Liikenne- ja viestintäministeriö

Suomi tietoturvan suunnannäyttäjäksi

Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämiseen

Kansallisen tietoturvastrategian toimenpideohjelman hankkeen 5 loppuraportti

Julkaisuja 17/2011

Liikenne- ja viestintäministeriön

toiminta-ajatus
Liikenne- ja viestintäministeriö edistää yhteiskunnan toimivuutta ja väestön hyvinvointia huolehtimalla siitä, että kansalaisten ja elinkeinoelämän käytössä on laadukkaat, turvalliset ja edulliset liikenne- ja viestintäyhteydet sekä alan yrityksillä kilpailukykyiset toimintamahdollisuudet.

visio
Suomi on eturivin maa liikenteen ja viestinnän laadussa, tehokkuudessa ja kansainvälisessä osaamisessa.

arvot
Rohkeus
Oikeudenmukaisuus
Yhteistyö

Liikenne- ja viestintäministeriö

	Julkaisun päivämäärä

Julkaisun nimi Suomi tietoturvan suunnannäyttäjäksi. Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön	
Tekijät Hankeryhmä 5, pj. Reijo Savola, VTT (Ed.)	
Toimeksiantaja ja asettamispäivämäärä Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä 28.12.2009	
Julkaisusarjan nimi ja numero Liikenne- ja viestintäministeriön julkaisuja 17/2011	ISSN (verkkojulkaisu) 1798-4045 ISBN (verkkojulkaisu) 978-952-243-236-0 URN http://urn.fi/URN:ISBN:978-952-243-236-0 HARE-numero
Asiasanat tietoturva, Suomen kilpailukyky, standardisointi	
Yhteyshenkilö Ylitarkastaja Mirka Meres-Wuori, liikenne- ja viestintäministeriö	
Muut tiedot	

Tiivistelmä

Kansallisen tietoturvastrategian toimenpideohjelman hankkeen 5 työryhmän erityistavoitteena oli Suomen kilpailukyvyn kasvattaminen. Työryhmän painopistealueet olivat suomalaisen tietoturvaosaamisen levittäminen, kansainvälisten standardien käyttöönoton edistäminen sekä aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön.

Suomella voi profiloitua kansainvälisesti johtavana tietoturvamaana ja toimia alan suunnannäyttäjänä. Työryhmä esittää tavoitteeseen tähtäämistä seuraavilla toimenpiteillä:

1. Perustamalla Suomeen tietoturvan huippuosaamiskeskittymä

2. Tukemalla asiantuntijoiden osallistumista kansainvälisiin standardisointikokouksiin

3. Panostamalla tietoturvaan liittyvään koulutukseen ja keskinäiseen verkostoitumiseen.

Toimenpiteiden toteuttaminen vaatii rahoitusta ja tätä raporttia tarkempaa suunnittelua. Tämä raportti tarkastelee hankkeen painopistealueiden nykytilannetta Suomessa ja esittää edellä mainittuihin toimenpiteisiin tähtäävät kehittämissuunnitelmat.

Kommunikations-
ministeriet

Publikationsdatum	

Publikation

Finland kan bli vägvisare inom informationssäkerhet – Spridning av finländskt kunnande om informationssäkerhet och aktivt deltagande i internationellt arbete för utveckling av standarder

Författare

Projektgrupp 5, ordförande Reijo Savola, VTT (Ed.)

Tillsatt av och datum

Arbetsgruppen Informationssäkerheten i vardagens informationssamhälle 28.12.2009

Publikationsseriens namn och nummer	
Kommunikationsministeriets publikationer 17/2011	ISSN (webbpublikation) 1798-4045 ISBN (webbpublikation) 978-952-243-236-0 URN http://urn.fi/URN:ISBN:978-952-243-236-0 HARE-nummer

Ämnesord

informationssäkerhet, Finlands konkurrenskraft, standardisering

Kontaktperson	Rapportens språk
Överinspektör Mirka Meres-Wuori, Kommunikationsministeriet	Rapporten är skriven på finska.

Övriga uppgifter

Sammandrag

Arbetsgruppen för projekt 5 i det åtgärdsprogram som ingår i den nationella informationssäkerhetsstrategin hade förbättring av Finlands konkurrenskraft som speciell målsättning. Arbetsgruppens tyngdpunktsområden var att sprida det finländska informationssäkerhetskunnandet, att främja införandet av internationella standarder samt att aktivt delta i internationellt arbete för utveckling av standarder.

Finland kan profilera sig som ett internationellt ledande informationssäkerhetsland och fungera som en vägvisare i denna bransch. Arbetsgruppen föreslår följande åtgärder i syfte att nå denna målsättning:

1. Finland grundar ett kluster för spetskunnande i informationssäkerhet.

2. Finland stöder informationssäkerhetsexperternas deltagande i internationella standardiseringsmöten.

3. Finland satsar på utbildning som rör informationssäkerhet och på ömsesidiga samarbetsnätverk.

För att genomföra åtgärderna krävs finansiering och planering som preciserar målen i denna rapport. I rapporten granskas nuläget i Finland på projektets tyngdpunktsområden och utstakas utvecklingsplaner för att genomföra ovan nämnda åtgärder.

Ministry of Transport and Communications

	Date

Title of publication

Finland: Towards a leading light in information security – Dissemination of Finnish information security competence and active participation towards the development of global standards

Author(s)

Project group 5, Chair Mr Reijo Savola, VTT (Ed.)

Commissioned by, date

Information security group of the Ubiquitous Information Society Advisory Board, 28 September 2009

Publication series and number	
Publications of the Ministry of Transport and communications 17/2011	ISSN (online) 1798-4045 ISBN (online) 978-952-243-236-0 URN http://urn.fi/URN:ISBN:978-952-243-236-0 Reference number

Keywords

information security, competitiveness of Finland, standardization

Contact person	Language of the report
Ms Mirka Mers-Wuori, Senior Officer, Ministry of Transport and Communications	The report is in Finnish.

Other information

Abstract

The special objective of the Working Group of Project 5 for the Action Programme of the National Information Security Strategy was to increase the competitiveness of Finland. The special areas of emphasis for the Working Group were: dissemination of Finnish information security knowledge, promoting the introduction of global standards, and active participation for the development of global standards.

Finland can play the role of a globally leading information security country and act as a leading light in the field. The Working Group proposes to realize this in the following ways:

1. Establishing a Center of Information Security Excellence in Finland

2. Supporting the participation of experts for global standardization meetings

3. Putting emphasis on information security education and mutual networking.

Implementation of the actions will require funding and more detailed planning than is presented in this report. This report reviews the current situation of the areas of emphasis in Finland. It also presents development plans aimed at the aforementioned actions.

Esipuhe

Kansallista tietoturvastrategiaa on toteutettu vuoden 2010 aikana toimenpideohjelmalla, jossa määriteltiin yhdeksän kärkihanketta edistämään tietoturvallisuutta Suomessa. Hanke 5:n puitteissa selvitettiin suomalaisen tietoturvaosaamisen levittämistä sekä aktiivista osallistumista standardien kansainväliseen kehittämiseen.

Suomi elää globaalissa tietoverkkotaloudessa, joten merkittävä osa tietoturvauhista ja – hyökkäyksistä kohdistuu meihin maamme rajojen ulkopuolelta. Suomi on useilla osa-alueilla tietoturvaosaamisen edelläkävijä, mutta sitä ei ole tarpeeksi hyvin osattu markkinoida kansainvälisesti. Tietoturvaosaamisemme esiintuomisella voidaan vaikuttaa merkittävällä tavalla Suomen asemoitumiseen globaalisti tietoturvan mallimaana ja sitä kautta edistää kansallista kilpailukykyämme sekä investointeja Suomeen. Vahva tietoturvaosaaminen varmistaa myös osaltaan kansallista turvallisuutta sekä Suomen asemaa keskeisillä tietoyhteiskunnan alueilla kuten palvelusektoreilla ja uusien tuotteiden sekä tietovarantojen infrastruktuurin rakentamisessa ja hyödyntämisessä. Suomella on mahdollisuus profiloitua kansainvälisesti johtavana tietoturvamaana ja toimia alan suunnannäyttäjänä sekä vaikuttaa aktiivisesti myös kansainväliseen sääntelyyn.

