WWW.JAMK.FI

Turvallisuussuunnittelu ilmapuolustuksen kohdearkkitehtuurissa

Petri Kiiskilä

Opinnäytetyö
Syyskuu 2010

Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma
Liiketalouden ja hallinnon ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t)	Julkaisun laji	Päivämäärä
KIISKILÄ, Petri	Opinnäytetyö, Ylempi ammattikorkeakoulututkinto	17.09.2010
	Sivumäärä 89 + 15	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
Turvallisuussuunnittelu ilmapuolustuksen kohdearkkitehtuurissa

Koulutusohjelma
Yrittäjyys ja liiketoimintaosaaminen. Ylempi ammattikorkeakoulututkinto

Työn ohjaaja(t)
JURVELIN, Jouni

Toimeksiantaja(t)
Ilmavoimien Materiaalilaitos
LUURI, Asko

Tiivistelmä

Nykypäivänä yhä useampi yritys on riippuvainen tietojärjestelmistä ja niiden käytettävyydestä. Tiedosta on tullut yksi yrityksen tärkeimmistä pääomista, jota pitää suojella. Tietoturvallisuus alkaa hankinnoista, joissa hankittavalle tuotteelle asetetaan vaatimuksia joilla pyritään turvaamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Yrityksen johdon tehtävänä on määrittää tietoturvallisuuden tavoitetila ja käytettävät resurssit.

Opinnäytetyön tavoite on ongelmalähtöinen. Puolustusvoimissa on useita esimerkkejä tuotteista, joissa tuotteen käyttöönotto suunnitellussa laajuudessa on viivästynyt tai estynyt tietoturvallisuuteen liittyvien ongelmien takia. Tämän lisäksi puolustusvoimien lisääntynyt kansainvälinen toiminta on asettanut paineita toteuttaa tietoturvallisuutta kansainvälisesti vertailukelpoisilla menetelmillä.

Opinnäytetyön teoriaosassa käsitellään riskienhallintaa, turvallisuuspolitiikkaa ja Common Criteria (ISO/IEC 15408) tietoturvallisuusstandardia. Teorian perusteella kehitetään konkreettinen konstruktio eli Ilmavoimien turvallisuussuunnittelumalli, joka kuvaa puolustusvoimien kansallisen tietoturvallisuuden tahtotilan sekä laajentaa sitä Common Criteriasta tuotetuilla turvallisuusprofiileilla. Ilmavoimien turvallisuussuunnittelumallia testataan viiden ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimuksilla ja tuloksien perusteella tehdään esityksiä tutkimusongelman ratkaisemiseksi.

Tuloksien perusteella ilmavoimien toteutusvastuulla olevien projektien tietoturvallisuusvaatimukset toteuttavat laadullisesti puolustusvoimien tietoturvallisuuden tahtotilaa. Ongelmana on tietoturvallisuusvaatimuksien määrä, joka ei riitä kattamaan kuin murto-osan tietoturvallisuuden osa-alueista. Puolustusvoimien tulisi panostaa tietoturvallisuuden tahtotilan tarkempaan määrittämiseen ja valvontamekanismien tehostamiseen.

Avainsanat (asiasanat)

Riskienhallinta, turvallisuuspolitiikka, Common Criteria, tietoturvallisuus

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s) KIISKILÄ, Petri	Type of publication Master's Thesis	Date 17.09.2010
	Pages 89+15	Language Finnish
	Confidential ( ) Until	Permission for web publication (X)

Title
Information security planning in Finnish Air Defense

Degree Programme
Master's Degree Programme in Entrepreneurship and Business Competence

Tutor(s)
JURVELIN, Jouni

Assigned by
Finnish Air Force Materiel Command
LUURI, Asko

Abstract

Nowadays, more and more companies are dependent on information systems and their usability. Information has become one of the company's main capitals, which must be protected. Information security begins from procurement where purchased product is subject to the requirements aimed at ensuring information availability, integrity and confidentiality. It is company's management who determine the aims for information security and for resources to be used.

The objective of the thesis is based on problem-solving. In the Finnish Defence Force there are several of examples, where product introduction in planned scope has been delayed or prevented because of information security issues. In addition, the Finnish Defence Forces increased international action has set the pressure to implement information security by using internationally comparable methods.

The theoretical part deals with risk management, organization information security policy and Common Criteria (ISO/IEC 15408) standard. Based on theory a new model, the Finnish Air Force security design model, is created. Model describes desirable status of national information security in Finnish Defence Force and extends it with Protection Profiles from Common Criteria. The Finnish Air Force security design model will be tested with real-world security requirements which are gathered from Finnish Air Force projects.

Based on the testing, Finnish Air Force projects security requirements meets quality criteria which are required for desirable information security. The problem is not the quality but quantity. Current projects security requirements covers only small part from the area which should be filled before introduction. Finnish Defence Force should determinate information security goals for more accurate way and improves its ability to ensure that all projects follow the rules.

Keywords

Risk management, information security policy, Common Criteria, information security

Miscellaneous

SISÄLTÖ

1 JOHDANTO 6

1.1 Opinnäytetyön tausta 7

1.2 Opinnäytetyön tavoitteet ja rajaus 7

1.3 Tutkimusote 11

1.4 Keskeiset käsitteet 13

1.4.1 VAHTI 13

1.4.2 Pysyväisasiakirjat ja normit 14

1.4.3 Tietohallintopäätösmenettely (THP) 14

2 RISKIENHALLINTA 16

2.1 Riskienhallinnan käsitteet 16

2.1.1 Uhka 16

2.1.2 Riski 16

2.2 Riskienhallinnan periaatteet 17

2.2.1 Tunnistaminen 18

2.2.2 Hallinta 19

2.2.3 Varautuminen 20

2.2.4 Seuranta ja raportointi 21

2.3 Riskienhallinnan käytännön toteutus ja tavoitteet 22

2.3.1 Organisoituminen 22

2.3.2 Uhkien tunnistaminen 23

2.3.3 Uhkien todennäköisyyden arviointi 25

2.3.4 Seurausten vakavuuden arviointi 26

2.3.5 Riskin suuruus ja luokittelu 28

2.3.6 Toimenpiteiden määrittely ja toteuttaminen 30

3 ORGANISAATION TIETOTURVALLISUUSPOLITIIKKA 31

3.1 Mitä on tietoturvallisuuspolitiikka? 31

3.2 Tietoturvallisuuspolitiikka osana riskienhallintaa 34

3.2.1 Tietoturvallisuusuhka 35

3.2.2 Tietoturvallisuusriski 35

3.3 Tietoturvallisuuspolitiikan tavoitteet ja tekniset osa-alueet 36

3.3.1 Käyttäjien tunnistaminen ja todentaminen 37

3.3.2 Järjestelmien todentaminen 38

3.3.3 Valtuuttaminen 39

3.3.4 Pääsynhallinta 40

3.3.5 Kryptografia 41

3.3.6 Valvonta 42

4 COMMON CRITERIA (CC) 44

4.1 Historia 44

4.2 Osa 1: Johdanto ja yleismalli 45

4.3 Osa 2: Tietoturvan toiminnalliset vaatimukset 48

4.4 Osa 3: Tietoturvan luottamusvaatimukset 51

5 ILMAVOIMIEN TURVALLISUUSSUUNNITTELUMALLI JA SEN KEHITTÄMINEN ... 54

5.1 Ilmavoimien turvallisuussuunnittelumallin luonti ja rakenne ... 54

5.2 Puolustusvoimien riskienhallinta ... 56

5.3 Puolustusvoimien tietoturvallisuuspolitiikka ... 57

5.4 Kansainvälinen yhteensopivuus: Common Criteria ... 59

6 TURVALLISUUSSUUNNITTELUMALLIN TESTAUS ... 61

6.1 Tapaustutkimuksen taustaa ... 61

6.2 Tutkimusprosessi ... 62

6.3 Projektien kuvaus ... 65

6.3.1 CORE ... 65

6.3.2 LSSJ FOMS ... 65

6.3.3 KAVA MLU ... 66

6.3.4 LINK-16 Ground Systems ... 67

6.3.5 MST ... 68

7 OPINNÄYTETYÖN TULOKSET ... 68

7.1 Tapaustutkimuksen tulokset ... 68

7.2 Uhkien testaus ... 70

7.3 Tietoturvallisuuspolitiikan testaus ... 71

7.4 Common Criterian testaus ... 73

7.5 Ilmavoimien turvallisuussuunnittelumallin tulkinta ... 74

8 YHTEENVETO JA JOHTOPÄÄTÖKSET ... 76

8.1 Tutkimustulokset 76

8.2 Tulosten luotettavuus 80

8.3 Saavutettu hyöty 81

8.4 Jatkotutkimusaiheita 83

LÄHTEET 85

LIITTEET 90

KUVIOT

KUVIO 1. Tutkimuksen lähestymistapa 12

KUVIO 2. VAHTI tietoturvallisuuden kehittämisalueet (VAHTI kehitysohjelma 2004, 35.) 13

KUVIO 3. Puolustusvoimien tietohallintopäätösprosessi 15

KUVIO 4. Riskienhallintaprosessi (Riskienhallintaprosessin vaiheet 2009.) 18

KUVIO 5. Riskianalyysin vaiheet (PEturv-os PAK 01:03 2005, 17;VAHTI 2003, 16.) 24

KUVIO 6. Riskin suuruuden arviointi (Hampton 2009, 10.) 28

KUVIO 7. Common Criteria parts 1-3 (Tipton & Krause 2006, 1492.) 45

KUVIO 8. PP:n, ST:n ja TOE:n välinen suhde (CCPART1V3.1R3 2009, 53.) 47

KUVIO 9. Functional class structure (CCPART2V3.1R3 2009, 23.) 49

KUVIO 10. Functional family structure (CCPART2V3.1R3 2009, 24.) 50

KUVIO 11. Functional component structure (CCPART2V3.1R3 2009, 26.) 51

KUVIO 12. Tietoturvallisuusvaatimuksien jakautuminen 69

KUVIO 13. Ilmavoimien turvallisuussuunnittelumallin toteutuminen 75

TAULUKOT

TAULUKKO 1. Esimerkki riskitaulukosta (VAHTI 2003, 43.).....29

TAULUKKO 2. Standard EAL Packages (Tipton & Krause 2006, 1496.) 46

TAULUKKO 3. Luottamustason yhteenveto (CCPART3V3 2009, 31.).....53

TAULUKKO 4. Ilmavoimien turvallisuussuunnittelumallin rakenne.....55

TAULUKKO 5. Puolustusvoimien tietoturvallisuusuhat.....57

TAULUKKO 6. Esimerkki projektikohtaisesta havaintomatriisista 64

TAULUKKO 7. Tietoturvallisuusuhkien testauksen tulokset 70

TAULUKKO 8. Tietoturvallisuuspolitiikan testauksen tulokset 72

TAULUKKO 9. Common Criterian testauksen tulokset.....73

1 JOHDANTO

Nykypäivänä on vaikea kuvitella liiketoimintaa, joka ei olisi jossain määrin riippuvainen tietojärjestelmistä, verkoista ja niiden toimivuudesta. Tietojärjestelmiä hankitaan helpottamaan päivittäisiä rutiineja, tehostamaan toimintaa, varastoimaan tietoa, sekä luomaan tilannekuvia ja raportteja joiden pohjalta johto voi ohjata organisaation toimintaa. Tietojärjestelmiin varastoitu tieto on yksi organisaation tärkeimmistä pääomista. Tieto pääomana on ongelmallista siksi, että sen arvo on vahvasti sidoksissa tiedon käytettävyyteen, joka on olennainen osa liiketoiminnan jatkuvuutta. Tiedon suojaaminen on riskienhallintaa, jossa organisaation johto tekee päätökset resursseista ja menetelmistä, joilla organisaation toiminnankannalta kriittinen materiaali suojataan.

Ilmavoimat on ilmapuolustusta johtava moderni puolustushaara, joka osallistuu kansallisiin yhteisoperaatioihin ja jolla on kyky kansainvälisiin kriisinhallinta operaatioihin. Ilmavoimilla on uhkaympäristöön nähden uskottava suorituskyky, joka perustuu osaamiseen, korkeaan teknologiaan sekä kansalliseen ja kansainväliseen yhteistoimintakykyyn (Ilmavoimat missio, visio, strategiat 2010, 2). Ilmavoimat vastaa maamme ilmatilan valvonnasta ja vartioinnista sekä reaaliaikaisen ilmatilannekuvan muodostamisesta. Yksi toiminnan kriittisistä menestystekijöistä on tietojärjestelmien käytettävyyden, eheyden ja luottamuksellisuuden turvaaminen.

Valtioneuvoston ulko- ja turvallisuuspoliittisessa selonteossa vuonna 2004 ilmavoimille annettiin tehtäväksi luoda kyky osallistua kansainvälisiin sotilaallisiin kriisinhallintaoperaatioihin (VNS 6/2004, 110). Suomen Ilmavoimilla on vuoden 2010 alusta alkaen perusvalmiudessa kansainvälinen kriisinhallintaoperaatioihin kykenevä Hornet-valmiusyksikkö. Yksikön tavoitteena on varmistaa kansainvälinen yhteensopivuus, niin lentokaluston kuin tietojärjestelmienkin osalta (Ilmavoimien kansainvälinen toiminta 2010). Turvallisuussuunnittelun näkökulmasta tämä tarkoittaa sitä, että organisaatiolle kriittisen pääoman suojaaminen ja käytettävyys pitää täyttää, sekä kansalliset että kansainväliset vaatimukset.

1.1 Opinnäytetyön tausta

Tietoturvallisuus on riskienhallintaa, jossa organisaation johto määrittelee keinot ja periaatteet joilla riskienhallinta toteutetaan. Riskienhallintaan velvoitetaan useilla säädöksillä ja sopimuksilla. Velvoitteiden lisäksi organisaation omat intressit johtavat usein sisäisten ohjeiden ja määräysten syntyyn. Ohjeet ja määräykset edustavat organisaation johdon tahtotilaa. Tahtotilan toteutuminen riippuu yksittäisten työntekijöiden päivittäisistä toiminnoista ja niihin kohdistuvista seurantamekanismeista.

Tietoturvallisuus on yksi riskienhallinnan osa-alueista, joka riskienhallinnan yleisperiaatteiden mukaisesti noudattaa samaa kaavaa. On olemassa organisaation tahtotila, jota toteutetaan työntekijöiden toimesta. Työntekijöiden toimintoihin kohdistuu seurantamekanismeja, joilla pyritään varmistamaan organisaation tahtotilan toteutuminen. Seurantamekanismit ovat välttämättömiä siksi, että työntekijä voi tietoisesti tai tiedostamattaan toimia organisaation tahtotilan mukaisesti tai vastaisesti. Puolustusvoimien seurantamekanismina toimii tietohallintopäätösmenettely, jonka sisältö on kuvattu tämän opinnäytetyön kappaleessa 1.6.3.

Tietoturvallisuuden toteutuminen alkaa hankinnoista, joissa organisaation yksittäinen työntekijä toimii työnantajansa edunvalvojana. Tietoturvallisuuden näkökulmasta tämä tarkoittaa sitä, että työntekijän on oltava tietoinen edustamansa organisaation tahtotilasta ja hänen on kyettävä välittämään tämä tietoisuus hankinnan kohteena olevan tuotteen toimittajalle. Käytännössä tämä tapahtuu tuotteeseen kohdistuvilla tietoturvavaatimuksilla.

1.2 Opinnäytetyön tavoitteet ja rajaus

Tämän opinnäytetyön tavoitteet ovat käytännönläheisiä ja liittyvät suoraan tekijän työhön Ilmavoimien Materiaalilaitoksen projektipäällikkö- ja asiantuntijatehtävissä. Tutkimuksen tavoitteena on selvittää tietoturvallisuusvaatimuksien taustalla oleva organisaation tahtotila ja tutkimusongelmaan liittyvä syy-seuraussuhde. Tutkimuksen osana laaditaan ilmavoimille turvallisuussuunnittelumalli, joka toimii konstruktiona puolustusvoimien tietoturvallisuuden tahtotilasta. Toteutetun mallin toimivuutta

testataan viiden ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimuksilla.

Puolustusvoimien turvallisuustoiminnan strategia perustuu neljään osa-alueeseen: toiminnan turvallisuuteen, henkilöstöturvallisuuteen, tietoturvallisuuteen ja fyysiseen turvallisuuteen (PEturv-os PAK 01:02 2005, 4). Tämän tutkimuksen kohteena on tietoturvallisuus ja Ilmavoimien turvallisuussuunnittelumallin toteuttaminen edellyttää tietoturvallisuuden taustalla olevien uhkien ja riskien selvittämistä olemassa olevista puolustusvoimien asiakirjoista, ohjeista, määräyksistä sekä riskienhallintaan liittyvästä teoriasta. Uusien uhkien ja riskien tunnistaminen on rajattu tämän tutkimuksen ulkopuolelle. Tästä tarkastelusta on johdettavissa opinnäytetyön ensimmäinen tavoite:

Tavoite 1: ***Tunnistaa puolustusvoimien tietoturvallisuuteen liittyvät uhat ja riskit olemassa olevista asiakirjoista, ohjeista ja määräyksistä***

Puolustusvoimien tietoturvallisuuden tavoitteena on mahdollistaa osaltaan puolustusvoimien toimintakyky kaikissa tilanteissa. Tämä tarkoittaa tietojen korkeaa käytettävyyttä, eheyttä ja luottamuksellisuutta (PEturv-os PAK 4:2 2003, 2). Organisaation tietoturvallisuusstrategia ja tietoturvallisuuspolitiikka määrittelee reunaehdot tietoturvallisuuteen liittyvien uhkien ja riskien hallintamekanismeille. Tämä on välttämätöntä, koska strategia tai politiikka on sidoksissa johdon hyväksymiin resursseihin strategian toteuttamiseksi. Organisaation tietoturvallisuuspolitiikan tarkastelusta on johdettavissa tutkimuksen toinen tavoite:

Tavoite 2: ***Tunnistaa puolustusvoimien tietoturvallisuuspolitiikassa vaaditut käytännön toimenpiteet, joilla tunnistettuja uhkia ja riskejä on tarkoitus hallita***

Organisaation sisäisten turvallisuustoimintaa ohjaavien asiakirjojen, ohjeiden ja määräysten lisäksi tavoitteena on tarkastella Common Criteria (ISO/IEC 15408) tietoturvallisuusstandardia osana Ilmavoimien turvallisuussuunnittelumallia. Common Criteria on valittu siksi, että se on kansainvälisesti laajasti käytössä oleva standardi ja sitä on jo sovelluttu erinäisissä ilmavoimien hankkeissa. Toinen kansainvälisesti tunnettu standardi BS 7799 (ISO 17799) on rajattu tämän tutkimuksen ulkopuolelle.

Kansainvälisen tietoturvallisuusstandardin käyttöä puolustusvoimien hankkeissa ei suoranaisesti vaadita, mutta puolustusvoimien turvallisuustoiminnan strategia vaatii, että toiminnan on oltava kansainvälisen vertailun kestävällä tasolla (PEturv-os PAK 01:02 2005, 5). Tämän lisäksi valtionvarainministeriön ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa suosittelee kansainvälisen tietoturvallisuusstandardin käyttöä (VAHTI 2003, 22–23). Kansainvälisen tietoturvallisuusstandardin tarkastelusta osana Ilmavoimien turvallisuussuunnittelumallia voidaan johtaa tutkimuksen kolmas tavoite:

Tavoite 3: ***Tarkastella Common Criteria (ISO/IEC 15408) tietoturvallisuusstandardia osana Ilmavoimien turvallisuussuunnittelumallia***

Esiteltyjen tavoitteiden pohjalta luodaan ilmavoimien turvallisuussuunnittelumalli, jonka toimivuutta testataan viiden Ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimuksilla. Tästä syntyy tutkimuksen neljäs tavoite:

Tavoite 4: ***Ilmavoimien turvallisuussuunnittelumallin toteutus ja testaus***

Testausmateriaalin muodostavat tietoturvallisuusvaatimukset on rajattu hetkeen, jolloin ne ovat lähteneet tarjouspyynnön muodossa toimittajille. Käytetty tutkimusmateriaali edustaa ns. asiakkaan tahtotilaa tarjouspyyntöhetkellä. Tarjouspyynnön jättämisen jälkeiset päätökset tai muutokset vaatimuksiin on rajattu tämän tutkimuksen ulkopuolelle.

Tutkimuksen kohteeksi otetut projektit on valittu sillä periaatteella, että ne kuuluvat ilmapuolustuksen kohdearkkitehtuuriin, ne ovat ilmavoimien toteutusvastuulla, niiden arvioitu toteutuminen on ajankohtainen (2000–2016) ja projekteilla on merkittäviä integraatiovaatimuksia. Projektien tietoturvallisuusvaatimukset ovat osa laajempaa vaatimuskokonaisuutta, joka kuvaa erittäin tarkasti tavoitellun suorituskyvyn. Tästä syystä vaatimusdokumentaatio on turvaluokiteltua ja tietoturvallisuusvaatimuksia julkaistaan sekä käsitellään vain tutkimuksen toteutuksen kannalta välttämättömässä laajuudessa.

Puolustusvoimissa on lukuisia esimerkkejä hankinnoista, joissa hankittavan tuotteen käyttöönotto suunnitellussa laajuudessa on viivästynyt tai estynyt tietoturvallisuu-

teen liittyvien ongelmien vuoksi. Tämä toimii tutkimuksen pääongelmana ja alaongelmana toimii puolustusvoimien turvallisuustoiminnan strategiassa esitetty vaatimus kansainvälisestä yhteensopivuudesta. Ongelmien ratkaisemiseksi muodostetaan käytäntöön perustuva malli (konstruktio), jota evaluoidaan todellisilla ilmavoimien toteutusvastuulla olevien projektien tietoturvallisuusvaatimuksilla. Toiminnalla haetaan vastauksia seuraaviin tutkimuskysymyksiin:

1. *Onko tietoturvallisuuden tahtotilaa kuvattu riittävässä laajuudessa?*
2. *Miten yhdistetään kansallinen ja kansainvälinen yhteensopivuus?*
3. *Onko tietoturvallisuutta osattu vaatia ilmavoimien toteutusvastuulla olevissa projekteissa?*

Tutkimuksessa toteutettavan konstruktion kontribuutiota organisaatiolle tukee kaksi aiempaa tutkimusta aihealueelta, joissa Jari Oinonen (2010) käsittelee puolustusvoimien riskienhallintaa ja Ville Taponen (2003) puolustusvoimien tietoturvaprosesseja.

Oinonen (2010, 32) toteaa omissa johtopäätöksissään, että puolustusvoimien turvallisuustoiminnot sekä niihin välittömästi liittyvä riskienhallinta ja sisäinen valvonta eivät ole tutkimuksen perusteella puolustusvoimien toiminnan huomioon ottaen riittävällä tasolla.

Taponen toteaa omissa johtopäätöksissään, että puolustusvoimien tietoturvaohjeistus ja toimintatavat ovat pirstoutuneet. Ohjeita ja vaatimuksia on paljon, julkaisumuoto ja sijainti vaihtelevat suuresti, eikä versionhallinnasta ole tietoakaan. (Taponen 2003, 61.)

Tutkimustavoitteisiin pääsy edellyttää tietoturvallisuusvaatimusten taustalla olevien ilmiöiden tarkastelua. Tarpeen kuvauksen ja sen täyttämisen suunnittelu tulee aina pitää erillään toisistaan. Tarpeen kuvauksen puuttuminen on aina toteutusmahdollisuuksia rajaava ja voi johtaa elinkaarikustannusten tarpeettomaan kasvamiseen, sekä suorituskykytavoitteen saavuttamatta jäämiseen (Kosola 2007, 149–150).

Tutkimusongelmaan haetaan vastauksia tarkastelemalla teoriaa riskienhallinnasta, tietoturvallisuuspolitiikasta ja Common Criteria tietoturvallisuusstandardista. Tarkas-

telun pohjalta toteutetaan Ilmavoimien turvallisuussuunnittelumalli, jota testataan ilmavoimien toteutusvastuulla olevien projektien tietoturvallisuusvaatimuksilla.

1.3 Tutkimusote

Opinnäytetyö noudattaa konstruktiivisen tutkimuksen periaatteita, jossa tutkimusongelma on muodostunut tutkijan omakohtaisen kokemuksen ja tutkimuksen tilaajan havaintojen perusteella. Heikkinen (2001, 119) toteaa, että konstruktiossa ihminen rakentaa tietonsa aikaisemman tietonsa ja kokemustensa varaan. Konstruktiivinen tutkimus on soveltava tutkimus, jossa tuotetaan uutta tietoa ja jonka päämääränä on ongelman ratkaisu. Konstruktiivinen tutkimus alkaa käytännön ongelman havaitsemisella ja alustavan tiedon hankkimisella tutkimuskohteesta. Taustalla olevien teorioiden perusteella rakennetaan ratkaisumalli eli konstruktio (Hirsjärvi & Hurme 2004, 22–26).

Tutkimuksessa käsitellään reaalimaailmaa, jossa tietoturvallisuusvaatimusten taustalla olevien teorioiden avulla luodaan konstruktio puolustusvoimien tietoturvallisuuden tahtotilasta. Seppänen (2004, 6) toteaa, että konstruktiivinen tutkimus on:

- suunnittelua ja todellisuuden muuttamista havaittujen ongelmien ratkaisemiseksi
- käsitteellistä konstruointia (mallintamista)
- konkreettista konstruointia (mallien toteutusta ja testaamista).

Tämä tutkimus on luonteeltaan konkreettinen konstruointi, jossa toteutettava Ilmavoimien turvallisuussuunnittelumalli testataan reaalimaailman empiirisellä aineistolla. Hirsjärvi, ym. (2001, 125) toteaa, että kvantitatiivinen ja kvalitatiivinen tutkimus voivat olla toisiaan tukevia. Ilmavoimien turvallisuussuunnittelumallin tarkoituksena on taata, että ilmavoimien toteutusvastuulla olevien projektien turvallisuusvaatimuksilla suoritettava mittaus on tutkimusongelman kannalta mielekästä (Hirsjärvi 2001, 125). Pelkkiä turvallisuusvaatimuksia mittaamalla ei olisi mahdollista tehdä päätelmiä vaatimuksien laadusta tai suhteesta puolustusvoimien tietoturvallisuuden tahtotilaan.

Tutkimus jakautuu kuvion 1 osoittamalla tavalla kolmeen osaan. Tutkimuksen teoriaosassa kartoitetaan kirjallisuustutkimuksen avulla tietoturvallisuusvaatimuksien taustalla olevien ilmiöiden säännönmukaisuuksia ja piirteitä, joiden pohjalta luodaan konstruktio todellisuudesta. Lopuksi konstruktiota testataan viiden ilmavoimien toteutusvastuulla olevan projektin turvallisuusvaatimuksilla ja tuloksien perusteella tehdään esityksiä tutkimusongelman ratkaisemiseksi.

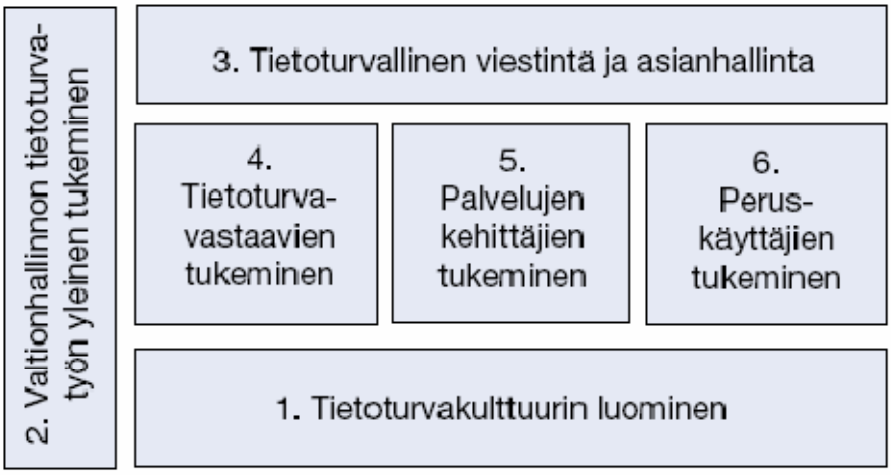
KUVIO 1. Tutkimuksen lähestymistapa

1.4 Keskeiset käsitteet

1.4.1 VAHTI

Valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Valtionhallinnossa tietoturvallisuuden yhteisinä lähtökohtina ovat jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta, säädöksissä määritellyt tietoturvavelvoitteet, valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä sekä valtiovarainministeriön antamat VAHTI-tietoturvaohjeet ja muut linjaukset. (Valtionvarainministeriö VAHTI 2004.)

VAHTI muodosti elokuussa 2003 työryhmän valmistelemaan Suomen valtionhallinnon tietoturvallisuuden kehittämisohjelmaa. Kuvion 2 mukaisesti tietoturvallisuuden kehitysohjelma sisältää 6 kehittämisaluetta, joissa on yhteensä 28 kehittämiskohdetta.



KUVIO 2. VAHTI tietoturvallisuuden kehittämisalueet (VAHTI kehitysohjelma 2004, 35.)

VAHTI kehitysohjelman tarkoituksena on omalta osaltaan konkretisoida tietoyhteiskuntaohjelmia ja kansallista tietoturvastrategiaa ehdottamalla yksinkertaisia, toteuttamiskelpoisia ja käytännönläheisiä hankkeita. Ohjelman ulkopuolelle on rajattu jul-

kishallinnon yksiköiden sisällä tapahtuva tietoturvallisuustyö, joka mahdollistaa eri organisaation omien sisäisten käytäntöjen luomisen. (mts. 22).

1.4.2 Pysyväisasiakirjat ja normit

Puolustusvoimien tietoturvallisuutta ohjeistetaan ja koordinoidaan Pääesikunnan turvallisuusosaston ja johtamisjärjestelmäosaston käskyillä, määräyksillä ja ohjeilla. Näitä linjaorganisaation julkaisuja kutsutaan pysyväisasiakirjoiksi (PAK) ja yhdessä muiden asiakirjojen, määräyksien ja ohjeiden kanssa ne muodostavat normitietokannan. Pysyväisasiakirjojen tarkoituksena on ohjeistaa organisaation toimintaa toimialan johdon näkökulmasta. Asiakirjojen sisältö perustuu usein Suomen lakiin tai Valtionvarainministeriön VAHTI ohjeistukseen, josta organisaation tekee oman sisäisen ohjeen.

Pysyväisasiakirjat ovat normaaleiden organisaation toimintaa ohjaavien asiakirjojen tapaan määräaikaisia tai toistaiseksi voimassaolevia. Pysyväisasiakirjat määrittävät puolustusvoimien tietoturvallisuuspolitiikan, joten tietoturvallisuusarkkitehtuuri on jakautunut useiksi eri käskyiksi, määräyksiksi ja ohjeiksi.

