on todennäköisesti se, jota vastaaja itse tekee työkseen.</p> |

| | |
|---|--|
| <p>Onko johto tiedostanut turvallisuuden merkityksen?</p> <p>Jos on, niin:</p> <ul style="list-style-type: none"> • Onko johto sitoutunut turvallisuuden kehittämiseen? • Onko turvallisuus osa yrityksen prosesseja? • Onko turvallisuus osa yrityskulttuuria? • Onko se yrityksen kilpailutekijä? | <p>Seuraava moniosainen kysymys, saattaa vaikuttaa ensilukemalta hieman erikoiselta, varsinkin kun vastaukset ovat muodossa kyllä/ei. Kysymyksellä on kuitenkin ihan tietty tarkoitus, nimittäin Juha Miettisen Yritysturvallisuuden käsikirjassa (2002) on esitetty sivulla 21 kuvassa 4 yritysturvallisuuden kehitysvaiheet yrityksen elinkaaren mukaan. Edellä mainittu löytyy kuvasta 4.1. Organisaatiot voidaan vastauksien perusteella sijoittaa järjestykseen yritysturvallisuuden kehitysvaiheiden mukaan ja katsoa, miten saatu tulos käyttäytyy muiden vastauksien kanssa.</p> |
|---|--|



Kuva 4.1: Organisaation yritysturvallisuuden kehitysvaiheet yrityksen elinkaaren mukaan (Miettinen 2002 s. 21 kuva 4).

4.4 Tietoturvallisuuden kehittäminen

Jotta tietoturvallisuutta voitaisiin kehittää, niin on tutkittava organisaation asenne tietoturvaan yleensä. Kehittämistä kokevissa kysymyksissä (Taulukko 4.3) kerätään tietoa myös organisaation ja sen sidosryhmien nykyisistä tietoturvallisuuden kehitysprosesseista. Lisäksi kartoitetaan organisaation tietoturvakoulutustavat mukaan lukien sidosryhmät.

Taulukko 4.3: Tietoturvallisuuden kehittämistä käsittelevät kysymykset.

| | |
|--|--|
| Miten yrityksessä kehitetään tietoturvaluustietoisuutta eli henkilökunnan asenteita ja motivaatiota tietoturvaluusta kohtaan yhteistyökumppanit ja alihankkijat mukaan lukien? | Tällä kysymyksellä hankitaan tietoa organisaation asenteista, nyt kuitenkin asenteiden muuttumisesta, koska yleensä asenteet ovat esteenä kaiken uuden kehittämiselle. Ihmiset ovat tottuneet rutiineihinsa eivätkä mielellään tee muutoksia, koska uuden kehittäminen vaatii ponnistuksia ja rutiinit tuovat turvallisuudentunnetta, kun työ sujuu lähes ajattelematta. Kehittämisessä ei pidä unohtaa muita sidosryhmiä, esimerkiksi alihankkijoita. Jos sidosryhmien tietoturvan tasoa ei kehitetä vastaavalle tasolle kuin ydinorganisaation, niin päädytään vertauskuvalisesti tilanteeseen, että meillä on ämpäri, joka vuotaa, koska organisaation liityntäpisteet muihin sidosryhmiin on jätetty tarkastelun ulkopuolelle. |
| Miten yrityksessä kehitetään tietämystä tietoturvaluudesta yhteistyökumppanit ja alihankkijat mukaan lukien? | Pelkkä asenteiden muokkaus ei riitä. Tarvitaan myös tietoa ja sen hankkimista, huomioiden myös sidosryhmät. |
| Miten työntekijöitä koulutetaan hallinnolliseen tietoturvaluuteen liittyvissä asioissa yhteistyökumppanit ja alihankkijat mukaan lukien? Miten työntekijöitä koulutetaan tekniseen tietoturvaluuteen liittyvissä asioissa yhteistyökumppanit ja alihankkijat mukaan lukien? | Edellisessä kysymyksessä vastaaja sai vapaasti kertoa tietojen hankkimisesta. Kouluttaminen on eräs tapa hankkia tietoja. Nyt tarkennetaan kysymystä ja jaetaan se hallinnolliseen ja tekniseen osakokonaisuuteen. |

4.5 Osaamisprofiili

Taulukon 4.4 profiilikysymyksissä verrataan Miettisen yritysturvallisuusasiantuntijan profiilia käytäntöön ja kysytään haastateltavan omia tietoturvatiedon hankintatapoja.

Taulukko 4.4: Yritysturvallisuusasiantuntijan profiiliin ja tiedonhankintaan liittyvät kysymykset.

| | |
|--|--|
| <p>Eräässä kirjassa osaamisprofiiliksi määritellään:</p> <ul style="list-style-type: none">ammattillinen peruskoulutusyritysturvallisuus³tietotekniikkakansainvälisyys⁴ihmissuhdetaidottoimialan tuntemus <p>Mikä on oma profiilisi (painota asiat asteikolla 1-5, 1 on vähiten 5 eniten)?</p> <p>Mikä mielestäsi olisi ihanneprofiili (painota asiat asteikolla 1-5, 1 on vähiten 5 eniten)?</p> <p>Mitä olet mieltä tällaisesta jaottelusta?</p> <p>Tuleeko mieleesi muita mahdollisia jaotteluita?</p> | <p>Juha Miettinen esittää kirjassaan Yritysturvallisuuden perusteet (2002) sivulla 80 yritysturvallisuusasiantuntijan osaamisprofiilin. Kysymyksen tarkoituksena on keskustelunavauksena esittää tämä profiili haastateltavalle, pyytää argumentoimaan profiilia ja miettiä, mikä on vastaajaan oma profiili. Tämän kysymyksen perusteella yritetään miettiä myös muita mahdollisia malleja.</p> |
| <p>Miten ja mistä itse hankit tietoa hallinnolliseen tietoturvaluuteen liittyvistä asioista?</p> <p>Miten ja mistä itse hankit tietoa tekniseen tietoturvaluuteen liittyvistä asioista?</p> | <p>Profiilikysymyksellä on sopivasti saatu haastateltava unohtamaan organisaation tiedonhankkimiskysymys. Nyt päästään ikään kuin puhtaalta pöydältä keskittymään haastateltavan henkilökohtaisiin tiedonhankkimistapoihin sekä tekniseltä että hallinnolliselta näkökannalta.</p> |

³ Yritysturvallisuus jakaantuu tässä alakohtiin seuraavasti: turvallisuuden johtaminen, toimitilaturvallisuus, henkilöstöturvallisuus, vakuuttaminen, tietoturvaluuteen, poikkeusoloihin varautuminen, paloturvallisuus, ympäristönsuojelu, ulkomaan toimintojen turvallisuus, matkustusturvallisuus, rikosturvallisuus, työsuojelu, tuotannon turvallisuus.

⁴ Kansainvälisyys jakaantuu tässä alakohtiin seuraavasti: kulttuurien tuntemus, kielitaito, kommunikointi.

4.6 Mielikuva organisaation tietoturvatietoisuudesta

Tässä keskitytään haastateltavan mielipiteeseen organisaationsa ja hänen itsensä tietoturva-osaamisesta taulukon 4.5 kysymysten avulla.

Taulukko 4.5: Haastateltavan omaan mielikuvaan organisaatiostaan liittyvät kysymykset.

| | |
|---|--|
| Tunnetko, että organisaatiossasi tiedetään riittävästi hallinnollisesta tietoturvasta, jos et, niin mitä puuttuu? | Haastateltavilla on yleensä tapana vastata jokaiseen kysymykseen jotakin, mutta ei suinkaan kaikkea oleellista kerralla. Nyt keskitytään kysymään puutteita organisaation tietoturvasta, kun aikaisemmin on kysytty tietoturvan kehityskohteita. Osittain samaan asiaan kohdistuvat viimeiset kysymykset, joilla kartoitetaan lisätiedon kohteita. |
| Tunnetko, että organisaatiossasi tiedetään riittävästi teknisestä tietoturvasta, jos et, niin mitä puuttuu? | |
| Tunnetko, että itse tiedät tarpeeksi hallinnollisesta tietoturvasta tehtäviesi hoitamiseksi, jos et, niin mistä tarvitsisit lisää tietoa? | |
| Tunnetko, että itse tiedät tarpeeksi teknisestä tietoturvasta tehtäviesi hoitamiseksi, jos et, niin mistä tarvitsisit lisää tietoa? | |

4.7 Tietoturvaopetuksen kehittäminen

Kehittämiseen liittyvissä kysymyksissä (Taulukko 4.6) kerätään haastateltavan kehitysehdotuksia tietoturvaopetukseen.

Taulukko 4.6: Tietoturvaopetuksen kehittämiseen liittyvät kysymykset.

| | |
|--|--|
| Mitä asioita on mielestäsi tarpeellista opettaa opiskeluaikana? | Kehittämisosiossa keskitytään pohtimaan tietoturvaopetuksen tarpeellisuutta yleensä. Lopuksi annetaan haastateltavalle mahdollisuus kommentoida tietoturvaa ja haastattelua. |
| Mitä asioita olet joutunut oppimaan tietoturvallisuudesta työelämässä, kun niitä ei ole ollut opiskeluaikaisessa opetuksessa? | |
| Mikä on mielestäsi ammatillisen tietoturvaopetuksen tarkoitus esim. yliopistoissa eli miksi tietoturvakursseja kannattaa järjestää ja kenelle? | |
| Haluaisitko sanoa vielä jotain tästä haastattelusta ja/tai tietoturvasta? | |

5. TUTKIMUSTULOKSET

5.1 *Kyselytutkimuksen suoritus*

Esihaastattelun perusteella joitakin kysymyksiä täsmennettiin ja kyselyä täydennettiin parilla tarkentavalla kysymyksellä. Esihaastatteluun meni aikaa noin 70 minuuttia, joten ajallisesti kysymyksiä tuntui olevan sopiva määrä. Haastattelutilanteissa kysymykset ovat toimineet keskustelun runkona, joten niitä ei ole kysytty jokaiselta haastateltavalta täsmälleen samoin sanoin. Kysymyksiä on muokattu kulloisenkin haastateltavan tarpeen mukaiseksi tarkentavilla lisäkysymyksillä, järjestystä vaihtamalla ja jättämällä tarpeettomia kysymyksiä kokonaan pois. Jotkut haastateltavat halusivat kysymykset luettavaksi ennen haastattelua. Havaitsin, että kysymykset kannattaa lähettää haastateltaville etukäteen, koska useimmat heistä tutustuivat kysymyksiin etukäteen, vaikka eivät niitä pyytäneetkään, ja näin haastatteluun kuluva aika lyheni hieman. Kysymyspaketissa osa kysymyksistä meni päällekkäin. Tämä oli harkittua, koska osa vastaajista ei voinut vastata, jos kysymys oli vastaajan kannalta aseteltu ongelmallisesti.

Kahtatoista potentiaalista haastateltavaa lähestyttiin sähköpostitse pyynnöllä osallistua haastatteluun. Kahdeksan heistä suostui haastateltavaksi. Lisäksi "puskaradion" kautta saatiin neljä haastateltavaa, joista kuitenkin kaksi perui osallistumisensa kiireittensä vuoksi. Kysely suoritettiin syys-lokakuun vaihteessa 2004. Itselleni oli yllätys, että haastateltavien hankinta oli helpompaa kuin olin kuvitellut. Haastatteluun osallistuneet tietoturva-ammattilaiset näyttävät suurelta osin työskentelevän Helsingin Pasilassa, mikä aiheutti jonkin verran aikatauluongelmia, kun yritin saada useamman haastattelun samaksi päiväksi. Aikatauluongelmaksi oli vähällä myös muodostua tulostimen lämpenemisen odottelu eräässä yrityksessä, koska haastattelun edellytyksenä oli salassapitosopimuksen allekirjoittaminen. Aikatauluongelmien vuoksi yksi haastateltava haastateltiin puhelimitse. Tutkimuksen otokseksi muodostui näin kymmenen varsinaista haastateltavaa esihaastattelun lisäksi. Haastattelut kestivät hieman vajaasta tunnista lähes kahteen tuntiin, riippuen siitä, kuinka paljon haastateltavalla oli sanottavaa ja kuinka tiukasti pysyttiin asiassa. Haastatteluista tehtiin muistiinpanoja ja kuusi haastateltavaa salli lisäksi haastattelunsa tallentamisen muistiinpanojen tueksi. Yksi haastattelutalenne tuhoutui tallennettaessa kiintolevyllä, mutta siitä saatiin jälkikäteen pelastettua noin puolet.