Hankeryhmän puheenjohtajana toimi VTT:n Reijo Savola ja hänen panoksensa tässä työssä on ollut korvaamaton. Kiitos kuuluu myös kaikille laajan ja asiantuntevan hankeryhmän jäsenille.

Mirka Meres-Wuori
Ylitarkastaja

Sisällysluettelo

Yhteenveto: Suomesta tietoturvan suunnannäyttäjä 5
Työryhmän kokoonpano 7
1. Johdanto 8
2. Painopiste 1: Suomalaisen tietoturvaosaamisen levittäminen 10
2.1 Nykytilanne 10
2.1.1 Tietoturvan merkitys on suuri ja kasvaa entisestään 10
2.1.2 Tietoturvaosaamisen tärkeimmät osa-alueet 11
2.1.3 Tietoturvaosaaminen Suomessa tutkimus- ja kehitysnäkökulmasta 13
2.1.4 Tietoturvaosaaminen muualla maailmassa 16
2.1.5 Suomen vahvuuksia 17
2.1.6 Osaamisesta kertominen maailmalla 17
2.1.7 Johtopäätökset 19
2.2 Kehittämissuunnitelma: Suomeen tarvitaan tietoturvan huippuosaamiskeskittymä 21
2.2.1 Huippuosaamiskeskittymän tarve ja hyödyt 21
2.2.2 Oulun tietoturvaklusterista Suomen huippuosaamiskeskittymään 22
2.2.3 Jatkotoimenpiteet 22
3. Painopiste 2: Suomalainen osallistuminen tietoturvastandardisointiin 24
3.1 Nykytilanne 24
3.1.1 Standardien merkitys liiketoiminnalle 24
3.1.2 Tietoturvaan liittyvä standardisointi 24
3.2 Kehittämissuunnitelma: Standardisointityöhön tarvitaan lisää tukirahoitusta 27
3.2.1 Aktiivisen kansainvälisen osallistumisen malli 27
3.2.2 Jatkotoimenpiteet 27
4. Muut toimenpiteet 28
4.1 Tietoturvakoulutus 28
4.2 Avoin verkostoyhteistyö 28
4.3 Tietovarastoinnin potentiaali 29
Viitteet 30

Yhteenveto: Suomesta tietoturvan suunnannäyttäjä

Suomella on mahdollisuus profiloitua kansainvälisesti johtavana tietoturvamaana ja toimia alan suunnannäyttäjänä. Kansallisen tietoturvastrategian toimenpideohjelman hankkeen 5 työryhmä esittää tähän tavoitteeseen tähtäämistä seuraavilla toimenpiteillä:

1. Perustetaan Suomeen tietoturvan huippuosaamiskeskittymä

2. Tuetaan asiantuntijoiden osallistumista kansainvälisiin standardisointikokouksiin

3. Panostetaan tietoturvaan liittyvään koulutukseen ja keskinäiseen verkostoitumiseen.

Toimenpiteiden toteuttaminen vaatii rahoitusta ja tätä raporttia tarkempaa suunnittelua.

Suomeen tulee muodostaa uutta liiketoimintaa ideoiva ja synnyttävä tietoturvan huippuosaamiskeskittymä, jossa tuotekehitys- ja tutkimusverkostot risteävät ruokkien tietoturvallisuuden parantamista ja huippuosaamispääomamme kasvattamista aihepiirissä. Toiminta tulee rakentaa kaikenkokoisten yritysten, tutkimusmaailman ja valtionhallinnon yhteistyölle. Huippuosaamispääomamme vaikuttaa oleellisesti Suomen asemoitumiseen globaalisti tietoturvan mallimaana ja houkuttelevana sijoituskohteena. Vahva tietoturvaosaaminen varmistaa kansallista turvallisuutta sekä Suomen asemaa keskeisillä tietoyhteiskunnan alueilla kuten palvelusektoreilla ja uusien tuotteiden sekä tietovarantojen infrastruktuurin rakentamisessa ja hyödyntämisessä.

Suomen merkittävin tietoturvan tutkimus- ja kehitystoiminnan tarpeista syntynyt osaamiskeskittymä on Oulussa. Työskentelytapa Suomen tietoturvan huippuosaamiskeskittymälle voi rakentua kyseisen keskittymän kokemusten pohjalta. Keskittymään tarvitaan tutkimuksen, yritysmaailman ja valtionhallinnon toimijoiden yhteistyötä kaikkialta maassamme. Nykyisin tietoturvaosaaminen on pirstoutuneena ja laajan hyödyntämisen kannalta vaikeasti saavutettavissa yrityksissä, tutkimusorganisaatioissa ja valtionhallinnon organisaatioissa. Oleellisten parannusten saavuttaminen vaatii eri alojen asiantuntijoiden ja näkökulmien järjestelmällistä ja valikoivaa yhteensovittamista. Tietoturvan huippuosaamiskeskittymä vaatii riittävän rahoituksen ja tarkkaa suunnittelua, johon esitämme erillistä suunnittelu- ja käynnistämisprojektia tämän mietinnön jatkotoimenpiteenä.

Kansainväliset standardit ovat välttämättömiä tietoturvalliselle liiketoiminnalle. Suomalaisten asiantuntijoiden osallistuminen kansainvälisten standardien laadintaan varmistaa suomalaisen teollisuuden vahvan kilpailuaseman kansainvälisillä liiketoiminta-areenoilla sekä suomalaisten toimijoiden tarpeiden ja erityispiirteiden huomioimisen standardeissa. Standardien mukaisesti suunnitellut tuotteet, palvelut ja tekniset ratkaisut ovat keskenään toiminnallisesti yhteensopivia ja vertailukelpoisia. On lisäksi varmistettava, että Suomi tulee olemaan vahva ehdokas ulkomaisille investoinneille ja uusille ratkaisuille. Tietoturva on nykyään keskeisessä roolissa investointipäätöksiä tehtäessä, ja tulevaisuudessa sen rooli on yhä suurempi.

Eräiden suurten yritysten systemaattisen osallistumisen lisäksi standardisointityö pohjautuu laajamittaiseen asiantuntijoiden vapaaehtoistoimintaan. Varsinkin pienissä ja keskisuurissa yrityksissä ja tutkimusorganisaatioissa suurin este standardisointiin

osallistumiselle on soveltuvan kokousmatkarahoituksen puute. Siksi organisaatioille tulee tarjota nykyistä enemmän suoria kanavia hyödyntää standardeja liiketoiminnassaan ja osallistua niiden kehittämiseen. Suomen Standardisoimisliiton SFS:n IT-alan standardisointiyksikkö on tunnistanut suorat kokousmatkojen rahoitukset tehokkaimpana välineenä standardisointityön edistämiseen sekä työn laajuuden ja vaikuttavuuden lisäämiseen. SFS:llä on mahdollisuus koordinoida kokousmatkarahoituksen myöntäminen asiantuntijoille laadittavien ohjeiden mukaisesti.

Kolmantena toimenpide-ehdotuksena mainittua kansalaisille ja yrityksille suunnattua tietoturvan perus- ja asiantuntijatasojen koulutusta työryhmä pitää erittäin tärkeänä ja suosittelee, että ehdotusta tarkastellaan erillisessä työryhmässä. Koulutuksen sisältö on suunniteltava tarkasti ottaen huomioon yhteiskunnan ja yritysmaailman tarpeet.

Teknologiateollisuuden innovaatiopolitiikan työryhmän raportissa vuodelta 2010 todetaan, että Suomi on kansallisen kilpailukyvyn näkökulmasta ennennäkemättömien haasteiden edessä ja korostaa innovaatioiden merkitystä Suomen kasvulle ja menestykselle. Parempien edellytyksien luominen Suomen kilpailukyvylle tietoturvaosaamisen kautta on erityisen tärkeää alan jatkuvasti kasvavan merkityksen ja aihepiirin laajan turvallisuusvaikutuksen vuoksi. Tietoturvaan liittyvät ohjelmistomarkkinat kasvavat parhaillaan lähes kymmenen prosentin vuosivauhtia globaalisti. Suomen vahva teknologiaosaaminen, tutkimus- ja kehitystyön tavoiteohjautuvuus sekä tutkimus- että tuotekehitysorganisaatioissa ja saavutettu asema monissa erityisteemoissa tietoturvan mallimaana Euroopassa luovat välttämättömän perustan tietoturvan huippuosaajaksi kasvamiselle. Kasvu huippuosaajiksi vaatii merkittävää panostusta. Lähtöasetelma on hyödynnettävä rohkeasti nyt, kun se on vielä mahdollista.