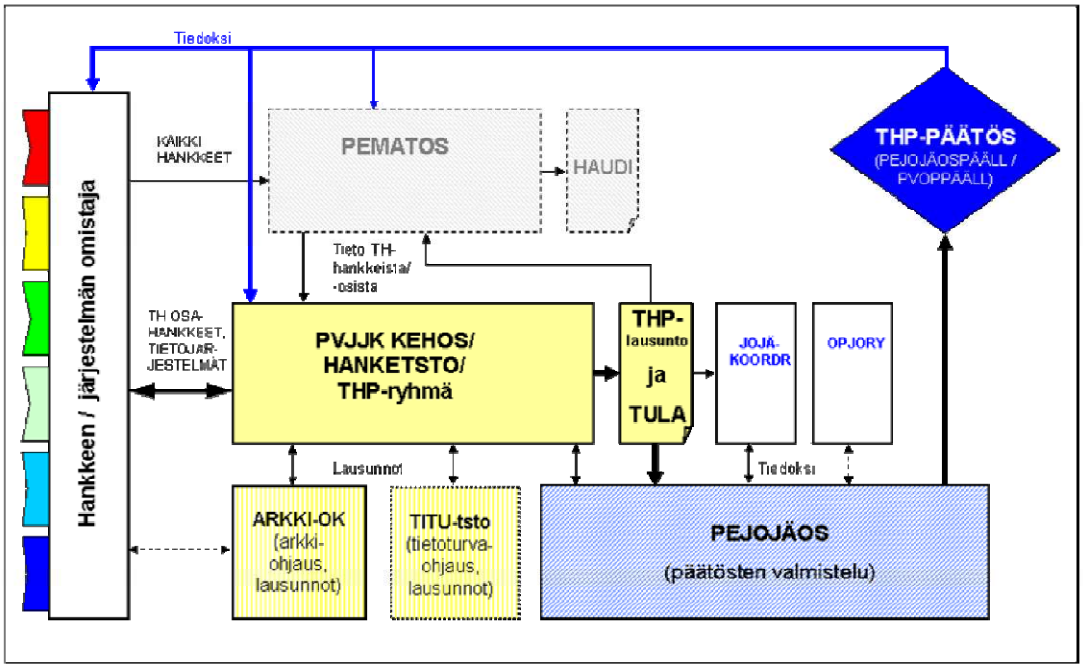
1.4.3 Tietohallintopäätösmenettely (THP)

Tietohallintopäätösmenettely on puolustusvoimien päätöksentekoprosessi, jonka lopputuloksena on tietohallintopäätös. Tietohallintopäätös on haettava kaikkiin tietojärjestelmähankkeisiin ja – projekteihin ennen muita päätöksentekoprosesseja. (PEJojä-os THP-PAK 2007, 1.)

Puolustusvoimien tietohallintoa johtavat operaatiopäällikkö ja johtamisjärjestelmäpäällikkö. Tietohallintopäätöksellä tietohallinnon johto hyväksyy tai hylkää tietohallintohankkeen, -projektin ja tietoteknisenjärjestelmän etenemisen tai järjestelmän merkittävät muutokset. Tietohallintoasian omistaja vastaa tietohallintopäätöksen hakemisesta ennen muita päätöksentekoprosesseja.

Kuvion 3 mukaisesti THP-ryhmä on käytännön toimija tietohallintoasian omistajan vastuuhenkilöiden ja puolustusvoimien tietohallinnon johdon välillä, koskien prosessin läpivientiä. ARKKI-ryhmä vastaa tietohallintopäätösmenettelyyn tuodun tietojär-

jestelmän tai projektin arkkitehtuurinmukaisuudesta ja TITUTSTO antaa tietoturvalausunnon.



KUVIO 3. Puolustusvoimien tietohallintopäätösprosessi

Tietohallintopäätösmenettelyllä ja varsinkin tietoturvatoimiston (TITU-tsto) tietoturvalausunnolla on merkittävä rooli puolustusvoimien turvallisuusstrategiaan kuuluvan tietoturvallisuuden toteutumisessa. Tietoturvallisuus jaetaan kahdeksaan toimenpidealueeseen: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus (PEturv-os PAK 01:02 2005, 14.). THP:ssä näiden turvallisuustavoitteiden toteutuminen kuvataan vapaamuotoisesti hankkeen omistajan toimesta. Tämän vapaamuotoisen kuvauksen perusteella TITU-tsto muodostaa tietoturvalausunnon, jonka pohjalta arvioitava kohde joko toteuttaa tai ei toteuta puolustusvoimien tietoturvallisuusstrategiaa.

2 RISKIENHALLINTA

Riskienhallinta on keskeinen osa organisaation strategista johtamista. Riskienhallinnalla vähennetään toimintaan kohdistuvien häiriöiden syntymistä ja niistä aiheutuvien haittavaikutuksien merkitystä. Riskienhallinnan näkökulmasta keskeinen käsite on uhka, jonka tunnistaminen ja toteutumisen todennäköisyyden arviointi on keskeisessä asemassa jatkotoimenpiteiden kannalta.

2.1 Riskienhallinnan käsitteet

2.1.1 Uhka

Uhka on vahingollisen tapahtuman aiheuttava tekijä (PEturv-os PAK 01:03 2004, 5). Usein uhka on varsin vaikeasti määriteltävä kokonaisuus, koska käytettävissä ei ole sopivaa tilastotietoa uhan toteutumistiheydestä. Usein ajaudutaan tilanteisiin, jossa uhka ei ole koskaan toteutunut mutta toteutuminen on selvästi mahdollinen.

Esimerkiksi uhka voi olla tuntemattoman käyttäjän pääsy organisaation operatiivisiin tietojärjestelmiin. Kyseisen uhkan toteutuminen saattaisi aiheuttaa riskejä tiedon luottamukselle, eheydelle tai käytettävyydelle.

2.1.2 Riski

Riski on sarja todennäköisyyksiä ja niiden seurauksia (A Risk Management Standard 2002, 2). Hampton (2009, 4-5) on tunnistanut kyseessä olevan riskin, mikäli sen seurauksena on aineellista hävikkiä, henkilövahinkoja, ei toivottu seuraus tai mahdollisesti tulevaisuudessa konkretisoituva ei toivottu tapahtuma. Garvey (2008, 3) määrittelee riskin materiaalin näkökulmasta. Riski on joukko tapahtumia, jotka aiheuttavat ei toivottuja muutoksia kustannuksiin, aikatauluihin tai kohteen tekniseen suorituskykyyn.

Riskit jaetaan sekä sisäisiin että ulkoisiin riskeihin. Riskin toteutumiseen vaikuttaa se, kuinka hyvin on osattu varautua riskin taustalla olevia uhkia vastaan. Riskiä voidaan pitää hallittuna tai tietoisena, kun riskin toteutuessa tiedetään mitä tapahtuu ja seu-

rauksiin on varauduttu. Toisin kuin uhka, riski ei ole pelkästään haitallinen asia vaan siihen liittyy myös mahdollisuus.

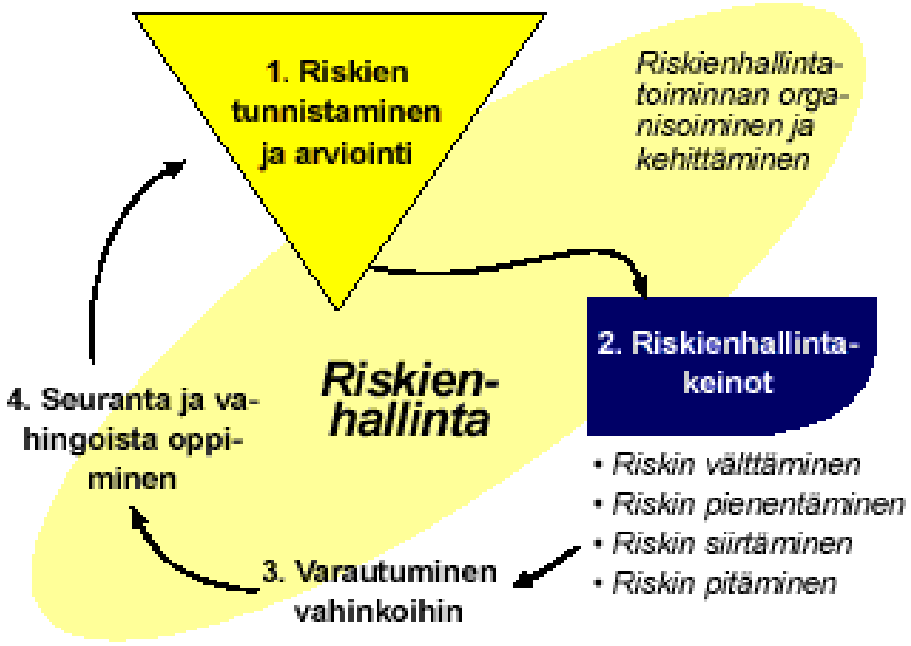
2.2 Riskienhallinnan periaatteet

Organisaation johdon sitoutuminen on ensimmäinen askel kohti järjestelmällistä riskienhallintaa. Riskienhallinta edellyttää organisaation toimintojen tuntemusta, jotta toiminnan kannalta välttämättömät menestystekijät ja niihin kohdistuvat uhat sekä riskit voidaan tunnistaa. Järjestelmällisellä uhkien tunnistamisella, riskien analysoinnilla sekä parannustoimenpiteillä voidaan saavuttaa korkea turvallisuustaso.

Hamptonin mukaan organisaatioon kohdistuvat riskit voidaan jakaa riskienhallinnallisesti kolmeen alueeseen: liiketoiminta, talous ja ”hasardit”. Liiketoimintaa uhkaavia riskejä ovat tilanteet, joissa liiketoimintaa ei voida jatkaa kannattavasti. Taloudellisia riskejä ovat tilanteet, joissa maksukyvyttömyys estää organisaation normaalin toiminnan. ”Hasardeiksi” luokitellaan riskit, jotka ovat vaikeasti ennustettavissa ja uhkaavat liiketoimintaa sekä taloutta. Tyypillisimpiä ”hasardeja” ovat sairastumiset, luonnonkatastrofit, oikeustoimet, lakot ja muut vastaavat tapahtumat, joista on vaikea toipua. (Hampton 2009, 5-8.)

Hamptonin esittelemien alueiden lisäksi useat organisaation käsittelevät liiketoiminnan strategiaa yhtenä itsenäisenä riskienhallinnan osa-alueena (A Risk Management Standard 2002, 3). Liiketoiminnan strategiaan kohdistuvia riskejä ovat kilpailu, asiakasvaatimukset, asiakaskunta ja toimialamuutokset. Organisaation riskienhallinnan painopiste vaihtelee riippuen toimialasta, toimintaympäristöstä, taloudellisista resursseista ja muista vaikuttavista tekijöistä (Hampton 2009, 5). Riskienhallinta on kuitenkin luonteeltaan velvoittava ja ainakin työturvallisuus-, pelastustoimi- ja ympäristösäädökset velvoittavat Suomessa toimivia yrityksiä riskienhallintaan.

Riskienhallinta on prosessi -ja turvallisuusjohtamisen tärkein apuväline. Kuvio 4 kuvaa riskienhallintaprosessin vaiheet, jotka jakautuvat karkeasti: tunnistamiseen, hallintaan, varautumiseen ja seurantaan.



KUVIO 4. Riskienhallintaprosessi (Riskienhallintaprosessin vaiheet 2009.)

Valtaosan riskeistä aiheutuvat ihmisistä, toiminnasta, ympäristöstä ja materiaalista. Tyypillisesti organisaation toiminnassa ihmisten aiheuttamat riskit muodostavat valtaosan tunnistetuista riskeistä. Riskiarvioinnissa on hyvä ottaa huomioon se, että ihmisellä on taipumus aiheuttaa riskejä tahallisesti tai tahattomasti. Esimerkiksi ihminen voi ajaa ylinopeutta tahallisesti tai tahattomasti. Organisaation toiminta voi aiheuttaa riskejä henkilöstölle, toiminnalle, ympäristölle ja maineelle. Ympäristö voi aiheuttaa riskejä organisaatiolle ja sen toiminnalle. Materiaali voi aiheuttaa riskejä, jotka johtuvat itse materiaalista tai materiaalin puutteellisista käyttöperiaatteista.

2.2.1 Tunnistaminen

Riskienhallintaprosessi alkaa uhkien ja riskien tunnistamisella, jota kutsutaan yleisesti riskianalyysiksi. Riskianalyysi koostuu uhkien tunnistamisesta ja niiden riskien suuruuden arvioinnista. Tämän lisäksi riskianalyysi pitää sisällään riskien merkityksen arvioinnin ja toimenpiteet riskin pienentämiseksi. (SFS 60300, 16–19.)

Tunnistamisen edellytyksenä on tarkasteltavan liiketoiminnan ja operatiivisten päämäärien syvällinen tuntemus (A Risk Management Standard 2002, 5). Riskien tunnis-

taminen ei ole yksittäinen tapahtuma, vaan jatkuva prosessi. Tästä johtuen riskienhallinnan teettäminen organisaation ulkopuolisena työnä ei ole kustannustehokasta.

Riskien tunnistaminen koskee kaikkia organisaation toimintoja, joten yhteistyö on välttämätöntä (Riskienhallintaprosessin vaiheet 2009). Riskianalyysi etenee järjestelmällisesti tunnistaen toiminnot ja niihin kohdistuvat uhat. Se arvioi uhkien toteutumisen todennäköisyyden ja seurausten vakavuuden suhteutettuna olemassa olevaan turvallisuustasoon. Tarkasteltavat toiminnot on hyvä jakaa osiin, jotta tarkastelusta ei tule liian raskas ja se ei kohtuuttomasti häiritse varsinaista liiketoimintaa.

2.2.2 Hallinta

Riskien hallinnalla tarkoitetaan käytännön toimenpiteitä, joilla tunnistettua riskiä halutaan hallita. Arvioidaan käytännön toimenpiteitä, miten vahingot voidaan välttää ja niiden seurauksia lieventää (Riskienhallintaprosessin vaiheet 2009)? A Risk Management Standardin mukaan organisaation hallintamekanismiin tulisi sisällyttää vähintään kolme osa-aluetta:

1. Organisaation sisäiset toiminnot, joilla riskin toteutumisen todennäköisyyttä pienennetään ja vahinkoja lievennetään
2. Organisaation ulkopuoliset toiminnot, kuten vakuuttaminen ja takuut
3. Riskejä hallitaan vähintään lakien ja säädöksien edellyttämässä laajuudessa

Oikean hallintamekanismin valinta edellyttää kustannuslaskentaa, jossa riskin toteutumisesta aiheutuvat kustannukset ovat selvillä. Kustannuslaskenta toimiin päätöksenteon tukena, kun mietitään sopivia hallintamekanismeja riskin hallintaan (A Risk Management Standard 2002, 10–11).

Garvey (2008) määrittelee hallintamekanismin tavoitteiksi riskin välttämisen, riskin pienentämisen, riskin siirtämisen ja riskin pitämisen. Sisällöllisesti hallintamekanismit on määritelty seuraavasti:

Riskin välttämisellä tarkoitetaan toimenpiteitä, joilla mahdollisesti suuren vahingon aiheuttava riski korvataan pienemmällä. Riskiä voidaan välttää kiinnittämällä huomiota materiaaliin, toimintatapoihin ja varusteisiin. Riskin poistaminen on usein

mahdotonta, koska se uhkaisi liiketoiminnan jatkuvuutta tai se aiheuttaisi muita riskejä.

Riskin pienentämisellä tarkoitetaan tilannetta, jossa riskin olemassaolo on tiedossa mutta omalla toiminnalla vaikutetaan sen toteutumisen todennäköisyyteen ja/tai lievennetään seurauksia. Parhaiten riskejä voidaan pienentää suunnitteluvaiheessa, jossa otetaan huomioon toimintatavat, ohjeistus ja koulutus.

Riskin siirtämisellä tarkoitetaan tilannetta, jossa riski siirretään tai jaetaan toisen osapuolen kanssa. Riskin siirtäminen on tehokas tapa hallita riskin välittömiä vaikutuksia, mutta välilliset vaikutukset saattavat olla kauaskantoisia ja täten siirtämisellä harvoin päästään riskittömään ratkaisuun. Tyypillisin riskin siirtämisen muoto on vakuuttaminen.

Riskin pitäminen tarkoittaa sitä, että riski on tunnistettu mutta pienentävät toimenpiteet ovat kustannustehokkuudeltaan kannattamattomia suhteessa vaikutuksiin. Soveltuu parhaiten riskeihin, joissa mahdolliset vahingot ovat kokonaistoimintaan nähden pieniä. (Garvey 2008, 165–168.)

Organisaation sisäiset toiminnot, joilla pyritään pienentämään uhan todennäköisyyttä ja pienentämään vahingon suuruutta ovat yleensä kustannustehokkain tapa hallita riskiä. Ohjeet, määräykset, kouluttaminen, oikeanlainen materiaali ja turvallinen työympäristö ovat vain joitain esimerkkejä lukuisista mahdollisuuksista. Vakuutukset ovat yleisin tapa hallita riskiä ulkoisesti. Suomessa on myös velvoite työntekijöiden vakuuttamisesta, sekä tapaturmien että eläkevakuutuksen osalta (L 20.8.1948/608;L 395/2006).

2.2.3 Varautuminen

Järjestelmällisestä ja hyvin suunnitellusta riskienhallinnasta huolimatta organisaation on varauduttava vahinkoihin. Varautumisella huolehditaan siitä, että lisävahinkoja ei pääse syntymään ja toimenpiteet vahingon korjaamiseksi on määritetty.

Vahingon sattuessa on usein kiire, joten päätöksien täytyy syntyä nopeasti. Tietoisuus riskistä ja sen aiheuttamista vahingoista helpottavat päätöksentekoa nopeassa aikataulussa. Tunnistamattoman riskin toteutuminen ja epätietoisuus seurauksista,

yhdistettynä nopeisiin päätöksiin, on otollinen ilmapiiri uusien vahinkojen syntymiselle.

A Risk Management Standardin mukaan organisaation tulisi profiloida tunnistetut riskit. Profiloinnissa tulisi huomioida itse riski, riskin aiheuttaja, riskin toteutumisen todennäköisyys, arvioidut vaikutukset toimintaan, suunnitellut hallintatoimenpiteet ja jatkotoimenpiteet. (A Risk Management Standard 2002, 6-11).

Varautumisessa on hyvä muistaa, että suunnitelmat eivät ole pelkästään organisaation johtoa varten. Riskienhallintaa toteutetaan organisaation jokaisella tasolla ja viestinnällä on suuri rooli riskienhallinnassa. Valtaosa vahingoista tunnistetaan tai aiheutetaan organisaation työntekijöiden toimesta. Yhtenä varautumisen onnistumisen mittarina voidaan pitää sitä, että työntekijä reagoivat vahingon sattuessa organisaation riskienhallintasuunnitelman mukaisesti.

2.2.4 Seuranta ja raportointi

Järjestelmällisessä riskienhallinnassa seurannalla on keskeinen merkitys. Seurannan tarkoituksen on mitata riskien ja vahinkojen trendejä. Se joko vahvistaa organisaation riskienhallinnan tuloksia tai antaa konkreettista näyttöä siitä, että menetelmiä täytyy kehittää (A Risk Management Standard 2002, 11). Seurannalla myös arvioidaan toimenpiteiden tehokkuutta ja huolehditaan siitä, että toimenpiteet tulee tehtyä. Kehittäminen vaatii jatkuvaa seurantaa ja uudelleen tarkastelua.

Uuden liiketoiminnan yhteydessä seurantaa tulisi suorittaa tehostetusti. Usein kaikkia suojaustoimenpiteitä ei voida toteuttaa heti analyysin jälkeen, joten seurannalla voidaan luoda prioriteettilista korjattavista toimenpiteistä. Jos toimenpiteet vaikuttavat hyväksyttävällä tavalla kohteeseen, pelkkä seuranta riittää.

Tyypillisesti organisaatio mittaa, seuraa tai arvioi oman toimintansa tehokkuutta. Usein puhtaasti liiketoiminnan tunnuslukujen seurannasta ja raportoinnista käytetään nimitystä johdon raportointi. Tiettyyn ajanjaksoon ja tiettyihin tunnuslukuihin kohdistuvasta seurannasta tuotetaan raportti, jota käytetään organisaation johdon päätöksenteon tukena.

A Risk Management Standard jakaa raportoinnin riskienhallinnan näkökulmasta sisäiseen ja ulkoiseen raportointiin. Sisäisen raportoinnin tarkoituksena on kertoa riskianalyysin tuloksista ja toimenpide-ehdotuksista johdolle. Johto tekee päätöksen kehittämistoimenpiteitä ja tavoiteltavasta riskitasosta. Ulkoisen raportoinnin tarkoituksena on vakuuttaa sidosryhmät organisaation laadusta, jossa yhtenä osatekijänä on riskienhallinta. (A Risk Management Standard 2002, 8.)

Sisäiset raportit sisältävät usein organisaation toiminnan kannalta kriittistä tietoa, joten ne eivät ole tarkoitettu ulkopuolisten tarkasteltaviksi. Julkisuuteen levinneet haavoittuvuudet heikentäisivät kilpailuasemaa, altistaisivat rikollisuudelle ja tahraisivat mainetta. Ulkoisten raporttien tarkoitus on kuvata organisaation riskienhallintaprosessia, johdon sitoutumista riskienhallintaan ja seurantamekanismeja (A Risk Management Standard 2002, 9-10).

2.3 Riskienhallinnan käytännön toteutus ja tavoitteet

2.3.1 Organisoituminen

Riskienhallinta on jatkuvaa toimintaa, jolla pyritään takaamaan organisaation toimintojen turvallinen toteutuminen kaikissa olosuhteissa. Hamptonin (2009, 8) mukaan on harhakuvitelmaa luulla, että riskienhallinta muodostuisi itsestään työntekijöiden toimesta. Organisaation täytyy sisäisesti organisoitua riskienhallintaan, jotta sitä voidaan käyttää jokapäiväisessä päätöksentekoprosessissa.

Organisoitumisen tavoitteena on luoda organisaatio, joka vastaa riskienhallinnan osa-alueista. Garvey (2008) määrittelee viisi keskeisintä osaamisen osa-aluetta, jotka tulisi sisällyttää riskienhallintaorganisaatioon: ennakoiva ja jatkuva tunnistaminen, vaikutuksien hallinta, kustannusten hallinta, resurssien hallinta ja trendit. Sisällöllisesti osa-alueet on määritelty seuraavasti (Mts. 2-3):

Ennakoiva ja jatkuva tunnistaminen: toteutetaan organisaation työntekijöiden toimesta, joilla on paras tietämys tarkasteltavasta kohteesta. Tavoitteena on tunnistaa mahdolliset uhkat ja riskit ennen kuin ne uhkaavat varsinaista toimintaa.

Vaikutuksien hallinta: riskien vaikutuksien analysointiin keskittyvä yksilö tai ryhmä, jonka tavoitteena on analysoida tunnistettujen riskien tuotannollista vaikutusta organisaation toimintaan.

Kustannusten hallinta: riskien kustannusanalyysin erikoistunut yksilö tai ryhmä, jonka tavoitteena on hallita riskienhallinnan kustannustehokkuutta.

Resurssien hallinta: organisaation riskienhallintaan käytettyjen resurssien valvonta, jonka tavoitteena on tuottaa johdolle ehdotuksia tehokkaasta resurssien käytöstä.

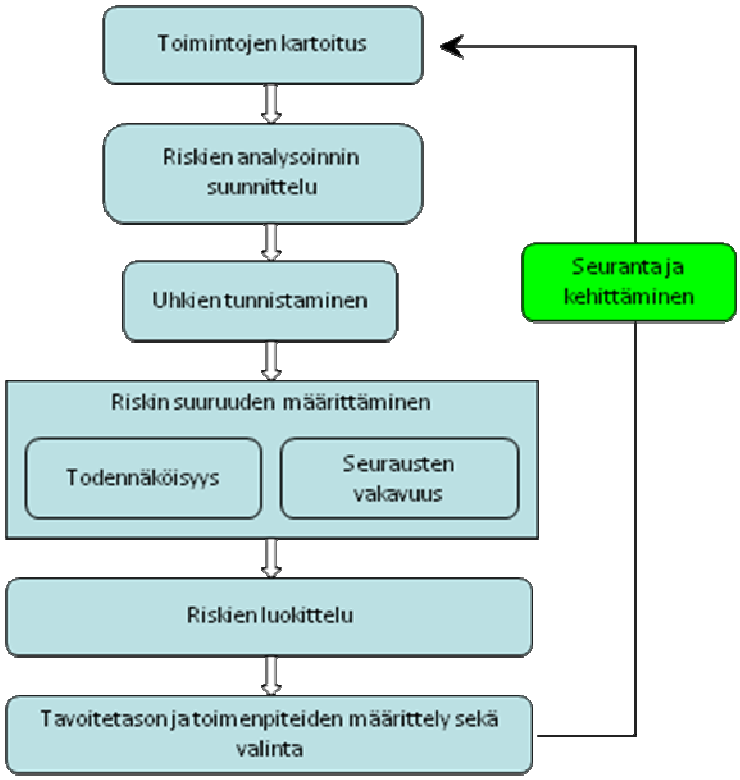
Trendit: johdon raportointiin erikoistunut yksilö ja ryhmä, jonka tavoitteena on pitää organisaation johto tietoisena riskienhallinnan tilanteesta.

Organisaation koko ja toiminnan laajuus määrittelee eri osa-alueiden resurssit. Varsinainen riskianalyysi edellyttää työryhmän perustamista, jossa on mukana ym. osa-alueiden asiantuntemusta. Organisaation normaaliin kokoonpanoon ei välttämättä kuulu analyysimenetelmien asiantuntijaa, joka voidaan tapauskohtaisesti hankkia ulkopuolelta.

2.3.2 Uhkien tunnistaminen

Riskien analysoinnista vastaa toiminnan tai kohteen vastuuhenkilö tukeutuen riskienhallinnan ohjeistukseen, riskienhallinnan asiantuntijoihin sekä ohjausvastuussa olevan toimialan ammattilaisiin.

Riskianalyysin keskeisimmät tavoitteet ovat: uhkien tunnistaminen, riskien kuvaus, toteutumisen todennäköisyyden arviointi, vaikutuksien arviointi ja riskien luokittelu (A Risk Management Standard 2002, 5-11). Kuvion 5 avulla on kuvattu riskianalyysin eteneminen vaiheittain.



KUVIO 5. Riskianalyysin vaiheet (PEturv-os PAK 01:03 2005, 17;VAHTI 2003, 16.)

Riskianalyysi aloitetaan omien toimintojen kartoituksella, joka mahdollistaa niihin kohdistuvien uhkien analysoinnin. Toimintojen tunnistamisessa voidaan käyttää apuna esimerkiksi toimintavirta-analyysiä, jossa kootaan organisaatiosta lähtevät ja siihen tulevat ihmis-, materiaali- ja tietovirrat. Toimintavirta-analyysin avulla luodaan pohja uhkien tunnistamiselle ja arvioidaan toiminnot, jotka vaativat tarkempaa tarkastelua. (PEturv-os PAK 01:03 2005, 18.)

Riskianalyysin suunnitteluvaiheessa määritellään tarkasteltava kohde ja tutustutaan kohteen taustatietoihin. Tämän lisäksi valitaan käytettävät riskianalyysimenetelmät ja laaditaan toteutusaikataulu. Riskianalyysillä on aina oltava myös tavoite, joka antaa reunaehdot toteutuksen laajuudelle ja käytettäville menetelmille. Tunnusomaisia piirteitä hyvälle riskianalyysille ovat: tavoitteiden määrittely, kohteen rajaus, oikeat menetelmät, lähtötietojen laatu, vetäjän pätevyys, resurssien varaus, dokumentointi, tulosten tavoitteenmukaisuus ja raportointi. (Heikkilä, Murtonen, Nissilä, Virolainen & Hämäläinen 2007, 8-12.)

Riskin suuruuden määrittämiseksi tulee arvioida tai tietää uhan todennäköisyys. Uhan todennäköisyyden arvioinnissa voidaan käyttää olemassa olevia tilastotietoja, jotka saattavat perustua vastaavanlaisen organisaation julkaisuihin tai omien riski-analyysien tuloksiin. Uhkien ja vaarojen tunnistamiseen voidaan käyttää kohde-/tapauskohtaisesti useita riskianalyysimenetelmiä, kuten: poikkeamatarkastelua (HAZOP), potentiaalisten ongelmien analyysia (POA), reaktiomatriisia, satunnaispäästöriskianalyysia (SARA), toimintavirheanalyysia (TVA), työn turvallisuusanalyysia (TTA), vaarallisten skenaarioiden analyysia (HAZSCAN) tai vika- ja vaikutusanalyysia (VVA). (VAHTI 2003, 26;VTT Riskianalyysin menetelmät).

2.3.3 Uhkien todennäköisyyden arviointi

Uhkien todennäköisyyden arvioinnissa voidaan käyttää useita eri asteikkoja ja dokumentoinnin tyylejä. A Risk Management Standard kuvaa uhkien todennäköisyyttä kolmiportaisella asteikolla: suuri (high), keskisuuri (medium) ja pieni (low), jossa todennäköisyys on määritelty seuraavasti (A Risk Management Standard 2002, 6-7):

Suuri (high), uhkan toteutumisen todennäköisyys on kerran vuodessa tai toteutumisen todennäköisyys on yli 25 %

Keskisuuri (medium), uhkan toteutumisen todennäköisyys on kerran kymmenessä vuodessa tai toteutumisen todennäköisyys on alle 25 %

Pieni (low), uhkan toteutuminen kymmenessä vuodessa ei ole todennäköistä tai toteutumisen todennäköisyys on alle 2 %.

VAHTI ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa kuvaa uhkien todennäköisyyttä neliportaisella asteikolla: korkea(3), keskimääräinen(2), alhainen(1) ja ei merkitystä (0), jossa todennäköisyys on määritelty seuraavasti (VAHTI 2003, 41-42):

Korkea(3), uhka ilmenee kerran kuukaudessa

Keskimääräinen(2), uhka ilmenee 1-2 kertaa vuodessa

Alhainen(1), uhka ilmenee kerran vuodessa

Ei merkitystä(0), uhka ei voi toteutua missään olosuhteissa.

Merkittävin ero uhkien todennäköisyyden arvioinnissa syntyy organisaation toiminnan luonteesta, joka vaikuttaa erityisesti tarkasteltaviin aikajaksoihin. Suuret organisaatiot, jotka ovat jo vakiinnuttaneet asemansa markkinoilla, tarkastella toimintaansa jopa 25 vuoden päähän. Pienemmät organisaatiot tai yritykset tarkastelevat toimintaansa enemmillään 1-3 vuoden aikajaksoilla.

2.3.4 Seurausten vakavuuden arviointi

Seurausten vakavuuden arvioinnissa tarkastellaan, kuinka vakavia vahinkoja uhka voisi toteutuessaan aiheuttaa. Seurausten vakavuudessa tulee ottaa huomioon, ihmisiin, toimintaan, omaisuuteen, tietoon, maineeseen ja ympäristöön kohdistuvat vahingot. Suoranaisten vaikutuksien lisäksi tulee ottaa huomioon myös välilliset vaikutukset.

Seurauksien vakavuuden arvioinnissa käytetään hyvin samankaltaista mittaristoa, kuin uhkien todennäköisyyden arvioinnissa. A Risk Management Standard määrittelee seurauksien vakavuudet samalla periaatteella kuin uhkien todennäköisyyden seuraavasti (A Risk Management Standard 2002, 7):

Suuri (high), taloudellinen seuraus organisaatiolle on suuri, josta aiheutuu merkittäviä vaikutuksia organisaation strategioiden toteutumiselle ja operatiivisille toiminnoille

Keskisuuri (medium), taloudellinen seuraus organisaatiolle on keskisuuri, josta aiheutuu muutoksia organisaation strategioille ja operatiivisille toiminnoille

Pieni (low), taloudellinen seuraus organisaatiolle on pieni, josta ei koidu merkittäviä muutoksia organisaation strategioille tai operatiiviselle toiminnalle.

A Risk Management Standardin määritys on hyvin liiketoimintalähtöinen, joten vaikutukselle pitää antaa konkreettinen rahallinen arvo, jota suhteutetaan organisaation maksukykyä kuvaavaan mittariin. Standardin lähtökohta on siinä, että kaikille seurauksille on olemassa tai pystytään laskemaan rahallinen arvo.