5.2 *Kyselyn tulokset*

5.2.1 *Taustatiedot*

Tutkimuksen kannalta merkityksellisiä nykyisiä ja entisiä toimenkuvia olivat: tietoturvakonsultti, tietoturvapääällikkö, projektipääällikkö, tuotepääällikkö, turvallisuuspääällikkö, tekninen asiantuntija, tietoturva-asiantuntija, ATK-pääällikkö,

tietoturvan kouluttaja, toimitusjohtaja, tekninen johtaja, tietohallintojohtaja ja ylläpitäjä. Yhdellä vastaajalla voi siis olla useampia toimenkuvia ja toisaalta haastateltavilla saattoi olla samoja toimenkuvia. Ylivoimaisesti yleisin tutkinto oli diplomi-insinööri. Toisella sijalla olivat filosofian maisteri ja insinööri. Muita tutkintoja olivat ekonomi ja tekniikan ylioppilas. Viisi vastaajaa oli suorittanut tai suorittamassa erilaisia sertifikaatteja. Eräällä haastateltavalla oli peräti viisi ammatillista tutkintoa ja kuudes suorituksen alla. Yksikään haastateltava ei ollut suorittanut tohtorin tutkintoa, mutta seitsemän haastatelluista oli ainakin aloittanut tohtorin tai lisensiaatin opinnot.

Yleisesti opinnoistaan haastateltavat pitivät tarpeellisina tietoja seuraavilta osa-alueilta:

- tietojenkäsittely: tietojärjestelmätieteet, ohjelmistotuotanto, protokollaohjelmointi, tietoliikennetekniikka, tietoliikenneverkot, tietoliikenneprotokollat
- kauppatieteet: liiketaloustieteet, laskentatoimi, johtaminen, yrityksen hallinto
- kielet, erityisesti englanti
- muut: esiintyminen, kommunikointi, fysiikan perusilmiöt, matematiikka, opettaminen, päättelytaito, kokonaisuuksien hallinta, jäsentäminen.

Vähiten tarpeellisina opinnoistaan haastateltavat pitivät kemiaa, tuotantotekniikkaa, matematiikkaa, fysiikkaa, teoreettista sähkötekniikkaa, teollisuustaloutta, markkinointia, ruotsin kieltä ja ohjelmointia. Tästä huomataan, että teollisuustalous, matematiikka ja ohjelmointi näyttävät olevan taitoja, joita on joko tarvittu tai sitten ei, riippuen toimenkuvasta.

Vastaajilla ei juurikaan ole ollut tietoturvallisuutta opinnoissaan, mikä sinänsä on odotettavissa oleva tulos, koska tietoturvallisuus on omana tieteenalanaan hyvin nuori. Esimerkiksi Tampereen teknillisellä yliopistolla (TTY) ensimmäinen kokeiluluontoinen tietoturvan peruskurssitasoinen kurssi järjestettiin syksyllä 1997. Kurssi vakinaistettiin kahden vuoden kuluttua. Tietoturvan sivuaine tuli tarjolle syksyllä 2003. Kuitenkin joillakin vastaajilla on ollut tietoturvan perusteet tasoinen kurssi ja jonkin verran kryptologiaa. Erillinen kryptologian kurssi on ollut jo ennen tietoturvakursseja tarjolla TTY:llä. Jatko-opinnoissaan tai keskeneräisissä perusopinnoissaan haastateltavilla näytti olevan kohtalaisen hyvä tietoturvakurssitarjonta, riippuen oppilaitoksesta. Tietoturvaopinnoistaan haastatellut olivat hyödyntäneet lähes kaiken mitä olivat opiskelleet, koska en saanut vastausta, mitä he olisivat tarvinneet vähiten. Tietoturvaopinnoistaan he olivat tarvinneet eniten:

- tietoliikenne: verkon tietoturva, tietoturvaprotokollat, toimittajien sertifikaattikurssit
- matematiikka: kryptologia

- hallinnollinen tietoturva: liiketoimintakriittisten prosessien suojaaminen, yritysturvallisuus, ihmisten käyttäytyminen, lainsäädäntö, valtionhallinnon VAHTI-ohjeiden (7/2003 s.29) mukainen kahdeksanosainen tietoturvallisuuden jaottelu, tietojen luokittelu, tietoturvaprosessin hallinta.

Haastateltujen työkokemus vaihteli kuudesta kahteenkymmeneenkolmeen vuoteen, keskimääräisen työkokemuksen ollessa kolmetoista vuotta. Tietoturvatehtävien osuus työkokemuksesta vaihteli vuodesta neljääntoista vuoteen, keskimääräisen tietoturvatehtävien osuuden ollessa viisi vuotta. Kaikki haastatellut pitivät yllä tietämystään lukemalla kirjoja. Toinen hyvin yleinen tapa oli kiertää konferensseja/seminaareja ja käyttää niitä verkostoitumisen välineinä. Konferensseissa verkostoituminen oli jopa suuremmassa roolissa kuin itse seminaarien asiat. Toki oli myös henkilöitä, jotka kävivät niissä pelkästään itse asian vuoksi. Todennäköisesti kaikki hankkivat tietoa myös lehdistä, Internetistä, kollegoilta, joukkotiedotusvälineistä, vaikka vain osa vastaajista mainitsi ne. Muita tiedonhankinnan lähteitä olivat tieteelliset artikkelit, erilaiset sähköpostilistat, toimittajien antama tuotekoulutus, erilaiset kurssit ja itseopiskelu. Ainoastaan yksi mainitsi jatko-opiskelun tiedonhankinnan lähteenä, vaikkakin moni oli suorittamassa jatkotutkintoa. Muita vain yhden vastaajan mainitsemia tietolähteitä olivat Tietoturva ry ja Ficora.

Haastateltujen organisaatioiden toimialoina olivat tietoturvan opetus, tietoturvan kaupallinen koulutus, tietoturvan konsultointi, tietoliikennelaitteiden suunnittelu, tietoliikennelaitteiden valmistus, tietoliikenne ja vakuuttaminen. Organisaatioiden henkilömäärä vaihteli viidestä 22300:an keskiarvon ollessa noin 6900. Organisaatioiden henkilömäärän mediaani oli noin 6800. Organisaatioiden henkilömäärässä on huomioitu Suomessa työsuhhteessa oleva henkilöstö.

Kysymykseen, minkälaista tietoa organisaatiossa käsiteltiin tietojen luokittelun näkökulmasta, saatiin vastaukseksi: julkista, organisaation sisäistä, luottamuksellista ja salaista tietoa. Salaiseksi tieto oli määrätty lainsäädännön esimerkiksi henkilötietolain perusteella tai sidosryhmien vaatimuksesta. Salaiset tiedot oli hyvin tiedostettu organisaatioissa. Muiden tietojen luokittelussa joillakin organisaatioilla on parantamisen varaa. Tietoja käsittelevät henkilöt eivät välttämättä tiedä, mihin luokkaan tiedot kuuluvat tai onko tietojen luokitusta muiden kuin salaisten tietojen osalta edes tehty.

Auditointeihin ja sertifikaatteihin liittyvillä kysymyksillä pyrittiin selvittämään tunnistavatko haastateltavat listassa olleita standardeja, ovatko heidän organisaationsa ottaneet niitä käyttöön ja onko heillä tiedossaan muita tietoturvallisuuden mittaamiseen liittyviä menetelmiä. ISO 17799 on sisällöltään sama kuin lähdeluettelossa mainittu tietoturvastandardi BS 7799-1. Tässä mainittu BSI-standardi on sama kuin BS 7799-standardi. SAS 70 (2004) on Statement on Auditing Standards (SAS) No. 70. CMM

(2004) on The Capability Maturity Model for Software. Tulos oli odotetun kaltainen. Joissakin organisaatioissa ei ollut asiasta mitään tietoa, toisissa henkilöt tunnistivat lähes kaikki. Tämän listan ulkopuolelta jokunen haastateltava lisäsi listaan VAHTI-ohjeet. Samoilla lyhenteillä saattoi olla eri merkityksiä. Eräs haastateltava oli sitä mieltä, että BSI on jokin saksalainen kysymyskokoelma, jolla voisi tarkistaa tietoturvan tilan. Kyseinen BSI (2005) on löydettävissä lähdeluettelosta. SAS 70 oli ylivoimaisesti huonoiten tunnistettu ja eräs haastateltava epäili sitä joksikin Statistical Analysis Systemiksi. Statistical Analysis System on hyvin yleisesti käytetty nimitys, joten en pysty jäljittämään tarkasti, mitä hän epäili sen olevan. Seitsemässä organisaatioissa oli tehty auditointeja, riskikartoitusta ja itsearviointeja joko itse tai asiakkaiden tekemänä. WebTrust, ISO 9001 ja ISO 17799 olivat ainoita, mitä vastaan oli hankittu sertifikaatteja. Nämä hankitut sertifikaatit olivat kolmessa eri organisaatioissa Yhdessäkään organisaatioissa ei ollut useampia eri sertifikaatteja käytössä. ISO 17799-standardia oli jossain määrin hyödynnetty parissa organisaatioissa, mutta sen vaatimuksia ei ollut toteutettu.

5.2.2 Omistajuus ja tietoturvapoliittikka

BS 7799-standardi edellyttää tietojen ja tietojärjestelmien vastuuttamista, eli tiedoille ja tietojärjestelmille on nimettävä omistaja, joka vastaa tietojen käsittelystä. Vastuu ei edellytä, että omistajat itse hoitaisivat tietojenkäsittelyn, se sisältää ainoastaan valvontavastuun ja päätöksentekovelvollisuuden. Itse toiminta voidaan ulkoistaa. Kaikissa organisaatioissa oli tietojen omistajuus määritelty jollakin tasolla. Kysymykseen, mitä vastuu edellyttää vastuuhenkilöiltä, BS 7799-standardi ei ota kantaa. Organisaatioissakin asia on osittain määrittelemättä. Osa haastatelluista ei vastannut tähän kysymykseen. Osa organisaatioista oli vasta määrittelemässä tietoturvapoliittikkaansa, joten se vaikuttaa tämän kysymyksen vastauksiin. Vaatimuksia olivat omistajan valvontavastuu, vastuu tietojen oikeellisuudesta, vastuu tietojen lakien ja määräysten mukaisuudesta, vastuu suorittavan portaan ammattitaidosta. Parhaimmissa organisaatioissa omistaja tiesi järjestelmän ominaisuudet, järjestelmä oli dokumentoitu ja omistaja tiesi, mitä järjestelmän ominaisuudet edellyttävät tietoturvalta. Eräässä organisaatioissa omistajuus velvoitti järjestelmän oman tietoturvapoliittikan noudattamiseen, politiikan ylläpitoon, politiikan noudattamisen valvontaan ja politiikan toteuttamiseen.