Työryhmän kokoonpano

Reijo Savola, VTT, puheenjohtaja
Pasi Anttila, Navicre
Tuomas Aura, Aalto-yliopisto
Esa Einola, Insta
Andrei Gurtov, Oulun yliopisto
Aaro Hallikainen, Hallinnon tietotekniikkakeskus
Marko Hautakangas, Insta
Juhani Heikka, Oulun kaupunki
Seppo Heikkinen, Tampereen teknillinen yliopisto
Harri Heimbürger, Säteilyturvakeskus
Marko Helenius, Tampereen teknillinen yliopisto
Jarkko Holappa, Nixu
Tua Huomo, VTT
Pekka Jäppinen, Lappeenrannan teknillinen yliopisto
Janne Järvinen, F-Secure
Urpo Kaila, CSC ja Tietoturva ry
Jorma Kajava
Erkki Kataja, Nokia
Erka Koivunen, CERT-FI
Mika Koskela, Säteilyturvakeskus
Petri Kuivala, Nokia
Jari Kunnari, Rovaniemen kehitys
Olavi Köngäs, Netum
Matti Lehtimäki, Ericsson
Taina Mantovaara, Finanssialan keskusliitto
Mirka Meres-Wuori, Liikenne- ja viestintäministeriö
Janne Mustonen, Business Oulu
Kari Nykänen, Oulun yliopisto
Ari Pietikäinen, Ericsson
Anu Puhakainen, Ericsson
Göran Pulkkis, Arcada - Nylands svenska yrkeshögskola
Pekka Ruotsalainen, Terveyden ja hyvinvoinnin laitos
Jari Råman, Poliisi
Juha Röning, Oulun yliopisto
Pekka Savolainen, VTT
Charles Sederholm, Ubisecure
Manu Setälä, Teknologian ja innovaatioiden kehittämiskeskus Tekes
Juha Sääskilahti, Ericsson
Jari Still, F-Secure
Antti Sulosaari, Kansaneläkelaitos
Ari Takanen, Codenomicon
Markku Tyynelä, Metso Automation
Janne Uusilehto, Nokia
Jukka Valkonen, Aalto-yliopisto
Juha Vartiainen, Suomen Standardisoimisliitto SFS
Antti Vähä-Sipilä, Nokia
Timo Wiander, Oulun yliopisto
Pauli Wihuri, Nokia

1. Johdanto

Valtioneuvoston hyväksymä kansallinen tietoturvastrategia vuosiksi 2009–2015 keskittyy kolmeen painopistealueeseen: perustaitoihin arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallintaan ja toimintavarmuuteen sekä kilpailukykyyn ja kansainväliseen verkostoyhteistyöhön. Kansallisen tietoturvastrategian toimenpideohjelma hyväksyttiin marraskuussa 2009. Ohjelmassa toteutettiin yhdeksän keskeistä hanketta, joissa paneuduttiin uusiin ajankohtaisiin tietoturva-asioihin ja parannetaan olemassa olevia toimintoja. Tämä raportti on kyseisen ohjelman hankkeen 5 loppuraportti.

Kansallisen tietoturvastrategian toimenpideohjelman hankkeen 5 tehtävämäärittelyn mukaisesti pääaiheina hankkeessa olivat:

- suomalaisen tietoturvaosaamisen levittäminen ja kansainvälisten standardien käyttöönoton edistäminen sekä
- aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön.

Tavoitteena oli luoda aikaisempaa parempia edellytyksiä kansainvälisille toimijoille tulla tai investoida Suomeen. Tämä raportti käsittelee tietoturvallisuutta ja tietosuojaa kokonaisvaltaisesta näkökulmasta ja syventyy erityisesti Suomen kilpailukykyyn ja kansainväliseen verkostoyhteistyöhön.

Teknologiateollisuuden innovaatiopolitiikan työryhmän raportissa vuodelta 2010 [1] todetaan, että Suomi on kansallisen kilpailukyvyn näkökulmasta ennennäkemättömien haasteiden edessä ja korostaa innovaatioiden merkitystä Suomen kasvulle ja menestykselle. Raportin mukaan yritysten pitää pystyä uusiutumaan ja kehittämään uusia liiketoimintoja. Tietoturvaan liittyvien ohjelmistomarkkinoiden kasvun ennustetaan lähivuosina jatkuvan lähes kymmenen prosentin vuosivauhtia globaalisti. Lisäksi tietoturvan merkitys palveluissa ja tuotteissa tulee kasvamaan huomattavasti.

Suomella on tilaisuus hyödyntää olemassa oleva tietoturvaan liittyvä markkinapotentiaali ja profiloitua globaalisti merkittävän tietoturvan huippuosaamiskeskittymän sijaintipaikkana sekä johtavana tietoturvamaana ja kansainvälisenä suunnannäyttäjänä. Suomen vahva teknologiaosaaminen, tutkimus- ja kehitystyön tavoiteohjautuvuus tutkimus- ja tuotekehitysorganisaatioissa sekä saavutettu asema tietyissä erityisteemoissa tietoturvan mallimaana Euroopassa luovat tarvittavan pohjan potentiaalin hyödyntämiselle. Tämä lähtöasetelma on hyödynnettävä rohkeasti nyt, kun se on vielä mahdollista.

Aikaisempaa parempien edellytyksien luominen Suomen kilpailukyvylle tietoturva-aihepiirissä on erittäin merkittävä, mutta haasteellinen asia, ja suuri osa tämän raportin pohdinnasta koskee tätä tavoitetta. Tietoturvaan liittyvällä osaamisella ja ratkaisuilla on mahdollista vaikuttaa Suomen kansantalouteen uusien merkittävien kansainvälisten investointien kautta. Lisäksi tietoturva on keskeinen osa tulevaisuuden tuote- ja palveluinnovaatioita. Oikein toteutettu tietoturvallisuus luo edellytyksiä tuotteille ja palveluille, joissa erityisesti tiedon luottamuksellisuus, eheys ja saatavuus tietosuojan lisäksi ovat merkittävässä roolissa. Kyse ei ole siis pelkästään siitä, mitä liiketoimintaa tietoturva suoranaisesti tuottaa, vaan myös siitä, mikä osa globaalin tietoteknisen kehityksen luomista markkinoista ja siitä syntyvästä

liiketoiminnasta jää ulottumattomiimme ellei tietoturvan huippu- ja perusosaamiseen panosteta riittävästi.

Hankkeessa toimi tietoturvan ammattilaisista ja sidosryhmistä koostuva asiantuntijatyöryhmä, joka kokoontui vuonna 2010 kaksi kertaa ja vuonna 2011 kerran. Hankkeen pääasialliset työmenetelmät olivat työryhmäkeskustelut, työryhmän jäsenten asiantuntijamielipiteiden kerääminen ja niiden iteratiivinen analyysi. Lisäksi hankkeessa haastateltiin myös 33:a pitkän kokemuksen tietoturva- ja tietosuoja-asiantuntijaa Suomesta ja ulkomailta yritys- ja tutkimusmaailmasta sekä valtionhallinnosta. Kiitämme haastateltuja arvokkaista näkemyksistä työryhmän työssä.

Tässä raportissa tietoturvan standardisointityöhön panostaminen korostuu, koska se on toinen hankkeen pääkohdista. Kokonaisvaltaisesta tietoturvan kehittämisen näkökulmasta tarkasteltuna kuitenkin riittävä tietoturvakoulutus on painoarvoltaan vielä standardisointiakin merkittävämpi asia.

2. Painopiste 1: Suomalaisen tietoturvaosaamisen levittäminen

Tarkastelemme suomalaisen asiantuntijatason tietoturvaosaamisen nykytilannetta ja esitämme siihen asiantuntijamielipiteisiin pohjautuvan karkean tason kehittämissuunnitelman. Suunnitelma painottaa sitä, että Suomen kiinnostavuus ulkomaisen tietoturvaan liittyvän yhteistyön näkökulmasta kasvaa oleellisesti. Pääpaino on suomalaisen tietoturvan tutkimus- ja kehitystoiminnan tehostamisessa, tietoturvaosaamisen jalkautumisen ja levittämisen ollessa seuraus tehostamisesta. Tässä mietinnössä esitetyt toimenpiteet edellyttävät jatkotoimenpiteenä riittävän yksityiskohtaista suunnitteluaktiviteettia.