VAHTI ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa lähestyy seurausten vakavuuden arviointia keskittyen toiminnallisiin vaikutuksiin. Seurausten vakavuudet on luokiteltu kolmeen luokkaan seuraavasti (VAHTI 2003, 41–42):

Erittäin vakavat(3)

- Seuraukset koskevat kaikkia käyttäjiä
- Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä
- Uhkan toteutuminen aiheuttaa raportointia ylemmille organisaatioille
- Uhkan toteutuminen aiheuttaa toiminnan keskeytymistä
- Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia
- Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen
- Toiminta on lainsäädännön velvoitteiden vastaista

Vakavat(2)

- Seurauksilla on vaikutusta työntekijöiden työmäärään
- Seuraukset koskevat useita käyttäjiä
- Uhkan toteutuminen aiheuttaa tiedotteen tekemisen
- Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia

Vähäiset(1)

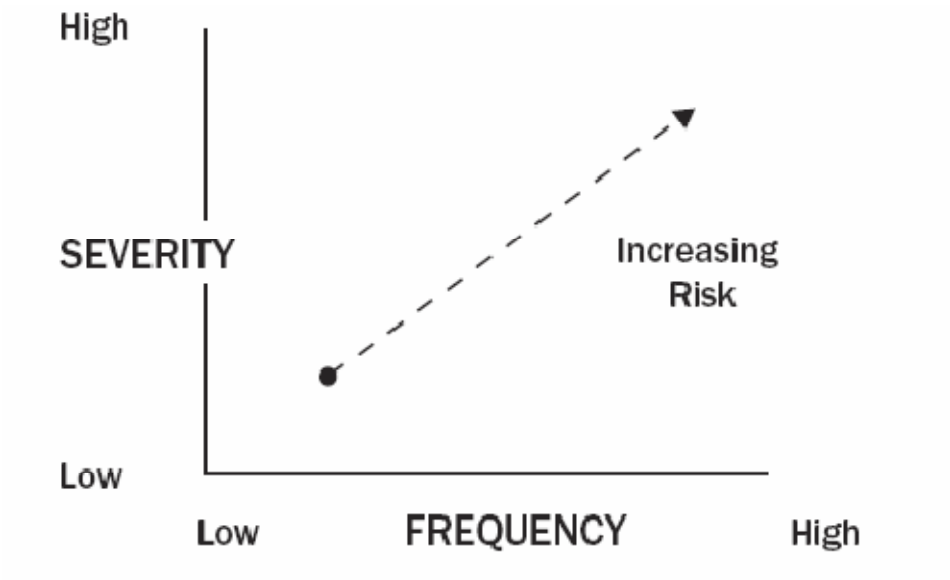
- Seuraukset koskevat muutamia käyttäjiä
- Uhkan toteutuminen ei aiheuta välittömiä toimenpiteitä
- Uhkan toteutuminen aiheuttaa sisäisen raportoinnin
- Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia

- Toiminnan keskeytyminen on vähäistä.

VAHTI ohjeistuksen lähestymistapa vaikutuksien arvioimiseksi on monipuolisempi. Se auttaa tunnistamaan organisaation toiminnan kannalta keskeiset riskit, myös toiminnallisten vaikutuksien näkökulmasta. Tämä mahdollistaa riskin tehokkaan luokittelun, vaikka kustannusvaikutukset eivät olisi kokonaisuudessaan tiedossa.

2.3.5 Riskin suuruus ja luokittelu

Hampton (2009, 10) kuvaa riskin suuruutta vektorimaisesti kuvion 5 osoittamalla tavalla. Riskin suuruuteen vaikuttaa uhan toteutumisen todennäköisyys (frequency) ja vaikutuksien vakavuus (*severity*).



KUVIO 6. Riskin suuruuden arviointi (Hampton 2009, 10.)

Uhan toteutumisen todennäköisyydestä ja seurauksien vakavuudesta voidaan muodostaa myös riskitaulukoita, joiden tarkoituksena on havainnollistaa organisaation toiminnan kannalta keskeisimmät riskit. Riskitaulukot ovat käytännön apuvälineitä havainnollistamaan Hamptonin esittämää vektorimallia. Riskitaulukolla kuvataan uhkan todennäköisyyttä ja seurausten vakavuutta tarkastelussa valitulla asteikolla. Taulukko 1 esittää VAHTI-ohjeistuksen esimerkin riskitaulukosta:

TAULUKKO 1. Esimerkki riskitaulukosta (VAHTI 2003, 43.)

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1.Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Organisaation tulisi kiinnittää erityistä huomiota riskeihin joilla on suuri toteutumisen todennäköisyys ja vakavat vaikutukset. Näiden riskien tunnistamiseksi ja riskitaulukoiden tueksi voidaan antaa riskiluku, jolla ilmaistaan todennäköisyyttä ja vaikutusta. Riskiluvun tarkoituksena on luokitella riskit ja se voidaan muodostaa mittavien matemaattisen todennäköisyyslaskelmien perusteella tai yksinkertaistaa riskitaulukoiden välittämästä tiedosta. (Garvey 2008, 13–18).

Yksinkertainen riskiluku voidaan johtaa kaavalla: riskin suuruus = uhkan toteutumisen todennäköisyys X seurausten vakavuus. Mikäli käytettävä asteikko uhkan toteutumisen todennäköisyydelle ja seurausten vakavuudelle olisi 1-5, niin korkein riskiluku olisi 25 (toteutumisen todennäköisyys(5) X seurausten vakavuus (5) = 25). Riskiluvun perusteella riskit voidaan luokitella esimerkiksi (PEturv-os PAK 01:03 2004, 26;VAHTI 2003, 45–46):

Sietämätön riski (25–15), toiminta lopetettava heti ja toimenpiteet riskin poistamiseksi tai pienentämiseksi on aloitettava välittömästi

Merkittävä riski (12-9), toiminta on pyrittävä lopettamaan mahdollisimman pian. Toimenpiteet riskin pienentämiseksi on aloitettava.

Kohtalainen riski (8-5), toimintaa voidaan jatkaa, mutta toimenpiteiden suunnittelu riskin pienentämiseksi on aloitettava

Vähäinen riski (4-2), toimenpiteitä ei välttämättä tarvita, mutta kohdetta tulee seurata

Merkityksetön riski (1-0), toimenpiteitä ei tarvita. Voidaan tutkia tarkemmin suojaustoimenpiteiden kustannustehokkuutta.

Luokittelun tavoitteena on löytää tehokkaimpia toimenpiteitä riskin hallinnalle. Suuri riskiluku kertoo siitä, että riskin hallintamekanismeja ei ole, ne ovat riittämättömiä tai ne ovat toteutettu väärin. Toiminnan jatkaminen tämän kaltaisissa olosuhteissa johtaa väistämättä vahinkojen syntyyn.

2.3.6 Toimenpiteiden määrittely ja toteuttaminen

Riskianalyysin lopuksi tarkastellaan saatuja tuloksia ja muodostetaan toimenpide-ehdotuksia riskianalyysin suunnitteluvaiheessa asetettujen raamien puitteissa. Riskien luokittelussa ja toimenpide-ehdotusten suunnittelussa on otettava huomioon uhkien taustalla olevat syyt ja riskiluvun muodostuminen. Riskin suuruudesta riippuen on mietittävä eri keinoja riskin hallintaan.

Jotta suojaustoimenpiteet voidaan suunnitella, on selvitettävä syyt, jotka mahdollistavat uhkan toteutumisen. Suojaustoimenpiteillä pyritään pienentämään uhkan todennäköisyyttä ja seurausten vakavuutta. Johdon hyväksymille suojaustoimenpiteille suunnitellaan toteutusaikataulu ja sovitaan vastuuhenkilö, joka vastaa toimenpiteiden toteutumisesta sekä seurannasta. (PEturv-os PAK 01:03 2004, 27; VAHTI 2003, 45–38).

Usein kaikkia suojaustoimenpiteitä ei voida toteuttaa heti analyysin jälkeen. Dokumentoinnin avulla saadaan tarkat tiedot analyysin vaiheista ja voidaan tarkastella uhkien taustalla olevia syitä sekä suunniteltujen toimenpiteiden perusteluja myöhemmin suunnitelmien mahdollisesti muuttuessa.

3 ORGANISAATION TIETOTURVALLISUUSPOLITIIKKA

Organisaation riskienhallinnassa tunnistetut uhat ja riskit voivat vaikuttaa välillisesti tai välittömästi liiketoiminnan jatkuvuuteen tietojärjestelmien kautta. Käytännön toimenpiteet, joilla tietoturvallisuuden uhkia ja riskejä hallitaan, määritellään organisaation tietoturvallisuuspolitiikassa. Tietoturvallisuuspolitiikassa määritetään teknisen tietoturvallisuuden välineet ja hallinnollisen tietoturvallisuuden toimintatavat niin, että tietoturvallisuus on toteutettavissa johdon antamilla resursseilla.

Tietoturvallisuus on riskienhallintaa, jolla tarkoitetaan tietojen, tietojärjestelmien, palveluiden ja tietoliikenneyhteyksien asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, hasardien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. (VM 0024:00/02/99/1998, 3).

Tietoturvallisuus on kokonaisuus, joka muodostuu hallinnollisesta tietoturvallisuudesta, henkilöstöturvallisuudesta, tilaturvallisuudesta, tietoliikenneturvallisuudesta, laitteistoturvallisuudesta, ohjelmistoturvallisuudesta, tietoaineistoturvallisuudesta ja käyttöturvallisuudesta. (VM 0024:00/02/99/1998, 4).

Politiikalla tarkoitetaan tässä opinnäytetyössä suunnitelmaa tai toimenpiteitä, joilla pyritään vaikuttamaan kohdealueeseen toivotulla tavalla. Politiikka on joukko dokumentteja, joilla kuvataan kohdealue ja siihen liittyvät organisaatiokäytännöt. Politiikan laatimisesta vastaa kohdealueen omistaja tai vastuullinen henkilö. (Bacik 2008, 21).

3.1 Mitä on tietoturvallisuuspolitiikka?

Tietoturvallisuuspolitiikan avulla organisaation johto määrittelee tietoturvallisuuden tavoitteet ja toimintatavat (VAHTI 2001, 9). Tietoturvallisuuspolitiikka on joukko asiakirjoja, ohjeita ja määräyksiä, joilla määritetään organisaation suhtautuminen tieto-

turvaan. Organisaation tietoturvallisuuspolitiikassa tulisi käsitellä ainakin seuraavia asioita:

Tietoturvallisuuspolitiikan pääjulkaisu: pääjulkaisu on johdon viesti siitä, että organisaatiolla on olemassa tietoturvallisuuspolitiikka, jonka noudattamista edellytetään organisaation kaikilla tasoilla. Pääjulkaisu toimii sisällysluettelona organisaation tietoturvallisuuden osa-alueisiin ja niihin liittyviin tarkempiin ohjeistuksiin ja toimintatapoihin. Pääjulkaisu itsessään on luonteeltaan julkinen, joten siinä ei kuvata teknisiä menetelmiä, joilla tietoturvallisuustavoitteisiin päästään. Tyypillisesti pääjulkaisussa kuvataan tietoturvallisuuden tavoitteet ja vastuuhenkilöt. (Gregory 2003, 78).

Työntekijöille asetetut vaatimukset: henkilöstön tietoturvaohje on tietoturvallisuuspolitiikan merkittävin riskienhallinnan väline. Organisaation merkittävin tietoturvauhka on tietämätön, motivoitumaton ja piittaamaton työntekijä. Tästä johtuen tietoturvaohjeen tulisi olla kaikkien työntekijöiden saatavilla ja sen sisällön omaksumista tulisi vaatia ennen käyttöoikeuksien myöntämistä tietojärjestelmiin. Tietoturvaohjeen sisältö täytyy rakentaa niin, että se on ymmärrettävissä myös ei-teknisten työntekijöiden toimesta. (Gregory 2003, 12).

Tiedon luokittelu: tieto voidaan luokitella usealla eri tasolla ja menetelmällä, mutta tärkeintä on tiedonkäsittelijän ymmärrys käsiteltävän materiaalin luottamuksellisuudesta. Tietoturvallisuuspolitiikassa tulisi kuvata organisaation käyttämä tiedon luottamuksellisuutta kuvaava menetelmä ja toimintatavat tiedon käsittelylle. Valtionhallinnossa tiedon luottamuksellisuus perustuu julkisuuslakiin ja käsittelyohjeet ovat kuvattu Valtiovarainministeriön ohjeella. Julkisuuslaki ei koske esimerkiksi yrityssalaisuuksiin, joten liiketoiminnalle luottamuksellinen materiaali voidaan luokitella organisaatiolle sopivalla tavalla. (Gregory 2003, 78–79;VAHTI 200, 6-10).

Organisaation kommunikaatio: tietoturvapolitiikassa tulisi määrittää periaatteet ja hyväksytyt menetelmät, joilla työntekijät kommunikoivat sisäisesti sekä ulkoisesti. Tässä yhteydessä kommunikaatiolla tarkoitetaan organisaatiossa tapahtuvaa viestintää, jota toteutetaan teknisellä apuvälineellä (sisäinen puhelin, kännykkä, sähköposti, kollaboraatio-työkalut, intranet). Työasioiden hoitaminen kolmannen osapuolen tarjoamalla sähköpostilla, puhelimella tai kollaboraatio-työkalulla muodostaa merkittävän tietoturvariskin. (Peltier 2005, 5).

Tiedon elinkaari: valtaosa organisaatiossa tuotetusta tiedosta on lyhyen elinkaaren tietoa. Tietoturvallisuuden, käytettävyyden ja kustannustehokkuuden kannalta on välttämätöntä, että tietoa myös poistetaan. Vanhentuneen tiedon poistaminen edellyttää sitä, että organisaation toiminnan kannalta vanhentunut tieto voidaan tunnistaa. Tyypillisesti tämä tarkoitta tiedon luokittelun kaltaista ns. meta-tietoa tai menetelmää, jossa tuotetulle tiedolle annetaan vanhentumispäivä. (Peltier 2005, 6).

Tilaturvallisuus: tietojärjestelmien ja tietoteknisten laitteiden kehittyneet turvallisuusominaisuudet eivät ole poistaneet tilaturvallisuuden ratkaisevaa merkitystä. Turvallisuuspolitiikassa määritetään reunaehdot tiloille, joissa organisaatiolle arkaluontoista materiaalia voidaan käsitellä (työntekijöiden toimipisteet) tai joissa arkaluontoinen materiaali sijaitsee (palvelinsalit, ristiinkytkentäkaapit, päätelaitteet). Tilaturvallisuuden rooli korostuu erityisesti tiedon käytettävyyden suojaamisessa. (Peltier 2005, 5.)

Ohjelmistoturvallisuus: myös tietojärjestelmillä ja ohjelmilla on oma elinkaarensa. Uusia tietojärjestelmiä otetaan käyttöön ja vanhoista luovutaan. Uuden tietojärjestelmän hankinnan yhteydessä on hyvä muistaa, että organisaatiolla on jo toiminnassa oleva tietotekninen infrastruktuuri, joka asettaa tiettyjä vaatimuksia uudelle tietojärjestelmälle. Toimitilat, päätelaitteet, käyttäjähallinta, huoltosopimukset ja henkilökunnan osaaminen ovat vain muutamia esimerkkejä osa-alueista, jotka vaikuttavat uuden järjestelmän käyttöönottoon. Tietoturvallisuuspolitiikassa täytyy asettaa reunaehdot uuden tietojärjestelmän hankinnalle ja käyttöönotolle. (Bacik 2008, 69–96).

Laitteistoturvallisuus: aivan kuten ohjelmistossa, myös tietoteknisissä laitteissa on elinkaari. Tietoturvan teknisessä toteutuksessa palvelimilla, päätelaitteilla, reitittimillä, kytkimillä, toimikorteilla ja tulostimilla on merkittävä rooli. Usein laitteistoja hankitaan kaupallisten asianhoitajien toimesta hankintapolitiikan mukaisesti, jossa hinnalla on ratkaiseva merkitys. Tämä voi olla myös tietoturvallisuuspolitiikan tavoite, mutta se rajoittaa laitteen ominaisuuksiin sidottujen turvamekanismien hyödyntämistä. (Bacik 2008, 69–96).

Toipuminen: toipumisella tarkoitetaan toimenpiteitä ja käytäntöjä, joilla organisaatio turvaa liiketoiminnan jatkuvuuden vahingon sattuessa. Tietoturvallisuudessa keskitytään tietojärjestelmien, tietoliikenteen ja laitteistojen toipumiseen. Toipuminen on

osa käytettävyyden turvaamista, johon on mahdollista käyttää loputtomasti resursseja. Organisaation resurssit ovat rajallisia, joten on oltava johdon määrittelemä tavoitetila jonka puitteissa resursseja käytetään. (Tipton & Krause 2006, 1629–1633).

3.2 Tietoturvallisuuspolitiikka osana riskienhallintaa

Tietoturvallisuus on organisaation liiketoimintaa tukevaa toimintaa. Tietoturvallisuudella varmistetaan oman liiketoiminnan jatkuvuus ja ylläpidetään luotettavaa julkisuuskuvaa. Tietoturvallisuuspolitiikan tavoitteena on varmistaa tiedon käytettävyys, eheys ja luottamuksellisuus. Organisaatiotasolla tieto on vain yksi suojattava pääoma, joten tietoturvallisuutta ei voida pitää kaiken kattavana uhkien ja riskien hallintamekanismina.

Tietoturvallisuuspolitiikka tulisi olla osa organisaation riskienhallintaa. Riskienhallinnan tavoitteet ovat liiketoimintalähtöisiä, joten johto olettaa että liiketoimintaan kohdistuvat uhat ja riskit ovat hallittuja. Tietoturvallisuuden ammattilaisten tavoitteena on laatia tarvittavat suunnitelmat ja toimintatavat, jotka mahdollistavat liiketoiminnan jatkuvuuden tietoturvallisuuden näkökulmasta (Peltier 2004, 16).

Vacca toteaa, että tietoturvallisuuspolitiikka voidaan sitouttaa organisaation liiketoimintaan kahdella tavalla. Yksi tapa on arvioida tiedon merkitys organisaatiolle ja kohdentaa turvallisuusresursseja arvion perusteella. Toinen tapa on uhkaperusteinen riskienhallinta, jossa tietoturvallisuuden uhkia ja riskejä käsitellään saman mallin mukaisesti kuin liiketoiminnan vastaavia (Vacca 2009, 6-7).

Tiedon merkitykseen perustuva resurssien kohdentaminen voi olla tehokasta, jos organisaatiolla on hyvin vähän suojattavia kohteita ja kohteiden tunnistaminen sekä arviointi on voitu toteuttaa luotettavasti. Uhkaperusteinen tietoturvallisuuspolitiikka sopii organisaatioille, joissa suojattavia kohteita on paljon ja tiedon arviointia ei voida toteuttaa luotettavasti. Puolustusvoimien tietoturvallisuuspolitiikka perustuu uhkaperustaiseen suojaamiseen.

3.2.1 Tietoturvallisuusuhka

Tietoturvallisuusuhka voi olla suoraan riskienhallinnan riskianalyysistä tuotettu uhka, joka kohdistuu organisaation tietoverkkoihin, tietokoneisiin, tietojärjestelmiin tai tietoon. Liiketoimintaan kohdistuvasta uhasta on voitu myös jalostaa tietoturvauhka, jotta sitä voidaan käsitellä tietoturvallisuuden näkökulmasta.

Gregory (2003, 11) määrittää tietoturvauhan tietoiseksi tapahtumaksi, jonka tavoitteena on aiheuttaa vahinkoa yksityisen henkilön tai organisaation tietoverkoille, tietokoneille, tietojärjestelmille tai tiedolle. Tietoturvallisuusuhan aiheuttama vahinko voi ilmetä esimerkiksi (Gregory 2003, 13–16):

- vahinkona tietokoneen laitteistolle tai ohjelmistolle
- luottamuksellisen tiedon paljastumisena tai varkautena
- hyökkäyksenä palvelun käytettävyyttä vastaan
- haittaohjelmina, joiden tarkoituksena on levittää vahinkoa

Tietoturvallisuusuhat ovat todennäköisyyksiä, joiden taustalla on tavoite aiheuttaa vahinkoa organisaatiolle. Sisäisenä uhkana organisaatiot työntekijät muodostavat suurimman tietoturvallisuusuhan, jos työntekijän tavoitteena on aiheuttaa vahinkoa. Tämä perustuu siihen, että työntekijöillä on usein työperusteinen tarve päästä tietoon käsiksi. Näkyvimmän tietoturvallisuusuhan muodostavat haittaohjelmat (virukset, madot, troijan-hevoset), joiden torjunnassa yhdistyvät toimintatavat ja tekninen tietoturvallisuus. Ulkoisena uhkana merkittävimpänä voidaan pitää hakkereita, joiden tavoitteena on hyödyntää organisaation tietoturvallisuudessa esiintyviä puutteita ja tätä kautta toteuttaa vahinkoa.

3.2.2 Tietoturvallisuusriski

Liiketoiminnassa riskiin liittyy olennaisesti myös mahdollisuus. Tietoturvallisuuden näkökulmasta uuden teknisen toiminnallisuuden käyttöönotto ja siihen liittyvä toiminnan tehostuminen on mahdollisuus. Tietoturvallisuusriski muodostuu, kun käyttöönotetusta toiminnallisuudesta paljastuu haavoittuvuus jota hyödyntämällä voidaan tuottaa vahinkoa organisaatiolle.

Gregoryn (2003, 18) mielestä tietoturvallisuusriski voi muodostua esimerkiksi:

- Ohjelmistovirheestä, joka mahdollistaa ohjelmiston väärinkäytön ja tunkeutumisen ohjelmiston taustalla olevaan järjestelmään
- Virheellisistä asetuksista, jotka mahdollistavat käyttöoikeuksien muuttamisen käyttäjien toimesta
- Virheellisistä prosesseista, jotka mahdollistavat uusien käyttäjätunnuksien tai järjestelmien haltuunoton esimerkiksi tunnetun oletussalasanan vuoksi
- Tietoturvallisuuspolitiikan vastaisesta toiminnasta, jossa käyttäjät asentavat omia järjestelmiään jotka eivät noudata organisaation turvallisuuskäytäntöjä

Tietoturvallisuusriski perustuu haavoittuvuuteen, joka voi aiheutua tietoturvallisuutta toteuttavan tuotteen ominaisuuksista (ohjelmistovirhe, haavoittuvuus tuotteessa) tai kyvystä käyttää tuotetta (väärät asetukset, tehdasasetukset, inhimilliset virheet).

Tietoturvallisuusriskien havaitsemiseksi on olemassa lukuisia teknisiä apuvälineitä, joista käytetyimpiä ovat erilaiset haavoittuvuus analysaattorit. Analysaattoreiden tarkoituksena on testata organisaation tietoverkkoja, tietokoneita, käyttöjärjestelmiä ja ohjelmistoja tunnettujen haavoittuvuuksien varalta (Vacca 2009, 383–292). Organisaation tietoturvallisuuspolitiikassa tulisi määrittää tämän kaltaisten teknisten apuvälineiden rooli organisaation tietoturvallisuuden toteutuksessa.

3.3 Tietoturvallisuuspolitiikan tavoitteet ja tekniset osa-alueet

Tietoturvallisuuspolitiikan päämääränä on toteuttaa turvallisuusmekanismit, joilla suojataan organisaation toiminnan kannalta kriittistä tietoa. Tavoitteisiin pääsy edellyttää, sekä hallinnollisia että teknisiä toimenpiteitä tiedon suojaamiselle. Hallinnollinen turvallisuus muodostaa perustan koko organisaation turvallisuustoiminnalle. Se on johtamista ja organisointia, jota tuetaan teknisen tietoturvallisuuden menetelmillä.

Organisaation tietoturvallisuuden keskeisin elementti on luotettu käyttäjä, joka on tietoinen organisaation tietoturvallisuuspolitiikasta ja sitoutunut noudattamaan sitä. Luottamus voidaan muodostaa erilaisilla turvallisuusselvityksillä, vaitiolositoumuksilla tai kokemuksen perusteella. Tietoisuus muodostetaan hallinnollisilla toimenpiteillä kuten koulutuksella, ohjeistuksella ja määräyksillä.

Tekninen tietoturvallisuus on ensisijaisesti tarkoitettu organisaation ulkopuolisia uhkia vastaan. Teknistä tietoturvallisuutta kohdennetaan myös organisaation luottamiin käyttäjiin pääsyoikeuksien ja valvontamekanismien muodossa, mutta tärkein kohderyhmä on tahot joihin ei luoteta (Gregory 2003, 29).

Tietoturvallisuuden parhaat käytännöt edellyttävät syvyyttä, jolla tarkoitetaan, että tietoa suojataan useammalla kuin yhdellä mekanismilla. Gregoryn (2003, 29–30) mielestä tekninen haavoittuvuus, väärät asetukset tai kohdennettu hyökkäys tiettyyn suojausmekanismiin voi johtaa tiedon vaarantumiseen, mikäli syvyydestä ei ole huolehdittu. Suojausmekanismin syvyys tulee aina suhteuttaa uhkaan, riskiin ja käytettäviin resursseihin.

3.3.1 Käyttäjien tunnistaminen ja todentaminen

Käyttäjien tunnistaminen ja todentaminen on organisaation yleisimpiä tietoturvallisuusmekanismeja. Tunnistaminen voi olla yksinkertaisimmillaan käyttäjätunnus, jolla kirjaudutaan organisaation tietokoneelle tai tietoverkkoon. Tunnistaminen ilman todentamista on heikko ja epäluotettava suojausmekanismi.

Todentamisen tarkoitus on varmistaa, että käyttäjä on kuka hän väittää olevansa. Tunnistamisen yhteydessä kysyttävä salasana on yleisin todentamisen toteuttava suojausmekanismi. Käyttäjätunnus yhdistettynä tunnusta vastaavaan salasanaan toteuttaa tyypillisimmän vakuuden käyttäjän identiteetistä (Gregory 2003, 30). Lähes kaikki nykypäivän tietojärjestelmät tarjoavat teknisen mahdollisuuden tämän kaltaiseen käyttäjän tunnistamiseen ja todentamiseen.

Yleisesti tunnistaminen ja todentaminen toteuttavat määritelmää: jotain jota käyttäjällä on ja jotain jota käyttäjä tietää. Heikko todentaminen on sitä, että vakuudet perustuvat yhteen käytäntöön kuten kirjoitettava käyttäjätunnus ja salasana. Vahva

todentaminen perustuu useamman käytännön yhdistelmään, kuten fyysiseen toimikortti ja PIN-koodi(*personal identification number) (Vacca 2009, 59).* Organisaation tietoturvallisuuspolitiikassa tulisi määrittää tunnistamiseen ja todentamiseen käytetyt menetelmät. Tämän lisäksi tulisi määrittää, missä yhteydessä vaaditaan vahvaa tunnistamista ja missä yhteydessä riittää heikko tunnistaminen?

3.3.2 Järjestelmien todentaminen

Käyttäjän ja tietojärjestelmän välistä rajapintaa (*people-to-system*) hallitaan käyttäjän tunnistamisella ja todentamisella. Käyttäjän lisäksi tietojärjestelmät toteuttavat rajapintoja myös toisiin tietojärjestelmiin (system-to-system). Käyttäjät ovat ensisijaisesti kiinnostuneita tiedosta, joka palvelee heidän tarkoitustaan. Tiedon tuottava järjestelmä ei välttämättä ole sama, kuin tiedon esittävä järjestelmä. Käyttäjän kannalta merkityksellistä on se, että esitettävä tieto on luotettavaa ja ajankohtaista.

Yksinkertaisimmillaan tietojärjestelmä koostuu käyttäjälle esitettävästä käyttöliittymästä ja tiedon tallentamiseen tarkoitetusta tietokannasta. Tämän tyyppisissä tietojärjestelmissä todentaminen tapahtuu ns. isäntä-pohjaisesti (*host-based authentication*), jolloin kaikki todentamiseen tarvittava tieto on yksittäisen tietojärjestelmän sisällä (Gregory 2003, 34). Useiden käyttäjätunnusten ja salasanojen tarve viittaa siihen, että organisaatiolla on käytössään paljon isäntä-pohjaiseen todentamiseen perustuvia tietojärjestelmiä.

Isäntä-pohjaiseen todentamiseen perustuvat tietojärjestelmät soveltuvat parhaiten pienten organisaatioiden tarpeisiin, jossa toiminta rakentuu muutaman tietojärjestelmän käyttöön. Toiminnan kasvaessa käyttäjähallinnasta muodostuu valtavia ylläpidollinen työkuorma ja käyttäjät alkavat suosimaan yksinkertaisia salasanoja oman toimintansa helpottamiseksi.

Isommissa organisaatioissa toiminta perustuu useiden tietojärjestelmien tuottaman tiedon hyödyntämiseen. Palvelu-pohjainen todentaminen (*service-based authentication*) perustuu keskitettyyn käyttäjähallintaan, jossa yhtä todentamista hyödynnetään lukuisissa tietojärjestelmissä. Organisaation LDAP (*lightweight directory access protocol*) on laajasti käytetty palvelu-pohjaisen todentamisen standardi (Gregory 2003, 34–37).

Organisaation tietoturvallisuuspolitiikassa tulisi kuvata järjestelmien välinen todentaminen ainakin yleisellä tasolla. Toteutetaanko uudet tietojärjestelmät isäntäpohjaisella todentamisella vai pitääkö kaikkien tietojärjestelmien kyetä keskitettyyn käyttäjähallintaan? Mikäli tavoitteena on palvelu-pohjainen todentaminen, niin minkälaisiin tekniikoihin on sitouduttu?

3.3.3 Valtuuttaminen

Valtuuttamisella tarkoitetaan konseptia, mekanismeja ja teknologioita joilla hallitaan käyttäjien oikeuksia. Organisaatiossa on työntekijöitä, joilla on tietty tehtävä ja tehtävän hoitaminen edellyttää pääsyä tiettyihin tietoihin. Valtuuttamisen tavoitteena on hallita organisaation omistamaa tietoa ja henkilöitä, joilla on tarve päästä tähän tietoon (Gregory 2003, 39).

Vacca (2009, 256) toteaa, että tietoa tai tietojärjestelmää operoivien henkilöiden on ymmärrettävä toimintaan liittyvät riskit. Valtuuttamista käsitellään hallinnoinnin helpottamiseksi rooleilla, jotka ovat sidoksissa henkilön tehtäviin organisaatiossa. Vaikka organisaation toimitusjohtajalla olisi teoriassa mahdollisuus toimia esimerkiksi tietokantojen ylläpitäjän roolissa, niin hän ei välttämättä ymmärrä toimintaan liittyviä riskejä joten rooli olisi organisaation näkökulmasta riski.

Roolipohjaisen valtuutuspolitiikan toteuttamisen ongelma on se, että teorioiden toteutukselle on olemassa heikosti teknisiä apuvälineitä. Organisaatio voi tunnistaa toiminnallisista rooleista johdetut tekniset roolit ja niihin liittyvät toiminnot, mutta tekninen toteutus vaatisi koko olemassa olevan infrastruktuurin muuttamista. Tämä johtuu siitä, että roolipohjaisille toteutuksille ei ole olemassa laajasti käytettyjä standardeja, joten valmisohjelmistot tukeutuvat omiin mekanismeihin.

Roolipohjaisten standardien puuttuminen on aiheuttanut sen, että valtuuttaminen perustuu edelleen voimakkaasti pääsylistojen (*access control lists*) kaltaisiin teknisiin toteutuksiin. Pääsylistat perustuvat siihen, että tietoa sisältävät resurssit on paloiteltu osiin joihin annetaan oikeuksia pääsylistojen kautta (Vacca 2009, 257). Tietoturvallisuuden kannalta tämän tekniikan ongelmana on se, että pääsylistojen tekninen ylläpito pääsee käsiksi kaikkeen tietoon. Tämän lisäksi pääsylistojen ylläpito on työlästä

ja pääsyoikeudet muovautuvat pikemminkin henkilökohtaisiksi kuin työtehtäviin liittyviksi.

3.3.4 Pääsynhallinta

Pääsynhallinnalla tarkoitetaan teknisiä toimenpiteitä, jolla rajoitetaan pääsyä tietoon ja tietotekniseen infrastruktuuriin. Pääsynhallinnan rooli teknisessä tietoturvallisuudessa on korostunut merkittävästi Internetin voimakkaan kasvun myötä. Internet on osaltaan mahdollistanut organisaation maantieteellisen riippumattomuuden ja yhteistyökumppaneiden välisen teknisen verkottumisen.