Tietoturvapoliittikka oli parhaimmissa organisaatioissa toteutettu osapolitiikkoina ja tietoturvapoliittikasta erillisinä toimintasuunnitelmina. Lisäksi oli vielä erilaisia ohjeita, esimerkiksi dokumenttien luokitusohjeet. Parhaimpien organisaatioiden tietoturvadokumentit olivat soveltuvien osin asiakkaiden auditoimia. Suurimmassa osassa organisaatioita oli olemassa dokumentoitu tietoturvapoliittikka ja vuosittainen toimintasuunnitelma. Muiden dokumenttien tila vaihteli hyvin paljon sen mukaan, vaatiiko lainsäädäntö tai asiakkaat niitä. Tässä kohden tutkimukseni antaa mielestäni turhan ruusuisen kuvan. Tutkimukseni hitaimmat organisaatiot olivat aloittaneet kartoituksen, ja niiden dokumentaatioiden arvioidaan valmistuvan vuoden kuluessa. Yllätyksekseni

enemmistö organisaatioiden johdosta oli sitoutunut tietoturvapoliittikkaan noudattamalla sitä ja antamalla riittävät resurssit. Osa vastaajista ei vastannut kysymykseen. Yhden organisaation edustaja valitteli, että riittävät resurssit annetaan vain osittain. Tietoturvapoliittikalla oli kaikissa organisaatioissa jonkinlainen vastuuhenkilö lukuun ottamatta yhtä organisaatiota, josta ei annettu vastausta. Parhaissa organisaatioissa tietoturvapoliittikka oli jaettu osapolitiikkoihin, joilla kullakin oli oma vastuuhenkilönsä. Vastuuhenkilönä oli yleensä tietoturvapääällikkö, tietoturvaryhmä tai johto itse. Tietoturvapoliittikan noudattamista valvottiin yleensä teknisillä keinoilla: lokien analysointi, verkon valvonta tai sosiaalisilla keinoilla: tietoturvapääällikkö valvoo organisaatioita, esimiehet alaisiaan. Myös ulkopuolelta on valvontaa; asiakkaat valvovat organisaatiota, ja yhteiskunta valvoo lakien noudattamista.

Tietoturvallisuuden tärkeys organisaatiossa oli monen tekijän summa. Joillekin yrityksille se oli jopa liiketoimintaedellytys. Muita merkittäviä syitä olivat tiedon eheys, tiedon luottamuksellisuus, tiedon saatavuus, lainsäädännön vaatimukset, sopimuksissa asetetut vaatimukset, resurssien saatavuus, häiriöiden esto, yksityisyyden suoja ja yrityksen imagon vaatimukset. Tähän kysymykseen en saanut kaikilta vastausta. Tietoturvallisuus ilmeni haastateltujen päivittäisissä työtehtävissä oletetusti. Lähes kaikilla oli tietojen luokittelua, ja siitä johtuvia käsittelyrajoituksia. Muita ilmenemismuotoja oli opastaminen tietoturvallisuusasioissa, organisaatioissa salaamattomat yhteydet kielletty, tietoturvallisuusohjeistuksen laatiminen, jatkuvuussuunnittelu, toipumissuunnittelu, tietoturvan ulkoistus, kulunvalvonta, tietoturvateknologian suunnittelu, tietoturvakonsultointi ja auditointi.

Tietoturvan näkyminen organisaatiossa ei eronnut toimenkuvassa muutoin kuin, että hallinnollisen tietoturvan osuus oli 50–100% toimenkuvien työtehtävistä. Tekninen näkökulma näkyi seuraavissa asioissa: tiedon tekninen turvaaminen, lokien automaattinen tarkkailu, käyttäjän tunnistaminen, liikenne rajoitukset palomuuressa, systeemien testaus, nopea reagointi päivityksiin ja tietoturvaratkaisuiden toteuttaminen. Hallinnollinen näkökulma näkyi seuraavasti: tietojen luokittelu, tietoturvan johtaminen, konsultointi, tietoturvakulttuuri, ohjeistus, olla esimerkkinä, asioiden miettiminen ja selvittäminen.

Vastausten perusteella organisaatiot voidaan sijoittaa yritysturvallisuuden kehitysvaiheiden mukaisille portaille organisaation elinkaarivaiheen mukaan. Portaat on esitetty Juha Miettisen Yritysturvallisuuden käsikirjassa (2002) sivulla 21 kuvassa 4 ja tässä työssä kuvassa 4.1. Enemmistö eli neljä organisaatiota arvioi olevansa korkeimmalla tasolla, eli yritysturvallisuus on heille kilpailutekijä. Toiseksi eniten eli kolme kappaletta oli tasojen 3 ja 4 välissä. Muut yksittäiset organisaatiot olivat tasojen 1-2 välissä, tasolla 3, tasolla 4 ja tasojen 4-5 välissä. Keskiarvona organisaatiot olivat yrityskulttuuritasolla, mikä on mielestäni hämmästyttävän hyvä tulos. Tämä johtunee sattumasta, jonka tekee ymmärrettäväksi haastattelujen rajoitettu lukumäärä.

5.2.3 Tietoturvallisuuden kehittäminen

Tietoturvatietoisuutta eli henkilökunnan asenteita ja motivaatiota kehitettiin organisaatioissa sisäisellä koulutuksella, asiakkaiden kanssa keskustelemalla, valvonnalla, ohjeistusta perustelemalla esim. lainsäädännöllä, tarjoamalla tietoisuuksia esim. intranetissä, tiedon saatavuuden keskittämällä yhteen paikkaan häiriötilanteiden varalle ja harrastamalla asioista positiivista kommunikointia.

Kysymys tietoturvatietämyksen kehittämisestä oli ilmeisesti yllättävä, siitä johtuen vaikea vastattavaksi, ja meni osittain edellisen kysymyksen kanssa päällekkäin. Organisaatioissa kehitettiin tietämystä verkostoitumisella, sisäisellä ja ulkoisella koulutuksella, mentoroinnilla, tiedottamisella ja keskustelulla toimittajien kanssa.

Hallinnolliseen ja tekniseen tietoturvaan liittyvissä asioissa työntekijöitä koulutettiin: toimittajakumppanien järjestämällä kursseilla, sisäisellä ja ulkoisella koulutuksella, tulokaskoulutuksella ja jakamalla ohjeistusta. Joissakin organisaatioissa myös tietoturvapääällikkö antoi henkilökohtaista koulutusta. Joissakin organisaatioissa edellytettiin teknisen tietoturvan pitämistä mahdollisimman läpinäkyvänä, jotta käyttäjät eivät tarvitse siihen koulutusta.

5.2.4 Osaamisprofiili

Juha Miittisen kirjassa Yritysturvallisuuden perusteet (2002) sivulla 80 esitetään yritysturvallisuusasiantuntijan osaamisprofiili. Vastajat arvioivat kutakin kohtaa asteikolla 1-5, jossa 1 on huonoin ja 5 paras. Osa vastaajista halusi antaa tarkemman arvion, niinpä joissakin kohdissa on käytetty puolikkaita arvoja. Prosenttiluvut kuvaavat kukin osakokonaisuuden suhdetta muihin osakokonaisuuksiin. Taulukon 5.1 luvuista nähdään, että jokainen osakokonaisuus on lähes yhtä tärkeä sekä omassa että ihanneprofiilissa. Verrattaessa keskiarvoprofiilien prosenttilukuja nähdään, että ihmissuhdetaidot ja toimialan tuntemus ovat sellaisia kokonaisuuksia, joiden toivottaisiin olevan paremmin hallinnassa. Nämä kokonaisuudet kasvattaisivat osuuttaan ammatillisen peruskoulutuksen, tietotekniikan ja kansainvälisyyden kustannuksella. Jos tarkastellaan mediaaniprofiilien prosenttilukuja, niin ihmissuhdetaidot ja toimialan tuntemus käyttäytyvät päinvastaisesti verrattuna keskiarvoihin. Prosenteissa tietotekniikan osuus pysyy mediaaniprofiileissa samana, vaikka keskiarvoprofiileissa sen osuus pieneni. Yritysturvallisuus kasvattaa mediaaniprofiileissa prosenttiosuuttaan, vaikka keskiarvoprofiileissa se pysyi samana. Tuloksista voidaan päätellä, että mallin laatija on onnistunut laatimaan ainakin keskimääräisesti toimivan profiilin.

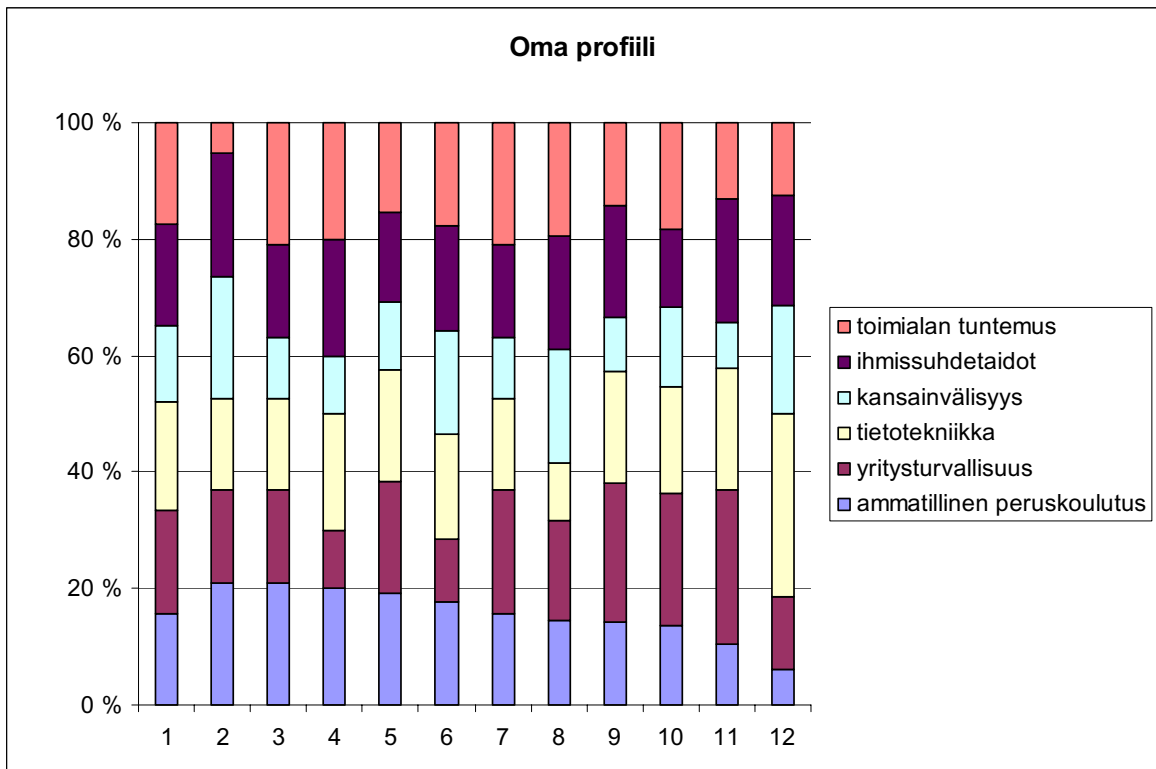
Taulukko 5.1: Osaamisprofiilit.

| Keskiarvo omista profiileista | Keskiarvo ihanneprofiileista | Mediaani omista profiileista | Mediaani ihanneprofiileista | |
|-------------------------------|------------------------------|------------------------------|-----------------------------|-----------------------------------|
| 3,4 (16 %) | 3,3 (15 %) | 3,0 (14 %) | 3,0 (14 %) | ammattillinen peruskoulutus |
| 3,7 (18 %) | 3,9 (18 %) | 3,5 (16 %) | 4,0 (18 %) | yrittäjäturvallisuus ⁵ |
| 3,8 (18 %) | 3,6 (17 %) | 4,0 (18 %) | 4,0 (18 %) | tietotekniikka |
| 2,9 (14 %) | 2,8 (13 %) | 3,0 (14 %) | 3,0 (14 %) | kansainvälisyys ⁶ |
| 3,7 (18 %) | 4,0 (19 %) | 4,0 (19 %) | 4,0 (18 %) | ihmissuhdetaidot |
| 3,4 (16 %) | 3,8 (18 %) | 4,0 (19 %) | 4,0 (18 %) | toimialan tuntemus |