2.1 Nykytilanne

2.1.1 Tietoturvan merkitys on suuri ja kasvaa entisestään

Verkottuneet tietoliikenne- ja ohjelmistojärjestelmät ovat houkutteleva rikollisen toiminnan kohde. Tietoturvarikollisuus on viime vuosina ammattimaistunut ja on nykypäivänä usein asiantuntevaa ja järjestelmällistä liiketoimintaa. Tietojärjestelmät monimutkaistuvat, verkottuvat ja niiden osina käytetään yhä moninaisempia laitteita pienistä sensoreista valtavien konesalien järjestelmiin. Vastaava kehityskulku on nähtävissä palvelujen verkostoitumisessa: keskittämisen ja suuruuden ekonomiaa tavoitellaan IT-ostopalveluista palvelimien virtualisointiin kolmannen osapuolen palveluna. Tulevaisuudessa painopiste siirtyy yhä enemmän tiedon hallintaan verkottuneiden laitteiden ja järjestelmien ”viidakossa”. Hyvien tietoturvaratkaisujen merkitys yhteiskunnalle, yrityselämälle, organisaatioille ja kuluttajille kasvaa jatkuvasti. Hyvin toteutettu tietoturvallisuus edesauttaa toimintojen muuntautumiskykyä ja tuottavuutta, kun taas puutteet siinä saavat tietoturvaratkaisut näyttäytymään ”riippakivinä”.

Puutteet tietoturvallisuudessa johtuvat ennen kaikkea siitä, että alan käytännöt, menetelmät ja työkalut ovat haasteisiin nähden yhä edelleen varsin kehittymättömiä, joka on taas merkittävästi tietoturvan haastavuuden, dynaamisuuden ja asiantuntijaosaamisen pirstoutuneisuuden syytä:

- Haastavuuden saa aikaan tietoturvaan luonnollisesti liittyvä tarve yhtäaikaisesta kokonaisuuksien, eri asiantuntija-alojen ja –näkökulmien sekä yksityiskohtien osaamisesta.
- Tietoturvauhkien dynaamisuus on pitkälti seurausta nykyisistä puutteellisista ratkaisuista.
- Asiantuntijatason tietoturvaosaaminen on pirstoutuneena ja laajan hyödyntämisen kannalta hyvin vaikeasti saavutettavissa yrityksissä, tutkimusorganisaatioissa ja valtionhallinnon organisaatioissa.

Huono tietoturvallisuustoteutus vaarantaa organisaatioiden toiminnan, tuotteisiin ja palveluihin liittyvän liiketoiminnan ja jopa yhteiskunnalle tärkeitä perusrakenteita, kuten esimerkiksi sähkön- ja energiantuotannon ja suurten teollisuuslaitosten toimintoja. Tietojärjestelmät ja -verkot ovat myös yhteiskunnan toiminnalle kriittisiä perusrakenteita. Niitä käytetään myös osana muita kriittisiä perusrakenteita.

Tarvitsemme kehittyneen tietoturvallisuustoimintakyvyn yhteiskunnan toimintojen varmistamiseksi.

Heijasteena tietoturvaratkaisujen merkityksen kasvulle on havaittavissa tietoturvaan liittyvien globaalien ohjelmistomarkkinoiden jatkuva voimakas kasvu. Gartnerin [2] arvion mukaan kyseisten vuonna 2013 noin 19 miljardiin Yhdysvaltain dollariin nousevien markkinoiden keskimääräinen kasvu aikavälillä 2008–2013 on 9,3 %. Euroopan alueen kasvu jää hieman tätä matalammalle noin 7 %:n vuotuiselle tasolle, Yhdysvaltain kasvulukujen ollessa keskimääräisellä tasolla, kehittyvien maiden yltäessä huomattavasti nopeampaan, vuositasolla jopa 15 %:n ylittävään kasvuun. Myös tietoturvanhallinnassa on vastaava kasvupotentiaali olemassa. On muistettava, että tietoturvallisuus on ensisijaisesti tuotteiden ja palveluiden ominaisuus ja kiinteä osa organisaatioiden toimintaa. Se on harvoin erikseen myytävä tuote tai palvelu. Näin ollen edellä esitetyt kasvuluvut ovat vain osa totuutta, ja tarve tietoturvaratkaisuille on paljon monitahoisempi asia. Frost & Sullivan arvioi raportissaan *The 2011 (ISC)^2 Global Information Security Workforce Study* [3], että vuonna 2010 maailmassa oli noin 2,3 miljoonaa tietoturva-ammattilaista, ja vuoteen 2015 tarve on kasvanut noin 4,2 miljoonaan ammattilaiseen.

Näiden kasvavien markkinoiden markkinapotentiaalin hyödyntäminen on suomalaisille toimijoille merkittävä mahdollisuus. Käytännössä potentiaalin hyödyntäminen vaatii nykyistä merkittävämpää osaamisen integraatiota toimijoiden kesken.

Tietojärjestelmät ovat yhä useammin moniulotteisia sosiaalisteknisiä toimintaympäristöjä. Tietoteknisten taitojen lisäksi tarvitaan järjestelmien suunnittelussa eettisten arvojen ja lainsäädännön osaamista ja tuntemista. Eräillä sektoreilla, kuten sosiaali- ja terveydenhuollossa ja pankkialalla, on tietoturvallisuuden säätely vakiintunutta ja paikallista. Tietosuojalainsäädäntö on hyvin paikallista ja käsitykset tietosuojavaatimuksista eroavat hyvin paljon eri kulttuureissa. Tämä asettaa organisaatioiden ja valtioiden rajat ylittäville järjestelmille suuria vaatimuksia. Suomen kehittynyt tietosuojalainsäädäntö yhdessä muun osaamisen kanssa antaa meille hyvät lähtökohdat toimia kansainvälisillä markkinoilla.

2.1.2 Tietoturvaosaamisen tärkeimmät osa-alueet

Asiantuntijatason tietoturvaan ja tietosuojaan liittyvää osaamista voidaan karkeasti ottaen tarkastella seuraavasta kolmesta näkökulmasta.

- Teknologinen tietoturvaosaaminen. Liiketoiminnalliselta kannalta teknologista tietoturvaosaamista voidaan käyttää erityisesti tietoturvallisuutta parantavien teknisten ratkaisujen tutkimukseen ja kehitykseen. Tällaisten teknisten ratkaisujen tuottaminen on
    - suoraa liiketoimintaa tietoturvatuotteina ja -palveluina ja
    - liiketoiminnan tukemista ja sen jatkuvuuden varmistamista tuotteisiin ja palveluihin rakennettuina tietoturvaratkaisuina (tuotetietoturva). Tuotekehityksessä on tärkeää pystyä integroimaan toiminnallisia ja ei-toiminnallisia tietoturvaratkaisuja tietoteknisiin sovelluksiin ja palveluihin.

  Pitkäjänteisyys on edellytys jatkuvaan kehitykseen perustuvalle riittävän korkealle tuote- ja palvelutietoturvallisuudelle nykyaikaisessa avoimien innovaatioiden liiketoimintaverkostossa. On huomattavaa, että teknologinen tietoturvaosaaminen vaatii usein sovellusorientoitunutta tarkastelua, ja sovellusriippumattomien ratkaisujen kehittäminen on haastavaa.

- Tietoturvanhallintaosaaminen. Hyvä tietoturvanhallintaosaaminen on kriittinen asia yritysten liiketoiminnalle ja organisaatioiden toiminnalle. Puutteet siinä saattavat johtaa merkittäviin taloudellisiin menetyksiin, jopa yhtäkkisesti. Tietoturvanhallinnan menettelyjä tulee soveltaa laajamittaisesti, johdonmukaisesti ja pitkäjänteisesti organisaatioissa, niin yrityksissä kuin valtionhallinnossa. Vaikuttavien ja tehokkaiden ratkaisujen pitää olla integroituja niin julkisten kuin yksityisten organisaatioiden liiketoimintoihin, ja erityisesti johtamiseen, riskienhallintaan ja prosesseihin. Organisaation ylin johto on niistä vastuullinen. Nykyisin kuitenkin johdon tietoisuus tästä asiasta on usein vajavainen tai fokus on yksinomaan suoraviivaisessa taloudellisessa ajattelussa. Tietoturvallisuutta ei voi organisaatioissa saada aikaan vain ulkopuolisilla tarkastuksilla, eikä sertifioitu järjestelmä takaa todellista tietoturvallisuutta. Organisaatioiden johtamisjärjestelmä kattaa koko organisaation ja sen kaikki toiminnalliset tasot aina strategisesta johtamisesta operatiivisen toiminnan ja ihmisten johtamiseen. Tietoturvallisuuden toimenpiteet on sovitettava tähän kokonaisuuteen sekä teknisesti että hallinnollisesti. Tietoturvanhallintaosaamisen ongelmakenttään kuuluu toimenpiteiden ja käytäntöjen sovittaminen organisaation toiminnan kannalta oikealle tasolle niin, että vältytään riittämättömän tietoturvallisuuden aiheuttamilta liiketaloudellisilta katastrofeilta, mutta toisaalta myös tietoturvanhallinnan ylilyönneiltä. Tuotekehitysorganisaatioissa erityisesti tuotekehityksen, tuotannon ja ylläpidon toimintojen tietoturvallisuuteen tulee kiinnittää huomiota.