Pääsynhallinta on organisaation yleisin suojausmekanismi, jolla suojataan organisaatiolle arvokasta pääomaa. Fyysisiä toimitiloja suojataan lukollisilla ovilla, valvontakameroilla, aidoilla ja vartijoilla. Näiden toimenpiteiden tarkoituksena on konkreettisesti rajoittaa pääsyä tiloihin tai ennaltaehkäisevästi viestittää ulkopuoliselle turvallisuusmekanismien olemassaolosta.

Fyysisten toimitilojen lisäksi organisaation täytyy huolehtia pääsynhallinnasta tietoteknisessä infrastruktuurissa. Organisaation tietoverkkojen liittäminen Internetiin tai yhteistyökumppanin tietoverkkoihin edellyttää pääsynhallinnan toteuttamista. Toteutuksen haasteellisuutta lisää se, että uudet ohjelmistot ja tietojärjestelmät vaativat toimiakseen kasvavassa määrin yhteyksiä tietoverkkoihin (Gregory 2003, 41;Vacca 2009, 349).

Palomuuri on parhaiten tunnettu pääsynhallinnan tekninen apuväline, kun suojataan organisaation tietojärjestelmiä ja tietoverkkoja. Nykyisessä uhkaympäristössä palomuurista on muodostunut tietoturvallisuuden kriittinen elementti. Palomuurin tavoitteena on toteuttaa pääsynhallintaa tietokoneiden, tietoverkkojen ja palvelimien välillä. Tästä syystä sitä hyödynnetään yleisesti rajapinnoissa, joissa yhdistyvät luotettava ja epäluotettava tietoverkko (Vacca 2009, 349–350).

Palomuurin toimintaperiaate on kuin organisaation tietoturvallisuuspolitiikka supistetussa kokonaisuudessa. On tapahtumia, joihin reagoidaan ennalta määritettyjen sääntöjen mukaisesti. Palomuuri ottaa vastaan tietoliikennepaketteja ja vertaa niitä luotuihin sääntöihin. Vertailun perusteella paketin kulku, joko estetään tai sallitaan.

Vertailu perustuu tietoliikennepaketin tunnistetietoihin, joita ovat: käytetty protokolla, lähteen osoite, lähteen portti, kohteen osoite ja kohteen portti (Vacca 2009, 350–351).

Tunkeutumisen havaitsemis- ja estojärjestelmät (IDS-järjestelmät) ovat tietoverkkojen valvontakameroita. IDS-järjestelmät kuuntelevat passiivisena verkkoa ja niiden tavoitteena on havaita epäilyttävää liikennettä, joka voisi johtua mahdollisesta hyökkäyksestä. IDS-järjestelmät voidaan jakaa kahteen ryhmään perustuen niiden toimintaperiaatteeseen: verkkopohjaiset ja isäntäpohjaiset. Verkkopohjaiset IDS-järjestelmät ovat yhteydessä tietoverkkoon ja tarkkailevat kaikkea siellä tapahtuvaa liikennettä. Isäntäpohjaiset IDS-järjestelmät ovat ohjelmistopohjaisia, jotka asennetaan tiettyyn kohteeseen ja niiden tavoitteena on tunnistaa mahdolliset hyökkäysyritykset kohdetta vastaan (Gregory 2003, 44).

Palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät ovat organisaation tietoverkkojen pääsynhallinnan perusta. Palomuurit voidaan rinnastaa fyysisessä pääsynhallinnassa lukittuihin oviin ja IDS-järjestelmät kameravalvontaan. Tietoturvallisuuspolitiikassa tulisi ehdottomasti kuvata näiden turvallisuusmekanismien rooli organisaatiossa ja niiden vaikutus muiden turvallisuusmekanismien käyttöönottoon.

3.3.5 Kryptografia

Kryptaus on prosessi, jossa selkokielinen tieto muutetaan salaiseksi ja jonka lukeminen vaatii salausta vastaavan avaimen. Kryptaus on tekniikka, jolla ensisijaisesti torjutaan uhkaa, jossa tiedon fyysinen hallinta menetetään. Fyysisen hallinnan menettämisellä tarkoitetaan tilanteita, jossa organisaation tietoa voidaan käsitellä muiden turvallisuusmekanismien ulottumattomissa. Tyypillisimpiä tilanteita ovat laitevarakaudet, tiedonsiirto sekä onnistuneet hyökkäykset.

Kryptauksen taustalla on aina ihmisen tekemä matemaattinen funktio, joka toteuttaa varsinaisen kryptauksen. Tämä on välttämätöntä, koska kryptauksen tarkoitus ei ole tärvellä tietoa vaan mahdollistaa sen käyttö luotettavien osapuolien toimesta. Vacca (2009, 397) toteaa, että kaikissa ihmisen tekemissä järjestelmissä on olemassa myös haavoittuvuus ja on vain ajan kysymys kun joku löytää sen. Tästä syystä kryptauksen

luotettavuuteen tulisi suhtautua skeptisesti ja käsitellä sitä yhtenä suojausmekanismina muiden joukossa.

Kryptauksella on olemassa kaksi pääasiallista käyttökohdetta: tallennetun tiedon suojaus ja tiedonsiirron suojaus. Tallennetun tiedon suojauksessa kryptaus mahdollistaa lisäturvan tilanteisiin, joissa pääsynhallinta ja valtuuttaminen on pystytty ohittamaan. Lisäturva perustuu siihen olettamukseen, että epäluotettavalla osapuolella ei ole mahdollista purkaa kryptausta tai purkamiseen arvioitu aika vähentää tiedon merkitystä (Gregory 2003, 48).

Tiedonsiirrossa kryptauksen merkitys korostuu, koska yleisimmät tiedonsiirtoprotokollat välittävät tietoa selväkielisenä. Kustannustehokkain tapa korjata tämä puute on VPN (virtual private network) tuotteet, joilla tiedonsiirto salataan käytettäessä epäluotettavia tietoverkkoja kuten Internetiä. Oman tiedonsiirtoverkon vuokraaminen teleoperaattorilta tai kokonaan oman verkon rakentaminen ovat kustannuksiltaan huomattavasti kalliimpia vaihtoehtoja.

Kryptausta hyödyntävien tuotteiden elinkaari on vaikeasti ennustettavissa. Algoritmista löydetty ja helposti hyödynnettävä heikkous, joka ei ole korjattavissa romuttaa koko suojaustekniikan mielekkyyden (Tipton & Krause 2006, 1030). Kryptauksen merkitys tietoturvallisuudessa perustuu luottamukseen ja uskomukseen algoritmin ominaisuuksista. Tietoturvallisuuspolitiikassa tulisi ottaa kantaa luotettaviin algoritmeihin ja niiden rooliin organisaatiossa. Kryptauksen roolia määriteltäessä on hyvä muistaa, että tehdyt investoinnit voivat valua hukkaan algoritmin murtuessa.

3.3.6 Valvonta

Tietoturvallisuudessa valvonnalla (*audit*) tarkoitetaan tietoteknisten laitteiden, tietojärjestelmien, tietoverkkojen ja ohjelmistojen tapahtumien nauhoittamista ja kirjaamista (*log*). Kirjatuista tapahtumista käytetään nimitystä ”audit trail”, jota käytetään apuna tietoteknisten ongelmatilanteiden selvittämisessä ja tietoturvallisuuteen liittyvissä tutkimuksissa (Gregory 2003, 66).

Nykyiset tietotekniset järjestelmät sisältävät runsaasti ominaisuuksia tapahtumien tallentamiseksi ja ympäristöjen kasvaessa tapahtumien määrä voi aiheuttaa hallitse-

mattoman tietomäärän. Tapahtumien tallentaminen ei varsinaisesti tuo organisaatiolle lisäarvoa, jos nauhoitettuja tapahtumia ei seurata tai niihin ei reagoida. Nauhoitetut tapahtumat voivat sisältää arvokasta tietoa mahdollisista tietomurtoyrityksistä tai käytettävyyteen liittyvistä ongelmista.

Tietoturvallisuudessa valvonnalla on keskeinen rooli, koska sitä kautta pystytään saamaan ajankohtaista tietoa turvallisuusmekanismien riittävyydestä ja toimivuudesta. Tämän lisäksi tehokkaalla valvonnalla on ennaltaehkäisevä vaikutus organisaation sisältä tapahtuviin tietoturvaloukkauksiin. Tehokkaan valvonnan tavoitteena on kirjata kriittiset tapahtumat, sijoittaa ne oikeaan aikaikkunaan ja huolehtia tapahtumatietojen eheydestä (Vacca 2009, 17). Tapahtumatietojen eheydellä on keskeinen rooli, jos niitä aiotaan käyttää esimerkiksi juridisena todisteena tietoturvaloukkauksissa.

Valvonta on toiminto, johon on mahdollista kohdentaa huomattava määrä resursseja. Tietoturvallisuuspolitiikassa valvontaa tulisi käsitellä tavoitteiden ja vaatimusten muodossa. Onko pyrkimyksenä reagoida kaikkiin epäilyttäviin tilanteisiin lähes reaaliajassa? Tämä tavoite edellyttäisi huomattavien resurssien kohdentamista valvontaan. Huomattavasti vähemmillä resursseilla tullaan toimeen, jos tavoitteena on huolehtia siitä että mahdolliset epäilyttävät tilanteet ovat jälkikäteen todennettavissa tallennetuista tapahtumatiedoista.

4 COMMON CRITERIA (CC)

Common Criteria (ISO/IEC 15408) on kansainvälinen tietoturvallisuusstandardi, jolla voidaan kuvata tietoturvallisuustavoitteita, vaatimuksia ja luottamuksellisuutta kansainvälisesti tunnustettujen menetelmien mukaisesti.

4.1 Historia

Common Criterian (Common Criteria for information Technology Security Evaluation) historia ulottuu yli 30-vuoden kehitysjaksoon, johon on osallistunut useita organisaatioita useista eri maista. Pitkäjänteisen kehitystyön ja usean eri organisaation panoksen johdosta, sitä on alettu pitää johtavana tietoturvallisuusstandardina.

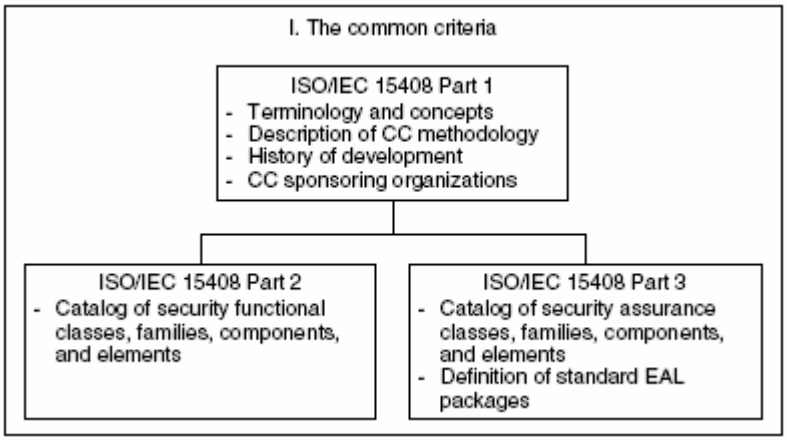
Yhdysvalloissa kehitettiin vuonna 1983 ns. Orange Book eli Trusted Computer System Evaluation Criteria (TCSEC), joka julkaistiin standardina CSC-STD-001-83. Tätä pidetään yleisesti CC:n ensimmäisenä epävirallisena julkaisuna, koska sen sisältö oli hyvin samankaltainen kuin CC:n sisältö aina tänä päivänäkin. Standardi oli suunnattu puolustusvoimien tarpeisiin tehtyjen ohjelmistojen tietoturvallisuus evaluointeihin tuon ajan tekniikat huomioiden. Standardin ongelmana oli se, että tekniikan kehittyessä kohti verkottunutta ja tietokantapohjaista tietojenkäsittelyä, standardin sisältämät käytännöt eivät sopineet uuden tekniikan tuomiin haasteisiin. (Tipton & Krause 2006, 1487–1488.)

Samoihin aikoihin Yhdysvaltojen ulkopuolella vuosina 1990–1993 the Commission of the European Communities, the European Computer Manufacturers Association (ECMA), the Organization for Economic Cooperation and Development (OECD), the U.K. Communications-Electronics Security Group ja Canadian Communication Security Establishment (CSE) julkaisivat omia tietoturvallisuusstandardejaan. (Mts. 1489.)

Organisaatiot päättivät yhdistää voimansa vastapainoksi kasvaville tietoturvallisuus vaatimuksille ja Kanadasta, Ranskasta, Saksasta, Hollannista, Englannista sekä Yhdysvalloista tuli ensimmäiset CC projektiin sitoutuneet valtiot vuonna 1993. Valtioiden

muodostama CC Editing Board (CCEB) julkaisi ensimmäisen version CC:stä julkiseen tarkasteluun vuonna 1996. (Mts. 1490.)

Common Criterian (ISO/IEC 15408) uusin versio on v3.1. Release 3, joka julkaistiin heinäkuussa 2009. CC jakautuu kolmeen osa-alueeseen kuvion 7 esittämällä tavalla.



KUVIO 7. Common Criteria parts 1-3 (Tipton & Krause 2006, 1492.)

4.2 Osa 1: Johdanto ja yleismalli

Osa 1 sisältää lyhyen kuvauksen Common Criterian historiasta ja organisaatioista kehityksen takana. Kuvaa konseptin perusteet, käytettävät käsitteet sekä yleiset toimintaperiaatteet. Ensimmäisessä osassa esitellään myös konseptin neljä keskeisintä osa-aluetta: Protection Profiles (PPs), Security Targets (STs), Target of Evaluation (TOEs) ja Packages.

Protection Profile (PP) on kokoelma tietoturvatavoitteita ja – vaatimuksia tuotteille, jotka edustavat asiakastarpeita. Tyypillisesti PP:tä käytetään tuoteperheissä, joilla pyritään lisäämään organisaation tietoturvallisuutta kuten palomuurit, kytkimet, reitittimet ja toimikortit. Asiakkaat voivat käyttää profilointia apuvälineenä määrittäessään turvallisuustavoitteitaan ja tuotteen toimittajat käyttävät sitä referenssinä tietoturvaominaisuuksista.

TAULUKKO 2. Standard EAL Packages (Tipton & Krause 2006, 1496.)

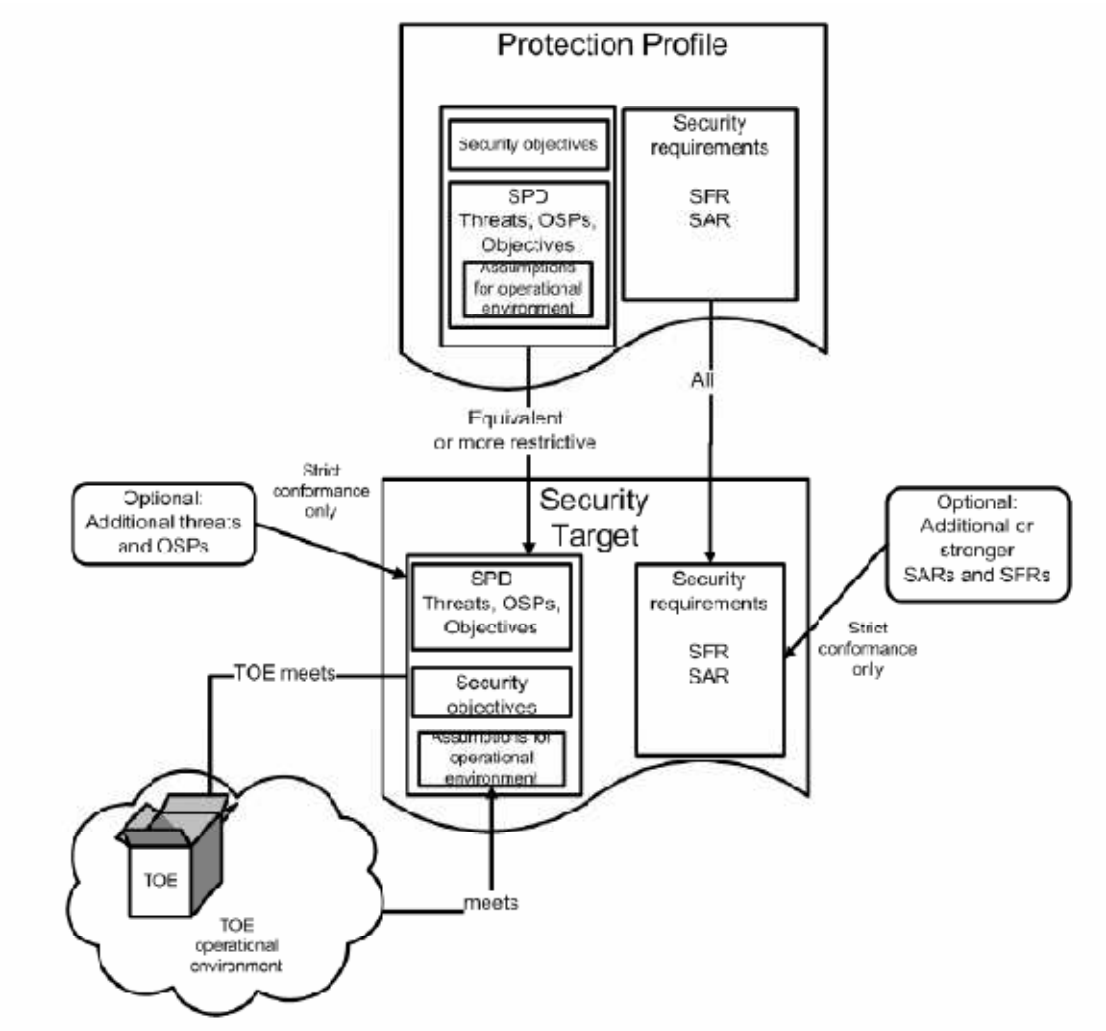
Short Name	Long Name	Level of Confidence
EAL 1	Functionally tested	Lowest
EAL 2	Structurally tested	
EAL 3	Methodically tested and checked	
EAL 4	Methodically designed, tested, and reviewed	Medium
EAL 5	Semi-formally designed and tested	
EAL 6	Semi-formally verified design and tested	
EAL 7	Formally verified design and tested	Highest

Taulukon 2 mukaisesti Protection Profileille määritellään toiminnallisten tietoturvavaatimusten lisäksi Common Criterian mukainen luottamustaso, jota kuvataan EAL (Evaluation Assurance Level) määritteellä. EAL tasoja on olemassa 1-7, joista EAL1 edustaa pienintä luottamustasoa ja EAL7 suurinta luottamustasoa.

Security Target (ST) on tuoteriippuvainen vastine PP:lle. ST on tietyn tuoteperheen tietylle mallille tehty osoitus siitä, miten malli toteuttaa PP:ssä asetetut tietoturvallisuustavoitteet ja – vaatimukset. Tyypillisesti esim. palomuurivalmistajat pyrkivät toteuttamaan tuoteperheitään tietyn PP:n mukaisesti ja tietyille korkeaa luottamusta vaativille malleille tehdään ST.

Target of Evaluation (TOE) on arvioinnin kohteena oleva tuote, tietojärjestelmä tai tietoverkko. Arvioinnissa otetaan huomioon myös kohteen ylläpitotoiminnot ja loppukäyttäjän ohjeistus. TOE on ST:n fyysinen ilmentymä ja konkreettinen tuote, jota halutaan arvioida luottamuksellisuuden, eheyden ja käytettävyyden näkökulmista.

Kuviossa 8 esitetään Common Criterian keskeisimpien käsitteiden välinen yhteys. Security Target kuvaa tietylle konkreettiselle tuotteelle (esim. StoneGate FW-1020 (palomuuri)) asetettuja tietoturvallisuus tavoitteita ja vaatimuksia. Protection Profile puolestaan kuvaa yleisellä tasolla tälle tuoteperheelle (palomuurit) asetettuja tavoitteita ja vaatimuksia. Tästä syystä valmista Protection Profilea voidaan käyttää mallina Security Targetin evaluoinnissa.



KUVIO 8. PP:n, ST:n ja TOE:n välinen suhde (CCPART1V3.1R3 2009, 53.)

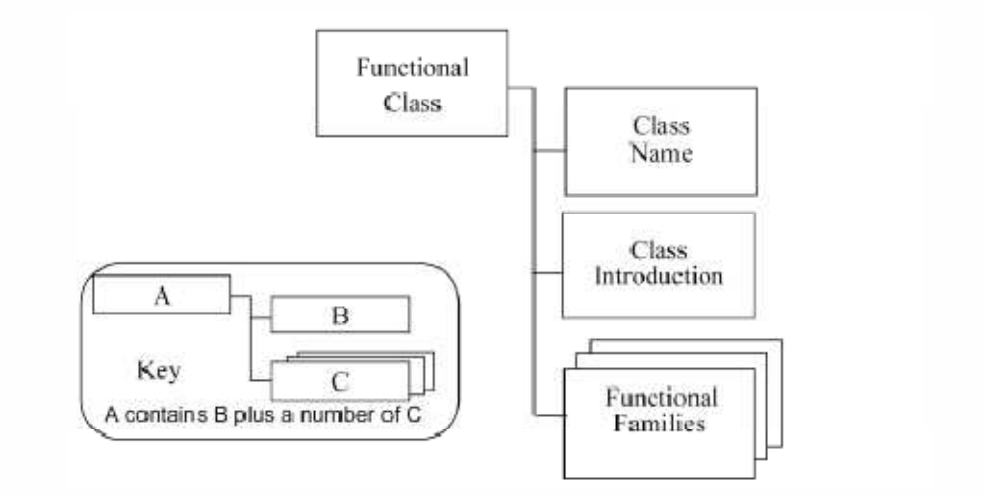
Package on joukko itsenäisiä toiminnallisia vaatimuksia tai todentamismekanismeja, joita kerätään kasaan toteuttamaan tunnistetut turvallisuustavoitteita. Näitä joukko- ja alatason vaatimuksia käytetään esim. rakennettaessa uusia PP:tä tai ST:tä. Tyypillisesti esim. palomuurin yksi turvallisuustavoite on estää ulkopuolisen tunkeutuminen organisaation sisäverkkoihin. Tämän turvallisuustavoitteen saavuttaminen saattaa tarkoittaa satojen alatason toiminnallisten vaatimusten toteutumista. Nämä tietyn turvallisuustavoitteen toteuttavat vaatimukset kerätään joukoksi, jota kutsutaan CC:ssä termillä Packages.

4.3 Osa 2: Tietoturvan toiminnalliset vaatimukset

Osa 2 esittelee joukon standardoituja toiminnallisia komponentteja, jotka luovat pohjan Protection Profilessa (PP) tai Security Targetissa (ST) esitellyille toiminnallisille turvallisuusvaatimuksille. Valituilla toiminnallisilla vaatimuksilla kuvataan TOE:n käyttäytyminen tietoturvallisuuden näkökulmasta. (CCPART2V3.1R3 2009, 13). Ennen siirtymistä toiminnallisiin vaatimuksiin on huolehdittava, että torjuttavat uhat ovat tiedostettu ja turvallisuustavoitteet ovat olemassa. Tämän lisäksi on oltava käsitys TOE:n operatiivisesta käyttöympäristöstä ja oletukset sen torjumista uhista.

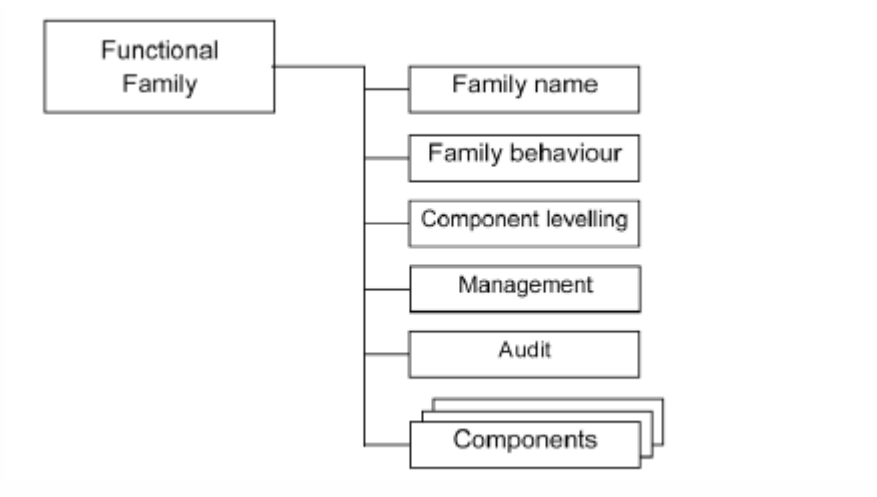
Luokka (*functional class*) on aina joukko turvallisuusvaatimuksia, jotka tähtäävät tiettyyn yhteiseen päämäärään esim. tunnistaminen ja todentaminen (*FIA: Identification and authentication class*). Common Criterian versiossa 3.1 on näitä toiminnallisia luokkia 11 kappaletta. Luokat ovat standardin korkein aste tietoturvavaatimusten näkökulmasta ja luokkien välillä ei ole keskinäistä hierarkiasuhdetta. Luokkien sisällä on ns. perheitä (*functional family*), jotka koostuvat toiminnallisista tietoturvavaatimuksista ja jakavat saman turvallisuustavoitteen. Tiettyyn luokkaan kuuluva perhe saa luokan tunnisteen esim. käyttäjän todentaminen (user authentication) olisi FIA_UAU. Näitä perheitä on yhteensä 67 kappaletta.

Kuviossa 9 on esitetty, miten luokka sisältää kohdat luokan nimen (*class name*), luokan esittelyn (*class Introduction*) ja yhden tai useamman perheen. Luokan nimi toteuttaa tietokentän yksilölliselle tunnisteelle. Luokan esittelyssä esitellään tapa ja riippuvuudet joilla eri perheitä on aikomus ottaa käyttöön, jotta turvallisuustavoitteet täyttyvät.



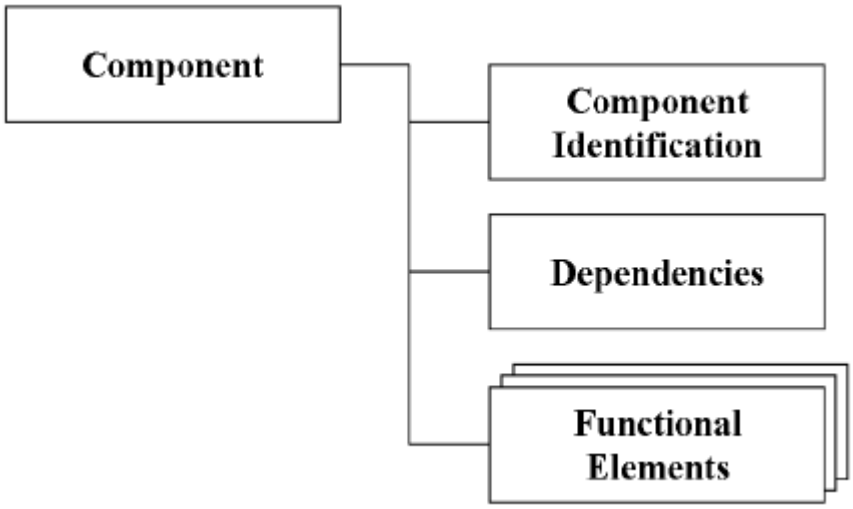
KUVIO 9. Functional class structure (CCPART2V3.1R3 2009, 23.)

Kuviossa 10 on esitetty, miten perhe sisältää kohdat perheen nimi (*family name*), käyttäytymismalli (*family behaviour*), komponenttivalinta (*component levelling*), hallinta (management), audit ja yhden tai useamman komponentin (*components*). Perheen nimi toteuttaa yksilöivän tunnisteen käytettävälle joukolle. Käyttäytymismalli toteuttaa kuvauksen turvallisuustavoitteista ja toiminnallisista vaatimuksista, joihin tämän perheen komponenteilla pyritään vaikuttamaan. Komponenttivalinta pitää sisällään yhden tai useamman komponentin, joilla on merkittävä rooli valitun perheen toteuttamissa turvallisuusvaatimuksissa. Hallinta-kenttä on tarkoitettu Protection Profilen tai Security Targetin ylläpitäjille tiedoksi siitä, että kyseiseen komponenttiin liittyy ylläpidollisia velvoitteita. Audit tietosisältö on käytössä silloin, kun turvallisuustavoitteet vaativat turvallisuustapahtumien kirjaamisen.



KUVIO 10. Functional family structure (CCPART2V3.1R3 2009, 24.)

Luokkien ja perheiden lisäksi Common Criteria versio 3.1 sisältää 138 kappaletta turvallisuus komponentteja (*security functional components*) ja 250 kappaletta turvallisuus elementtejä (security functional elements). Komponentti on kuvion 11 esittämän mallin mukaisesti määritelty joukko turvallisuusvaatimuksia, jotka on luotu elementeistä. Elementti on siis yksittäinen turvallisuusvaatimus, jonka toteutuminen on todennettavissa. Komponentti puolestaan pitää sisällään yhden tai useamman elementin eli turvallisuusvaatimuksen. Komponentti on pienin ryhmä turvallisuusvaatimuksia, joka voidaan sisällyttää Protection Profileen tai Security Targettiin.



KUVIO 11. Functional component structure (CCPART2V3.1R3 2009, 26.)

Organisaatio voi hyödyntää Common Criteriaa poimimalla siitä oman toimintansa kannalta parhaita käytäntöjä. Valmiiden tietoturvallisuus tavoitteiden ja vaatimuksien kopioimiseen CC:n osio 2 tarjoaa parhaat käytännöt. Toinen tapa on tarkastella valmiita Protection Profileja, jotka edustavat esimerkiksi hankinnan kohteena olevaa tuotetta. Varsinainen kolmannen osapuolen myöntämä sertifiointi, joka takaisi kansainvälisesti vertailukelpoisen kokonaisuuden edellyttää Common Criterian mukaista formaalia kuvausta.

4.4 Osa 3: Tietoturvan luottamusvaatimukset

Common Criteria perustuu periaatteeseen, jossa luottamus varmistetaan tuotteeseen kohdistuvalla evaluoinnilla. Luottamus muodostetaan standardissa kuvatuilla luottamusvaatimuksilla (*security assurance requirements*), jotka kuvaavat kriteerit PP:n, ST:n ja TOE:n evaluoinnille. CC:ssa luottamusvaatimukset muodostavat toiminnallisten vaatimuksien kaltaisen hierarkkisen kokonaisuuden, joka koostuu luottamusluokista (*assurance classes*), perheistä (*families*), komponenteista (*components*) ja elementeistä (*elements*). CC:n osiossa 3 on kuvattu 10 luottamusluokkaa, 42 perhettä ja 93 komponenttia (CCPART3V3 2009, 16;Tipton & Krause 2006, 1494).

Common Criteria standardi ei rajoita evaluointiprosessissa käytäviä vaiheita, mutta suosittaa seuraavanlaista mallia (CCPART3V3 2009, 17):

1. prosessien ja toimintatapojen analyysi sekä tarkastus
2. tarkastetaan, että kuvatut prosessit ja toimintatavat ovat käytössä
3. analysoidaan TOE toimintaa kuvaavat dokumentit
4. verrataan toimintaa kuvaavia dokumentteja vaatimuksiin
5. vahvistetaan todennukset
6. analysoidaan ohjeistuksen dokumentaatio
7. analysoidaan toiminnallisuuden testaus ja saadut tulokset
8. toteutetaan riippumaton toiminnallinen testaus
9. analysoidaan haavoittuvuudet

Evaluoinnin laajuus ja yksityiskohtaisuus perustuu tavoiteltuun luottamustasoon, jota ilmaistaan CC:ssa EAL-luokalla (*Evaluation Assurance Level*). Luottamustasolla pyritään vakuuttamaan kuluttaja tai asiantuntija siitä, että tuote täyttää sille asetetut turvallisuusvaatimukset. Luottamuksen pohjaksi on tehty vuonna 2000 kansainvälinen CCRA-sopimus (Common Criteria Recognition Agreement), jolla jäsenvaltiot ovat sitoutuneet luottamaan tuotteisiin, joille on myönnetty EAL-luokka. Sopimus käsittää EAL-luokat 1-4 ja sitouttaa jäsenet hyväksymään tuotteet ilman erillisiä evaluointeja. Sopimuksen on allekirjoittanut 12 valtiota joiden joukossa on myös Suomi (CCRA 2000, 1-6).