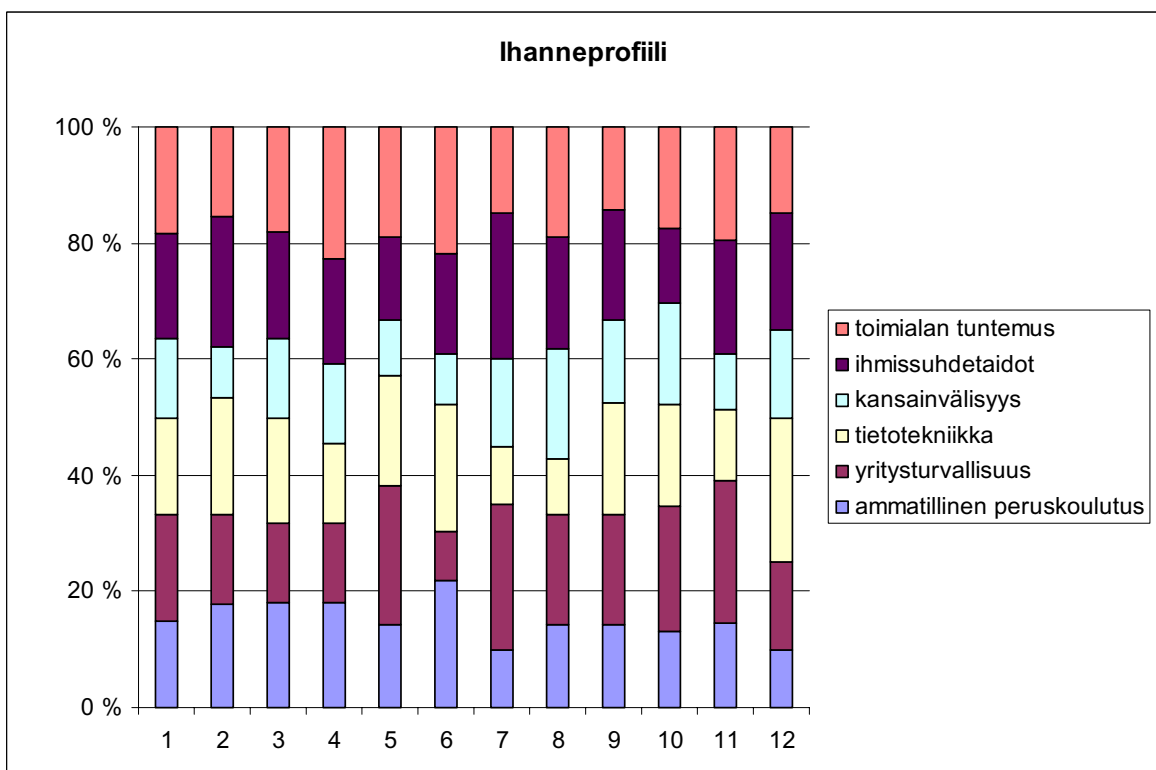
Profiilikuvista 5.1 ja 5.2 voidaan tarkastella yksittäisten haastateltavien profiilien eroavaisuuksia. Numerot 2-12 kuvaavat haastateltuja, ja 1 on taulukossa 5.1 tarkemmin käsitelty keskiarvo. Molemmassa kuvissa samat numerot vastaavat samaa haastateltavaa, joten on mahdollista verrata saman henkilön omaa ja ihanneprofiilia keskenään. Yksittäisissä vastauksissa on nähtävissä eroavaisuuksia oman profiilin ja ihanneprofiilin välillä toisin kuin keskiarvoprofiileissa. Tähän profiilimalliin haastateltavat kaipasivat täydennyksenä tuoteturvallisuutta, tuotteitten vikasietoisuutta, ohjelmointiturvallisuutta, lainsäädäntöä ja paineensietoa. Haastateltavat muokkasivat mallia jakamalla tietotekniikan tietotekniikkaan ja muuhun menetelmäosaamiseen sekä eriyttämällä toimialan tuntemuksen alaotsikoksi uhkamallinnuksen. Kansainvälisyysotsikosta oltiin useampaa mieltä. Eräs haastateltava olisi halunnut nostaa kansainvälisyyden alakohdat muiden pääkohtien rinnalle. Toinen puolestaan olisi halunnut yhdistää kansainvälisyyden ja ihmissuhdetaidot. Eräs taas olisi halunnut jaon kuuteentoista pääkohtaan. Yksi haastateltava esitti kysymyksen, miten ammattillinen peruskoulutus ja yrittäjäturvallisuus liittyvät tietoturvasuoritusasiantuntijan tehtäviin. Tämä kommentti on ymmärrettävä, sillä vastaaja ei tiennyt haastattelutilanteessa mallin oikeasti olevan yrittäjäturvallisuusasiantuntijan osaamisprofiilin.

⁵ Yrittäjäturvallisuus jakaantuu tässä alakohtiin seuraavasti: turvallisuuden johtaminen, toimitilaturvallisuus, henkilöstöturvallisuus, vakuuttaminen, tietoturvasuoritus, poikkeusoloihin varautuminen, paloturvallisuus, ympäristönsuojelu, ulkomaan toimintojen turvallisuus, matkustusturvallisuus, rikosturvallisuus, työsuojelu, tuotannon turvallisuus.

⁶ Kansainvälisyys jakaantuu tässä alakohtiin seuraavasti: kulttuurien tuntemus, kielitaito, kommunikointi.



Kuva 5.1: Haastateltujen omat profiilit.



Kuva 5.2: Haastateltujen ihanneprofiilit.

Haastatellut hankkivat tietoa hallinnollisesta ja teknisestä tietoturvasta samaan tapaan, kuin aiemmin kysymyksessä tiedonhankintatavat opiskelun jälkeen. Poikkeuksena oli kuitenkin se, että teknistä tietoturvaa haettiin tuotekohtaisilta kursseilta enemmän kuin hallinnollista tietoturvaa, ja tietoturvaan hankittiin tietoja VAHTI-ohjeista, lainsäädännöstä ja standardeista, mitä ei mainittu yleisen tiedonhankinnan lähteinä.

5.2.5 Mielikuva organisaation tietoturvatietoisuudesta

Viisi vastaajaa oli sitä mieltä, että hänen organisaatiossaan tiedetään riittävästi hallinnollisesta tietoturvasta. Viisi taas tunsu, että organisaatiolla olisi tarvetta lisätietoon. Yhdellä vastaajista ei ollut selvää mielikuvaa. Puutteita organisaatioissa oli lainsäädännön tietämyksessä ja vastuukysymyksien jakamisessa. Vastuiden jakamisen erityisenä ongelmana oli, että ihmiset eivät ymmärrä olevansa vastuussa tietoturvasta omalta osaltaan. Myös tietojen luokittelussa oli puutteita. Yleinen ongelma oli, että organisaation jäsenet eivät ymmärrä, mihin kaikkeen tietoturva liittyy, erityisesti tietotekniikan loppukäyttäjät, joiden tietotaidosta puuttuu tietoturvan peruskäsitteistö. Teknisestä tietoturvasta tiedettiin vastaajien mielestä riittävästi neljässä organisaatiossa, kehittämisen varaa oli seitsemässä organisaatiossa. Ero hallinnollisen ja teknisen turvallisuuden tietämyksessä selittyy todennäköisesti sillä, että teknisen tietoturvan puutteet on helpompi havaita, ja ne ovat helpommin mielletävissä, esimerkiksi virustorjuntaohjelmat ovat asennettuna ja toimivat. Jos taas tutkitaan toipumissuunnitelmaa, niin se voi näyttää toimivalta, ja vasta tositalanteessa huomataan kaikki mahdolliset puutteet. Organisaatioiden teknisessä tietoturvallisuudessa kehitystarpeita oli uhkamallinnuksessa, ohjelmistoarkkitehtuurien suunnittelussa, turvallisuuden huomioinnissa kehitettäessä tuotteita, loppukäyttäjien tietämyksen tasossa, verkkotekniikan perusteiden tuntemuksessa, kokonaisnäkemyksessä tietoturvasta ja uusissa asioissa. Lisäksi välinpitämättömyyttä esiintyi liikaa.

Seitsemässä tapauksessa organisaation ja haastatellun tietoisuus tai tietämättömyys hallinnollisesta tietoturvasta olivat yhteneviä. Yhdeksän haastelluista tiesi mielestään tarpeeksi hallinnollisesta tietoturvasta tehtäviensä hoitamiseksi, yksi tarvitsisi lisää tietoa ja yksi ei osannut sanoa. Haastatellut tarvitsisivat lisää tietoa jatkuvuussuunnittelun käytännön toteutuksesta, sertifiointista, riskienhallinnasta, tietoturvan johtamisesta ja ylläpidosta. Teknisen tietoturvan osalta haastatellun ja organisaation tietoisuus tai tietämättömyys oli yhtenevä viidessä tapauksessa. Näillä vastaajilla ja organisaatioilla olivat yhtenäiset käsitykset myös hallinnollisella tietoturvan osa-alueella. Kahdeksan henkilöä tunsu tietävänsä teknisestä tietoturvasta riittävästi tehtäviensä hoitamiseksi, kolmella oli mielestään tarvetta lisäkoulutukseen. Lisätiedon tarpeita oli ASIC-suunnittelussa, kryptografiassa, VPN-sertifikaateissa, verkkotietoturvassa, WWW-sovellusten tietoturvassa, lokien analysoinnissa, tunkeutumisen havainnoinnissa, sovelluskohtaisissa palomuuereissa ja protokollaturvallisuudessa.

5.2.6 Tietoturvaopetuksen kehittäminen

Kysymykseen, mitä on tarpeellista opettaa opiskeluaikana, saatiin vastaukseksi mm. seuraavia asioita. Tietoturvallisuudesta kaivattiin tietoa peruseriaateista, käsitteistöstä ja termistöstä. Käytännön kokemusta ja näkemystä, mihin kaikkeen tietoturva liittyy, olisi myös hyvä olla. Samoin pitäisi tietää, mitä vaatimuksia tietty teknologia aiheuttaa tietoturvalle ja miten ne ratkaistaan. Teknisestä tietoturvasta kaivattiin ymmärtämystä tekniikoista ja teknologioista. Erityisesti haluttiin tietää, mitä niillä saavutetaan ja miksi. Pienempiä kaivattuja teknisiä kokonaisuuksia olivat uhka-analyysit, tietoturva-arkkitehtuurit, verkkoteknologiat, TCP/IP heikkoudet ja vahvuudet, kryptologia ja oman työaseman suojaus. Hallinnollisesta tietoturvasta kaivattiin erityisesti tiedon luokittelun periaatteita: luottamuksellisuus ja tiedon arvottaminen. Lisäksi kaivattiin hallinnollisen tietoturvan peruseriaatteita, tietoturvastandardien sisällön esittelyä, lainsäädäntöä, normeja, kokonaisvaltaista yritysturvallisuutta, ja erityisesti tietojohtajille pitäisi olla hallinnollisen tietoturvan koulutusta. Haastateltavien kaipaamia asioita olivat myös matematiikka, englannin kieli ja ohjelmointikieli perl, prosessiajattelu, tiedon jäsentäminen, laajempien kokonaisuuksien hahmottaminen, tiedonhaku, ongelmanratkaisutaito ja asenteiden muokkaus, ts. turvallinen toiminta on laadukasta.

Vastaajat kertoivat joutuneensa opiskelemaan työelämässä alla olevia asioita, koska niitä ei sisällynyt opiskeluaikaisiin opintoihin. Teknisen tietoturvan alueelta haastatellut olivat opiskelleet TCP/IP:tä yleisesti, heikkouksien hyödyntämiseltä suojautumista, ylläpitoa yleensä, kryptologiaa, protokollaturvallisuutta. Hallinnollisen tietoturvan alueelta opiskelujen kohteena oli ollut hallinnollinen tietoturva yleensä, käytännön yhteensovittaminen tietoturvastandardeihin, tiedon luokittelu, riskianalyysi, lait ja käytännöt ja tietoturvan johtaminen. Ohjelmoinnin alueelta oli opiskeltu ohjelmistoturvallisuutta ohjelmistoprojekteissa ja uhka-analyysin tekemistä ohjelmiston määrittelydokumentille. Muita opiskeltuja asioita oli tietoturvan liittyminen kaikkeen toimintaan, ihmissuhdetaidot, kommunikointi, viestintä, tietoturvaongelmasta tiedottaminen työyhteisössä ja sen korjaamisen aiheuttama työmäärän lisääntyminen.