- Tietoturvaan ja -suojaan liittyvä lainsäädäntöosaaminen sekä tietojärjestelmiin liittyvien eettisten kysymysten osaaminen. Ilman tietoturvaan liittyvää lainsäädännön ja eettisten näkökohtien hyvää osaamista ei ole mahdollista toteuttaa kansalaisten ja viranomaisten hyväksymiä tietojärjestelmiä. Lähivuosina monilta tällaisilta järjestelmiltä, kuten terveydenhuollon järjestelmiltä, tullaan edellyttämään riittävän tietoturvan ja tietosuojan tason osoittamista esimerkiksi sertifioinneilla tai muilla tietoturvanvarmistustoimenpiteillä. Onkin selvää, että tulevaisuudessa erityisesti pienten ja keskisuurten yritysten osaamisen lisääminen avaa mahdollisuuksia uusille innovatiivisille kansainvälisille tuotteille ja palveluille.

Hyvä teknologinen tietoturvaosaaminen, tietoturvanhallintaosaaminen sekä tietoturvaan ja -suojaan liittyvä lainsäädäntöosaaminen mahdollistavat laajamittaista liiketoimintaa ja varmistavat sen jatkuvuutta. Näiden osa-alueiden riittävän korkean osaamistason synnyttäminen ja ylläpito vaatii jatkuvaa oppimista sekä vaikuttamista. Tällä hetkellä näyttävät erityisesti tietoturvan teknologisen ja hallinnan näkökulmat olevan kovin erillään – asiantuntijat ja jopa käsitteistö painottavat vain toista näkökulmaa, usein unohtaen toisen. Tietoturvaosaamisen kokonaisvaltainen kehittäminen vaatii molempien näkökulmien yhdistämistä. Nykyinen tietoturvaosaamisen sirpalemaisuus näkyy selvästi myös eri toimialojen tietoturvakäytäntöjen eroissa.

On ilmiselvää, että hyvän ja kilpailukykyisen tietoturvaosaamisen luomiseksi ja ylläpitämiseksi vaaditaan aktiivista, tavoiteohjautuvaa ja eri asiantuntijoita hyödyntävää yhteistyömuotoa. Vain yksi toimija tai näkökulma tietoturvaan ei riitä oleellisten parannusten tekemiseksi. Tarpeet suoralle keskustelulle ongelmista ja ratkaisumalleista sekä ratkaisujen jalkautuminen käytännön tasolle korostuvat tietoturvassa. Pelkkä keskustelu foorumeissa ja tiedonjako ei ole riittävä toimenpide, vaan lisäksi tarvitaan valikoitujen tietoturvan osa-alueiden osaamisen yhdistävää vahvaa yhteistä kehitysagendaa. Koska tietoturva on haastava ja erittäin monitahoinen kenttä, on siinä kyettävä löytämään merkityksellisiä kehittämiskohteita, jotka tarjoavat yhteen toimivia ja toisiaan tehokkaasti tukevia tietoturvallisuuden osaratkaisuja eri näkökulmista.

Osaratkaisujen kehitys vaatii useiden sosio-teknis-taloudellisten näkökulmien ymmärrystä.

2.1.3 Tietoturvaosaaminen Suomessa tutkimus- ja kehitysnäkökulmasta

Suomalaiset yritykset tuottavat tietoturvallisia tuotteita ja palveluita sekä toisaalta palveluita tietoturvan eri osa-alueille. Painotus on selkeästi teknologioissa. Suomalaista tietoturvaosaamista hyödynnetään mm. seuraavien tuotteiden ja palvelujen tuottamiseen:

- tietoturvan teknisiä osaratkaisuja ohjelmistojen, laitteiden ja järjestelmien muodossa, kuten esim. suojaus haittaohjelmilta ja tunkeutumisyrityksiltä sekä tietoliikenne- ja verkkopalvelujen turvalliset käyttöyhteydet (esim. Ericsson, F-Secure, Hallinnon tietotekniikkakeskus HALTIK, Insta DefSec, Nokia, Nokia Siemens Networks, Stonesoft ja Ubisecure),

- teknisten järjestelmien tietoturvan ja siihen läheisesti liittyvän ohjelmistolaadun testaustyökaluja ja –palveluja (esim. Codenomicon),

- sovelletaan suomalaista tietoturvaosaamista erityisesti tietoliikenne- ja automaatioalan globaalissa tuote- ja palvelukehityksessä; riittävä tietoturva on välttämätön vaatimus ICT- ja automaatio-alan tuotteille (esim. Nokia, Nokia Siemens Networks, Ericsson, Metso Automation) sekä

- palveluja vaatimustenmukaisuuden ja tietoturvan hallintaan ja tarkastuksiin sekä turvalliseen ohjelmistokehitykseen (esim. Navicre, Netum ja Nixu).

Suomessa toimivilla suurilla tietoliikennealan yrityksillä Nokialla, Nokia Siemens Networksillä ja Ericssonilla on vahvat maassamme toimivat konsernien sisäiset tietoturvan osaamisorganisaatiot. Kyseiset organisaatiot panostavat mm. standardisointiin, tietoturva-aiheiseen tutkimukseen, tuotekehityksen tietoturvaan liittyvien prosessien ja metodien kehitykseen ja ylläpitoon sekä haavoittuvuuksien hallintaan. Pienemmissä yrityksissä on myös jossain määrin vastaavaa toimintaa, mutta useimmissa se on varsin ohutta. Parantamiselle on selkeä kasvuun ja menestykseen tähtäävä peruste. Tuote- ja palvelualojen yritystoiminnan jatkuvuuden turvaaminen edellyttää, että tulevat vaatimukset, myös tietoturvavaatimukset, pystytään ennakoimaan.

Suurissa yrityksissä ja valtionhallinnon organisaatioissa panostetaan Suomessa jossain määrin tietoturvanhallinta-asioihin, mutta pienissä ja keskisuurissa yrityksissä (pk-yrityksissä) on suuria ongelmia tämän suhteen. Pk-yritysten merkitys kansantaloudellisesti on erittäin suuri ja niiden rooli esimerkiksi alihankkijoina asettaakin haasteita tietoturvallisuuden näkökulmasta: kasvu liiketoimintaverkoston itsenäiseksi toimijaksi edellyttää oman osaamisen kehittämistä.