TAULUKKO 3. Luottamustason yhteenveto (CCPART3V3 2009, 31.)

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Taulukossa 3 on kuvattu CC:n luottamustason muodostumisen periaatteet. Tavoiteltua luottamustasoa (EAL) testataan luottamusluokilla (*assurance class*) ja niiden sisältämillä perheillä (*assurance family*). Perheet sisältävät komponentteja, jotka koostuvat yhdestä tai useammasta vaatimuksesta. Vaatimuksien määrää ja laajuutta on kuvattu taulukossa numeroin. Vaatimusten täyttyminen toimii vakuutena tuotteen tietoturvallisuudesta. Mitä suurempaa luottamusluokkaa tavoitellaan, sitä suurempia vakuuksia täytyy toteuttaa.

5 ILMAVOIMIEN TURVALLISUUSSUUNNITTELUMALLI JA SEN KEHITTÄMINEN

Tässä opinnäytetyössä kehitetyllä Ilmavoimien turvallisuussuunnittelumallilla kuvataan puolustusvoimien tietoturvallisuuden tahtotilaa, jotta reaalimaailman tietoturvallisuusvaatimuksilla suoritettavasta testauksesta olisi mahdollista tehdä tutkimusongelman kannalta mielekkäitä johtopäätöksiä. Malli on toteutettu tarjoamaan käytännön hyötyä julkaisemalla valmiita uhkia torjuvia tietoturvallisuusvaatimuksia, joita ilmavoimien projektipäälliköt ja asiantuntijat voivat hyödyntää tulevissa tarjouspyynnöissä.

5.1 Ilmavoimien turvallisuussuunnittelumallin luonti ja rakenne

Ilmavoimien turvallisuussuunnittelumalli on konstruktio puolustusvoimien tietoturvallisuuden tahtotilasta. Se perustuu opinnäytetyön teoriaan, jossa organisaation riskienhallinnasta on tunnistettu tietoturvallisuuteen kohdistuvia uhkia ja riskejä. Uhkien toteutumisen todennäköisyyden pienentämiseksi ja riskien vahinkojen lieventämiseksi organisaation tietoturvallisuuspolitiikassa on määritetty tietoturvallisuustavoitteita ja vaatimuksia. Kansainvälisen yhteensopivuuden saavuttamiseksi Ilmavoimien turvallisuussuunnittelumalliin on tuotu Common Criteria standardin määrittämiä tietoturvallisuustavoitteita ja vaatimuksia, joilla torjutaan vastaavia uhkia kuin kansallisilla vaatimuksillakin.

Ilmavoimien turvallisuussuunnittelumallin luonnissa torjuttavat uhat ja riskit on tuotettu puolustusvoimien riskienhallinnan asiakirjoista. Uhkia ja riskejä torjuvat tietoturvallisuuspolitiikat ovat tuotettu puolustusvoimien toimintaa ohjaavien lakien, pysyväisasiakirjojen ja VAHTI-ohjeistuksen sisällöstä niin, että niistä on muodostettu konkreettisia tietoturvallisuusvaatimuksia. Kansainväliset vaatimukset on tuotettu Common Criteria standardin valmiista turvallisuusprofiileista, joihin on valittu puolustusvoimien tietojärjestelmien kannalta keskeisiä osa-alueita. Mallin käytännön hyötyä on lisätty kytkemällä kansallisia ja kansainvälisiä tietoturvallisuuspolitiikoita torjuttavaan uhkaan.

TAULUKKO 4. Ilmavoimien turvallisuussuunnittelumallin rakenne

Riskienhallinta (U.PV.X)	**Tietoturvallisuuspolitiikka** (P.PV.X)	**Common Criteria** (P.CC.X)
U.PV.1	P.PV.1, P.PV.2, P.PV.3	P.CC.4
U.PV.2	P.PV.1, P.PV.2, P.PV.3	P.CC.4
U.PV.3	P.PV.1, P.PV.2, P.PV.3	P.CC.4
U.PV.4	P.PV.1, P.PV.3, P.PV.4, P.PV.5, P.PV.7	P.CC.1, P.CC.2, P.CC.3, P.CC.5
U.PV.5	P.PV.1, P.PV.5, P.PV.7	P.CC.2
U.PV.6	P.PV.1, P.PV.6, P.PV.7	P.CC.1, P.CC.2, P.CC.3
U.PV.7	P.PV.6	P.CC.1, P.CC.2
U.PV.8	P.PV.6	P.CC.1
U.PV.9	P.PV.5, P.PV.6	
U.PV.10	P.PV.6, P.PV.7	P.CC.1, P.CC.2
U.PV.11	P.PV.1, P.PV.3, P.PV.4, P.PV.6	P.CC.1, P.CC.5
U.PV.12	P.PV.1, P.PV.7	P.CC.1
U.PV.13	P.PV.1, P.PV.7	P.CC.1
U.PV.14	P.PV.7	
U.PV.15	P.PV.1	
U.PV.16	P.PV.3, P.PV.4, P.PV.5, P.PV.6, P.PV.7	P.CC.2, P.CC.5

Taulukko 4 kuvaa ilmavoimien turvallisuussuunnittelumallin rakenteen. Organisaation riskienhallinnasta tuotettuja tietoturvallisuusuhkia ja riskejä kuvataan lyhenteellä U.PV.X. Organisaation tietoturvallisuuspolitiikassa on kuvattu tietoturvallisuustavoitteita ja vaatimuksia, joilla tunnistettua uhkaa tai riskiä on tarkoitus hallita. Näistä tavoitteista ja vaatimuksista on koostettu politiikoita, joita kuvataan lyhenteellä P.PV.X. Common Criteriasta on otettu valmiita turvallisuusprofiileja (Protection Profiles), joiden sisältämät komponentit on koostettu politiikoiksi joita kuvataan lyhenteellä P.CC.X.

Tyypillisesti uhan tai riskin hallitseminen vaatii toimenpiteitä usealla eri tietoturvallisuuden osa-alueella. Tästä syystä Ilmavoimien turvallisuussuunnittelumallissa hallinta perustuu yhden tai useamman politiikan toteutumiseen. Mallia sovellettaessa on hyvä muistaa, että se on uhkien ja kansallisten tietoturvallisuuspolitiikoiden osalta konstruktio puolustusvoimien tietoturvallisuuden tahtotilasta – ei tutkijan näkemys

asiasta. Common Criteriasta tuotetut politiikat perustuvat tutkijan näkemykseen parhaista turvallisuusprofiileista puolustusvoimien kohdeympäristössä.

5.2 Puolustusvoimien riskienhallinta

Puolustusvoimien riskienhallintaa ohjataan pysyväisasiakirjalla PEturv-os PAK 01:03 Riskienhallinta puolustusvoimissa. Pysyväisasiakirjan sisältö on luonteeltaan oppikirjamainen, jolla kuvataan riskienhallinnan periaatteet ja käytännön toteutus puolustusvoimissa. Sisältö noudattaa vahvasti Valtiovarainministeriön VAHTI-ohjeistusta ja on sisällöllisesti kattava.

Pysyväisasiakirjan tärkein tavoite on järjestelmällisen riskienhallinnan liittäminen osaksi johtamista ja jokapäiväistä toimintaa. Se velvoittaa kaikkia puolustusvoimien työntekijöitä osallistumaan riskienhallintaan ja antaa perusteet sen toteuttamiselle. Varsinaisia puolustusvoimien toimintaan liittyviä uhkia tai riskejä ei kyseisessä pysyväisasiakirjassa mainita. PEturv-os PAK 01:03 mainitaan, että ohjausvastuussa oleva Pääesikunnan osasta vastaa oman toimialansa riskienhallinnan kehittämisestä, yksityiskohtaisesta ohjeistuksesta sekä koulutuksesta (PEturv-os PAK 01:03 2004, 3). Todellisuudessa toimialojen yksityiskohtaisia ohjeita ei ole olemassa.

Oinonen (2010, 32) totesi omassa tutkimuksessaan puolustusvoimien riskienhallinnasta, että se ei ole riittävällä tasolla. Yksittäisellä työntekijällä ei ole kapasiteettia tai resursseja toteuttaa riskianalyysiä, jossa tunnistetaan puolustusvoimien toimintaan kohdistuvia uhkia ja riskejä.

Puolustusvoimien toimintaan kohdistuvia uhkia on julkaistu PEturv-os PAK 01:02 puolustusvoimien turvallisuustoiminnan strategiassa. Strategia jakaa puolustusvoimien turvallisuuden: toiminnan turvallisuuteen, henkilöstöturvallisuuteen, tietoturvallisuuteen ja fyysiseen turvallisuuteen (PEturv-os PAK 01:02 2005, 4).

TAULUKKO 5. Puolustusvoimien tietoturvallisuusuhat

Lähde	Tunniste	Uhka
Peturv-os PAK 01:02	U.PV.1	Tietoverkkojen häirintä
Peturv-os PAK 01:02	U.PV.2	Tietoverkkojen lamauttaminen
Peturv-os PAK 01:02	U.PV.3	Tietoverkkojen tuhoaminen
Peturv-os PAK 01:02	U.PV.4	Tietojärjestelmien muuttaminen
Peturv-os PAK 01:02	U.PV.5	Tietojärjestelmien tuhoaminen
Peturv-os PAK 01:02	U.PV.6	Tietojärjestelmien käytön estäminen
Peturv-os PAK 01:02	U.PV.7	Tietovarannon ja asiakirjojen oikeudeton muuttaminen
Peturv-os PAK 01:02	U.PV.8	Väärän informaation levittäminen
Peturv-os PAK 01:02	U.PV.9	Puutteellinen asianhallinta
Peturv-os PAK 01:02	U.PV.10	Tiedon käsittelyoikeuksien hallitsemattomuus
Peturv-os PAK 01:02	U.PV.11	Luvaton haltuunotto
Peturv-os PAK 01:02	U.PV.12	Taitamaton toiminta
Peturv-os PAK 01:02	U.PV.13	Huolimattomuus
Peturv-os PAK 01:02	U.PV.14	Ohjeiden vastainen toiminta
Peturv-os PAK 01:02	U.PV.15	Tiedon käsittelyvaiheiden moninaisuus
Peturv-os PAK 01:02	U.PV.16	Hallitsematon jäljitettävyys

Taulukossa 5 on kuvattu puolustusvoimien turvallisuustoiminnan strategiassa kuvatut tietoturvallisuuteen kohdistuvat uhat ja riskit, jotka edustavat ilmavoimien turvallisuussuunnittelumallissa puolustusvoimien riskienhallinnan tahtotilaa.

5.3 Puolustusvoimien tietoturvallisuuspolitiikka

Puolustusvoimien tietoturvallisuuspolitiikan pääjulkaisuna toimii PEturv-os PAK 4:2: Tietoturvallisuus puolustusvoimissa. Pysyväisasiakirjan mukaan puolustusvoimien tietoturvallisuuden tavoitteena on mahdollistaa osaltaan puolustusvoimien toimintakyky kaikissa tilanteissa. Tämä tarkoittaa korkean käytettävyyden, hallitun eheyden sekä luottamuksellisuuden turvaamista hyvää tiedonhallintatapaa noudattaen (PEturv-os PAK 4:2 2003, 2).

Tietoturvallisuuden toteuttamisesta vastaavat joukkoyksiköiden vastuulliset johtajat. Tietoturvallisuus toteutetaan koko henkilöstön ja sidosryhmien toiminnan tuloksena. Puolustusvoimat kiinnittää erityistä huomiota henkilöstön tietoturvallisuustietoisuuteen tarjoamalla koulutusta ja ylläpitämällä kaikkien käytettävissä olevaa turvallisuus- ja tietoturvallisuusohjeistoa. Pääesikunta vastaa tietovarannolle ja tietopalveluille asetettavista tietoturvallisuustavoitteista, menettelytapojen ohjeistamisesta, tietoturvallisuustason todentamisesta ja raportoinnista (PEturv-os PAK 4:2 2003, 3).

Puolustusvoimien tietoturvallisuuspolitiikka muodostuu Suomen lain asettamista vaatimuksista ja pääesikunnan asettamista tietoturvallisuustavoitteista ja ohjeista. Tämän lisäksi PEturv-os PAK 4:13 VAHTI-ohjeiston käyttö puolustusvoimissa määrittää, että puolustusvoimat ottaa toiminnassaan huomioon VAHTI-ohjeiston. Mikäli puolustusvoimissa ei ole laadittu VAHTI-ohjeiston käsittelemältä osalta omaa PAK-asiakirjaa, suositellaan tällöin noudatettavaksi kyseistä VAHTI-asiakirjaa (PEturv-os PAK 4:13 2006, 2).

Taponen totesi omassa tutkimuksessaan, että puolustusvoimien tietoturvaohjeisto on pirstoutunutta ja ohjeita on paljon. Tämän lisäksi hän mainitsi, että julkaisumuoto ja sijainti vaihtelevat suuresti, eikä versionhallinnasta ole tietoakaan (Taponen 2003, 61). Tämän tutkimuksen havainnot tukevat Taposen havaintoja. Puolustusvoimien tietoturvallisuuden toteutusta ohjaavat Suomen lait on kerätty opinnäytetyön liitteeseen 1. Liitteeseen 2 on kerätty pääesikunnan asettamat pysyväisasiakirjat sekä normit ja liitteeseen 3 on kerätty tietoturvallisuutta ohjaava VAHTI-ohjeistus.

Ilmavoimien turvallisuussuunnittelumallissa olemassa olevasta ohjeistuksesta on kerätty tietoturvallisuustavoitteita ja vaatimuksia. Tavoitteet ja vaatimukset on yhdistetty seitsemäksi politiikaksi:

1. Yleinen (P.PV.1), joka sisältää 31 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 4.

2. Tiedonsiirto (P.PV.2), joka sisältää 55 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 5.

3. Palvelut ja palvelimet (P.PV.3), joka sisältää 13 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 6.

4. Päätelaitteet (P.PV.4), joka sisältää 42 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 7.

5. Tieto (P.PV.5), joka sisältää 25 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 8.

6. Käyttövaltuushallinta (P.PV.6), joka sisältää 20 tavoitetta/vaatimusta ja jonka sisältö on kuvattu liitteessä 9.

7. Hallinta ja valvonta (P.PV.7), joka sisältää 24 tavoitetta/vaatimusta ja jonka sisältä on kuvattu liitteessä 10.

Ilmavoimien turvallisuussuunnittelumallissa näillä seitsemällä politiikalla kuvataan puolustusvoimien tietoturvallisuusjohdon tahtotilaa tietoturvallisuustavoitteiden ja vaatimusten muodossa. Tuotetulla politiikalla tai sen sisältämällä yksittäisellä vaatimuksella on tarkoitus vaikuttaa tunnistetun uhkan toteutumisen todennäköisyyteen tai vahingon suuruuteen.

5.4 Kansainvälinen yhteensopivuus: Common Criteria

Puolustusvoimien tietoturvallisuus painottuu VAHTI-ohjeistukseen, jonka sisällöstä on tuotettu sisäisiä ohjausdokumentteja. Lisääntynyt kansainvälinen toiminta ja hankintojen volyymin kohdistuminen COTS (commercial of-the-self) sekä MOTS (military of-the-shelf) tuotteisiin asettaa paineita kansainvälisien turvallisuusstandardien käytölle. Kansainväliset toimittajat pyrkivät vakuuttamaan tuotteen tietoturvallisuusominaisuuksia standardien tuottamilla luottamusluokilla.

Puolustusvoimille kansainvälisellä turvallisuusstandardilla on olemassa kaksi pääasiallista tehtävää. Valmistuotteiden osalta on kyettävä ymmärtämään standardiin pohjautuvan luottamuksellisuuden osoitus ja sen vastaavuus kansallisissa vaatimuksissa. Räätälöityjen tuotteiden osalta on oltava kyky vaatia kansainvälistä yhteensopivuutta, joka tarkoittaa käytettävän standardin valintaa ja tietoturvallisuusvaatimuksien

esittämistä standardin mukaisilla menetelmillä. Molemmissa tapauksissa puolustusvoimilla on oltava riittävä asiantuntemus käytetystä standardista.

Ilmavoimien turvallisuussuunnittelumallissa on käytetty Common Criteria (ISO/IEC 15408) tietoturvallisuusstandardia soveltaen valmiita turvallisuusprofiileja. Valmiista turvallisuusprofiileista on tuotettu politiikoita, jotka sisältävät toiminnallisia tietoturvallisuuskomponentteja. Common Criteriassa komponentti sisältää yhden tai useamman tietoturvallisuusvaatimuksen ja on pienin yksittäinen joukko, joka voidaan sisällyttää turvallisuusprofiiliin. Turvallisuusprofiileista on tuotettu viisi politiikkaa:

1. Access control (Firewall PP V2.0 EAL4) (P.CC.1), joka sisältää 28 komponenttia ja jonka sisältö on kuvattu liitteessä 11.

2. Data protection (Cryptographic modules V1.0 EAL4)(P.CC.2), joka sisältää 43 komponenttia ja jonka sisältö on kuvattu liitteessä 12.

3. Databases (U.S Goverment PP V1.1 EAL2) (P.CC.3), joka sisältää 20 komponenttia ja jonka sisältö on kuvattu liitteessä 13.

4. Network (IP Encryptor PP V1.9 EAL3+) (P.CC.4), joka sisältää 34 komponenttia ja jonka sisältö on kuvattu liitteessä 14.

5. Operating systems (CCOPP-OS V2.0 EAL4+)(P.CC.5), joka sisältää 62 komponenttia ja jonka sisältö on kuvattu liitteessä 15.

Turvallisuusprofiilit on valittu sillä periaatteella, että ne edustavat tietoturvallisuuden osa-alueita joilta löytyy vastaavuus puolustusvoimien tietoturvallisuuspolitiikassa. Politiikkaan on kerätty turvallisuusprofiilista turvallisuusluokka ja luokan sisältämät toiminnalliset komponentit. Komponenttien yhteydessä oleva numeraalinen arvo (esim. FAU_GEN.**1** Audit data Generation) kuvaa toteutuksen laajuutta turvallisuusprofiilin luottamusluokassa.

6 TURVALLISUUSSUUNNITTELUMALLIN TESTAUS

Tutkimuksen empiirisen osuus muodostuu tapaustutkimuksesta, jonka kohteena ovat viiden ilmavoimien toteutusvastuulla olevan projektin tarjouspyyntömateriaalit. Hirsjärvi ja muut ovat todenneet, että tutkimusaineistojen keruussa olisi syytä pyrkiä ekonomiseen ja tarkoituksenmukaiseen ratkaisuun. Suurissa projekteissa saattaa hyvin olla analysoimatonta materiaalia, josta voi saada vastauksia tutkimusongelman joihinkin osiin (Hirsjärvi ym. 2001, 173).

Tarjouspyyntömateriaaleja tutkimalla haetaan vastausta kysymykseen: onko tietoturvallisuutta osattu vaatia ilmavoimien toteutusvastuulla olevissa projekteissa? Saadut tulokset eivät vielä itsenäisesti anna vastausta varsinaiseen tutkimusongelmaan. Tutkimusongelmaan haetaan ratkaisua testaamalla ilmavoimien turvallisuussuunnittelumallia projektien tietoturvallisuusvaatimuksilla.

6.1 Tapaustutkimuksen taustaa

Ilmavoimien Materiaalilaitos on 1.1.2010 perustettu Ilmavoimien komentajan alainen joukko-osasto, jonka ydintehtävänä on toimia puolustusvoimien ilmailun erikoismateriaalin elinjakson hallinnasta vastaavana materiaali- ja logistiikkalaitoksena (Ilmavoimien Materiaalilaitoksen työjärjestys 2010, 5).

Ilmavoimien Materiaalilaitoksen hankeosasto vastaa ilmavoimien toteutusvastuulla olevan materiaalisen suorituskyvyn tavoitetilan laatimisesta, materiaalisen suorituskyvyn kehittämisen suunnittelusta, materiaalisen suorituskyvyn ja ylläpidon rakentamisen suunnittelusta sekä materiaalisen suorituskyvyn rakentamisesta (Ilmavoimien Materiaalilaitoksen hankeosaston työjärjestys 2010, 1-3).

Ilmavoimien Materiaalilaitoksella ja erityisesti sen hankeosastolla on merkittävä rooli Ilmavoimien turvallisuussuunnittelun toteuttamisessa, koska se osallistuu suunnitteluvaiheeseen ja rakentamiseen. Käytännön vaikuttaminen tapahtuu, joko omin toimin sisäisesti tai projektinhallinnallisesti vaatimusten muodossa hankittavan tuotteen toimittajalta. Valtaosa materiaalisesta suorituskyvystä hankitaan ulkopuoliselta

toimittajalta, joko kotimaiselta tai ulkomaalaiselta teollisuudelta, joten vaatimustenhallinta on keskeisessä asemassa turvallisuussuunnittelussa.

Ilmavoimien toimintamallin mukaisesti operatiivinen toimiala tuottaa hankittavan suorituskyvyn toiminnalliset ja suorituskykyvaatimukset. Toiminnallisissa vaatimuksissa ilmaistaan selkokielellä se tahtotila, joka hankittavan tuotteen kautta pyritään saavuttamaan. Selkokielellä tarkoitetaan sitä, että tavoitteet ovat ymmärrettävässä muodossa myös niille toimijoille joilla ei ole vahvaa ilmapuolustuksen substanssiosaamista.

Toiminnalliset vaatimukset eivät ota kantaa hankittavaan tuotteeseen tai sen operoinnista välillisesti tai välittömästi aiheutuviin turvallisuusriskeihin. Tuotteeseen tai sen käytöstä aiheutuviin turvallisuusriskeihin vaikutetaan teknillisillä vaatimuksilla, jotka ovat tuotteen hankinnasta vastaavan organisaation vastuulla. Käytännössä teknilliset vaatimukset ja riskienhallinta toteutetaan projektissa, joka vastaa tuotteen hankinnasta. Vastuu henkilöityy projektipäällikköön ja mahdollisesti projektissa oleviin asiantuntijoihin.

6.2 Tutkimusprosessi

Tutkimuksen empiirinen aineisto on kerätty valmiista aineistosta. Hirsjärvi ja muut määrittävät, että valmiit aineistot voidaan jakaa viiteen luokkaan: viralliset tilastot ja tilastorekisterit, tilastotietokannat, arkistojen materiaalit, aikaisempien tutkimusten tuottamat materiaalit ja muut dokumenttiaineistot (Hirsjärvi ym. 2001, 174–176).

Tämän tutkimuksen empiirinen aineisto on arkistomateriaalia, joka on tuotettu osana hankintaprosessia Ilmavoimien Materiaalilaitoksen toimesta. Arkistomateriaali käsittää viiden Ilmavoimien toteutusvastuulla olevan projektin tarjouspyyntöasiakirjat ja sijaitsevat puolustusvoimien arkistossa. Osa tarjouspyyntöasiakirjoista on julkisuuslain mukaisesti turvaluokiteltuja, joten niitä käsitellään tutkimuksen toteutuksen kannalta välttämättömässä laajuudessa.

Tutkimusaineiston valintakriteerinä on toiminut tutkittavan kohteen toteutusvastuu, operatiiviset tavoitteet, ajankohtaisuus ja laajuus. Kaikki valitut tutkimuskohteet ovat

Ilmavoimien toteutusvastuulla olevia operatiivisia järjestelmiä, joilla on merkittäviä turvallisuustavoitteita ja arvioitu toteutuminen on vuosien 2000–2016 välisenä aikana. Laajuudella tarkoitetaan tässä yhteydessä arvioitua toteutuksen hintaa ja tutkimuskohteeksi on valittu, sekä muutaman miljoonan räätälöityjä järjestelmiä että kymmenien miljoonien MOTS-toteutuksia.

Tutkimusaineisto on sisällöllisesti kvalitatiivista eli laadullista. Tarjouspyyntömateriaalit pitävät sisällään kolmen tyyppistä dokumentaatiota:

1. Operatiivista määrittelyä, jonka on tuottanut Ilmavoimien operatiivisesta toiminnasta vastaavat tahot. Tällä dokumentaatiolla kuvataan hankittavalle kohteelle asetetut toiminnalliset tavoitteet ja käyttöperiaatteet.

2. Kaupallisia asiakirjoja, jotka on tuottanut Ilmavoimien hankintatoimi. Kaupalliset asiakirjat käsittävät sopimusluonnoksia ja sopimusehtoja.

3. Tekniset asiakirjat, jotka on tuottanut hankinnasta vastaava projekti. Teknisillä asiakirjoilla kuvataan hankittavalle kohteelle asetetut toiminnalliset tavoitteet ja käyttöperiaatteet vaatimusten muodossa.

Tapaustutkimuksen aineistoanalyysi kohdistuu tarjouspyyntömateriaalin teknisiin asiakirjoihin, joissa on kuvattu hankittavalle kohteelle asetetut tietoturvallisuusvaatimukset. Tutkimusaineiston tekniset asiakirjat käsittävät yhteensä 6238 vaatimusta, joista tietoturvallisuusvaatimusten osuus on 118.

Varsinaiseen tutkimusongelmaan liittyvä aineistoanalyysi on toteutettu testaamalla Ilmavoimien turvallisuussuunnittelumallia tapaustutkimuksessa kerätyillä tietoturvallisuusvaatimuksilla. Testauksen toteuttamiseksi jokaiselle projektin turvallisuusvaatimukselle on esitetty seuraavat kysymykset:

1. Torjutaanko vaatimuksella puolustusvoimien riskienhallinnasta tuotettua tietoturvallisuusuhkaa?

2. Toteuttaako vaatimus Ilmavoimien turvallisuussuunnittelumallissa esitettyä kansallista tietoturvallisuuspolitiikkaa?

3. Toteuttaako vaatimus Ilmavoimien turvallisuussuunnittelumallissa esitettyä kansainvälistä tietoturvallisuuspolitiikka?

Projektien tietoturvallisuusvaatimukset kerätään projektikohtaisiin havaintomatriiseihin, jossa yksittäisenä havaintoyksikkönä on tietoturvallisuusvaatimus ja muuttujina Ilmavoimien turvallisuussuunnittelumallissa toteutetut uhat, kansalliset tietoturvallisuuspolitiikat ja kansainväliset tietoturvallisuuspolitiikat.

TAULUKKO 6. Esimerkki projektikohtaisesta havaintomatriisista

Vaatimus		U.PV.X	P.PV.X	P.CC.X
1	Käyttöoikeus kuhunkin tietoalkioon tai niiden itse määriteltävään joukkoon/koontiin määritellään roolikohtaisesti.	U.PV.10	P.PV.6.13	P.CC.1
2	Järjestelmässä on vain käyttäjäkohtaisia tunnuksia	U.PV.10	P.PV.6.3	P.CC.1
3	Järjestelmä pitää itse huolen ohjelmaversionsa oikeellisuudesta ja koskemattomuudesta esim. tarkistussummin. Oikeellisuus tulee voida todentaa myös manuaalisesti järjestelmän käytön siitä kärsimättä. Ulkopuolisista yrityksistä puuttua järjestelmäversioon ilmoitetaan hälytyksin.	U.PV.13	P.PV.7.3	P.CC.2
4	Kaikki ylläpitotapahtumat (ei koske hakuja) käyttäjä-, rooli- ja ajankohtatietoineen tallennetaan lokiin jäljitettävyyden varmistamiseksi. Entä export-, ym. toiminnot?	U.PV.16	P.PV.7.12	P.CC.1

Taulukko 6 kuvaa projektikohtaista havaintomatriisia. Testaustapahtuma suoritetaan kolmessa vaiheessa, jossa ensimmäisessä vaiheessa verrataan projektien tietoturvallisuusvaatimuksia tunnistettuihin uhkiin (U.PV.X). Tietoturvallisuusvaatimuksen torjuma uhka kirjataan havaintomatriisiin uhkaa vastaavalla tunnuksella (esim. U.PV.10). Toisessa vaiheessa turvallisuusvaatimuksia verrataan toteutettuihin kansallisiin tietoturvapoliitikoihin (P.PV.X). Mikäli kansallisista tietoturvallisuuspolitiikoista löytyy vastaavuus, niin vaatimuksen tunniste kirjataan projektin havaintomatriisiin (esim. P.PV.6.3). Kolmannessa vaiheessa projektien tietoturvallisuusvaatimuksia verrataan Common Criteriasta johdettuihin poliitikoihin (P.CC.X) ja vastaavuudet kirjataan politiikkaa vastaavalla tunnuksella (esim. P.CC.2).

6.3 Projektien kuvaus

6.3.1 CORE

CORE (Common Operational Resources) on tietojärjestelmä, jonka tarkoituksena on tuottaa palveluja operatiivisen suunnittelun, johtamisen ja ryhmätyön tueksi. Palveluilla on tarkoitus tukea ilmavoimien johdon päätöksentekoa ylläpitämällä lähellä reaaliaikaa olevaa tilannekuvaa ilmapuolustuksen suorituskyvystä.

Järjestelmän palvelut pitävät sisällään toiminnot, joilla kerätään tietoa muista lähdejärjestelmistä ja loppukäyttäjiltä. Kerätty tieto varastoidaan tietokantoihin, joiden pohjalta on mahdollista luoda analyysejä sekä havainnollisia tilannekuvia johdon tarpeisiin. Järjestelmä voidaan luokitella ilmapuolustuksen tietämyksenhallintajärjestelmäksi Ilmavoimien tasolla ja se tullaan integroimaan osaksi Puolustusvoimien tiedustelun, valvonnan ja johtamisen järjestelmäkokonaisuutta. (CORE tekninen eritelmä 2005, 7-8.)

Hanke on tarkoitus toteuttaa kolmessa jaksossa, siten että vuosien 2006–2008 aikana toteutetaan Ilmavoimien operatiivisen suunnittelun ja johtamisen järjestelmätuki. Vuosien 2009–2011 välisenä aikana toteutetaan ilmapuolustuksen tilannekuva, yhteisoperaatioiden järjestelmätuki sekä liikkuvan sodankäynnin mahdollistaminen. Vuosien 2012–2014 aikana kehitetään ilmapuolustuksen simulointia. (Mts. 7-8.)

6.3.2 LSSJ FOMS

LSSJ FOMS (Flight Operations Management Service) on tietojärjestelmä, jonka tarkoituksena on rakentaa puuttuvia lento- ja taistelunjohto- ja lentoteknisen palveluksen suunnittelun, johtamisen ja seurannan palveluita ja kehittää tuotantokäytössä olevan tietojärjestelmän lentopalveluksen seurantaprosessia tukevia palveluja.

Ilmavoimien hävittäjälaivueet ja koulutuslentolaivueet ovat siirtyneet lentopalveluksen keskitettyyn johtamiseen. Lento- ja taistelunjohto- sekä lentoteknisen palveluksen suunnittelu ja johtaminen eivät ole tietojärjestelmätuen piirissä, vaan toiminta perustuu manuaalisiin työvaiheisiin ja tiedon monistamiseen. Laivueilla ja torjuntakeskuksilla on käytössään erilaisia taulukkolaskentaohjelmiin perustuvia työkaluja,

jotka eivät hyödynnä tietojärjestelmissä olevaa tietoa, vaan perustuvat tietojen manuaaliseen monistamiseen ja seurantatietojen syöttöön. (LSSJ FOMS tekninen eritelmä 2008, 10–11.)

Rakennettavat palvelut tuottavat myös lähellä reaaliaikaa olevan tilannekuvan henkilöstön palveluksen ja koulutuksen etenemisestä. Palvelut mahdollistavat OPSO:n (Operations Officer), FC10n (Fighter Controller 10 = taistelujohtopalveluksen esimies) ja MOCO:n (Maintenance Operations Center Officer = laivueen päivittäisen lentoteknisen palveluksen johtaja) välittömän reagoimisen ja muutokset päiväsuunnitelmaan esim. kalustoon tai järjestelmiin liittyvien vikaantumisten, henkilöiden sairastumisten, sään muuttumisen tai käskyn vuoksi. (Mts. 11–12.)