Yleisesti ammatillisen tietoturvaopetuksen tarkoituksena haastateltavien mielestä oli antaa valmiudet työelämään, opettaa kriittiseksi tiedon todenperäisyydelle, antaa kokonaiskuva tietoturvasta, opettaa hallitsemaan tietoturvallisuuden osa-alueet ja niihin liittyvät ongelmat. Ammatillisen tietoturvaopetuksen tuloksena pitäisi tulla osaavia ihmisiä puolustamaan tietojärjestelmiä, ja teknisten ihmisten pitäisi osata tehdä tietojärjestelmät läpinäkyviksi käyttäjille. Haastateltavien mielestä tietoturvan perusteiden ja tietojen luokittelun pitäisi olla osana kaikkien opiskelijoiden opintoja. Teknisen tietoturvan osa-alueelta nähtiin tarkoituksenmukaiseksi yleisen teknisen osaamisen opettaminen perusteellisesti, uhkamallien opettaminen, palomuurien toiminnan opettaminen ja haittaohjelmilta suojautumisen opettaminen. Hallinnollisen tietoturvan osa-alueelta tärkeätä olisi opettaa, kuinka ohjeistetaan tietoturva organisaatiossa ja tietoturvan

perusdokumenttien toteutus. Perusdokumentit tässä yhteydessä ovat tietoturvapoliittikka, tietoturvasuunnitelma, jatkuvuussuunnitelma, toipumissuunnitelma ja ohjeistus käyttäjille. Organisaation johtajien pitäisi perehtyä myös hallinnolliseen tietoturvaan, vaikka organisaatiossa onkin oma asiantuntijansa tätä varten. Johdon pitäisi olla perillä esimerkiksi matkustusturvallisuudesta ja turvata näin avainhenkilöstönsä. Ohjelmoinnin alueelta tietoturvaopetuksessa pitäisi opettaa turvallista ohjelmointia, turva-arkkitehtuureja ja ymmärtämystä, mitä ohjelmakoodi todellisuudessa tekee. Haastateltujen mielestä ohjelmistojen koodausturvallisuuden pitäisi olla osana kursseja eikä erillisinä kursseina. Opetustavan suhteen haasteltavat toivoivat tietoturva-asioita osaksi muita kursseja, jotta asia tulisi opiskeltua aidoissa tilanteissa. Muita toivomuksia opetuksen suhteen olivat: uusien tutkimustulosten hyödyntäminen, teknisen nippelitiedon poisjättäminen ja oikeita ammattilaisia opettamassa kirjatiedon lisäksi. Eräs haastateltava laati oman ehdotuksensa opetuskokonaisuuden muotoon. Se sisältää seuraavat kokonaisuudet: miten käytät Internetiä turvallisesti, tietoturvan perusasiat, TCP/IP, hallinnollisen tietoturvan perusteet, VPN-liikenteen analyysin perusteet ja portti-skannauksen.

Muita haastateltavien kommentteja olivat seuraavat: Työväenopistoon tai avoimen yliopiston pitäisi järjestää kurssi tietoturvan perusteista. Onko tietoturva ongelma? Epäsuorat vahingot ovat suuria, mutta niitä voidaan vähentää palokuorman minimoinnilla. Palokuorman minimoinnilla tarkoitetaan tässä tapauksessa resurssien ja tietojen suojaamista siten, että vahingon sattuessa mahdollisimman pieni osa tiedoista tai resursseista altistuu. Erään haastateltavan mielestä VAHTI-ohjeiden (7/2003 s.29) mukainen kahdeksanosainen tietoturvallisuuden jaottelu on tarpeettoman laaja. Niinpä hän ehdotti tietoturvan jakamista neljään osa-alueeseen:

1. loogiseen eli ohjelmistolliseen
2. fyysiseen
3. ylläpidolliseen
4. hallinnolliseen.

Erään haastateltavan mielestä turvallisuusopetuksen laatuun pitää panostaa enemmän kuin nyt tehdään. Opettamassa pitää olla oikeita ammattilaisia eikä pelkkiä kirjoista oppineita. Lisäksi opetettavan tiedon pitää olla ajantasaista syvällistä tietoa, ei nippelitietoa.

6. TULOSTEN TARKASTELU

6.1 *Erlaisia tietoturva-ammattilaisten profiileita*

Profiileihin on koottu tyypillisiksi katsomiani ominaisuuksia ja eroja toisiin profiileihin. Profiilit on laadittu haastatteluvastausten perusteella. Kaikkien haastateltujen vastauksia ei ole käytetty alla olevien profiilien muodostamiseen pois lukien yleinen profiili. Yhden profiilin muodostamiseen on käytetty 2-4 henkilön vastauksia lukuun ottamatta yleistä profiilia. Yksittäisen vastaajan muodostamia profiiliryhmiä en ole muodostanut, koska tyypillisiksi katsottavat ominaisuudet riippuisivat liiaksi haasteltavan persoonasta, eikä se antaisi missään suhteessa objektiivista kuvaa edustamastaan ryhmästä. Tosin näihinkin ominaisuuksiin on syytä suhtautua varauksella otoksen pienuuden vuoksi. Esimerkiksi tietoturvakonsultin koulutustaustaan tulisi useampia vaihtoehtoja, jos olisin haastatellut vaikkapa sataa eri tietoturvakonsulttia.

Tietoturvakonsultti konsultoi asiakkaita teknisestä ja hallinnollisesta tietoturvasta. Hän myy asiakkaille konsultointia ja teknisiä ratkaisuja sekä suorittaa auditointeja ja riskikartoituksia. Hän osaa soveltaa ISO 17799-standardia ja tunnistaa useita eri tietoturvastandardeja vähintäänkin nimeltä. Tietoturvakonsultti voi työskennellä suurissa tai hyvinkin pienissä yrityksissä. Pienen yrityksen ollessa kyseessä se on yleensä konsulttiyritys. Konsultin työskentelyorganisaatio on yleensä sitoutunut tietoturvapolitiikan kehittämiseen ja noudattamiseen, koska se on liiketoimintaedellytys. Koulutustaustana on diplomi-insinööri tai insinööri ja mahdollisesti lisäksi suoritettu CISSP-sertifikaatti. Työkokemusta on noin 16 vuotta, josta tietoturvatehtävissä noin kuusi vuotta. Tietoturvakonsultit ovat tarvinneet työtehtävissään mm. seuraavia asioita: tietoturva, tietoliikennetekniikka, verkot ja protokollat. Lisätiedon tarpeena heillä on lainsäädäntöön ja sertifiointiin liittyvät asiat. Opiskeluaikana heidän mielestään on tarpeellista opiskella tietoturvan peruskäsitteet, ajattelumalli ja teknologioiden ymmärtäminen.

Tuotepäällikkö toimii projektipäällikkönä yrityksen tai asiakasyrityksen tuoteprojekteissa. Tuotteet voivat olla ohjelmistoja, laitteita tai näiden yhdistelmiä. Projektien erilaisuudesta johtuen hän saattaa olla myös ohjelmistotuotannon ammattilainen. Tuotepäällikkö tunnistaa useita eri tietoturvastandardeja ainakin nimeltä. Hän työskentelee tietoliikennealan suuryrityksissä. Työskentely-yritysten tietoturvaorganisaatio ja projektien omistajat ovat sitoutuneet tietoturvapolitiikan kehittämiseen ja noudattamiseen, koska se on asiakasvaatimus. Koulutustaustana on diplomi-insinööri tai filosofian maisteri ohjelmistotekniikan, tietoliikennetekniikan tai kryptologian alalta. Työkokemusta on noin kahdeksan vuotta, josta tietoturvatehtävissä noin viisi vuotta. Tuotepäälliköt ovat tarvinneet työtehtävissään mm. seuraavia asioita: tietoliikennetekniikka, protokollaohjelmointi, kokonaisuuksien hallinta, systemaattisuus ja

kryptologia. Erityisvaatimuksina tähän tehtävään on tuoteturvallisuuden ja vikasietoisuuden osaaminen. Lisätiedon tarpeena on uhkamallinnus, tietoturva-arkkitehtuurit, ASIC-suunnittelu, kryptografia ja protokollaturvallisuus. Opiskeluaikana heidän mielestään on tarpeellista opiskella teknistä tietoturvaa ja hankkia peruskäsitys hallinnollisesta turvallisuudesta. Lisäksi on opiskeltava perusasiat IPSEC:stä, palomuureista, koodausturvallisuudesta, uhka-analyysista erityisesti määrittelydokumentille, kryptologiasta, protokollaturvallisuudesta ja tietoturva-arkkitehtuureista.

Organisaation **tietoturvapääällikkö** on erityisesti hallinnollisen tietoturvan erityisasiantuntija. Hän kouluttaa organisaation omaa ja yhteistyökumppaneiden henkilökuntaa hallinnollisissa tietoturva-asioissa. Tietoturvapääällikkö tunnistaa useita eri tietoturvastandardeja vähintäänkin nimeltä. Hänen työskentelyorganisaationsa ovat hyvin erikokoisia, pois lukien pienyritykset. Tietoturvapääällikköiden organisaatiot ovat sitoutuneet tietoturvapoliittikan kehittämiseen ja noudattamiseen, koska se on yleensä lainsäädännön vaatimus. Koulutustaustana on insinööri tai ekonomi. Työkokemusta on noin 12 vuotta, josta tietoturvatehtävissä noin neljä vuotta. Tietoturvapääälliköt ovat tarvinneet työtehtävissään mm. liiketaloustieteitä, laskentatointa, johtamista, tietojärjestelmätieteitä, kielitaitoa, esiintymistaitoa, yritysturvallisuuden tuntemusta, hallinnollista tietoturva-osaamista, lainsäädännön tuntemusta ja psykologin taitoja. Lisätiedon tarpeena tietoturvapääälliköillä on lokien analysoinnin ja jatkuvuussuunnittelun käytännön toteuttaminen organisaatiossa. Teknisestä tietoturvasta kaipaavat lisätieto lähinnä sellaiset henkilöt, joiden aikaisempi koulutus ei ole ollut teknisesti suuntautunutta. Opiskeluaikana heidän mielestään on tarpeellista opiskella hallinnollisen ja teknisen tietoturvan perusteet, yleiskatsaus tietoturvastandardeihin, tietojärjestelmien suojaamisen tarpeet eli järjestelmien arvottaminen, yritysturvallisuus, TCP/IP:n heikkoudet ja vahvuudet, verkkoteknologiat, englannin kieli, ihmissuhdetaidot, kommunikointi ja viestintä.

6.2 Tietoturva-ammattilaisten profiili yleisesti

Tietoturvatehtäväkenttä oli kyselyni ammattilaisilla laaja-alainen painottuen kuitenkin enemmän hallinnollisen tietoturvan alueelle. Tutkimuksessa tärkeimpiä mukana olleita toimenkuvia olivat tietoturvakonsultti, tuotepääällikkö, tietoturvapääällikkö, turvallisuuspääällikkö, tekninen asiantuntija, tietoturva-asiantuntija ja tietoturvan kouluttaja. Koulutustaustana yleisin oli akateeminen loppututkinto. Akateemisista loppututkinnoista yleisin oli diplomi-insinööri. Työkokemusta ammattilaisella oli keskimäärin 13 vuotta, josta tietoturvatehtävien osuus noin viisi vuotta. Nykyisestä tehtäväkuvasta riippuen opinnoista hyödyllisiksi koetut tiedot liittyivät joko tietoliikennetekniikkaan tai liiketaloustieteisiin. Hyödyttömiä opintoja ei käytännössä ollut, vaikka useammassa kuin yhdessä vastauksessa turhaksi mainittiin kemia. Varsinaisia tietoturvaluopintoja ammattilaisilla ei ole juurikaan ollut. Työelämässä heillä on ollut

toimenkuvaansa liittyviä muutaman päivän kestäviä kursseja, jotka ovat enimmäkseen liittyneet johonkin tuotteeseen. Tietoja ammattilaiset hankkivat lukemalla kirjoja, osallistumalla seminaareihin, verkostoitumalla, Internetistä, joukkotiedotusvälineistä, tieteellisistä julkaisuista ja kursseilta. Hallinnolliseen tietoturvaan haettiin lisäksi tietoja VAHTI-ohjeista, lainsäädännöstä ja standardeista. Tietoturvastandardeihin ammattilaiset ovat tutustuneet, mutta eivät yleensä tarkemmin perehtyneet.