Yliopistot, korkeakoulut ja VTT kuuluvat tietoturvaosaamisen edelläkävijöihin Suomessa. Yliopistoissa ja korkeakouluissa eri puolilla Suomea harjoitetaan merkittävää tietoturvan koulutus- ja tutkimustoimintaa. Varsinkin Oulun yliopistossa, Aalto-yliopistossa, Lappeenrannan teknillisessä yliopistossa, Tampereen teknillisessä yliopistossa ja Turun yliopistossa panostetaan tietoturvan kursseihin, tutkimukseen ja opinnäytetöihin. Tietosuojatutkimuksen osalta Suomessa painopiste on Lapin yliopistossa. VTT:n tietoturvatutkimus tekee aktiivista yhteistyötä yliopisto- ja korkeakoulumaailman kanssa. Suomalaisilla tutkimusorganisaatioilla ja yrityksillä on tietoturvatutkimusta erityisesti seuraavissa teemoissa: haavoittuvuuksien hallinta,

suojautuminen haittaohjelmilta, tietoturvaan liittyvä ohjelmistolaatu, tietoturvan varmistamistekniikat ja mittarit, tietoturvanhallinta, salaustekniikat, tietoturvaprotokollat, tietoliikenneverkkojen ja laitteiden tietoturva sekä tietosuojalainsäädäntö. Monet teemoista ovat potentiaalisia uuden liiketoiminnan mahdollistajia tai lähteitä. Merkittävä pitkäaikainen panostuskohde Internetin tietoturvassa Suomessa on ollut *Host Identity Protocol* (*HIP*) -tutkimus- ja standardisointityö [4]. Suomen suurimmassa ICT-alan TiVit SHOK-hankkeen Cloud Software -projektissa tietoturva [5] on koko ohjelmaa poikkileikkaava tutkimusteema, jolla on keskeinen merkitys teknologiakehityksessä, liiketoiminnan uudistamisessa sekä tutkimus- ja tuotekehitysprosesseissa. Muihinkin hankkeisiin tarvitaan vastaavaa poikkileikkaavaa tarkastelua. Tampereen teknillisessä yliopistossa opetetaan ja tutkitaan muun muassa teollisuusautomaation, tietoverkkojen ja ohjelmistokehityksen tietoturvaa.

Tällä hetkellä Suomen merkittävin tietoturvan tutkimuksen osaamiskeskittymä on Oulussa. Oulun tietoturvaklusteri [6] on syntynyt tietoturvan tutkimus- ja kehitystoiminnan tarpeista yhteistyön voimin ilman varsinaista keskittymäsuunnittelua noin kymmenen vuoden yritys–tutkimus-yhteistyön tuloksena. Viime aikoina kokoavana voimana on toiminut Oulun kaupungin liikelaitos Business Oulu. Keskittymässä toimii iso joukko yrityksiä, Oulun yliopisto, VTT ja Oulun kaupunki. Oulun yliopistossa on kansainvälisesti tunnustusta saaneet tietoturvatutkimusryhmät sekä teknillisessä tiedekunnassa (OUSPG, Oulu University Secure Programming Group) että luonnontieteellisessä tiedekunnassa (ISSRC, Information Systems Security Research Center). Valtaosa VTT:n tietoturvatutkijoista työskentelee VTT:n Oulun yksikössä. Oulun yliopistossa ja VTT:llä Oulussa on noin 50 tietoturvatutkijaa. Klusterin toiminnassa on tällä hetkellä mukana 65 organisaatiota. Klusterille tai sen työtä jatkavalle ja kehittävälle yhteenliittymälle tulisi suunnitella oma kehitysagenda ja valita päätoiminen vetäjä, jotta Suomi ei menettäisi lupaavaa tilaisuutta tietoturvaan liittyvien innovaatioiden synnyttämisessä.

Rovaniemen ICT-turvaklusteri toimii turvallisuusalan tieto- ja tietoliikennealan osaamiskeskittymänä tarjoamalla yritysten, koulutuksen sekä tutkimus- ja kehitystoiminnan yhteistyöverkoston palveluita. Rovaniemen ICT-turvaklusterin visiona on olla merkittävä turvallisuusalan osaamiskeskittymä sekä kansallisella että kansainvälisellä tasolla. Rovaniemellä toimii turvasektorilla sekä toimintaa tukevia yrityksiä että julkishallinnon toimijoita, kuten HALTIK, Liikenteen turvallisuusvirasto TraFi ja Lapin korkeakoulukonserni. Korkeakoulukonserni muodostuu Lapin yliopistosta, Rovaniemen ja Kemi-Tornion ammattikorkeakouluista ja se tarjoaa koulutus-, tutkimus- ja kehittämispalveluita. ICT-turvaklusterin tavoitteena on perustaa ja kehittää IT-palveluiden tuotantokeskusta, joka määrittelee toimintamallinsa valtion IT-toiminnan johtamisyksikön asettamien periaatteiden mukaisesti.

Oulun alueeseen verrattuna Rovaniemellä korostuu vahvasti tietoturvan ja turvallisuuden operatiivinen työ. Tutkimukseen ja tuotekehitykseen ei keskitytä siinä määrin kuin Oulussa.

Pääkaupunkiseudulla ei ole selkeästi tunnistettavaa yhtenäistä tietoturvan osaamiskeskittymää. Kuitenkin pääkaupunkiseudun tutkimusorganisaatiot ja yritykset työskentelevät tiiviissä yhteistyössä keskenään. Toiminta on tässä yhteistyössä aktiivista, mutta eri ryhmittymät pääkaupunkiseudulla toimivat irrallaan toisistaan. Toiminta rakentuu merkittävissä määrin yritysten yhteistyölle. Aalto-yliopistolla on pitkä historia tietoturva-alan tutkimuksessa pääkaupunkiseudulla. Myös Jyväskylässä ja Tampereella on ollut suunnitteilla turvallisuusalan osaamiskeskittymätoimintaa. Tietoturvaan liittyvä tutkimustoiminta on ollut näillä paikkakunnilla pienimuotoisempaa, ja opinto-ohjelmat korostuvat enemmän. Tampereen

teknillisessä yliopistossa on muodostettu laitosrajat ylittävä tietoturvallisuuden opintokokonaisuus sekä yhteistyöverkosto paikallisia organisaatioita edustavien tietoturvallisuudesta kiinnostuneiden henkilöiden välille (Tampereen tietoturvapiiri).

Nykyisin eri klustereiden välinen yhteistyö on liian ohutta eikä liiketoimintaan tähtäävää riittävän fokusoitua yhteistä kehitysagendaa ole, jotta toiminnasta olisi merkittävää hyötyä osaamisen yhdistämisen näkökulmasta

Suomessa toimii valtionhallinnon ohjaamana suuri joukko tietoturvaan liittyviä työryhmiä, kuten esimerkiksi valtiovarainministeriön tietoturvaohjeistustoiminta VAHTI [7] ja liikenne- ja viestintäministeriön Kansallisen tietoturvastrategian toimenpideohjelma [8]. Valtionhallinnon työryhmätoiminta on tärkeää tietoturvakäytäntöjen parantamisen näkökulmasta, mutta ongelmana on se, että työryhmien välinen kommunikaatio on kevyttä. Valitettavasti tietoturvaohjeiden toteutus vaihtelee suuresti eri valtionhallinnon toimijoiden keskuudessa. Lisäksi toiminnan fokus on valtionhallintoon liittyvissä kysymyksissä, eikä juurikaan uuden liiketoiminnan luomisessa tietoturvaan liittyen. Valtionhallinnon foorumit eivät myöskään käsittele riittävästi tietoturvaan liittyvään tuotekehitystyötä eivätkä kansalaisten tietoturvakäyttäytymistä. Mainittua osaamista on maassamme, mutta se on hajallaan eri organisaatioissa. Kyseisen osaamisen yhdistämisen suhteen Suomessa on tyhjiö.

Lainsäädännön ja tietoturvallisuuteen liittyvän etiikan osaamisessa on Suomessa puutteita erityisesti pk-yrityksissä kansainvälisissä ja toimialakohtaisissa kysymyksissä. Tämä koskee erityisesti kansainvälistä ja toimialakohtaista osaamista.

Suomalaisten tietoturvaosaamisen kehittämistä on tukenut pitkään opetus- ja kulttuuriministeriön omistama CSC - Tieteen tietotekniikan keskus [9], jonka palveluihin kuuluu myös Suomen ensimmäinen CERT-toiminto, Funet CERT [10], joka välittää tietoa tietoturvapoikkeamista ja järjestää jäsenilleen tietoturvakoulutusta.

Sosiaali- ja terveydenhuollon tietosuojan ja tietoturvan alueilla Terveyden- ja hyvinvoinnin laitos (THL) on tehnyt pitkäjänteistä tietoturvallisuustyötä. THL on osallistunut koulutukseen ja tekee aktiivista tutkimus- ja asiantuntijatyötä aihepiirissä. THL on myös osallistunut terveydenhuollon tietoturvallisuutta ohjaavan lainsäädännön valmisteluun ja osallistuu tietosuojavaltuutetun terveydenhuollon tietosuojaa käsittelevän ryhmän työskentelyyn.