Tarkoituksena on tehostaa, nopeuttaa, automatisoida prosessin osia, kehittää suunnittelu- ja johtamisprosesseja, vähentää manuaalitoiminnoissa ilmeisten inhimillisten virheiden syntymistä mahdollistaen suunnittelun ja johtamisen keskittämisen lentolaivueissa ja torjuntakeskuksissa sekä lentoturvallisuuden paranemisen. Hanke rakentaa palvelut tukemaan koko puolustusvoimien lentotoimintaa kattaen ilmavoimien ja maavoimien lentotoiminnan.

6.3.3 KAVA MLU

KAVA MLU (Kaukovalvontatutkajärjestelmän päivitysmodifikaatio) on projekti, jonka tarkoituksena on päivittää viisi kappaletta kaukovalvontatutkajärjestelmiä ja näin ollen lisätä niiden operatiivista käyttöaikaa vuoteen 2025 asti.

Tutka-asemat ovat pääjohtokeskuksen valvontakeskuksen alaisia yksiköitä. Tutka-asemien tehtävänä on tuottaa valvonta-alueelta maalitietoa osana alueellisen koskemattomuuden valvontaa. Tutka-aseman henkilökuntaan kuuluu aseman päällikkö, tekninen henkilöstö ja tutkaoperaattorit. Aseman päällikkö johtaa aseman operatiivista toimintaa sekä teknisten laitteiden käyttöä, huolto ja ylläpitoa. (Kaisamatti 2008, 15.)

Kaukovalvontatutkajärjestelmä TRS 22 XX (KAVA) hankintapäätös Ranskasta tehtiin vuonna 1988. Järjestelmään kuuluu operatiivisen valvontatutkan lisäksi kahdennettu toisiotutkajärjestelmä. Kaukovalvontatutkien elinkaari on siinä pisteessä, että vanhe-

nevien osien saatavuus on heikko ja täten vaarantaa koko tutkan toimivuuden. Päivityksellä pyritään tehostamaan tutkan käytettävyyttä, luotettavuutta ja ylläpitokustannuksia. Tämän lisäksi päivityksellä korjataan käyttökokemuksiin perustuvia puutteita, joiden on havaittu aiheuttavan käytettävyysongelmia. (Kaisamatti 2008, 16–17;KAVA MLU RFQ 2007, 7-8.)

Fyysisten komponenttien lisäksi tutka integroidaan osaksi Puolustusvoimien integroitua tiedustelun, valvonnan ja johtamisen järjestelmäkokonaisuutta. Keskeisimpinä osa-alueina integroinnissa on tutkan etähallinta kyky, palvelukeskeisen arkkitehtuurin hyödyntäminen sekä liityntärajapinnat hankittavaan MST-järjestelmään (kts. 2.3.5 MST).

6.3.4 LINK-16 Ground Systems

LINK-16 Ground System (LGS) -järjestelmä korvaa nykyisen kansallisen taktisen tiedonsiirtojärjestelmän. LINK-16 – järjestelmä liitetään osaksi Puolustusvoimien integroitua tiedustelun, valvonnan ja johtamisen järjestelmäkokonaisuutta.

LINK-16 on Ilmavoimien nykyiseen datalinkkiin verrattuna kansainvälisesti yhteensopiva, suurikapasiteettinen, häiriötä hyvin kestävä ja tehokkaasti salattu tiedonsiirtojärjestelmä, joka tarjoaa lähes reaaliaikaisen taktisen tilannekuvan lisäksi navigointi- ja tunnistuspalveluita, salatun puheyhteyden, vapaamuotoisen tekstiviestipalvelun, maalitietojen korrelointia sekä mahdollisuuden sanomien releointiin tukiasemaverkon ulkopuolella oleviin aluksiin. LINK-16 mahdollistaa sanomien välityksen kaikkiin verkossa oleviin aluksiin yhtäaikaisesti. (LINK-16 Operatiivinen konsepti 2010, 9.)

LINK-16 on sanomiin perustuva tiedonsiirtojärjestelmä. Se perustuu J-sarjan sanomiin, jotka on määritelty Yhdysvaltain MIL-STD-6016 ja NATO:n STANAG 5516 – standardeissa. MIDS (Multifunction Information Distribution System) ja JTIDS (Joint Tactical Information Distribution System) ovat LINK-16 – järjestelmän käyttämiä J-sarjan sanomia välittäviä radiolaitteita. Järjestelmän käyttö edellyttää, sekä radiolaitetta että toiminnan integrointia alustaan ja sen johtamisjärjestelmään. (Mts. 10.)

6.3.5 MST

MST (Multi Sensor Tracking) on monisensorijärjestelmä, jonka avulla luodaan reaaliaikaista ilmatilannekuvaa koko valtakunnan alueelle. Hankittavalla järjestelmällä korvataan nykyisin käytössä oleva MRT (Multi Radar Tracking) järjestelmä, joka tuottaa ilmatilannekuvan pääasiassa lähi- ja kaukovalvontatutkien avulla.

Uuden sukupolven johtamisjärjestelmät tähtäävät voimakkaaseen verkostokeskeisyyteen, joka tarkoittaa vahvaa järjestelmien välistä integraatiota. Reaaliaikainen tilannekuva liitetään osaksi puolustusvoimien integroitua tiedustelun, valvonnan ja johtamisen järjestelmäkokonaisuutta. Verkostoitumisella tilannekuvaan saadaan myös muiden puolustushaarojen tilannetietoisuutta ja tilannekuva palvelee täten kaikkien puolustushaarojen tarpeita. (Salmivesi 2010, 3.)

Järjestelmän käyttö edellyttää tietojärjestelmäalustaa, varsinaista tietojärjestelmää ja integrointia tietosisältöä tuottaviin järjestelmiin. Tietojärjestelmäalustalla tarkoitetaan fyysisesti erillisiä toimipisteitä, joissa varsinainen MST-järjestelmä toimii. Tietosisältöä tuottavat tutkat, sensorit, puolustushaarat ja siviiliviranomaiset. (MST RFQ 2002.)

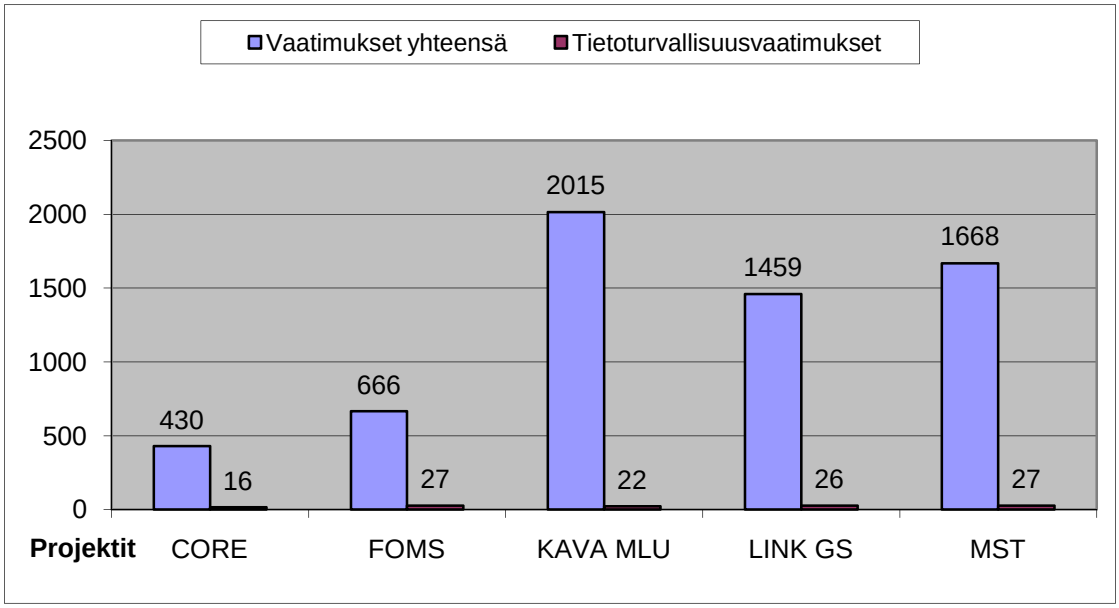
7 OPINNÄYTETYÖN TULOKSET

7.1 Tapaustutkimuksen tulokset

Tapaustutkimuksen tuloksena kerättiin viiden Ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimukset hankintaprosessissa syntyneen arkistomateriaalin perusteella. CORE:n, FOMS:n ja LINK-16 Ground Systemsin osalta tarjouspyyntömateriaalissa oli selkeästi jaoteltu tietoturvallisuusvaatimukset omaksi osioksi. KAVA MLU:n ja MST:n osalta tietoturvallisuusvaatimukset olivat hajautettu vaatimusmassaan, joten vaatimuksen tunnistaminen tietoturvallisuusvaatimukseksi edellytti tutkijan tulkintaa asiasta.

Kuviossa 12 esitetään vaatimusten jakautuminen projektien kesken. Mielenkiintoisena yksityiskohtana voidaan todeta se, että tietoturvallisuusvaatimuksien määrä ei

oleellisesti kasva vaatimusten kokonaismäärän lisääntyessä. Tälle ilmiölle mahdollinen selitys on se, että projektit toimivat itsenäisinä kokonaisuuksina ja kaikki torjuvat samoja uhkia.



KUVIO 12. Tietoturvallisuusvaatimuksien jakautuminen

Tietoturvallisuusvaatimuksien määrästä, suhteesta tai jakautumisesta projektien välillä ei ole mahdollista tehdä tutkimusongelman kannalta mielekästä analyysiä. Tämän tuloksen perusteella voidaan kuitenkin todeta, että Ilmavoimien toteutusvastuulla olevien projektien osalta tietoturvallisuusvaatimuksien osuus on keskimäärin alle 2 % vaatimusten kokonaismäärästä.

Kaikki tutkimuksen kohteena olleet projektit ovat käyneet puolustusvoimien tietohallintopäätösmenettelyn, jossa tietohallinnon ylin johto on antanut valtuudet siirtyä tarjouspyyntöjen lähettämiseen. Puolustusvoimien tietohallintojohto ottaa päätöksissään huomioon projektista tuotetun tietoturvallisuuslausunnon, jonka tuottaa THP-prosessissa puolustusvoimien johtamisjärjestelmäkeskuksen tietoturvallisuustoimisto projektin tuottaman materiaalin perusteella. Tästä voidaan todeta, että suhteellisen pienellä määrällä tietoturvallisuusvaatimuksia voidaan torjua puolustusvoimien operatiiviseen järjestelmään kohdistuvat uhat.

7.2 Uhkien testaus

Kerättyjä projektien tietoturvallisuusvaatimuksia verrattiin Ilmavoimien turvallisuussuunnittelumallin sisältämiin uhkiin. Uhkat ovat konstruoitu puolustusvoimien turvallisuustoiminnan strategiasta ja edustavat täten puolustusvoimien johdon näkemystä tietoturvallisuuden uhkaympäristöstä.

TAULUKKO 7. Tietoturvallisuusuhkien testauksen tulokset

Tunniste	CORE	LSSJ FOMS	KAVA MLU	LINK-16 GS	MST	Yht:	Osuus-%
U.PV.1	0	0	0	1	0	1	0,9 %
U.PV.2	0	0	0	0	0	0	0,0 %
U.PV.3	0	0	0	2	0	2	1,8 %
U.PV.4	1	1	0	0	0	2	1,8 %
U.PV.5	1	0	0	2	0	3	2,7 %
U.PV.6	3	3	4	7	0	17	15,3 %
U.PV.7	0	2	0	2	3	7	6,3 %
U.PV.8	0	2	1	0	3	6	5,4 %
U.PV.9	0	0	0	0	1	1	0,9 %
U.PV.10	3	4	5	4	2	18	16,2 %
U.PV.11	1	2	2	4	2	11	9,9 %
U.PV.12	0	1	0	0	4	5	4,5 %
U.PV.13	1	0	0	1	1	3	2,7 %
U.PV.14	3	5	0	0	1	9	8,1 %
U.PV.15	0	0	2	0	1	3	2,7 %
U.PV.16	1	4	6	3	9	23	20,7 %
Toteutuneet:	14	24	20	26	27	111	100,0 %
Osuus-%:	87,5 %	88,9 %	90,9 %	100,0 %	100,0 %	94,1 %	

Taulukko 7 esittää projektien tietoturvallisuusvaatimuksien jakautumisen torjuttavien uhkien kesken. Tulosta voidaan pitää vain osittain objektiivisena, koska puolustusvoimien turvallisuustoiminnan strategiassa uhat on ilmaistu yksittäisellä sanalla tai lauseella. Tämä jättää runsaasti tulkinnanvaraa ja tutkijan läheinen suhde tutkimuskohteeseen on voinut vaikuttaa tulkintaan.

Taulukko on rakentunut sillä perusteella, että tietoturvallisuusvaatimus on kohdistettu uhkaan jota se välittömästi torjuu. Tietoturvallisuusvaatimuksella on taipumus torjua välillisesti useita uhkia. Esimerkiksi tyypillisesti projektien tietoturvallisuusvaatimuksissa on vaadittu vahvaa käyttäjän tunnistamista. Välittömästi tällä vaatimuksella torjutaan tiedon käsittelyoikeuksien hallitsemattomuutta (U.PV.10), koska käyttäjän kiistämätön tunnistaminen on edellytys tietojärjestelmän valtuuttamisen luonnille.

Tuloksen ulkopuolelle jäi yhteensä seitsemän tietoturvallisuusvaatimusta, jotka eivät torju tunnistettuja uhkia. Nämä tietoturvallisuusvaatimukset vaativat tietoturvallisuusmekanismien suunnittelua ja toteutusta projektin toteutusvaiheessa, jolloin vaatimus ei konkretisoidu tutkimuksessa käytetyssä tarjouspyyntömateriaalissa. Esimerkki tämän tyyppisestä vaatimuksesta: ”*Järjestelmän turvallisuussuunnitelma luodaan kehittämisprojektin kuluessa ennen ensimmäisen palvelujen tuotantokäyttöön ottamista*”.

Yleisesti voidaan todeta, että tarkastelun kohteena olevien projektien tietoturvallisuusvaatimukset torjuvat kiitettävästi tunnistettuja tietoturvallisuuteen liittyviä uhkia. Hyvään tulokseen vaikuttaa merkittävästi se, että uhat on kirjoitettu hyvin korkealla tasolla eikä niiden sisältöä ole avattu tarkemmin. Tämän lisäksi projektien tietoturvallisuusvaatimukset ovat keskenään hyvin samankaltaisia, joka näkyy tuloksessa. Tietoturvallisuusvaatimukset kohdistuvat vahvaan käyttäjän tunnistamiseen (U.PV.10), tietojärjestelmän käytettävyyteen (U.PV.6) ja jäljitettävyyteen (U.PV.16).

7.3 Tietoturvallisuuspolitiikan testaus

Puolustusvoimien riskienhallinnasta tuotettuja tietoturvallisuusuhkia testaamalla saatiin selville se, että projektien tietoturvallisuusvaatimukset näyttäisivät torjuvan kiitettävästi tunnistettuja uhkia. Ilmavoimien turvallisuussuunnittelumallissa puolustusvoimien tietoturvallisuuspolitiikka on konstruoitu seitsemäksi politiikaksi, jotka käsittävät yhteensä 210 tietoturvallisuustavoitetta tai vaatimusta. Politiikat ja vaatimukset on johdettu puolustusvoimien tietoturvallisuuspolitiikan muodostavista asiakirjoista, ohjeista ja määräyksistä.

TAULUKKO 8. Tietoturvallisuuspolitiikan testauksen tulokset

Kansalliset politiikat	CORE	LSSJ FOMS	KAVA MLU	LINK-16 GS	MST	Yht:	Osuus-%
P.PV.1.Yleinen	9	5	6	5	2	27	24,3 %
P.PV.2.Tiedonsiirto	0	2	8	6	2	18	16,2 %
P.PV.3.Palvelut ja palvelimet	0	1	2	0	0	3	2,7 %
P.PV.4.Päätelaitteet	0	0	0	3	1	4	3,6 %
P.PV.5.Tieto	1	3	0	5	6	15	13,5 %
P.PV.6.Käyttövaltuushallinta	3	7	4	4	4	22	19,8 %
P.PV.7.Hallinta ja valvonta	2	5	2	2	11	22	19,8 %
Toteutuneet:	15	23	22	25	26	111	100,0 %
Osuus-%:	93,8 %	85,2 %	100,0 %	96,2 %	96,3 %	94,1 %	

Taulukko 8 esittää projektien tietoturvallisuusvaatimuksien jakautumisen toteutettujen politiikkojen kesken. Tuloksesta voidaan todeta, että projekteissa tuotetut tietoturvallisuusvaatimukset toteuttavat puolustusvoimien tietoturvallisuuspolitiikkaa. Tulos ei ole yllättävä, koska puolustusvoimien oma ohjeistus yhdistettynä VAHTI-ohjeistoon toteuttaa niin valtavan ohjeistomäärän, että on lähes mahdotonta kirjoittaa tietoturvallisuusvaatimusta joka ei olisi jonkin ohjeen mukainen.

Taulukko on rakennettu sillä periaatteella, että projektin tietoturvallisuusvaatimus tai tavoite on rinnastettu politiikan sisältämään vastineeseen. Rinnastamisessa on jouduttu tulkitsemaan vaatimusta, koska mikään projektin tietoturvallisuusvaatimuksista ei ollut sanasta sanaan identtinen politiikoissa esitettyjen vaatimusten kanssa. Tämän lisäksi KAVA MLU:n, LINK-16 Ground Systemsin ja MST:n vaatimukset ovat englanninkielisiä, joka omalta osaltaan lisää tulkinnanvaraa.

Tuloksen ulkopuolelle jäi seitsemän tietoturvallisuusvaatimusta, joista neljässä tietoturvallisuusvaatimuksen konkretisoituminen tapahtui vasta projektin edetessä. Kolmessa tapauksessa tietoturvallisuusvaatimus kohdistui projektinhallinnallisiin toimenpiteisiin. Esimerkkinä tämän tyyppisistä vaatimuksista voidaan esittää vaikka: ”*Hankkeen aikana toimittaja noudattaa toimittajan ja tilaajan välistä hankekohtaista*

turvallisuussopimusta". Vaatimuksella torjutaan uhkaa ja se edustaa ohjeiden vastaista toimintaa (U.PV15), mutta toteutetuista politiikoista sille ei löydy vastinetta.

Tietoturvallisuuspolitiikan testauksen tulokset tukevat jo uhkien testauksessa saatua mielikuvaa siitä, että projekteissa toteutetut tietoturvallisuusvaatimukset ovat laadullisesti edustavia. Laadulla tarkoitetaan tässä yhteydessä sitä, että tietoturvallisuusvaatimuksella torjutaan tunnistettua uhkaa ja se on tietoturvallisuuspolitiikan mukainen.

7.4 Common Criterian testaus

Ilmavoimien turvallisuussuunnittelumalli pitää sisällään viisi kansainväliseen yhteensopivuuteen tähtäävää politiikkaa. Politiikat perustuvat valmiiden turvallisuusprofiilien (Protection Profiles) sisältämiin tietoturvallisuuden toiminnallisiin vaatimuksiin. Politiikat eivät pyri konstruoimaan voimassaolevaa puolustusvoimien tietoturvallisuuden tahtotilaa, vaan tuottavat näkemyksiä kansainvälisesti vertailukelpoisen tietoturvallisuuden toteuttamisesta.

TAULUKKO 9. Common Criterian testauksen tulokset

Kansainväliset politiikat	CORE	LSSJ FOMS	KAVA MLU	LINK-16 GS	MST	Yht:	Osuus-%
P.CC.1.Access control	5	6	5	5	5	26	27,1 %
P.CC.2.Data protection	5	7	6	9	13	40	41,7 %
P.CC.3.Databases	2	1	0	3	1	7	7,3 %
P.CC.4.Network	0	2	6	6	2	16	16,7 %
P.CC.5.Operating systems	0	0	0	2	5	7	7,3 %
Toteutuneet:	12	16	17	25	26	96	100,0 %
Osuus-%:	75,0 %	59,3 %	77,3 %	96,2 %	96,3 %	81,4 %	

Taulukossa 9 on esitetty projektien tietoturvallisuusvaatimuksien jakautuminen Common Criteria standardista johdettujen politiikkojen kesken. Tuloksesta käy ilmi, että 81,4 % projektien tietoturvallisuusvaatimuksista toteutuu myös Common Crite-

riasta johdetuissa politiikoissa. Testauksessa käytetyt politiikat ovat sisällöllisesti tekniseen tietoturvallisuuteen painottuvia ja vain viidellä politiikalla pystyttiin kattamaan merkittävä osa projektien tietoturvallisuusvaatimuksista.

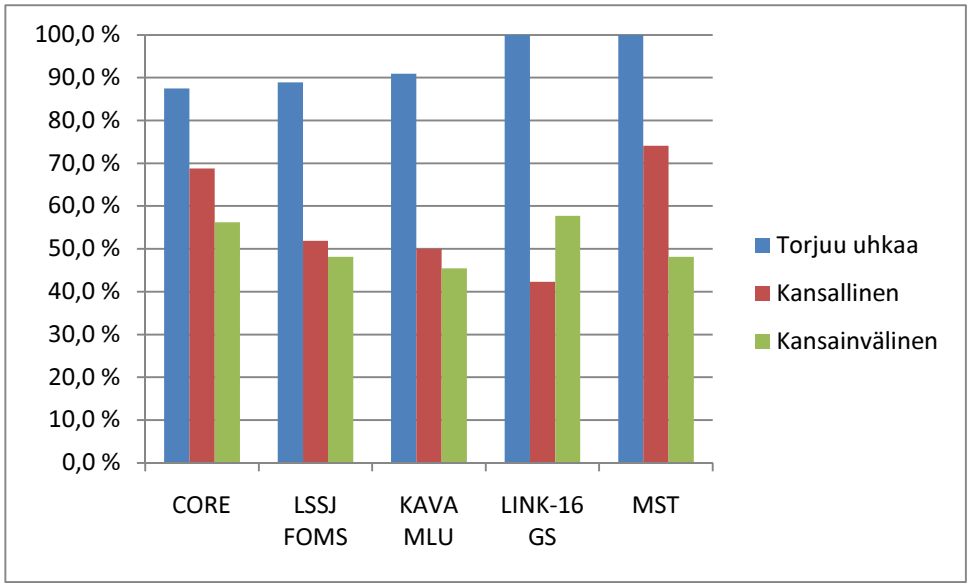
Tuloksista voidaan todeta se, että jo viidellä valmiilla turvallisuusprofiililla voidaan kattaa merkittävä osa testauksen kohteena olevien projektien tietoturvallisuusvaatimuksista. Tuloksesta ei pidä tehdä johtopäätöstä, että testauksen kohteena olleet projektit olisivat tietoturvallisuuden osalta kansainvälisesti vertailukelpoisia. Todellisuudessa projektien tietoturvallisuusvaatimukset vain raapaiset sitä vaatimuksien määrä, jota jokainen politiikka pitää sisällään.

Common Criterian turvallisuusprofiilit kuvaavat tietoturvallisuustavoitteet ja vaatimukset hyvin tarkalla tasolla. Käytännössä testattujen projektien tietoturvallisuusvaatimukset jakaantuvat turvallisuusprofiileissa kymmeniksi vaatimuksiksi joiden toteutuminen pitäisi osoittaa, jotta järjestelmät toteuttaisivat edes alimman tunnistetun (EAL1) luottamustason.

7.5 Ilmavoimien turvallisuussuunnittelumallin tulkinta

Ilmavoimien turvallisuussuunnittelumallilla haluttiin konstruoida puolustusvoimien tietoturvallisuuden tahtotilaa, jotta tapaustutkimuksen tutkimusmateriaalia voidaan analysoida tutkimusongelman kannalta mielekkäällä tavalla. Tämän lisäksi turvallisuussuunnittelumallin rakenteella haluttiin tuottaa lisäkontribuutiota organisaatiolle sitomalla kansallisia ja kansainvälisiä politiikoita tunnistettuun uhkaan. Tällä toiminnalla haluttiin edesauttaa mallin hyödyntämistä ehdottamalla politiikkoja, joista uhkaa torjuvat tietoturvallisuusvaatimukset todennäköisesti löytyvät.

Kuviossa 13 on kuvattu Ilmavoimien turvallisuussuunnittelumallin toteutuminen tapaustutkimuksessa olleiden projektien tietoturvallisuusvaatimuksien osalta. Optimaalinen tulos olisi tarkoittanut sitä, että satunnaisesti otettu tietoturvallisuusvaatimus olisi torjunut mallissa esitettyä uhkaa, sekä ehdotetun kansallisen että kansainvälisen politiikan mukaisesti. Tämän tuloksen perusteella toteutumisen todennäköisyys on tutkimuskohteiden osalta keskimäärin 67 %.



KUVIO 13. Ilmavoimien turvallisuussuunnittelumallin toteutuminen

Tuloksesta on nähtävissä, että LINK-16 Ground System projekti muodostaa poikkeaman yleisestä trendistä: projektin tietoturvallisuusvaatimukset toteuttavat enemmän kansainvälisiä politiikkoja kuin kansallisia. Projekti on tutkimuskohteista tuorein ja hankinta on kansainvälinen MOTS-tuote. Tulos selittyy sillä, että tietoturvallisuusvaatimuksissa on osattu ottaa huomioon hankinnan kansainvälinen luonne. Tietoturvallisuusvaatimuksissa ei ole viittauksia räätälöityihin kansallisiin toteutuksiin tai toimintatapoihin, jotka ovat luonnollisesti kansainvälisten standardien ulottumattomissa.

Tuloksien perusteella Ilmavoimien turvallisuussuunnittelumallia voidaan pitää lupaavana. Se konkretisoi puolustusvoimien tietoturvallisuuden tahtotilaa ja mallintaa uhkaperusteisen ajattelumallin. Tämän lisäksi se antaa konkreettisia tietoturvallisuusvaatimuksia, jotka mahdollistavat kansallisen ja kansainvälisen yhteensopivuuden.

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

8.1 Tutkimustulokset

Opinnäytetyön tavoitteet liittyivät käytännönläheiseen ongelmaan, jossa puolustusvoimissa hankittujen tuotteiden käyttöönotto suunnitellussa laajuudessa oli viivästynyt tai estynyt tietoturvallisuuteen liittyvien ongelmien vuoksi. Tämä tarkoitti sitä, että jossain tai jollain oli olemassa tietoturvallisuuden tahtotila jota hankittavien tuotteiden tulisi toteuttaa. Tämän lisäksi puolustusvoimien lisääntynyt kansainvälinen toiminta ja puolustusvoimien turvallisuustoiminnan strategiassa vaadittu kansainvälinen vertailukelpoisuus asetti lisätavoitteita toteutukselle.

Tutkimus perustuu konstruktiiviseen tutkimusotteeseen, jossa tutkimusongelmaa lähestyttiin kirjallisuustutkimuksen avulla. Teoriaosassa käsiteltiin riskienhallintaa, tietoturvallisuuspolitiikkaa ja Common Criteria (ISO/IEC 15408) turvallisuusstandardia, joiden perusteella luotiin konkreettinen konstruktio eli Ilmavoimien turvallisuussuunnittelumalli. Konkreettisessa konstruktiossa Ilmavoimien turvallisuussuunnittelumalliin tuotettiin reaalimaailman tietoturvallisuusuhkia puolustusvoimien riskienhallinnasta ja hallintamekanismeja puolustusvoimien tietoturvallisuuspolitiikasta, jolla vastattiin ensimmäiseen tutkimuskysymykseen. Tämän lisäksi Common Criteria standardista tuotettiin valmiita turvallisuusprofiileja konstruoimaan kansainvälistä yhteensopivuutta, jolla vastattiin toiseen tutkimuskysymykseen.

Tutkimuksen empiirisen osan muodosti tapaustutkimus, jossa viiden Ilmavoimien toteutusvastuulla olevan projektin tarjouspyyntömateriaalista tutkittiin tietoturvallisuusvaatimuksia. Ilmavoimien turvallisuussuunnittelumallia testattiin projektien tietoturvallisuusvaatimuksilla, jolla vastattiin kolmanteen tutkimuskysymykseen.

Seuraavaksi esitetään tutkimuksen lopulliset vastaukset tutkimuskysymyksiin, jotka perustuvat kirjallisuustutkimuksen teoriaan, Ilmavoimien turvallisuussuunnittelumallin toteutuksessa ja testauksessa tehtyihin havaintoihin sekä tapaustutkimuksen tuloksiin.

1. *Onko tietoturvallisuuden tahtotilaa kuvattu riittävässä laajuudessa?*

Konkreettisessa konstruktiossa tietoturvallisuuden tahtotila muodostui puolustusvoimien riskienhallinnassa tunnistetuista tietoturvallisuuteen liittyvistä uhista ja riskeistä, sekä puolustusvoimien tietoturvallisuuspolitiikassa määritetyistä hallintamekanismeista. Riskienhallinnassa tunnistettuja uhkia ja riskejä oli määrällisesti vähän, mutta ne oli toteutettu hyvin korkealla tasolla. Korkean tason kuvaus jättää runsaasti tulkinnanvaraa, joka heikentää uhkan tai riskin objektiivista tarkastelua.

Tapaustutkimuksen avulla toteutettu Ilmavoimien turvallisuussuunnittelumallin uhkien testaus osoitti, että projektin tietoturvallisuusvaatimukset torjuivat kiitettävästi tunnistettuja uhkia. Objektiivisuuden lisäämiseksi puolustusvoimien riskienhallinnassa tunnistettuja uhkia ja riskejä tulisi käsitellä riskienhallinnan teorian mukaisin toimenpitein. Puolustusvoimien riskienhallinnan uskottavuuden kannalta olisi tärkeää, että julkaistuja uhkia ja riskejä käsiteltäisiin edes organisaation omien määräysten mukaisesti.

Puolustusvoimien tietoturvallisuuspolitiikka muodostui Suomen lain, pysyväisasiakirjojen ja normien sekä VAHTI-ohjeistuksen muodostamasta kokonaisuudesta. Ohjeistuksen määrä oli niin valtavaa, että yksittäisen projektin kyky omaksua ohjeistuksen sisältö on vähintäänkin kyseenalaistettava. Ilmavoimien turvallisuussuunnittelumallissa asetuksista, määräyksistä ja ohjeista tuotettiin kansallisia politiikoita, jotka sisälsivät tietoturvallisuustavoitteita ja vaatimuksia.

Tapaustutkimuksen avulla tuotettu Ilmavoimien turvallisuussuunnittelumallin tietoturvallisuuspolitiikan testaus osoitti, että projektien tietoturvallisuusvaatimukset olivat tietoturvallisuuspolitiikan mukaisia. Käytännössä ohjeistuksen valtava määrä aiheuttaa sen, että tuloksesta tulisi tällä mittaustekniikalla vähintäänkin hyvä vaikka projektit eivät olisi tutustuneet koko ohjeistoon.

Tutkimuksen perusteella puolustusvoimien tietoturvallisuuden tahtotilaa on kuvattu tietoturvallisuustavoitteiden ja vaatimuksien osalta todella kattavasti. Varsinaiset ongelmat kohdistuvat riskienhallintaan ja tietoturvallisuuspolitiikan ohjeistuksen jakautumiseen sadoiksi yksittäisiksi dokumenteiksi. Riskienhallinnan lähes olematon kytkös varsinaisiin hallintamekanismeihin aiheuttaa sen, että projektien tietoturvallisuusvaatimuksia tuotetaan vain ja ainoastaan koska niitä pitää olla. Tällöin myös tie-

toturvallisuusresurssit kohdistuvat toimintoihin, jotka eivät välttämättä torju puolustusvoimien toiminnan jatkuvuuteen vaikuttavia uhkia.