Tietoturva-ammattilaisen osaamisen kehityskohteita hallinnollisen tietoturvan puolella ovat lainsäädännön tietämys, tietoturvasertifiointi, jatkuvuussuunnittelun käytännön toteutus, riskienhallinta, tietoturva-asioiden vastuunjaon toteutus, tietojen luokittelun käytännön toteuttaminen ja tietoturvan johtaminen. Teknisen tietoturvan puolella kehityskohteita ovat uhkamallinnus, ohjelmistoarkkitehtuurien suunnittelu, turvallisuuden huomiointi jo tuotesuunnittelussa, kryptografia, VPN-sertifikaatit, tietoverkkojen tietoturva, WWW-sovellusten tietoturva, lokien analysointi, tunkeutumisen havainnointi, sovelluskohtaiset palomuurit ja protokollaturvallisuus. Tärkeää on myös saada kokonaisnäkemys tietoturvasta. Opiskeluajankaisessa opetuksessa nähtiin tarpeelliseksi opettaa kaikille, ei siis pelkästään ammattilaisille, tietoturvallisuuden perusperiaatteet, käsitteistö, termistö, tiedon luokittelun periaatteet, peruskäsitys hallinnollisesta tietoturvallisuudesta, oman koneen suojaus haittaohjelmilta ja tietoturvan huomioiminen päivittäisessä työskentelyssä.

Varsinainen haaste tietoturva-ammattilaisen opetuksessa on, miten saada aikaiseksi ”tuote” eli tietoturva-ammattilainen, jolla on käytännön kokemusta ja näkemystä siitä missä kaikkialla tietoturva pitää ottaa huomioon, ja mitä vaatimuksia tekniikka ja teknologiat aiheuttavat tietoturvalle. Lisäksi ammattilaisen pitäisi pystyä ratkaisemaan tekniikan ja tietoturvan yhteensovittaminen siten, että jatkokehitys tulevaisuudessa on suoraviivaista ts. ei pakota suunnittelemaan koko järjestelmää uudestaan. Haastattelemieni tietoturva-ammattilaisten näkemysten perusteella heidän pitäisi hallita hallinnollisen tietoturvan osa-alueelta tietoturvadokumentit, joihin kuuluvat tietoturvapoliittikka, tietoturvasuunnitelma, jatkuvuussuunnitelma, toipumissuunnitelma ja ohjeistus käyttäjille. Lisäksi tulisi tietää, mitä tietoturvastandardit pitävät sisällään, osata sovittaa käytännön toiminta tietoturvastandardien vaatimuksiin, hallita lainsäädännön velvoitteet, toimia yleisten normien mukaan, ymmärtää yritysturvallisuus kokonaisvaltaisesti organisaation kannalta, toteuttaa riskianalyysi, hallita tiedon luokittelun periaatteet, erityisesti luottamuksellisuus ja tiedon arvottaminen. Teknisestä tietoturvasta puolestaan tarvittaisiin prosessiajattelumalli, ohjelmistoturvallisuuden näkökulman huomioiminen ohjelmistoprojekteissa, koodausturvallisuus osana suunnittelua, turvalliset tietojärjestelmäarkkitehtuurit, uhka-analyyseja jo määrittelydokumentille, tietoliikennettä, verkkoteknologioita, protokollaturvallisuutta, TCP/IP:tä ja kryptologiaa. Lisäksi odotetaan yleisiä taitoja, kuten keneltä tahansa ammattilaiselta: tiedon jäsentäminen, tiedonhaku, ongelmanratkaisutaito, englannin kieli, kokonaisuuksien hallinta, ihmissuhdetaidot, kommunikointi ja viestintä.

6.3 *Profiilien vertailu teoriaan*

Seuraavassa verrataan kohdassa 6.1 muodostamiani tietoturvakonsultin, tuotepäällikön ja tietoturvapäällikön profiileita kirjallisuudessa esitettyihin.

Miettisen (2002) määrittelemistä asiantuntijaprofiileista erikoisasiantuntija sopii parhaiten **tietoturvakonsultin** määritelmään. Tietoturvakonsultista löytyy lisäksi piirteitä esimiehen ja johtajan tehtäväkentistä. Koulutustausta sopii näihin kaikkiin. Erikoisasiantuntijan erityisosaamisalueena on yhden tai useamman yritysturvallisuuden osa-alueen erityisosaaminen. Mannisen (16.3.2004) tietoturva-ammattilaisprofiileista konsultit kuuluvat asiantuntemukseltaan tietoturvallisuuden johdon muodostamaan ryhmään, vaikkakin organisaation ulkopuoliset tietoturvakonsultit konsultoivat juuri tietoturvallisuuden johtoa ja organisaation ylintä johtoa. Tietoturvallisuuden johdon toimenkuva määrittelee tehtäväksi tietoturvallisuuden käytännön toteutuksen ja kehityksen asiantuntijuuden, joka on konsulttien toimenkuva. Wadlowin (2001) mallissa tietoturvakonsultin toimenkuva vastaa lähes sisäisen auditoijan toimenkuvaa. Tietoturvakonsulttihan voi olla myös organisaation sisäinen konsultti. Sisäisen auditoijan toimenkuvaan kuuluvat järjestelmien auditointi, suunnittelu ja suunnitelmien toteuttamisen johtaminen. Whitmannin & Mattordin (2005) luokittelussa tietoturvakonsultit sijoittuvat tietoturvajohtajien kategoriaan koulutukseltaan ja toimenkuviltaan, vaikkakaan organisaation ulkoinen konsultti ei tietenkään hoida johtajille yleisesti kuuluvia talousasioita. Tietoturvajohtajien toimenkuvaan kuuluu riskienhallinnan ja tietoturvaohjeistuksen kehittäminen. Tietoturvaprojektiryhmässä konsultit ovat tietoturvapoliittikan suunnittelijoita, riskienhallinnan asiantuntijoita tai tietoturva-asiantuntijoita. Jatkuvuussuunnitelman suunnitteluryhmässä ulkoiset konsultit ovat asiantuntijoina. VAHTI 1/2001-ohjeessa ulkoiset konsultit muodostavat oman asiantuntijaryhmänsä ja konsultoivat lähinnä muita ryhmiä valtionhallinnon yleisohjeistuksen mukaisissa tietoturva-asioissa. Sisäisinä konsultteina toimiessaan he kuuluvat VAHTI-ohjeiden 7/2003 & 1/2001 mukaan ryhmään tietoturva-asiantuntijat. Tässä ryhmässä toimiessaan he avustavat tietoturvan kehittämisessä, toimivat asiantuntijoina, järjestävät turvallisuuden seurannan ja informoivat johtoa.

Miettisen (2002) malleista päällikkö sopii **tuotepäällikön** kuvaukseen parhaiten. Kuvauksen mukaisesti hän vastaa ryhmän esimiehenä ryhmän toiminnanohjauksesta. Luomassani tuotepäällikön profiilissa en ole rajoittunut pelkästään yritysturvallisuuteen kuten Miettinen on tehnyt. Mannisen (16.3.2004) suuren organisaation tietoturvan mallissa tuotepäällikköä ei vastaa mikään, mikä on ymmärrettävää, koska mallissa kuvattu organisaatio on lähinnä viranomaisorganisaatio, joka ei valmista mitään tuotetta. Wadlowin (2001) tehtävistä kehityspäällikkö, joka toimii kehitysinsinöörin päällikkönä, sopii parhaiten tuotepäällikön kuvaukseen. Kehityspäällikön tehtävänä on koordinoita kehitysprojekteja turva-arkkitehdin kanssa. Whitmannin & Mattordin (2005) tietoturvaprojektiryhmästä ja jatkuvuussuunnitteluryhmästä löytyvä projektiryhmän

johtaja sopii tuotepäällikön kuvaukseen. Tuotepäällikköhän on kuvauksessani projektipäällikkö. VAHTI-ohjeiden 7/2003 & 1/2001 mukaisesti tuotepäällikkö voidaan sijoittaa esimiehen rooliin. Perustelu on sama kuin edellisessä, eli tuotepäällikkö on eräänlainen projektipäällikkö.

Miettisen (2002) asiantuntijaprofiileista löytyy päällikön profiilista suoraan **tietoturvapäällikkö**, joka sopii nimensä ja sisältönsä mukaisesti profiiliin. Tietoturvapäällikkö vastaa yritysturvallisuuden ryhmän esimiehenä toiminnan ohjauksesta. Koulutustaustaksi Miettinen mainitsee minkä tahansa korkean koulutuksen. Tämä sopii hyvin malliini, koska tietoturvapäällikön profiilista löytyi taustana muutakin kuin pelkkää teknistä koulutusta. Manniselta (16.3.2004) löytyy myös tietoturvapäällikkö aivan suoraan. Tietoturvapäällikön toimenkuva, johon kuuluu kehittämishankkeiden valmistelu, tietoturvallisuudesta tiedottaminen organisaatiossa, avustaminen toimeenpanossa ja turvallisuutta koskeva seuranta. Tämä toimenkuva sopii hyvin myös omiin tuloksiini. Wadlowin (2001) tehtäväkuvauksista tietoturvapäällikön tehtävät koostuvat turva-arkkitehdin, lainvalvojan, politiikan ja käytäntöjenhallinnan ja tiedottajien kuvauksista. Tietoturvapäällikkö toimii tiedottajana myös viranomaisille ja huolehtii tietoturvadokumentation ajantasaisuudesta. Whitmannilta & Mattordilta (2005) löytyy suoraan tietoturvapäällikön profiili, joka kuvaus sopii erittäin hyvin omaan kuvaukseeni. Pätevyysvaatimuksena kuitenkin esitetään CISSP-sertifikaatti, joka omassa tutkimuksessani löytyi vain tietoturvakonsultin profiilista. Akateemisesta loppututkinnosta mainitaan, että se voi olla myös taloudesta, mikä sopii tuloksiini. VAHTI-ohjeissa 7/2003 & 1/2001 tietoturvapäällikkö sijoittuu tietoturvallisuusjohdon alle. Jos tietoturvallisuusjohto on vain yksi henkilö, niin käytännössä se on juuri tietoturvapäällikkö. Tietoturvallisuusjohdon kuvaus vastaa siis tietoturvapäällikön kuvausta. BS 7799-1:sta (23.3.2000) löytyy myös pieni kuvaus tietoturvapäälliköstä, vaikka se ei yleisesti ota kantaa tietoturvallisuusorganisaatioon. BS:n mukaan tietoturvapäälliköllä on päävastuu turvallisuuden kehittämisestä ja toteuttamisesta sekä suojamekanismien määrittelyn tukemisesta. Tämä sopii myös omaan kuvaukseeni.