Suomessa on poikkeuksellisen aktiivista yhdistysten vetämää asiantuntijatason tietoturvatietoisuustoimintaa. Tietoturvaan liittyvää yhdistystoimintaa harjoittavat esimerkiksi Tietoturva ry [11], ISACAn (Information Systems Audit and Control Association) Suomen jaosto [12], Finnsecurity ry:n tietoturvallisuusjaosto [13] ja OWASP (Open Web Application Security Project) Helsinki Chapter [14]. Suomen suurin tietoturva-alan ammattilaisia kokoava yhdistys 950 jäsenen voimin on Tietoturva ry, joka järjestää koulutus- ja seminaaritapahtumia, keskustelutilaisuuksia ja edistää ammatillista tietoturva-alan sertifiointia. Yhdistys on toiminut kansallisena yhteistyökumppanina toimialariippumattomia ja laaja-alaisia kansainvälisen tason tietoturvakoulutuksia ja -sertifiointeja organisoivan $(ISC)^2$:n (International Information Systems Security Certification Consortium) [15] kanssa. $(ISC)^2$ vastaa mm. CISSP-sertifioinneista (Certified Information Systems Security Professional). Tietoturva ry toimii myös suomalaisena yhteistyökumppanina tietoturvakoulutusta tuottavan SANS-instituutin [16] kanssa. Lisäksi yhdistys edistää jäsenten verkostoitumista esimerkiksi yritysvierailujen ja yhteisöpalvelujen kautta ja on mukana tekemässä tietoturvayhteistyötä alan toimijoiden kanssa. Yhdistys antaa myös lausuntoja alaa koskevaa lainsäädäntöä ja tietoturvaohjeistusta kehitettäessä.

Teknologiateollisuuteen kuuluva PIA ry:n (Suomen Puolustus- ja Ilmailuteollisuusyhdistys) alaisuudessa toimii Turvallisuusteknologia-ryhmä, jossa aktiivisesti työskentelee yli 20 yritystä. Tietoturvaratkaisut sisältyvät kyseisen ryhmän intresseihin.

2.1.4 Tietoturvaosaaminen muualla maailmassa

Suomalaisten asiantuntijoiden pitäisi osata nykyistä paremmin hyödyntää maailmalla jo tuotettua materiaalia ja löytää sen avulla osa-alueita, joihin me yhteistyöllä voimme tuottaa uutta tietämystä ja kilpailuetua.

Tällä hetkellä globaalin asiantuntijatason tietoturvaosaamisen painopiste on Yhdysvalloissa. Yhdysvallat ja Kanada panostavat erittäin vahvasti kansallisilla tutkimus-, kehitys- ja yhteistyötoimenpiteillä tietoturvallisuuden parantamiseen. Yhdysvaltain liittovaltion monet organisaatiot yritysmaailma tukenaan ovat ottaneet tietoturva-asiat tärkeäksi kehittämiskohteeksi osana kansallisen turvallisuuden varmistamista. Erityisesti NIST (National Institute of Standards and Technology) [17] kehittää alalla yleisesti tunnustettuja standardeihin verrattavia ohjeistuksia, jotka perustuvat laajamittaisen yhteistyön tuloksiin ja käytännön kokemuksiin. Nämä ohjeistukset on sovitettu kuitenkin paikallisiin käytäntöihin ja erityistarpeisiin. Myös Yhdysvaltain DHS (Department of Homeland Security) [18] on panostanut tietoturvallisuuteen oman National Cyber Security Divisionin kautta, jonka kehittämää ohjeistusta on julkaissut mm. Build Security In -projekti [19].

Aasiassa tietoturva-ammattilaisia on väkilukuun suhteutettuna vielä hyvin vähän, mutta kehitys on viime vuosina ollut nopeaa erityisesti tutkimuksen saralla. Erityisesti Japani ja Kiina panostavat vahvasti tietoturvatutkimukseen.

Euroopasta puuttuu yhdysvaltalaista NISTiä vastaava organisaatio, eivätkä globaalit standardisointiorganisaatiot ole toistaiseksi kyenneet vastaavantasoiseen ohjeistukseen kuin NIST. Euroopan tietoturvavirasto ENISA [20] on jossain määrin NISTiin verrattava organisaatio, mutta se ei voi ottaa ohjeistusta siinä määrin tehtäväkseen kuin NIST resurssien niukkuuden takia. ENISA tekee Euroopassa hyvää asiantuntijatason työtä, ja se on tuottanut käyttökelpoista tietoutta ja ohjeistusta mm. riskienhallintaan, kriittisten perusrakenteiden suojaukseen, pilvipalvelujen tietoturvaan ja kansallisten CERT-organisaatioiden toimintaan.

Eurooppaan on syntynyt ja on syntymässä muutamia tietoturvatutkimuskeskittymiä. Tunnetuimpia lienevät Leuvenin katolisen yliopiston tutkimuskeskittymä Belgiassa ja erityisesti viime aikoina kasvanut Luxemburgin yliopistoalueen tutkimuskeskittymä. Molemmat keskittymät ovat syntyneet akateemisista tavoitteista, eikä yhteistyö yritysmaailman ja valtionhallintojen kanssa ole kovin tiivistä. Tällaisen keskittymän syntyminen Eurooppaan lienee kuitenkin vain ajan kysymys, koska sille on olemassa vahva tarve. Luxemburgilainen tutkimusrahoitusjärjestelmä kannustaa perus- ja soveltavan tutkimuksen eriyttämiseen projektitasolla, joka etenkin tietoturvassa hankaloittaa osaamisen yhdistämistä. Jos tämä haaste voitetaan, on Luxemburgin keskittymällä hyvät mahdollisuudet kehittyä mainittuun suuntaan.

Useat suomalaiset suuret ja eräät pienemmätkin organisaatiot kuuluvat kansainväliseen yritysvetoiseen tietoturvallisuuden alan foorumiin ISF:ään (Information Security Forum) [21], joka tekee hyvää työtä tietoturvaan liittyvän kriittisen tiedon levittämisessä ja toteuttaa laajoja analyysejä tietoturvatilanteesta jäsenorganisaatioidensa keskuudessa. ISF:n tulokset ovat kuitenkin monien toimijoiden saavuttamattomissa jäsenmaksun suuruuden takia.

Nykyisin selkeänä puutteena suomalaisessa tietoturvatyössä on vähäinen yhteistyö Venäjän ja muiden entisen Neuvostoliiton alueen valtioiden suuntaan. Venäläisten turvallisuustarpeiden ja käytäntöjen ymmärtäminen on tärkeää, jotta suomalaista tietoturvaosaamista voidaan levittää myös itään, tukea lähialueemme myönteistä turvallisuuskehitystä ja vahvistaa suomalaisten asemaa alueen markkinoilla. Venäjällä on kovatasoista matemaattista osaamista, jota voidaan hyödyntää tieturvan eri osa-alueilla, ja erityisesti salausmenetelmien tutkimuksessa. Viime vuosina venäläinen tietoturvatutkimus on alkanut yhdistämään vahvaa matemaattista osaamista lännen tietoturvaosaamiseen.

2.1.5 Suomen vahvuuksia

Suomen vahvuudet tietoturvaosaamisen hyödyntämisen näkökulmasta ovat tärkeysjärjestyksessä seuraavat:

- Teknologiaosaaminen: vahva teknisten innovaatioiden kulttuuri, josta osoituksena mm. suomalaisten tietoturvayritysten globaali menestys.

- Tavoiteohjautuvuus: erityisesti paikallisissa tietoturvan ja tietosuojan tutkimus- ja kehitysvetoisissa osaamiskeskittymissä on suoraa tavoiteohjautuvaa tiedonvaihtoa ja yhteistyötä. Tällainen tietoturvatyö lähtee käytännön haasteista.

- Maine: saavutettu asema tietoturvan mallimaana Euroopassa eräillä saroilla, kuten kansallinen CERT- ja tietoturvapäivätoiminta sekä tietosuojalainsäädäntö. Tämän lisäksi suomalaisilla on hyvä maine luotettavina yhteistyökumppaneina. Tämän työryhmän haastattelemat ulkomaalaiset asiantuntijat nostivat suomalaisten luotettavuuden erityisvahvuudeksi.

Tietoturvaan liittyvää menetelmäosaamista on myös Suomessa, ja eräät tietoturvanhallinnan toimijat toimivat merkittävissä kansainvälisissä asiantuntijapositioissa, mutta tämä osaaminen ei ole Suomessa laajamittaisesti korkealla tasolla.

Suomen vahvuuksia on vahvistettava edelleen ja hyödynnettävä ne suomalaisten toimijoiden kansainvälisen kilpailukyvyn kehittämisessä.