2. *Miten yhdistetään kansallinen ja kansainvälinen yhteensopivuus?*

Tutkimuksessa valittiin kansainväliseksi standardiksi Common Criteria (ISO/IEC 15408) tietoturvallisuusstandardi, jota oli jo hyödynnetty yksittäisissä Ilmavoimien hankkeissa. Tutkimuksen teoriaosassa käsiteltiin Common Criterian periaatteita, rakennetta, kuvaustekniikoita ja luottamusluokkia. Teorian pohjalta konkreettiseen konstruktioon tuotettiin viisi kansainvälistä tietoturvallisuuspolitiikkaa, joiden sisältö tuotettiin valmiista turvallisuusprofiileista.

Yhteensopivuutta tutkittiin tapaustutkimuksella, jossa Ilmavoimien turvallisuussuunnittelumallin kansainväliset tietoturvallisuuspolitiikat testattiin viiden Ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimuksilla. Tuloksissa todettiin, että projektien tekniset tietoturvallisuusvaatimukset toteutuivat hyvin kansainvälisissä tietoturvallisuuspolitiikoissa.

Testauksen aikana kävi ilmi, että kansallisten vaatimuksien toteuttaminen edellyttää vain murto-osan vaatimuksista verrattuna kansainväliseen yhteensopivuuteen. Kansallisten vaatimusten toteutuminen arvioidaan puolustusvoimien tietohallintopäätösmenettelyssä ja kansainvälisen yhteensopivuuden takaava luottamusluokka (EAL) kolmannen osapuolen suorittamalla evaluoinnilla.

Kansallisen ja kansainvälisen yhteensopivuuden yhdistäminen edellyttäisi puolustusvoimien tietoturvallisuuden tahtotilan toteutumisen valvonnan viemistä aivan uudelle tasolle. Puolustusvoimien tietoturvallisuuspolitiikan asettamat tietoturvallisuustavoitteet ja vaatimukset ovat lähellä kansainvälistä yhteensopivuutta, mutta käytännön totutukset ovat aivan jotain muuta. Projektien yksittäiset tietoturvallisuusvaatimukset olivat kansainvälisen tietoturvallisuuspolitiikan näkökulmasta pikemminkin tietoturvallisuustavoitteita, joista olisi pitänyt johtaa kymmeniä teknisiä tietoturvallisuusvaatimuksia.

3. *Onko tietoturvallisuutta osattu vaatia ilmavoimien toteutusvastuulla olevissa projekteissa?*

Tutkimuksen empiirisessä osassa tapaustutkimuksella tutkittiin viiden ilmavoimien toteutusvastuulla olevan projektin tarjouspyyntömateriaalia. Tarjouspyyntömateriaalia tutkittiin kvantitatiivisesti eli määrällisesti selvittämällä tietoturvallisuusvaatimuksien osuus projektien vaatimusmassasta. Tämän lisäksi itse tietoturvallisuusvaatimuksia tutkittiin kvalitatiivisesti eli laadullisesti testaamalla toteutettua Ilmavoimien turvallisuussuunnittelumallia projektin tietoturvallisuusvaatimuksilla.

Tuloksien perusteella projektien tietoturvallisuusvaatimukset olivat puolustusvoimien uhkaympäristön mukaisia eli ne torjuivat kiitettävästi puolustusvoimien riskienhallinnasta tuotettuja uhkia. Projektien tietoturvallisuusvaatimukset toteuttivat myös puolustusvoimien tietoturvallisuuspolitiikkaa ja kansainvälinen yhteensopivuus toteutui ainakin tietoturvallisuustavoitteiden muodossa.

Tutkimustuloksien perusteella voidaan todeta, että ilmavoimien toteutusvastuulla olevien projektien tietoturvallisuusvaatimukset olivat laadullisesti puolustusvoimien tietoturvallisuuden tahtotilan mukaisia. Todellinen tutkimusongelman muodostava tekijä löytyi projektien tietoturvallisuusvaatimuksien määrästä ja kattavuudesta. Tämän lisäksi ongelman muodostumista on edesauttanut valvontamekanismin (THP) ristiriitaiset päätökset suhteessa tietoturvallisuuden tahtotilaan.

Tapaustutkimuksen kohteet muodostavat tietoteknisen ympäristön, jossa on todennäköisesti satoja palvelimia ja päätelaitteita. Tutkimuksen tuloksien perusteella näihin kahteen tietoteknisen ympäristön peruselementtiin kohdistui yhteensä seitsemän tietoturvallisuusvaatimusta. Esimerkiksi kolmen projektin osalta tutkimuksessa ei löytynyt ainuttakaan operoitavalle päätelaitteelle kohdistettua tietoturvallisuusvaatimusta.

Yksittäisten tietoturvallisuusvaatimuksien laatu ei riitä toteuttamaan kokonaisvaltaista tietoturvallisuutta. Tietoturvallisuutta pitää osata vaatia laadullisesti ja määrällisesti niin, että se kattaa hankittavan kohteen keskeisimmät osa-alueet. Mikäli projektin käytössä olevilla resursseilla ei pystytä tätä toteuttamaan, niin viimeistään puolustusvoimien tietohallintopäätösmenettelyssä ongelmaan tulisi puuttua.

Tietoturvallisuuden toteuttaminen alkaa hankinnoista, jossa tietoturvallisuuden tahtotilalle saadaan toimittajalta konkreettinen hinta. Hinnan lisäksi, hankinnassa esite-

tyillä vaatimuksilla sitoutetaan toimittaja tietoturvallisuuden toteutukseen. Valmiille tuotteelle jälkikäteen tehtävät tietoturvallisuustoimenpiteet ovat aina kustannuksiltaan moninkertaisia, koska tietoturvallisuusmekanismien vaikutus tuotteen toiminnallisille vaatimuksille täytyy testata.

8.2 Tulosten luotettavuus

Tutkimuksen luotettavuutta arvioidaan validiuden ja reliaabeliuden avulla, jotka ovat peräisin kvantitatiivisesta tutkimuksesta. Tutkimus sisälsi kirjallisuuskatsaukseen perustuvan teoriaosan, konkreettisen konstruktion ja konstruktion testaamisen tapaustutkimuksen empiirisellä aineistolla.

Tutkimuksen luotettavuus ja uskottavuus perustuu vahvasti siihen, että konkreettinen konstruktio kuvaa puolustusvoimien tietoturvallisuuden tahtotilan. Konstruktion uskottavuutta lisättiin painottamalla tutkimuksen teoriaosassa valtiovarainministeriön julkaisuja, puolustusvoimien sisäisiä ohjeita ja kansainvälisiä standardeja sekä tukemalla näitä alan muulla kirjallisuudella. Tämän lisäksi konstruktion luotettavuutta parannettiin julkaisemalla toteutuksessa käytetty reaalimaailman aineisto kokonaisuudessaan (Liitteet 1-15).

Tässä tutkimuksessa konkreettisesta konstruktiosta käytettiin nimitystä Ilmavoimien turvallisuussuunnittelumalli, koska konstruktiolle suoritettavien mittauksien tuloksia voidaan pitää luotettavina vain puolustusvoimien kohdeympäristössä. Konstruktion testaaminen edellytti kansallisen tietoturvallisuuspolitiikan osalta asetettujen ohjeiden ja määräysten tulkintaa konkreettisemmiksi tietoturvallisuusvaatimuksiksi. Tulkinnan luotettavuutta parantaa tutkijan omakohtainen kokemus kohdeympäristöstä ja tulkintojen julkaisu, jolloin lukija voi tehdä päätelmiä tulosten siirrettävyydestä.

Ilmavoimien turvallisuussuunnittelumallin testaus suoritettiin tapaustutkimuksella, joka käsitti viiden ilmavoimien toteutusvastuulla olevan projektin tietoturvallisuusvaatimukset. Tutkimusmateriaalia voidaan pitää luotettavana, koska se perustuu arkistomateriaalin joka on saatavissa puolustusvoimien arkistosta. Materiaali oli julkisuuslain perusteella turvaluokiteltua, joten tutkimuksen uskottavuutta parannettiin kuvaamalla käytetty aineisto (Luku 6.3).

Tapaustutkimuksen tulokset pätevät vain kontekstissa, joka on kuvattu Ilmavoimien turvallisuussuunnittelumallin testauksessa (Luku 6). Tapaustutkimuksen luotettavuutta ja uskottavuutta on parannettu kuvaamalla testausprosessi ja testauksen yhteydessä esitetyt kysymykset aineistolle (Luku 6.2). Tapaustutkimuksen aineisto edustaa merkittävää osaa ilmavoimien toteutusvastuulla olevista projekteista vuosien 2000–2016 välisenä aikana. Tästä syystä tapaustutkimuksen tuloksia voidaan pitää yleispätevinä kuvatussa kontekstissa.

8.3 Saavutettu hyöty

Tutkimuksen tavoitteena oli tunnistaa puolustusvoimien tietoturvallisuuden tahtotila ja toteuttaa käytännön työväline, jolla ilmavoimien projektien tietoturvallisuusvaatimuksia voidaan toteuttaa tahtotilan mukaisesti. Tutkimuksen teoriaosalla selitettiin tietoturvallisuusvaatimuksien taustalla olevat syy-seuraussuhteet. Teoriasta johdettiin käytännön hyötyä tuottava konkreettinen konstruktio eli Ilmavoimien turvallisuussuunnittelumalli, jossa teorian osa-alueet on kuvattu puolustusvoimien reaalimaailman vastineilla.

Ilmavoimien turvallisuussuunnittelumallilla tuotettiin, sekä käytännöllistä että teoreettista kontribuutiota. Käytännön hyöty on mitattavissa vasta tulevaisuudessa laadullisesti parempien ja puolustusvoimien tahtotilan mukaisten tietoturvallisuusvaatimuksien muodossa. Käytännön hyötyä pyrittiin lisäämään keräämällä tietoturvallisuuden tahtotilan muodostavat ohjeet yhden mallin sisälle ja jalostamalla tietoturvallisuuspolitiikoita konkreettisiksi vaatimuksiksi.

Hankittujen tuotteiden käyttöönoton viivästyminen tai estyminen tietoturvallisuuteen liittyvien ongelmien vuoksi toimi tutkimuksen pääongelmana. Alaongelmana toimi lisääntyneet vaatimuksen kansainvälisestä yhteensopivuudesta. Tutkimusongelman ratkaisu edellytti tietoturvallisuuden tahtotilan tunnistamista, kuvaamista ja mittaamista. Ilmavoimien turvallisuussuunnittelumallin teoreettinen kontribuutio tapahtui tunnistamalla ja kuvaamalla puolustusvoimien tietoturvallisuuden tahtotila. Tapaustutkimuksen avulla kuvattua tahtotilaa mitattiin viidellä ilmavoimien toteutusvastuulla olevan projektin reaalimaailman tietoturvallisuusvaatimuksilla.

Mittaustuloksien perusteella voidaan suositella seuraavia parannuksia puolustusvoimien tietoturvallisuuden kehittämiseksi ja tutkimusongelman ratkaisemiseksi:

1. Puolustusvoimien riskienhallinnassa tulisi erotella uhat ja riskit. Uhka tulisi olla itsenäinen kokonaisuus, jonka toteutuminen aiheuttaisi riskejä. Riskien hallintamekanismeille tulisi asettaa tavoite (välttäminen, pienentäminen, siirtäminen, pitäminen) joka mahdollistaisi oikean hallintamekanismin valinnan.
2. Puolustusvoimien tietohallintopäätösmenettelyä tulisi kehittää tietoturvallisuuslausuntojen osalta. Tietohallintopäätösmenettelyssä tulisi vaatia oikeasti samoja käytäntöjä kuin yksittäisissä tietoturvallisuuspolitiikan asiakirjoissa. Projektien päästäminen suunnitteluvaiheesta toteutukseen puutteellisilla tietoturvallisuusvaatimuksilla on keskeisin tutkimusongelman aiheuttaja.
3. Hankittavan tuotteen suunnitteluvaiheessa tulisi tehdä päätös tietoturvallisuuden kansainvälisestä yhteensopivuudesta. Kansallisten ja kansainvälisten tietoturvallisuusvaatimuksien yhdistäminen aiheuttaa todennäköisesti tilanteen, jossa kumpikaan osa-alue ei toteudu. Päätöstä tehdessä on huomioitava, että kansainvälinen luottamuksellisuus edellyttää formaalia kuvaustapaa (osaaminen) ja kolmannen osapuolen suorittamaa evaluointia (luottamus).
4. Ilmavoimien toteutusvastuulla olevien projektien tietoturvallisuusvaatimuksissa tulisi huomioida vaatimuksien kattavuus. On tunnistettava olemassa olevat turvallisuusmekanismit ja vaatia näiden käyttöä. Uudet vaatimukset tulisi kohdistaa osa-alueille, jotka ovat ominaisia itse hankittavalle tuotteelle ja joihin ei ole olemassa valmiita turvallisuusmekanismeja.
5. Ilmavoimien tulisi lisätä tietoturvallisuuden ammattilaisten panosta projektien suunnitteluvaiheessa. Tämä säästää resursseja rakennus- ja käyttöönottovaiheessa havaittujen puutteiden korjauskustannuksista.

Käytännön hyödyn lisäksi Ilmavoimien turvallisuussuunnittelumallin toteutuksen yhteydessä verifioitiin kaksi aiempaa aihepiiriin kohdistunutta tutkimustulosta. Oinonen (2010, 32) totesi tutkimuksensa perusteella, että puolustusvoimien turvallisuustoiminnot sekä niihin välittömästi liittyvät riskienhallinta ja sisäinen valvonta eivät ole yleisen mielikuvan mukaisia. Tämän tutkimuksen perusteella puolustusvoimien riskienhallinta on tietoturvallisuuden osalta liian korkealla tasolla, joka heikentää hallintamekanismien tehokasta hyödyntämistä. Valvontaa suoritetaan tietohallintopää-

tösmenettelyn tietoturvallisuuslausunnolla, joka tutkimuksen tuloksien perusteella toimii heikosti.

Taponen totesi omassa tutkimuksessaan, että puolustusvoimien ohjeistus ja toimintatavat tietoturva-asioissa on pirstoutunut. Ohjeita ja vaatimuksia on paljon, julkaisumuoto ja sijainti vaihtelevat suuresti, eikä versionhallinnasta ole tietoakaan (Taponen 2003, 61). Tämän tutkimuksen perusteella puolustusvoimien tietoturvallisuuspolitiikka on jakaantunut lähes sadaksi yksittäiseksi dokumentiksi, jotka ovat osittain sisällöllisesti päällekkäisiä. Tämän lisäksi osa dokumenteista on yli 10 vuotta vanhoja, joka heikentää niiden käytettävyyttä.

8.4 Jatkotutkimusaiheita

Tämän opinnäytetyön lähtökohtana oli varsinainen tutkimusongelma, johon törmäsin päivittäisissä työtehtävissäni Ilmavoimien Materiaalilaitoksessa. Ennen syvällisempää perehtymistä aihealueeseen minulla oli kaksi mielikuvaa, jotka osoittautuivat vääriksi varsinaisen tutkimusprosessin edetessä. Näistä ensimmäinen liittyi puolustusvoimien riskienhallintaan, josta kuvittelin löytäväni valtavasti materiaalia tunnistettujen uhkien ja riskien sekä tavoitteiden muodossa. Tämän lisäksi kuvittelin, että olisi jo olemassa puolustusvoimien tietoturvallisuuden tahtotilaa kuvaava kriteeristö johon projektien tietoturvallisuusvaatimuksia verrataan.

Yksi mielenkiintoinen jatkotutkimusaihe olisi puolustusvoimien tietoturvallisuuteen liittyvä riskianalyysi, jossa tutkittaisiin kansainvälisesti tunnistettujen tietoturvallisuusuhkien ja niiden käyttökelpoisuutta Suomen puolustusvoimien uhkaympäristössä. Puolustusvoimissa riskienhallintaa käsitellään todella vähän verrattuna julkisesti saatavilla olevan teorian ja tutkimustulosten määrään. Puolustusvoimien tietoturvallisuuteen kohdistuva riskianalyysi, jossa uhkien toteutumisesta johdettaisiin riskejä ja turvallisuustavoitteita tuottaisi välitöntä hyötyä tietoturvallisuuden näkökulmasta.

Toinen tietoturvallisuutta edistävä jatkotutkimusaihe olisi puolustusvoimien tietohallintopäätösmenettelyn tietoturvallisuuslausunnon kehittäminen. Olisi hyödyllistä toteuttaa kansallinen tietoturvallisuuskriteeristö, josta projekteilla olisi mahdollisuus todeta tavoitteet ja laajuus tietoturvallisuusvaatimuksille. Oman tutkimukseni tulok-

sena syntyneet kansalliset tietoturvapolitiikat konstruoivat puolustusvoimien turvallisuuspolitiikassa esitettyjä hallintamekanismeja. Puolustusvoimien operatiiviselta järjestelmältä vaadittava toteutuksen laajuus jää vielä avoimeksi kysymykseksi.

LÄHTEET

A Risk Management Standard. 2002. AIRMIC, ALARM, IRM. Viitattu 12.7.2010. http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Bacik, S. 2008. Building an Effective Information Security Policy Architecture. Auerbach publications.

CCPART1V3.1R3. 2009. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Viitattu 2.7.2010. http://www.commoncriteriaportal.org/thecc.html

CCPART2V3.1R3. 2009. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Viitattu 2.7.2010. http://www.commoncriteriaportal.org/thecc.html

CCPART3V3.1R3. 2009. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Viitattu 3.7.2010. http://www.commoncriteriaportal.org/thecc.html

CCRA. 2000. Arrangement on the Recognition of Common Criteria Certificates. Viitattu 17.8.2010. http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf

CORE tekninen eritelmä. 2005. CORE-järjestelmän tarjouspyynnön tekninen eritelmä. Hankinta-asiakirja. Puolustusvoimien asianhallintajärjestelmä (PVAH).

Garvey, P., R. 2009. Analytical methods for risk management: a system engineering perspective. Boca Raton: CRC Press, Taylor & Francis Group.

Gregory, P., R. 2003. Enterprise Information Security: Information security for non-technical decision makers. Edinburgh: FT Prentice Hall.

Hampton, J. 2009. Fundamentals of Enterprise Risk Management. New York: AMACOM.

Heikkinen, L, T. 2001. Narratiivisuus konstruktivistisena tutkimusotteena. Teoksessa Ikkunoita tutkimusmetodeihin. Toim. J. Aaltola ja R. Valli. Jyväskylä: PS-kustannus, 119.

Heikkilä, A-M., Murtonen, M., Nissilä, M., Virolainen, K. & Hämäläinen, P. 2007. Riski-analyysien laatu: vaatimukset tilaajalle ja toteuttajalle. Tutkimusraportti. VTT-R-037 17–07. Tampere. Viitattu 22.7.2010. http://www.tsr.fi/tsarchive/files/TietokantaTutkittu/2006/106117Loppuraportti.pdf

Hirsjärvi, S. & Hurme, H. 2004. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2001. Tutki ja kirjoita. 6.-7. painos. Vantaa: Tummavuoren kirjapaino Oy.

Ilmavoimien missio, visio ja strategiat. 2010. Viranomaisasiakirja. Puolustusvoimien asianhallintajärjestelmä (PVAH).

Ilmavoimien Materiaalilaitoksen työjärjestys. 2010. Viranomaisasiakirja. Puolustus-voimien asianhallintajärjestelmä (PVAH).

Ilmavoimien kansainvälinen toiminta. 2010. Ilmavoimien kansainvälinen valmiusyk-sikkö. Viitattu 29.6.2010. http://ilmavoimat.fi/. Kansainvälinen toiminta.

Kaisamatti, U. 2008. Teemana ilmavalvonta. Ilmatorjuntalehti1/2008, 15–17. Viitattu 8.7.2010. http://www.ilmatorjuntaupseeriyhdistys.fi/1_2008/index-1_2008.htm

KAVA MLU RFQ. 2007. Request for Quotation: Long Range Air Surveillance Radar (TRS 22XX MLU). Hankinta-asiakirja. Puolustusvoimien asianhallintajärjestelmä (PVAH).

Kosola, J. 2007. Suorituskyvyn elinjakson hallinta. Julkaisusarja 5. Maanpuolustuskor-keakoulu, Sotatekniikan laitos.

LINK-16 Operatiivinen konsepti. 2010. Versio 0.9. Asiakirja. Puolustusvoimien asian-hallintajärjestelmä (PVAH).

LSSJ FOMS tekninen eritelmä. LSSJ-osahankkeen, FOMS-palveluiden hankinnan tekninen eritelmä. Versio 1.11. Hankinta-asiakirja. Puolustusvoimien asianhallintajärjestelmä (PVAH).

Luotettavuusjohtaminen, osa3: käyttöopas, luku 9: teknisten järjestelmien riskianalyysi. 2000. Standardi SFS-IEC 60300-3-9. Suomen standardisoimisliitto SFS ry. Helsinki.

MST RFQ. 2002. Request For Quotation: Finnish Air Force Multi Sensor Tracking Surveillance System. Hankinta-asiakirja. Puolustusvoimien asianhallintajärjestelmä (PVAH).

Oinonen, J. 2010. Riskienhallinnan järjestäminen puolustusvoimissa COSCO ERM-mallin mukaisesti; esimerkkinä puolustusvoimien johtamisjärjestelmäkeskus. Tutkielma. Teknillinen korkeakoulu, Turvallisuusjohdon koulutusohjelma. Viitattu 22.7.2010. http://lib.tkk.fi/Reports/2010/urn100165.pdf

Peltier, T, 2005. Information Security Policies and Procedures. Auerbach publications.

PK-RH. PK-yrityksen riskienhallinta. Viitattu 13.7.2010. http://www.pk-rh.fi/, Riskienhallintaprosessin vaiheet.

Pääesikunnan johtamisjärjestelmäosasto. 2007. Tietohallintopäätösmenettely. Pysyväisasiakirja. PEjojä-os THP PAK Versio 2.0. Puolustusvoimien normitietokanta.

Pääesikunnan turvallisuusosasto. 2006. VAHTI-ohjeiston käyttö puolustusvoimissa. Pysyväisasiakirja. PEturv-os PAK 4:13. Puolustusvoimien normitietokanta.

Pääesikunnan turvallisuusosasto. 2005. Puolustusvoimien turvallisuustoiminnan strategia. Pysyväisasiakirja. PEturv-os PAK 01:02. Puolustusvoimien normitietokanta.

Pääesikunnan turvallisuusosasto. 2004. Riskienhallinta puolustusvoimissa. Pysyväisasiakirja. PEturv-os PAK 01:03. Puolustusvoimien normitietokanta.

Pääesikunnan turvallisuusosasto. 2003. Tietoturvallisuus puolustusvoimissa. Pysyväisasiakirja. PEturv-os PAK 4:2. Puolustusvoimien normitietokanta.

Salmivesi, T. 2010. Tiedon hajautus johtamisjärjestelmässä ja DDS-teknologia. Dilplomityö. Lappeenrannan tekninen yliopisto, teknistaloudellinen tiedekunta, tietotekniikan osasto. Viitattu 8.7.2010. https://oa.doria.fi/bitstream/handle/10024/59830/nbnfi-fe201003221539.pdf?sequence=3

Seppänen, V. 2004. Konstruktiivinen tutkimus. PowerPoint-esitys. Viitattu 2.7.2010. http://media.tol.oulu.fi/video/jtmk/konstruktiivinen_tutkimus.ppt

Tapaturmavakuutuslaki. 1948. L 20.8.1948/608. Viitattu 14.7.2010. http://www.finlex.fi/fi/laki/ajantasa/1948/19480608

Taponen, V. 2003. Tietoturvastandardit puolustusvoimien tietoturvaprosessien sekä ekstranet-ratkaisun kehittämisessä. Diplomityö. Teknillinen korkeakoulu, Tietotekniikan osasto, Tietoliikenneohjelmistojen ja multimedian laboratorio. Viitattu 24.7.2010. http://www.tml.tkk.fi/Publications/Thesis/taponen.pdf

Työntekijän eläkelaki. 2006. TyEL 395/2006. Viitattu 14.7.2010. http://www.finlex.fi/fi/laki/alkup/2006/20060395

Tipton, H. & Krause, M. 2006. Information Security Management Handbook. Sixth Edition. New York: Auerbach Publications.

Vacca, J., R. 2009. Computer and Information Security Handbook. Morgan Kaufmann publishers.

Valtiovarainministeriö. 2004. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. Viitattu 30.6.2010. http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

Valtiovarainministeriö. 2004. Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006. Viitattu 30.6.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/70508_fi.pdf

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI-ohje VM 41/01/2003. Viitattu 22.7.2010.

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf

Valtiovarainministeriö. 2001. Valtion viranomaisen tietoturvallisuustyön yleisohje. VAHTI-ohje. Viitattu 26.7.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3373/3374_fi.pdf

Valtiovarainministeriö. 2000. Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje. VAHTI-ohje. Viitattu 27.7.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

Valtiovarainministeriö. 1999. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta. Periaatepäätös, VM 0024:00/02/99/1998. Viitattu 27.7.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/6294_fi.pdf

Valtioneuvoston kanslia. 2004. Suomen turvallisuus- ja puolustuspolitiikka 2004. Valtioneuvoston kanslian julkaisusarja 16/2004. Viitattu 29.6.2010. http://www.vnk.fi/julkaisut/julkaisusarja/julkaisu/fi.jsp?oid=130642

VTT Riskianalyysin menetelmät. Valtion teknillinen tutkimuskeskus. Viitattu 22.7.2010. http://www.vtt.fi/proj/riskianalyysit/riskianalyysit_menetelmat.jsp

LIITTEET

LIITE 1. TIETOTURVALLISUUTEEN VAIKUTTAVA LAINSÄÄDÄNTÖ 91

LIITE 2. PUOLUSTUSVOIMIEN TIETOTURVALLISUUDEN PYSYVÄISASIAKIRJAT 92

LIITE 3. TIETOTURVALLISUUTTA KÄSITTELEVÄ VAHTI-OHJEISTO 93

LIITE 4. P.PV.1.YLEINEN 94

LIITE 5. P.PV.2.TIEDONSIIRTO 96

LIITE 6. P.PV.3.PALVELUT JA PALVELIMET 99

LIITE 7. P.PV.4.PÄÄTELAITTEET 100

LIITE 8. P.PV.5.TIETO 102

LIITE 9. P.PV.6.KÄYTTÖVALTUUSHALLINTA 104

LIITE 10. P.PV.7.HALLINTA JA VALVONTA..... 105

LIITE 11. P.CC.1.ACCESS CONTROL (FIREWALL PP V2.0 EAL4) 106

LIITE 12. P.CC.2.DATA PROTECTION (CRYPTOGRAPHIC MODULES V1.0 EAL4) 107

LIITE 13. P.CC.3.DATABASES (U.S GOVERMENT PP V1.1 EAL2) 108

LIITE 14. P.CC.4.NETWORK (IP ENCRYPTOR PP V1.9 EAL3+) 109

LIITE 15. P.CC.5.OPERATING SYSTEMS (CCOPP-OS V2.0 EAL4+)..... 110

Liite 1. Tietoturvallisuuteen vaikuttava lainsäädäntö

Suomen perustuslaki (731/1999) 2.luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
Suomen perustuslaki (731/1999) 2.luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
Laki viranomaisten toiminnan julkisuudesta (621/1999)
Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
Valtion virkamieslaki (750/1994) 17§: Säädös valtion virkasuhteesta
Laki kunnallisesta viranhaltijasta (304/2003)
Työsopimuslaki (55/2001)
Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VAHTI 7/2009)
Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): Arkaluonteiset kansainväliset asiakirjat
Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
Laki turvallisuusselvityksistä (177/2002): Henkilöiden taustat
Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
Laki sähköisistä allekirjoituksista (14/2003)
Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
Rikoslaki (39/1889) 34.luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
Rikoslaki (39/1889) 38.luku 8 §: Tietomurto
Rikoslaki (39/1889) 38.luku 9 § 1. kohta: Henkilötietorikos
Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
Vahingonkorvauslaki (41/1974)

Liite 2. Puolustusvoimien tietoturvallisuuden pysyväisasiakirjat

PETURVOS PAK 3:7 Käyttöoikeuksien hallinta Puolustusvoimissa
PETURVOS PAK 3:8 Käyttöoikeuksien myöntämisen perusteet Puolustusvoimien tietoverkossa oleviin sovelluksiin ja tietoon
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa
PETURVOS PAK 4:3 Asiakirjojen luokittelu ja merkinnät luottamuksellisuuden perusteella
PETURVOS PAK 4:5 Asiakirjojen käsittely eri luottamuksellisuusluokissa
PETURVOS PAK 4:12 Salassa pidettävien asiakirjojen katoamiset ja tuhoutumiset
PETURVOS PAK 5:2 Tilaturvallisuuden toteuttaminen Puolustusvoimissa
PETURVOS:n ohje 41/13/D/I 29.4.2004
PVHSM 4.2.3.2 tietohallinto 006 PEJOJÄOS Tietoturvapoikkeamat Puolustusvoimien verkoissa
PVHSM 4.2.3 tietohallinto 007 PEJOJÄOS Teknisen tietoturvan hallintajärjestelmä
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen
PVHSM 4.2.3.2 tietohallinto 009 PEJOJÄOS Lokien hallinta puolustusvoimissa
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta
PVHSM 4.2.3.2 tietohallinto 012 PEJOJÄOS Monitasotietoturva
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttövaltuushallinta Puolustusvoimissa
PVHSM 4.2.3.2 tietohallinto 014 PEJOJÄOS Laitetunnistus ja tietoverkon pääsynhallinta
PVHSM 4.2.3.2 tietohallinto 015 PEJOJÄOS Puolustusvoimien varmennepolitiikka
PVHSM 4.2.2.1 tietohallinto 016 PEJOJÄOS Toiminnan jatkuvuuden hallinta
PVHSM 4.2.3.3 tietohallinto 017 PEJOJÄOS Teknisen tietoturvallisuuden auditointi ja tarkastus
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta
PVHSMK Hankintatoimi 004 - PEMATOS Hankinta-asiakirjojen julkisuusmääräys
PVOHJE asiakirjahallinto 006 PEHENKOS Puolustusvoimien sähköpostin käsittelysäännöt (HF1045, 9.9.2009)
PETURVOS PAK 01:02 Puolustusvoimien turvallisuustoiminnan strategia
PETURVOS PAK 01:03 Riskienhallinta puolustusvoimissa

Liite 3. Tietoturvallisuutta käsittelevä VAHTI-ohjeisto

VAHTI 1/1998 Internetin käyttö- ja tietoturvallisuussuositus
VAHTI 2/1999 Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus
VAHTI 1/2000 Valtionhallinnon tietoturvallisuuskäsitteistö
VAHTI 2/2001 Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje
VAHTI 3/2000 Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 4/2000 Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje
VAHTI 1/2001 Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 2/2001 Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 3/2001 Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 5/2001 Valtionhallinnon sähköpostien ja lokitiedostojen käsittelyohje
VAHTI 6/2001 Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista
VAHTI 7/2001 Toimet tietoturvaloukkaustilanteissa
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 2/2002 Valtion virastojen tietoturvallisuussuunnittelun yhteishanke
VAHTI 3/2002 Valtionhallinnon etätyön tietoturvallisuusohje
VAHTI 4/2002 Arkaluonteiset kansainväliset tietoaineistot
VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 4/2003 Valtionhallinnon tietoturvakäsitteistö
VAHTI 5/2003 Käyttäjän tietoturvaohje
VAHTI 6/2003 Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus
VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje
VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta
VAHTI 3/2006 Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 4/2006 Selvitys valtion ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 7/2006 Muutos ja tietoturvallisuus – alueellistamisesta ulkoistamiseen –hallittu prosessi
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 3/2007 Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 3/2008 Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 9/2008 Hankkeen tietoturvaohje
VAHTI 2/2009 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 6/2009 Kohdistetut hyökkäykset

Liite 4. P.PV.1.Yleinen

Lähde	Tunniste	Vaatimus
PETURVOS PAK 01:02 Puolustusvoimien turvallisuustoiminnan strategia	P.PV.1.1	Suojattavat kohteet (assets) on tunnistettu.
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.2	Vain operatiiviseen käyttöön hyväksyttyjä verkkoja ja järjestelmiä käytetään
PVHSM 4.2.3.1 tietohallinto 008 PEJO-JÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.1.3	Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. Tuotantojärjestelmän oltava erillinen, jotta kehitys- tai testaustoimet eivät aiheuta tuotantokatkoksia
PVHSM 4.2.3.2 tietohallinto 014 PEJO-JÄOS Laitetunnistus ja tietoverkon pääsynhallinta	P.PV.1.4	Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja todennusmenettelyjä
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.5	Suojaustason IV tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle
PVHSM 4.2.3.2 tietohallinto 021 PEJO-JÄOS Teknisen tietoturvan valvonta	P.PV.1.6	tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun tarkan ajanlähteen kanssa
PVHSM 4.2.3.2 tietohallinto 021 PEJO-JÄOS Teknisen tietoturvan valvonta	P.PV.1.7	Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti
PVHSM 4.2.3.2 tietohallinto 021 PEJO-JÄOS Teknisen tietoturvan valvonta	P.PV.1.8	Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa (Eroavaisuuksia käsitellään tietoturvapoikkeamina)
PVHSM 4.2.3.2 tietohallinto 021 PEJO-JÄOS Teknisen tietoturvan valvonta	P.PV.1.9	Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.10	Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.11	Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Vaaditaan vähintään, että prosessit edellyttävät
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.12	kryptografisesti vahvoja avaimia
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.13	turvallista avaintenjakelua
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.14	turvallista avainten säilytystä
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.15	säännöllisiä avaintenvaihtoja
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.16	vanhojen tai paljastuneiden avainten vaihdon
PVHSM 4.2.3.2 tietohallinto 015 PEJO-JÄOS Puolustusvoimien varmennepolitiikka	P.PV.1.17	valtuuttamattomien avaintenvaihtojen estämisen.
PETURVOS PAK 5:2 Tilaturvallisuuden toteuttaminen Puolustusvoimissa	P.PV.1.18	Kriittiset laitteistot ovat tunnistetut ja häiriöttömän sähkönsyötön (UPS) piirissä
PETURVOS PAK 5:2 Tilaturvallisuuden toteuttaminen Puolustusvoimissa	P.PV.1.19	Häiriöttömän sähkönsyötöntoimintavarmuus varmistetaan säännöllisesti testaamalla
PETURVOS PAK 5:2 Tilaturvallisuuden toteuttaminen Puolustusvoimissa	P.PV.1.20	LVIS-järjestelyt varmistettu toimintavaatimusten mukaisesti. Tärkeät laitteet ja laitetilat on suojattu ympäristötekijöitä vastaan (mm. murto, palo, lämpö, kaasut, vesi).
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.21	On varmistettu, että kriittisten verkkojen verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.22	Järjestelmästä on saatavilla ajantasainen jatkuvuus-/toipumissuunnitelma
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.23	Suunnitelmissa otetaan huomioon salassa pidettävien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.24	Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.25	Toipumissuunnitelma testataan säännöllisesti.

PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.26	Järjestelmille on määritetty käytettävyysvaatimukset ja mitoittaa toipumismekanismit riskienarvioinnin mukaisesti niihin
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.27	Avaintehtävät on tunnistettu ja niihin on nimetty varahenkilö tai –henkilöt
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.28	Kriittisten tehtävien suorittamiseksi ovat suunniteltu ja valmistel-tu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön varajärjestelyt.
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.29	Avainhenkilöstö harjoittelee säännöllisesti ylläpitämään kriittisiä toimintoja erityistilanteissa.
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.30	Kriittisissä tehtävissä vastuulliset avainhenkilöt on koulutettu toimimaan häiriötilanteissa
PETURVOS PAK 4:2 Tietoturvallisuus Puolustusvoimissa	P.PV.1.31	Kriittisten tehtävien toteuttamisen edellyttämät varajärjestelyt poikkeusoloissa on testattu ja harjoiteltu.

Liite 5. P.PV.2.Tiedonsiirto

Lähde	Tunniste	Vaatimus
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.1	Vain hyväksyttyjä etätyöyhteyksiä käytetään. Suojaustason III järjestelmien etähallinta on lähtökohtaisesti estetty. Etähallinta on sallittu vain viranomaisen erikseen hyväksymällä menettelyllä. Suojaustason II järjestelmien etähallinta on estetty
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.2	Sensitiiviset / salassa pidettävät tiedot välitetään asianmukaisesti suojaten
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.3	Yhteys sähköpostipalvelimen ja -asiakasohjelman välillä on suojattu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.4	Mikäli sähköpostissa, pikaviestimissä, VoIP -puheluissa ja vastaavissa käsitellään sensitiivistä tietoa, on liikenne (tai viesti) suojattava riskienarvioinnin mukaisesti siten, että sensitiivistä tietoa ei pääse vuotamaan ulkopuolisille
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.5	Yhteyden on oltava luotettavasti suojattu päästä päähän.
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.6	Liikenne kulkee salaamattomana vain organisaation luotetun verkon tai verkon osan sisällä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.7	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on hyväksytty
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.8	kansallisen tietoturvaviranomaisen toimesta
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.9	kansainvälisen tietoturvaviranomaisen toimesta
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.10	erillisessä ratkaisulle suoritetussa tarkastuksessa
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.11	Organisaation verkot tarkistetaan säännöllisesti luvattomien tietojärjestelmien (ohjelmistot, verkkopalvelut, jne.) löytämiseksi
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.12	Verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet, jotka eivät ole käytössä, on kytketty fyysisesti kytkentäpisteistä irti.
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.13	Kytkimien käyttämättömät portit on poistettu käytöstä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.14	Tuntemattomien laitteiden kytkeminen verkkoon estetään verkkoteknisin keinoin
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.15	Sähkökaapelointi sekä tietoja siirtävä tai tietotekniikkapalveluja tukeva tietoliikennekaapelointi on suojattu salakuuntelulta ja vaurioilta
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.16	Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa.
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.17	Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.18	Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.19	Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.20	merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.21	normaalitilaan nähden poikkeavat protokollat
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.22	luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä)
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.23	Langattomat verkot

PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.24	Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.25	Liikenne salataan luotettavasti
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.26	Langattoman ratkaisun tulee täyttää TLL II tietoturvatason vaatimukset
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.27	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan ainakin, että
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.28	oletussalasanat on vaihdettu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.29	vain tarpeellisia verkkopalveluita on päällä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.30	verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.31	Fyysinen verkko on jaettu turvavyöhykkeisiin
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.32	Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.33	verkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri tietoturvatason järjestelmät on sijoitettu erillisille verkkoalueille
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.34	Vyöhykkeisiin jakoperusteet on kuvattu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.35	Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain luvallinen liikenne sallitaan
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.36	Valvonnan ja rajoitusten periaatteet on kuvattu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.37	verkko salataan, kun se menee hallitun fyysisen tilan ulkopuolelle
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.38	Tietojenkäsittely-ympäristö on fyysisesti erotettu ja valvottu verkko
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.39	Liikenteen suodatus
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.40	Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny).
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.41	Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.42	Määrittelemätön liikennöinti on estetty molempiin suuntiin
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.43	Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.44	Suodatussäännöt on dokumentoitu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.45	Yleisiin verkkohyökkäyksiin on varauduttu konfiguroimalla palomuuri estämään verkkohyökkäykset (vähintään seuraavat toimenpiteet)
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.46	Osoitteiden väärentäminen (spooffing) estetty
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.47	Lähdereititys (source routing) oletuksena estetty kaikissa verkkolaitteissa
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.48	Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty

PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.49	Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.50	SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.51	On määritetty mitä ICMP-liikennettä sallitaan Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.52	Palomuurit ovat konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.53	Palvelunestohyökkäysten (DoS, DDoS) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.54	Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin
PVHSM 4.2.3.2 tietohallinto 011 PEJOJÄOS Tiedonsiirron tietoturvallisuuden hallinta	P.PV.2.55	Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisesti turva-auditoinnilla

Liite 6. P.PV.3.Palvelut ja palvelimet

Lähde	Tunniste	Vaatimus
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.1	Verkko ja sen palvelut / palvelimet skannataan säännöllisesti haavoittuvuuksien löytämiseksi
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.2	skannaus suoritetaan vähintään vuosittain ja merkittävien muutosten jälkeen
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.3	Ennen uuden järjestelmän käyttöönottoa testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.4	Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus)
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.5	Hankittavilta/ toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaatteiden, esim. Open Web Application Security Project Guide, toteuttamista. Toimittajilta vaaditaan selvitys miten tietoturvallisuus on otettu huomioon tuotekehityksessä (TLL III ympäristöt)
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.6	Kaikki koodi on avoimesti tarkastettavissa (esim. takaportit, turvattomat toteutukset, jne.) tai sopimuksessa on varattu oikeus lähdekoodin tarkastukseen. Vaihtoehdossa 2 on näytettävä todiste koodin luotettavaksi toteamisesta (esim. kuvaukset toimittajan prosesseista ja ulkopuolisen tekemäkatselmointiraportti). (TLL II ympäristöt)
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.7	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä.
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.8	Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.9	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.10	suljettujen istuntojen uudelleenaktivoinnin esto
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.11	istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.12	istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan
PVHSM 4.2.3.1 tietohallinto 008 PEJOJÄOS Palveluympäristöjen ja palveluiden toiminnan varmistaminen	P.PV.3.13	istuntojen pituuksien rajoitukset.

Liite 7. P.PV.4.Päätelaitteet

Lähde	Tunniste	Vaatimus
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.1	Työasema, pääte, kannettava tietokone tai vastaava laite on kyettävä lukitsemaan, kun laitteelta poistutaan
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.4.2	verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan säännöllisesti haavoittuvuuksien löytämiseksi
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.4.3	skannaus suoritetaan vähintään vuosittain ja merkittävien muutosten jälkeen
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.4	Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.5	Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus)
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.6	Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/ käytöstä poistetut laitteet
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.7	Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.8	Sensitiivistä tietoa sisältävät mobiililaitteet suojataan riskiarvion mukaisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.9	Pääsy mobiililaitteen muistikortin tietoihin suojataan salasanalla
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.10	Mobiililaitteissa on etätyhjennysmahdollisuus käytössä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.11	Verkko- ja haittaohjelmauhat huomioidaan riskienarvioinnin mukaisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.12	suojaustason II ja III tiedon käsittely sallitaan vain viranomaisen erikseen hyväksymällä menettelyllä salattuna tai muutoin suojattuna
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.13	haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet)
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.14	torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.15	torjuntaohjelmistot tuottavat havainnoistaan lokitietoja
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.16	haittaohjelmatunnisteet päivittyvät säännöllisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.17	haittaohjelmahavaintoja seurataan
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.18	Koventaminen
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.19	alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.20	tarjottavat (erityisesti verkko-) palvelut minimoitu ja rajattu vain välttämättömiin
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.21	käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.22	järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. ”administrator” ja ”guest”) on oikeudet rajattu minimiin tai poistettu käytöstä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.23	oletussalasanat on vaihdettu
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.24	työasemat lukittuvat automaattisesti, jos niitä ei käytetä määrättyyn aikaan
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.4.25	lokimenettelyt asetettu
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.26	käyttöoikeudet asetettu vaatimusten mukaisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.27	alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.28	palvelimet konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.29	Verkkojaot poistettu käytöstä tai minimoitu.
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.30	Ohjelmistot, erityisesti webselaimet ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja

VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.31	palvelimien, työasemien ja kannettavien tietokoneiden BIOS -asetukset on asetettu turvallisuutta tehostaviksi ja asetusten muuttaminen on estetty valtuuttamattomilta käyttäjiltä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.32	tarpeettomat palvelut ja portit on poistettu käytöstä.
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.33	käytössä mekanismi, menetelmä tai menettelytapa, jolla tietojärjestelmään tehtävät muutokset tallentuvat ja tehdyt muutokset voidaan jälkikäteen havaita
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.34	Työasemilla, kannettavilla tietokoneilla ja vastaavilla on käytössä (host-based) palomuuriratkaisu, myös organisaatioverkon sisällä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.35	Siirrettävät mediat
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.36	Sensitiivistä tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.37	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.38	Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuodatin
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.39	Toimintatavat joita järjestelmän on tuettava
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.40	Mikäli turvaluokiteltua tietoa sisältävä laite joudutaan jättämään tilaan, jossa siihen on fyysinen pääsy ei-luotetuilla (arvioitava tapauskohtaisesti: esim. organisaation ulkopuolisilla), salaus on aktivoitava laitteelta poistuttaessa
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.41	Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus	P.PV.4.42	Aktiiviset istunnot päätetään työn päättyessä ja tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan)

Liite 8. P.PV.5.Tieto

Lähde	Tunniste	Vaatimus
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.1	Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason II/III tiedot säilytetään aina luotettavasti salakirjoitettuna
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.2	Sensitiiviset / salassa pidettävät tiedot on tunnistettu
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.3	Varmistusten taajuus on suhteessa varmistettavan tiedon kriittisyyteen
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.4	Varmuuskopioinnin oikea toiminta ja palautusprosessi testataan säännöllisesti.
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.5	Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.6	Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.7	Salassa pidettävää tietoa sisältävät varmuuskopiot säilytetään tiedon suojaustason tai turvallisuusluokan edellyttämässä tilassa ja tarvittaessa salakirjoitettuna
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.8	Varmistusmedioista on olemassa listat
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.9	Palautusprosessi on dokumentoitu
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.10	Suojaustason II ja III tieto rekisteröidään viestintä- ja tietojärjestelmissä ennen välitystä ja vastaanotettaessa
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.11	rekisteristä tulee käydä ilmi kunkin asiakirjan sen hetkinen haltija tiedon elinkaaren loppuun asti
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.12	rekisteriä säilytetään, kuten suojaustason II asiakirjaa
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.13	Kun turvaluokiteltu tieto siirretään tietojärjestelmästä toiseen, se suojataan siirron aikana ja vastaanottavassa järjestelmässä tiedon alkuperäisen turvaluokituksen edellyttämällä tavalla
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.14	Tiedon tulostamisesta jää merkintä
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.15	Tiedon siirrosta ulkoiselle medialle jää merkintä
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.16	Tietojärjestelmien käytön yhteydessä syntyvät salassa pidettävää tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.17	Suojaustason II aineisto voidaan lähettää julkisen verkon yli salattuna viranomaisen hyväksymällä vahvalla päästä päähän salaustuotteella
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.18	Suojaustason II tietoa ei tallenneta, eikä siirretä missään muodossa sellaisessa verkossa tai tietolaitteessa, joka ei ole viranomaisen erikseen tähän tarkoitukseen hyväksymä. Tietoa tulee tallentaa vain määritetyn laitteen kautta
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.19	Työskentelyn jälkeen selväkielisessä muodossa oleva, mutta salassa pidettävä aineisto (ulkoiset muistivälineet ja vastaavat) siirretään kassakaappiin, lukittuun kaappiin tai vastaavaan säilytystilaan (EURO II -tason kassakaappiin tai vastaavaan säilytystilaan, kuten holviin)
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.20	Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.21	Kaikki salassa pidettävää tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä. Mikäli luotettava tyhjennys ei ole mahdollista, salassa pidettävää tietoa sisältävä osa on tuhottava mekaanisesti.
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovarantojen tietoturvallisuus	P.PV.5.22	Suojaustason II tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovaranto-	P.PV.5.23	Suojaustason III tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista

jen tietoturvallisuus		
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovaranto-jen tietoturvallisuus	P.PV.5.24	Tietojärjestelmien käytön yhteydessä syntyvät salassa pidettävää tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti
PVHSM 4.2.3.1 tietohallinto 010 PEJOJÄOS Tietovaranto-jen tietoturvallisuus	P.PV.5.25	Tiedon merkitsemistä (luokittelua), käsittelyä (sis. salaus) ja tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön.

Liite 9. P.PV.6.Käyttövaltuushallinta

Lähde	Tunniste	Vaatimus
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.1	Tietojärjestelmissä sensitiivisten tietojen jakelu hoidetaan käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.2	käytössä yksilölliset henkilökohtaiset käyttäjä-tunnisteet
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.3	kaikki käyttäjät tunnistetaan ja todennetaan
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.4	pääsyä käyttöjärjestelmään valvotaan turvalli-sen sisäänkirjausmenettelyn avulla
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.5	todennus tehdään vähintään salasanaa käyt-täen
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.6	järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä /sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumen-toidut salasanojen hallintakäytännöt yhteis-käyttöisille tunnuksille
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.7	Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.8	käytetään aina vahvaa käyttäjäntunnistusta
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.9	Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.10	Käyttö- ja pääsyoikeuksien muutokset välitty-vät sekä fyysiseen (kulunvalvonta jne.) että loogiseen pääsyyn ja käyttöön.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.11	Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.12	Käyttöoikeuksien käsittely ja myöntäminen ohjeistettu
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.13	Käyttäjillä on vain ne oikeudet, joita he tarvit-sevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verk-koihin, tietoihin ja järjestelmiin.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.14	Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.15	Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.16	Järjestelmän käyttäjätyypit on dokumentoitu.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.17	Järjestelmän käyttäjistä on olemassa lista.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.18	On olemassa menettelyohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välit-tömästi asiaankuuluville tahoille.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.19	Yhteistyökumppaneiden/ muiden ulkopuolis-ten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä.
PVHSM 4.2.3.2 tietohallinto 013 PEJOJÄOS Käyttöval-tuushallinta Puolustusvoimissa	P.PV.6.20	Käyttöoikeus operatiivisiin tietojärjestelmiin edellyttää kirjallista vaitiolositoumusta.

Liite 10. P.PV.7.Hallinta ja valvonta

Lähde	Tunniste	Vaatimus
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.1	Viranomaisten (esim. CERT), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.2	Käytössä selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.3	Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille).
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.4	Lokien käsittely
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.5	Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.6	Luottamukselliset lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.7	On käytössä menettely hyökkäyksen/väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan. Erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.8	Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkintä
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.9	Kriittisistä ylläpitotoimista tallennetaan kirjausketju (audit trail)
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.10	Lokitiedot ja niiden kirjauspalvelut ovat suojattuja väärentämiseltä ja luvattomalta pääsyltä. On käytössä jokin menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.11	Keskeiset lokitiedot varmuuskopioidaan säännöllisesti
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.12	Kriittisten tietojen käsittelystä muodostuu lokimerkintä
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.13	Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.14	Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.15	Tietoturvarikkomusten käsittely ja seuraukset määritelty.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.16	Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.17	Tulevista työasemien tietoturva-aukkojen päivityksistä tiedotetaan vähintään sillä tarkkuudella, että käyttäjät ovat tietoisia siitä, mitä toimia heiltä vaaditaan.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.18	Henkilöstö on ohjeistettu ja velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja -uhista.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.19	Käyttäjille tiedotetaan merkittävimmistä ajankohtaisista uhista, jotka kohdistuvat organisaation käyttäjiin (esim. kohdistetuista hyökkäyksistä)
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.20	Salassa pidettäviä tietoja käsitteleviin järjestelmiin on laadittu turvallisen käytön ohjeistus.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.21	Hyväksyttävän käytön säännöt on määritetty
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.22	Dokumentoidut säännöt ovat henkilöstölle helposti saatavilla.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.23	On olemassa selkeä ja toimiva tapa muutosten ilmoittamiseen ja tarvittavien muutosten tekemisiin.
PVHSM 4.2.3.2 tietohallinto 021 PEJOJÄOS Teknisen tietoturvan valvonta	P.PV.7.24	Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan, jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä

Liite 11. P.CC.1.Access control (Firewall PP V2.0 EAL4)

Security Functional Class	Security Functional Components
Security Audit	FAU_ARP.1 Security alarms
Security Audit	FAU_GEN.1 Audit data generation
Security Audit	FAU_SAA.1 Potential violation analysis
Security Audit	FAU_SAR.1 Audit review
Security Audit	FAU_SAR.3 Selectable audit review
Security Audit	FAU_SEL.1 Selective audit
Security Audit	FAU_STG.1 Protected audit trail storage
Security Audit	FAU_STG.3 Action in case of possible audit data loss
Security Audit	FAU_STG.4 Prevention of audit data loss
User Data Protection	FDP_IFC.2 Complete information flow control
User Data Protection	FDP_IFF.1 Simple security attributes
Identification and Authentication	FIA_AFL.1 Authentication failure handling
Identification and Authentication	FIA_ATD.1 User attribute definition
Identification and Authentication	FIA_SOS.1 Verification of secrets
Identification and Authentication	FIA_UAU.1 Timing of authentication
Identification and Authentication	FIA_UAU.4 Single-use authentication mechanisms
Identification and Authentication	FIA_UAU.7 Protected authentication feedback
Identification and Authentication	FIA_UID.2 User identification before any action
Security Management	FMT_MOF.1 Management of security functions behavior
Security Management	FMT_MSA.1 Management of security attributes
Security Management	FMT_MSA.3 Static attribute initialization
Security Management	FMT_MTD.1 Management of TSF data
Security Management	FMT_MTD.2 Management of limits on TSF data
Security Management	FMT_SMF.1 Specification of Management Functions
Security Management	FMT_SMR.1 Security roles
Protection of the TSF	FPT_TST.1 TSF testing
TOE Access	FTA_SSL.1 TSF-initiated session locking
TOE Access	FTA_SSL.3 TSF-initiated termination

Liite 12. P.CC.2.Data Protection (Cryptographic modules V1.0 EAL4)

Security Functional Class	Security Functional Components	Security Functional Components
Cryptographic operation and key management	FCS_CKM.1 Cryptographic key generation	FCS_CKM.4 Cryptographic key destruction
Cryptographic operation and key management	FCS_CKM.2/Import Cryptographic key distribution	FCS_COP.1 Cryptographic operation
Cryptographic operation and key management	FCS_CKM.2/Export Cryptographic key distribution	FCS_RNG.1 Random number generation
Identification and Authentication	FIA_ATD.1 User attribute definition	FIA_UAU.7 Protected authentication feedback
Identification and Authentication	FIA_UID.1 Timing of identification	FIA_USB.1 User-subject binding
Identification and Authentication	FIA_UAU.1 Timing of authentication	FIA_AFL.1 Authentication failure handling
Identification and Authentication	FIA_UAU.6 Re-authenticating	
Protection of user data	FDP_ACC.2/Key_Man Complete access control	FDP_ITC.2 Import of user data with security attributes
Protection of user data	FDP_ACF.1/Key_Man Security attribute based access control	FDP_ETC.2 Export of user data with security attributes
Protection of user data	FDP_ACC.2/Oper Complete access control	FDP_UCT.1 Basic data exchange confidentiality
Protection of user data	FDP_ACF.1/Oper Security attribute based access control	FDP_UIT.1 Data exchange integrity
Protection of user data	FDP_ACC.2/Mode_Trans Complete access control	FDP_RIP.2 Full residual information protection
Protection of user data	FDP_ACF.1/Mode_Trans Security attribute based access control	
Security Management	FMT_SMF.1 Specification of Management Functions	FMT_MSA.1/Key_Man_1 Management of security attributes
Security Management	FMT_SMR.2 Restrictions on security roles	FMT_MSA.1/Key_Man_2 Management of security attributes
Security Management	FMT_MOF.1/CO Management of security functions behaviour	FMT_MSA.2 Secure security attributes
Security Management	FMT_MTD.1/Admin Management of TSF data	FMT_MSA.3 Static attribute initialisation
Security Management	FMT_MTD.1/User Management of TSF data	
Protection of the TSF	FPT_STM.1 Reliable time stamps	FPT_SEP.1 TSF domain separation
Protection of the TSF	FPT_TDC.1 Inter-TSF basic TSF data consistency	FPT_TST.1 TSF testing
Protection of the TSF	FPT_FLS.1 Failure with preservation of secure state	FPT_TST.2 TSF self-testing
Protection of the TSF	FPT_EMSEC.1 TOE Emanation	FPT_PHP.3 Resistance to physical attack
Protection of the TSF	FPT_RVM.1 Non-bypassability of the TSP	FTP_ITC.1 Inter-TSF trusted channel

Liite 13. P.CC.3.Databases (U.S Goverment PP V1.1 EAL2)

Security Functional Class	Security Functional Components
Security Audit	FAU_GEN.1-NIAP-0410 Audit data generation
Security Audit	FAU_GEN_EXP.2 User and/or group identity association
Security Audit	FAU_SEL.1-NIAP-0407 Selective audit
Protection of user data	FDP_ACC.1 Subset access control
Protection of user data	FDP_ACF.1-NIAP-0407 Security attribute based access control
Protection of user data	FDP_RIP.1 Subset residual information protection
Identification and Authentication	FIA_ATD.1 User attribute definition
Security Management	FMT_MOF.1 Management of security functions behavior
Security Management	FMT_MSA.1 Management of security attributes
Security Management	FMT_MSA_EXP.3 Static attribute initialization
Security Management	FMT_MTD.1 Management of TSF data
Security Management	FMT_REV.1(1) Revocation (user attributes)
Security Management	FMT_REV.1(2) Revocation (subject, object attributes)
Security Management	FMT_SMF.1 Specification of management functions
Security Management	FMT_SMR.1 Security roles
Protection of the TSF	FPT_SEP_EXP.1 TSF domain separation
Protection of the TSF	FPT_TRC_EXP.1 Internal TSF consistency
TOE Access	FTA_MCS.1 Basic limitation on multiple concurrent sessions
TOE Access	FTA_TAH_EXP.1 TOE access history
TOE Access	FTA_TSE.1 TOE session establishment

Liite 14. P.CC.4.Network (IP Encryptor PP V1.9 EAL3+)

Security Functional Class	Security Functional Components
User Data Protection	FDP_IFC.1/Enforcement_policy Subset information flow control
User Data Protection	FDP_IFF.1/Enforcement_policy Simple security attributes
User Data Protection	FDP_ITC.1/Enforcement_policy Import of user data without security attributes
User Data Protection	FDP_ETC.1/Enforcement_policy Export of user data without security attributes
User Data Protection	FDP_RIP.1 Subset residual information protection
User Data Protection	FDP_ACC.1/VPN_policy Subset access control
User Data Protection	FDP_ACF.1/VPN_policy Security attribute based access control
User Data Protection	FDP_ITC.1/VPN_policy Import of user data without security attributes
User Data Protection	FDP_IFC.1/Key_policy Subset information flow control
User Data Protection	FDP_IFF.1/Key_policy Simple security attributes
User Data Protection	FDP_ITC.1/Key_policy Import of user data without security attributes
User Data Protection	FDP_UCT.1/Key_policy Basic data exchange confidentiality
User Data Protection	FDP_UIT.1/Key_policy Data exchange integrity
Security Management	FMT_MSA.3/VPN_policy Static attribute initialisation
Security Management	FMT_MSA.1/VPN_policy Management of security attributes
Security Management	FMT_SMF.1/VPN_policy Specification of Management Functions
Security Management	FMT_MSA.3/Key_policy Static attribute initialisation
Security Management	FMT_MTD.1/Network_param Management of TSF data
Security Management	FMT_MTD.1/Param Management of TSF data
Security Management	FMT_SMF.1/Config_supervision Specification of Management Functions
Security Management	FMT_SMR.1 Security roles
Cryptographic operation and key management	FCS_CKM.4/Key_policy Cryptographic key destruction
Cryptographic operation and key management	FCS_CKM.3/Key_policy Cryptographic key access
Cryptographic operation and key management	FCS_COP.1/Enforcement_policy Cryptographic operation
Security Audit	FAU_GEN.1/VPN Audit data generation
Security Audit	FAU_GEN.1/Administration Audit data generation
Security Audit	FAU_SAR.1 Audit review
Security Audit	FAU_SAR.3 Selectable audit review
Security Audit	FAU_STG.1 Protected audit trail storage
Security Audit	FAU_ARP.1/Alarm Security alarms
Security Audit	FAU_SAA.1/Alarm Potential violation analysis
Protection of the TSF	FPT_STM.1 Reliable time stamps
Identification and Authentication	FIA_UID.2 User identification before any action
Identification and Authentication	FIA_UAU.2 User authentication before any action

Liite 15. P.CC.5.Operating systems (CCOPP-OS V2.0 EAL4+)

Security Functional Class	Security Functional Components	Security Functional Components
Security Audit	FAU_GEN.1 Audit data Generation	FAU_SEL.1 Selective Audit
Security Audit	FAU_GEN.2 User Identity Generation	FAU_STG.1 Protected audit trail storage
Security Audit	FAU_SAR.1 Audit Review	FAU_STG.3 Action in case of Possible Audit Data Loss
Security Audit	FAU_SAR.2 Restricted Audit Review	FAU_STG.4 Prevention of audit data loss
Security Audit	FAU_SAR.3 Selectable Audit Review	
Protection of user data	FDP_ACC.1-A Discretionary Access Control Policy	FDP_IFC.1 Mandatory Access Control Policy
Protection of user data	FDP_ACF.1-A Discretionary Access Control Policy Rules	FDP_IFF.1 Mandatory Access Control Policy Rules
Protection of user data	FDP_ACC.1-B Role-Based Access Control Policy	FDP_ITC.1 Import Of User Data
Protection of user data	FDP_ACF.1-B Role-Based Access Control Policy Rules	FDP_RIP.2 Object Residual Information Protection
Protection of user data	FDP_ETC.1 Export Of User Data	FDP_RIP.CCOPP Subject Residual Information Protection
Identification and Authentication	FIA_AFL.1 Authentication Failure Handling	FIA_UAU.6 Re-authentication
Identification and Authentication	FIA_ATD.1 User Attribute Definition	FIA_UAU.7 Protected Authentication Feedback
Identification and Authentication	FIA_SOS.1 Verification of Passwords	FIA_UID.2 User Identification Before Any Action
Identification and Authentication	FIA_UAU.2 User Authentication Before Any Action	FIA_USB.1 User-Subject Bindin
Identification and Authentication	FIA_UAU.CCOPP Multiple Authentication Mechanisms Support	
Security Management	FMT_MSA.1-A Management Of DAC Object Security Attributes	FMT_MTD.1-D Management of Authentication Data Modification
Security Management	FMT_MSA.1-B Management Of RBAC Object Security Attributes	FMT_MTD.1-E Management of TOE Access Banner
Security Management	FMT_MSA.1-D Management Of User Security Attributes	FMT_MTD.1-F Management of Role Definitions
Security Management	FMT_MSA.2 Secure RBAC Attributes	FMT_MTD.3 Secure Role Definitions
Security Management	FMT_MSA.3-A DAC Static attribute initialization	FMT_REV.1-A Revocation of User Attributes
Security Management	FMT_MSA.3-B RBAC Static attribute initialization	FMT_REV.1-B Revocation of Object Attributes
Security Management	FMT_MSA.3-C MAC Static attribute initialization	FMT_SAE.1 Time-Limited Authorization
Security Management	FMT_MTD.1-A Management of Audit Trail	FMT_SMF.1 Specification of management functions
Security Management	FMT_MTD.1-B Management of Audited Events	FMT_SMR.2 Security Roles
Security Management	FMT_MTD.1-C Management of Authentication Data Initilization	
Protection of the TSF	FPT_FLS.1 Failure with preservation of secure state	FPT_STM.1 Reliable Time Stamps
Protection of the TSF	FPT_ITC.CCOPP Inter-TSF Confidentiality During Transmission	FPT_TEE.1 Testing of External Entities
Protection of the TSF	FPT_RCV.1 Manual recovery	FPT_TST.1 TSF Testing
Protection of the TSF	FPT_RCV.4 Function recovery	
Resource utilisation	FRU_PRS.1 Limited Priority of Service	FRU_RSA.1 Maximum quotas
TOE Access	FTA_LSA.1 Limitation on scope of selectable attributes	FTA_TAB.1 Default TOE access banners
TOE Access	FTA_MCS.1 Basic limitation on multiple concurrent session	FTA_TAH.1 TOE access history
TOE Access	FTA_SSL.4 User-initiated termination	FTA_TSE.1 TOE session establishment