6.4 Yleisen profiilin vertailu teoriaan

Yleisesti käsittelemässäni kirjallisuudessa profiilit eivät ole ristiriidassa muodostamieni profiilien kanssa. Miettisen (2002) ja Mannisen (16.3.2004) profiileista on yleisesti nähtävissä korkea-asteen peruskoulutus, vähintään yhden yritysturvallisuuden osa-alueen asiantuntijuus ja monissa tehtävissä toimitaan ryhmäpäällikkönä, mitkä sopivat tutkimukseeni. Wadlow (2001) on jakanut muista poikkeavalla tavalla tietoturvallisuushenkilöstön toimenkuvat suhteellisen pieniin osakokonaisuuksiin. Tuskin missään organisaatiossa todellisuudessa on näin montaa erillistä henkilöä hoitamassa asioita. Wadlowin tarkoituksena on ilmeisesti se, että tehtäväkuvauksista kootaan yhdelle henkilölle useammasta tehtävästä toimenkuva. Tässä hän on mielestäni onnistunut suhteellisen hyvin, koska hänen osakokonaisuuksistaan on muodostettavissa myös

tutkimukseni profiilit. Whitmannin & Mattordin (2005) mukaan entisiltä toimenkuviltaan nykyiset tietoturva-ammattilaiset ovat entisiä poliiseja, puolustusvoimien tehtävissä työskennelleitä ja entisiä IT-ammattilaisia. Tällä hetkellä entiset IT-ammattilaiset ovat selvä enemmistö. Lisäksi on pieni vähemmistö jolla ei ole entistä toimenkuvaa, vaan he ovat opiskelleet tietoturvallisuutta yliopistoissa. Tulevaisuudessa yliopistossa tietoturvallisuutta opiskelleiden osuus tulee kasvamaan. Tutkimukseni mukaan enemmistöllä on diplomi-insinöörin tutkinto IT-alalta, kun taas poliisin ammattitutkinto ja puolustusvoimien koulutus eivät olleet ollenkaan edustettuina. Whitman ja Mattord ovat listanneet yleisesti vaatimuksia tietoturva-asiantuntijalle. Mielestäni lista sopii tietoturvallisuuden osaajalle hyvin, mutta tutkimukseni perusteella hallinnollisten ihmisten ei tarvitse välttämättä osata hyvin teknologiaa eikä teknisten ihmisten hallintoa. VAHTI-ohjeissa 7/2003 & 1/2001 ja vielä erityisesti ohjeessa 1/2001 on nähtävissä tietty virkamiestoiminnan byrokraattinen hierarkkisuus selvemmin, kuin muissa malleissa.

6.5 Tavoitteiden saavuttaminen

Tietoturvatehtäväkentän kartoituksessa toimenkuvanimityksen osalta onnistuttiin. Tietoturvatehtäväkentän varsinaisista tehtävistä saatiin kuva, mutta täsmällisempään kuvaan olisi tarvittu enemmän tarkentavia kysymyksiä. Toisaalta, kun kysymys toimenkuvan sisältämistä tehtävistä esitetään ilman ennakovalmistautumista ja haastateltava ei ole aiemmin tullut asiaa ajatelleeksi, niin haastateltavalle tulee mieleen yleensä yksittäisiä asioita, mutta ei kokonaiskuvaa tietoturvatehtävistään. Koulutustausta saatiin selvitettyä hyvin, kysymyksiä oli tästä asiasta riittävästi. Työkokemuksen myötä tullutta pätevyymistä ei eroteltu erikseen muusta tietämyksestä. Voidaan kuitenkin sanoa, että lähes kaikki haastateltavat olivat hankkineet tietoturvatietämyksensä lähes kokonaisuudessaan vasta työelämässä, eli he ovat pätevyityneet lähes pelkästään työuransa aikana. Tietämys teknisestä tietoturvasta ei ollut tämän tutkimuksen painopiste, joten sitä ei erityisesti selvitetty muutoin kuin teknisten termien osalta. Yleisnäkemyistä hallinnollisesta tietoturvasta yritettiin selvittää, ja mielestäni siinä onnistuttiinkin lukuun ottamatta haastateltavia, jotka eivät antaneet vastausta.

Tietoturva-ammattilaisen tarvitsema osaaminen riippuu ammattilaisen toimenkuvasta eli yksikäsitteistä vastausta ei voida antaa, millainen tietoturva-ammattilaisen ammatillinen osaaminen pitäisi olla. Jos ammattilainen on jonkin teknisen järjestelmän ylläpitäjä, niin hän yleensä keskittyy järjestelmänsä tekniseen turvaamiseen. Jos ammattilaisen toimenkuva olisikin tietoturvapäällikkö, niin hän keskittyisi organisaation hallinnolliseen turvallisuuteen. Tutkimuksellani olen saanut selville, että kaikki ammattilaiset tarvitsevat perustason osaamisen, mutta sen jälkeen osaamistarve riippuu henkilön toimenkuvasta. Osaamistarve on kuitenkin jatkuvan muutoksen kohteena, koska henkilöiden toimenkuvat eivät pysy samoina vuodesta toiseen. Tietämystä standardeista ja ohjeista ei selvitetty suoraan, mutta kyselemällä tiedon omistajuuteen ja tietoturvapoliitiikkaan liittyviä asioita pyrittiin selvittämään, onko toiminta standardien ja ohjeiden mukaista. Suurimmassa

osassa tutkimuksen kohteena olleista organisaatioita, standardien mukaista ohjeistusta ollaan tekemässä, ellei se ole jo valmis, jolloin sitä ylläpidetään. Standardeista ja ohjeistuksista kaivataan kuitenkin lisää tietoa, koska ne ovat suhteellisen uusia asioita. Noin puolessa tutkimukseeni osallistuneissa organisaatioissa oli suoritettu auditointeja ja itsearviointeja. Lähes kaikki haastatellut olivat tietoisia, mitä ne ovat. Auditoinnit olivat tulleet organisaatioille useimmiten tutuiksi asiakkaiden tekeminä. Tietoturvallisuuden mittaamista ei käsitelty muutoin haastattelussa. Tietoturvasertifikaattien kohdalla tavoitteena oli selvittää eri sertifikaattien tunnettavuutta. Tunnistettavuudessa oli suurta hajontaa. Osa tunnisti kaikki ja osa ei tunnistanut ensimmäistäkään. Tietoturvastandardeja ja ohjeita organisaatioissa yleensä käytettiin apuna suunniteltaessa omaa tietoturvaohjeistusta.

Haastattelun kohteena olleet organisaatiot olivat lähes poikkeuksetta sitoutuneet tietoturvallisuuden kehittämiseen antamalla riittävät resurssit. Organisaatiot voisivat vielä parantaa sitoutumista antamalla enemmän resursseja ja vielä esimerkillisemmällä johdon käyttäytymisellä kuin tähän asti. Tietoturva-ammattilaisen osaamisen puutteita ja kehityskohteita löydettiin oletusten mukaisesti. Kehityskohteet ja puutteet ovat riippuvaisia henkilön toimenkuvasta. Kehityskohteista ja puutteista on luettavissa tarkemmin alakohdista 5.2.5, 5.2.6 ja kohdasta 6.1. Henkilöstön perehdyttämisen yhteydessä järjestetystä tietoturvakoulutuksesta ei kysytty suoraan, mutta se tuli esille koulutuskysymysten yhteydessä. Saatujen vastausten perusteella tietoturva ei yleensä kuulu perehdyttämiskoulutukseen. Tässä ne organisaatiot, jotka ovat kehittämässä ohjeistustaan tulevat varmaankin huomioimaan myös tämän asian. Täydennyskoulutusta tietoturva-asioista organisaatiot järjestävät tarpeen mukaan yleensä sisäisenä koulutuksena. Täydennyskoulutuksen kohteena ovat yleensä uudet asiat. Haastatteluiden perusteella organisaatioiden pitäisi kartoittaa tietoturvaosaamisensa puutteet paremmin ja laatia sen perusteella sopivaa koulutusta erilaisille henkilöiden toimenkuvien tarpeille pohjautuen. Tietojen hankkimisessa, päivittämisessä ja verkostoitumisessa ei mielestäni ole mainittavaa parannettavaa. Ammattilaiset ovat jo opiskeluaikanaan oppineet erilaisia tiedonhankintatapoja ja hyödyntävät niitä oman kiinnostuksensa ja tarpeensa mukaisesti. Verkostoitumisen kohdalla ammattilaiset hyödynsivät erilaisia tilaisuuksia hyvin verkostoitumisen välineinä, osa jopa meni joihinkin seminaareihin vain pelkästään tapaamaan kollegoita. Esiintymis- ja opettamistaidot riippuvat paljolti yksilöstä itsestään, varsinkin myyntityössä olevat konsultit tarvitsevat niitä. Ne tulivat esille joidenkin haastateltavien mainitsemana kehityskohteena. Osa toivoi näitä taitoja jopa osaksi ammattiopintoja.

Tutkimuksen tuloksena saatiin muodostettua yleisen profiilin lisäksi kolme erilaista tehtäväkuvaksiin pohjautuvaa profiilia. Tämä on enemmän kuin mitä osasin odottaa, mutta profiilit olisivat voineet olla yksityiskohtaisempia. Tähän olisi päästy laajemmalla haastattelulla ja suuremmalla otoskoolla. Parempi kattavuus olisi kuitenkin lisännyt työmäärää merkittävästi, ja tällöin kyseessä ei olisi ollut enää yksi diplomityö, ellei olisi

keskitytty pelkästään johonkin yksittäiseen osa-alueeseen. Tällöin työ luonne ja aihe olisivat muuttuneet huomattavasti.

7. YHTEENVETO

7.1 *Tutkimuksen arviointi*

Organisaatioiden suhtautuminen tietoturvaan on tänä päivänä luonteeltaan reaktiivista ja keskittynyt tekniseen tietoturvaluuteen. Tietoturvakonsultit ovat useamman vuoden ajan odottaneet milloin se siirtyisi enemmän proaktiiviseksi. Jolloin painopiste siirtyy hallinnollisen tietoturvaluuden alueelle. Tämä muutos on tutkimukseni perusteella nyt hitaasti käynnistynyt. Tutkimukseni hitaimmat organisaatiot olivat jo laatimassa tietoturvapoliittikkaansa. Hallinnollisen tietoturvan taso on yleensä organisaatioissa huonompi kuin mitä tutkimustulokseni osoittavat. Koska näin perustavanlaatuisen muutosprosessi on käynnissä, se heikentää merkittävästi saatujen tulosten paikkansapitävyyttä ajatellen, mitä tulevaisuuden tietoturva-ammattilaisten pitäisi osata. Jotta saadut tulokset olisivat käyttökelpoisia tulevaisuuden tietoturva-ammattilaisten ammatillista peruskoulutusta ajatellen, niin tutkimukseen osallistuvilla organisaatioilla pitäisi olla jo muutaman vuoden kokemus tietoturvapoliittikkansa ylläpidosta. Vasta silloin haastateltavat ovat käytännössä joutuneet oppimaan, mitä hallinnollisten tietoturvaprosessien ylläpitämiseen tarvitaan. Perustelen tämän kokemusvaatimuksen sillä, että opiskelijan opiskelut kestävät yleensä useamman vuoden. Tällöin on hyvin suuri riski, että sinä aikana opiskelleet eivät olekaan opiskelleet oikeasti työmarkkinoilla tarvittavia valmiuksia. Toisaalta ei ole tarkoituskaan, että koulun penkiltä saadaan ulos kaiken osaavia tietoturva-ammattilaisia, mutta riittävät valmiudet omaavia kylläkin. Tärkeää on saada turvallisuusajattelu esiin ja mukaan ajatusmaailmaan. Tutkimuksessa on hallinnollinen tietoturvaluus ylikorostunut, koska sitä oli painotettu ajankohtaisuutensa vuoksi. Työ oli myös haastava aiheen laajuuden vuoksi. Haastavuutta ei yhtään vähentänyt se seikka, että jouduin itsenäisesti rajaamaan ja pohtimaan aihetta, koska työllä ei ollut varsinaista tilaajaa, vaan se on tehty puhtaasti akateemisesta mielenkiinnosta.

7.2 *Suositus yliopistojen tietoturvaopetukseen*

Tutkimuksesta nousi esiin odotetun kaltaisia asioita, joiden perustella olen laatinut tämän suosituksen. Tietoturvan opetuksen pitäisi olla sisällytettynä ainakin ohjelmointikursseihin eikä toteuttaa sitä erillisinä kursseina. Kursseilla pitäisi olla ainakin vierailevina luennoitsijoina teollisuudessa työskennelleitä ammattilaisia. Heidän laajempaakin käyttöönsä opetuksessa suositeltaisiin käytännön näkemyksen välittämiseksi. Opetuksessa pitäisi olla kurssi, joka sisältäisi tietoturvaluuden peruskäsitteet, hallinnollisen ja teknisen tietoturvan perusteet ja sen tulisi olla kaikkien tietotekniikka-alan ihmisten opetusohjelmassa. Suppeampi versio edellisestä pitäisi olla sisällytettynä johonkin kaikille opiskelijoille opetettavaan opintojaksoon. Suosituksena opetuksen sisällöstä voidaan sanoa, että sen on annettava valmiuksia:

- hahmottaa eri kokonaisuuksiin liittyvät tietoturvallisuusriskit
- pienentää tietoturvallisuusriskejä tilanteeseen sopivilla teknisillä ja hallinnollisilla menetelmillä
- soveltaa tilanteeseen sopivia teknisiä ja hallinnollisia ratkaisumalleja ja ymmärtää ratkaisumenetelmien aiheuttamat lisäriskit
- muodostaa ja ylläpitää tiedon luokittelu perustuen tiedon arvottamiseen
- hallinnollisen tietoturvan perusdokumenttien toteuttamiseksi ja ylläpitämiseksi
- lainsäädännön, tietoturvastandardien ja ohjeiden sisällön ymmärtämiseksi ja niiden soveltamiseksi käytäntöön
- uhka-analyysien toteuttamiseksi ja tietoturva-arkkitehtuurien ymmärtämiseksi
- verkkoteknologioiden, erityisesti TCP/IP:n ymmärtämiseksi ja soveltamiseksi käytännössä.

Tietoturva-ammattilaisten osaamistarpeet painottuvat eri tavoin hallinnollisen ja teknisen tietoturvan välillä riippuen heidän toimenkuvistaan, kuten kyselytutkimuksen perusteella muodostetuista profiilimalleista voidaan havaita. Tästä johtuen mainittujen asioiden painotus opetuksessa on harkittava erikseen.

7.3 Jatkotutkimuskohteita

Jatkotutkimuskohteita työn perusteella löytyy useita. Yksi tällainen kohde on samantapaisen kartoituksen tekeminen noin 5-10 vuoden kuluttua, jotta voitaisiin nähdä miten asiat ovat muuttuneet, ja ovatko organisaatiot siirtyneet jo hallinnollisen tietoturvan ylläpitoon nykyisen toteuttamisvaiheen sijaan. Tutkimusta voisi tehdä myös keskittymällä esimerkiksi tietoturvapäällikön profiiliin ja tutkia juuri tälle ominaiset piirteet. Erään haastateltavan kommentin perusteella työstä voisi myös laajemmalla otoskokonaisuudella tehdä väitöskirjan. Laajemmalla otoksella saadaan lisää luotettavuutta. Tämä mahdollistaa keskittymisen johonkin pienempään kokonaisuuteen, esimerkiksi jollakin suppealla osa-alueella konsultoiiviin tietoturvakonsultteihin.

LÄHDELUETTELO

Ahola, A. & Godenhjelm, P. & Lehtinen, M. 2002. Kysymisen Taito. Helsinki, Tilastokeskus katsauksia 2/2002. 85s.

BS 7799-1:fi Tietoturvallisuuden hallinta. Osa1: Tietoturvallisuuden hallintaa koskeva menetteleyohje. 23.3.2000. 2.painos, Helsinki, Suomen Standardisoimisliitto. 107s.

BS 7799-2:fi Tietoturvallisuuden hallintajärjestelmät. Osa2: Vaatimukset ja soveltamisohjeet. 31.3.2003. 3.painos, Helsinki, Suomen Standardisoimisliitto. 38s.

BSI Federal Office for Information Security. 2005. "The BSI funktions".
[<http://www.bsi.bund.de/english/functions.htm>]. Luettu 19.7.2005.

CMM 2004. The Capability Maturity Model for Software. Carnegie Mellon Software Engineering Institute. [<http://www.sei.cmu.edu/cmm/>]. Luettu 31.12.2004.

Gamma Secure Systems Limited. 2004a. "History of 7799".
[<http://www.gammasl.co.uk/bs7799/history.html>]. Luettu 21.4.2004.

Gamma Secure Systems Limited. 2004b. "How 7799 Works".
[<http://www.gammasl.co.uk/bs7799/works.html>]. Luettu 21.4.2004.

GIAC 2005a. "Program Overview - GIAC Certification 2005".
[<http://www.giac.org/overview/brief.pdf>]. Luettu 19.5.2005.

GIAC 2005b. "GIAC Security Expert (GSE)".
[<http://www.giac.org/certifications/gse.php>]. Luettu 19.5.2005.

GIAC 2005c. "GIAC Certifications and Certificates".
[<http://www.giac.org/certifications/>]. Luettu 19.5.2005.

ISACA 2005a. Information Systems Audit and Control Association, Inc. 2005. "Code Of Professional Ethics".

[http://www.isaca.org/Template.cfm?Section=Code_of_Professional_Ethics&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=14&ContentID=5009]. Luettu 17.5.2005.

ISACA 2005b. Information Systems Audit and Control Association, Inc. 2005. "The CISA Exam".

[<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=14423&TEMPLATE=/ContentManagement/ContentDisplay.cfm>]. Luettu 17.5.2005.

ISACA 2005c. Information Systems Audit and Control Association, Inc. 2005. "CISM Examination Content Areas".

[http://www.isaca.org/Content/NavigationMenu/Security/CISM_Certification/Exam_Information1/Content_Areas1/CISM_Certification_Content_Areas.htm]. Luettu 17.5.2005.

(ISC)² 2005a. the International Information Systems Security Certification Consortium, Inc. 2005. "About (ISC)²".

[<https://www.isc2.org/cgi-bin/content.cgi?category=7>]. Luettu 13.5.2005.

(ISC)² 2005b. the International Information Systems Security Certification Consortium, Inc. 2005. "About the (ISC)² CBK®".

[<https://www.isc2.org/cgi-bin/content.cgi?category=8>]. Luettu 13.5.2005.

Koskinen, J. 2004. "8306200 Verkon tietoturva, 2004"

[<http://www.cs.tut.fi/kurssit/8306000/V-TT/index.html>]. Luettu 24.4.2005.

McCray, J. 2003. A Roadmap to Becoming Security Conscious. IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY.

[<http://ieeexplore.ieee.org/iel5/8722/27611/01232393.pdf>].

Manninen, M. 2004. Suuren organisaation tietoturva. Tietoturvallisuuden haasteet ja merkitys liiketoiminnassa –seminaari, Tampere, 16. -17.3.2004, Tampere, Edutech Tampereen teknillinen yliopisto, 35s.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Jyväskylä, Talentum Media Oy. 311s.

Nikulainen, K. 11.2.2004. Digitoday. Johto pihalla tietoriskeissä. [http://www.digitoday.fi/showPage.php?page_id=14&news_id=28208]. Luettu 11.2.2004.

Paavilainen, J. 1998. Tietoturva. Jyväskylä, Suomen Atk-kustannus Oy. 228s.

Parker, D. 17.5.2004. Securityfocus. ”TCP/IP Skills Required for Security Analysts”. [<http://www.securityfocus.com/printable/infocus/1779>]. Luettu 17.5.2004.

SAS 70. 2004. Statement on Auditing Standards (SAS) No. 70. American Institute of Certified Public Accountants (AICPA). [<http://www.sas70.com/index2.htm>]. Luettu 22.12.2004.

SFS. 2004. ”Luettelo myönnettyistä tietoturvallisuusjärjestelmäsertifikaateista”. [<http://www.sfs.fi/sertif/jraport/ijnapa.htm>]. Luettu 21.4.2004.

Tampereen teknillinen yliopisto. Ohjelmistotekniikan laitos. 2004. Ohjelmistotekniikan ammattilaisten osaamistarvekartoitus. [<http://www.cs.tut.fi/~kysely/>]. Luettu 26.5.2004.

Tampereen teknillinen yliopisto. Tiedonhallinnan laitos. 2004. Kurssin 2920470 Tietoturvallisuuden johtaminen tietoturvauditointikysymykset. [https://www.bim.tut.fi/protected/2920470/ohjeet_harkkatyohon_verkkoon.pdf] Luettu 11.6.2004. Linkki ei ole enää toiminnassa.

Tietojärjestelmien tarkastus ja valvonta ry 2005. ”ISACA Suomi”. [<http://www.isaca.fi/>] Luettu 16.5.2005.

Tietoturva ry 2005. ”CISSP”. [<http://www.tietoturva.fi/modules.php?op=modload&name=News&file=index&catid=&topic=8>] Luettu 16.5.2005.

VAHTI. Valtionhallinnon tietoturvallisuuden johtoryhmä. 1997-2004. Valtionhallinnon tietoturvallisuusohjeet. [<http://www.vm.fi/vahti-ohjeet/>].

VAHTI 1/2001. Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtion viranomaisen tietoturvallisuustyön yleisohje. Helsinki, Valtiovarainministeriö Hallinnon kehittämissosasto. 58s. [<http://www.vm.fi/vm/liston/page.lsp?r=3373&l=fi&menu=3246>].

VAHTI 7/2003. Valtionhallinnon tietoturvallisuuden johtoryhmä. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Helsinki, Valtiovarainministeriö Hallinnon kehittämissosasto. 80s. [<http://www.vm.fi/vm/liston/page.lsp?r=53828&l=fi&menu=3246>].

VAHTI-tietoturva CD. 2004. Valtionhallinnon tietoturvallisuuden johtoryhmä. Helsinki, Valtiovarainministeriö Hallinnon kehittämissosasto. [<http://www.yliopistojentt.fi/VAHTI-CD/>]. Luettu 11.6.2004.

Wadlow, T. A. 2001. The Process of Network Security. 2nd Printing. United States of America, Addison Wesley Longman Inc. 283s.

Whitman, M. E. & Mattord, H. J. 2005. Principles of Information Security. Second Edition, Canada, Thomson. 576s.

LIITE: CIAG:N SERTIFIKAATTEJA

- GIAC Security Audit Essentials (GSAE)
- GIAC Certified ISO-17799 Specialist (G7799)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Security Leadership Certification (GSLC)
- GIAC Certified Security Consultant (GCSC)
- GIAC Information Security Fundamentals (GISF)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Forensics Analyst (GCFA)
- GIAC Secure Internet Presence (GSIP)
- GIAC .Net (GNET)
- GIAC Auditing Wireless Networks (GAWN)
- GIAC Contracting for Data Security (GCDS)
- GIAC Law of Fraud (GLFR)
- GIAC Business Law and Computer Security (GBLC)
- GIAC Legal Issues in Information Technologies (GLIT)
- GIAC E-warfare (GEWF)
- GIAC Fundamentals of Information Security Policy (GFSP)
- GIAC Cyber Warrior (GCYW)
- GIAC HIPAA Security Implementation (GHSC)
- Ethics in IT (GEIT)
- Stay Sharp Program - Mastering Packet Analysis (SSP-MPA)
- Securing Solaris - The Gold Standard (GGSC-0200)
- Securing Windows 2000 - The Gold Standard (GGSC-0100)
- Stay Sharp Program - Defeating Rogue Access Points (SSP-DRA)
- Auditing Cisco Routers - The Gold Standard (GGSC-0400)
- GIAC Intrusion Prevention (GIPS)

- GIAC Cutting Edge Hacking Techniques (GHTQ)
- GIAC Web Application Security (GWAS)
- GIAC Reverse Engineering Malware (GREM)