2.1.6 Osaamisesta kertominen maailmalla

Nykyisin suomalaisesta tietoturvaosaamisesta ja työn tuloksista kertominen kansainvälisillä foorumeilla on kiinni ennen kaikkea yksittäisistä asiantuntijoista ja heidän aktiivisuudestaan. Pieni joukko yritysten, tutkimuslaitosten ja yliopistojen asiantuntijoita on varsin aktiivinen tässä suhteessa. Myös valtionhallinnon tietoturva-aktiviteettien tuloksista kerrotaan jossain määrin. Suomalaiset tutkijat ja yritysten asiantuntijat levittävät tietoa tietoturvaan liittyvistä tutkimustuloksistaan ja suomalaisesta osaamisesta mm. seuraavilla tavoilla:

- Julkaisu- ja konferenssitoiminta. Suomalaisten tutkijoiden julkaisutoiminta on vähintäänkin tyydyttävällä tasolla, mutta parantamisen varaa on selkeästi. Tutkimustuloksia esitellään tieteellisissä lehtijulkaisuissa, konferensseissa,

työpajoissa ja seminaareissa. Tapahtumiin osallistutaan tavallisimmin Euroopassa, mutta myös jonkin verran Amerikassa ja Aasiassa. Suomalaiset ovat myös järjestäneet tieteellisiä työpajoja Suomessa ja muissa maissa. Erityisesti tieteellisiin lehtijulkaisuihin pitäisi panostaa nykyistä enemmän. Panostus edellyttää pitkäjänteistä työtä ja entistäkin aktiivisempaa verkostoitumista hyvien kansainvälisten tutkimusryhmien kanssa.

- Globaalit yhteistyöfoorumit. Suomalaiset ovat aktiivisia eräissä tietoturvaan liittyvissä yhteistyöfoorumeissa, kuten esim. SAFECode (Software Assurance Forum for Excellence in Code) [22] (Nokia, VTT, Oulun yliopisto) sekä erityisalojen työryhmissä, kuten IAEA (International Atomic Energy Agency) [23], jonka tietoturvallisuustoimintaan Suomesta osallistutaan (Oulun yliopisto ja ydinenergiaklusteri), ICASI (Industry Consortium for Advancement of Security on the Internet) [24] (Nokia) ja FIRST (Forum for Incident Response and Security Teams) [25] (Ericsson). Kyseisiin yhteistyöfoorumeihin osallistuminen tukee erityisesti tuotekehitysyritysten ja teollisuuslaitosten käytännön toimintaa.

- Eurooppalaiset työryhmät. Suomalaisia tietoturva-asiantuntijoita on ollut mukana eurooppalaisissa asiantuntijatyöryhmissä, kuten Euroopan tietoturvaviraston ENISAn työryhmät sekä EU:n 7. puiteohjelman [26] tietoturvatutkimukseen liittyvät työryhmät, kuten esim. palvelujen tietoturvaa kehittävä NESSI [27] ja tietoliikenteen työryhmä Net!Works [28]. Nokia on aktiivinen esim. DigitalEuropessa [29], joka on maailmanluokan yritysten yhteistyöelin sekä tekee yhteistyötä Iso-Britannian CPNI:n (Centre for the Protection of National Infrastructure) [30] kanssa, jossa yritykset, kuten Nokia ja Ericsson, kuuluvat VSIE:hen (Vendor Security Information Exchange).

- Eurooppalaiset tutkimusprojektit. Eurooppalaisiin tutkimusprojekteihin osallistutaan aktiivisesti ja niitä vedetään. Hankkeet liittyvät yleisimmin EU:n 7. puiteohjelmaan ja Eurekan ITEA2 [31] - ja CELTIC [32] -klustereihin. Eureka-projektien osarahoittajana toimii Suomessa Tekes. Tutkimusprojekteissa on yleensä vahva verkottumis- ja tiedonlevitysagenda, joka tukee suomalaisen osaamisen levittämistä hyvin.

- Kansainvälinen asiantuntija- ja tutkijavaihtotoiminta. Suomalaiset tutkimus- ja tuotekehitysorganisaatiot sekä valtionhallinnon organisaatiot ovat aktiivisia kansainvälisessä tutkija- ja asiantuntijavaihdossa. Tutkijavaihto suuntautuu erityisesti muihin Euroopan maihin ja Yhdysvaltoihin. Tutkijavaihto on suuntautunut Euroopassa erityisesti Ranskaan ja Espanjaan Eureka-klustereiden tutkimusprojektien puitteissa ja Yhdysvalloissa muun muassa Marylandin yliopistoon, Berkeleyn yliopistoon ja Georgia State Universityyn (GSU).

Valtionhallinnon organisaatiot ovat panostaneet suomalaisesta tietoturvaosaamisesta kertomiseen maailmalla. Tästä on seuraavia esimerkkejä:

- OECD. Liikenne- ja viestintäministeriö (LVM) ja valtiovarainministeriö (VM) ovat osallistuneet OECD:n (Organisation for Economic Co-operation and Development) tietoturva- ja tietosuojatyöryhmän (WPISP, Working Party on Information Security and Privacy) [33] työhön, jossa käsitellään mm. eri maiden tietoturvastrategioita ja ajankohtaisia kysymyksiä ja tapahtumia tietoturvaan ja tietosuojaan liittyen.

- EU-yhteistyö. LVM on osallistunut EU:n teletyöryhmään, jossa on vuoden 2010 aikana käsitelty mm. ENISAn jatkomandaattia. Suomi on myös

osallistunut aktiivisesti ENISAn johtoryhmätyöskentelyyn. LVM on osallistunut myös ENISAn johtamaan suositusten tekoon toimintavarmasta (*resilient*) Internetistä. LVM on osallistunut vuonna 2009 kriittisen infrastruktuurin direktiivivalmisteluun, mikä on jatkunut vuonna 2010 ICT-sektorikohtaisten kriteerien määrittelytyöllä EFMS (European Forum for Member State officials) ja E3PR (European Private Public Partnership for Resilience). LVM on osallistunut myös tilannekuvajärjestelmistä käytäviin neuvotteluihin EU-tasolla.

- Pohjoismainen yhteistyö. LVM on keskustellut etuoikeustoiminteen toteutuksista Ruotsin, Norjan ja Tanskan kanssa. Pohjoismaista yhteistyötä on lisäksi varsinkin kriittisten perusrakenteiden tietoturvakysymyksissä eri viranomaisilla.

- Tietoturvaan liittyvät kriittisten perusrakenteiden harjoitukset. LVM on osallistunut ja kansallisessa osuudessa myös johtanut EU-laajuisia CIIP-harjoituksia (CIIP, Critical Information Infrastructure Protection) ja osallistunut tarkkailijana Viron ensimmäisiin CIIP-harjoituksiin 2010 syksyllä. Harjoitukset ovat tärkeää toimintaa käytännön CIIP-työn kehittämisessä.

Viestintävirastossa toimiva kansallinen tietoturvaviranomainen CERT-FI [34] on aktiivinen kansainvälisessä yhteistyössä, ja levittää tämän työn yhteydessä suomalaista tietoturvaosaamista. CERT-FI harjoittaa mm. asiantuntija- ja virkamiesvaihtoa, strategista yhteistyötä, järjestelmä-, prosessi- ja työkalukehitystä ja haavoittuvuuskoordinointia kansainvälisessä yhteistyössä. Vaikka kaikki kansainvälisen yhteistyön muodot eivät suoranaisesti edesauta CERT-FI:n toimintaa Suomessa, ovat ne erittäin tärkeitä kansainvälisen CERT-yhteisön kehittymisen kannalta. CERT-FI on pyrkinyt luomaan suhteita myös tietoturvallisuuden suhteen kehittyvien maiden kanssa. Tällä työllä on positiivisia vaikutuksia niin Suomen, Euroopan kuin muun maailman osalta. CERT-toiminnan näkökulmasta strategiayhteistyö Pohjoismaiden ja muiden EU-maiden kanssa on erittäin tärkeää. Varsinkin EU-tasolla tietoturvan merkitys korostuu koko ajan, jolloin myös CERT-toimijoiden tulee yhdessä analysoida ja kommentoida esimerkiksi EU-tason päätösten vaikutuksia CERT-toimintaan. CERT-FI on onnistunut luomaan aktiivisen yhteistyön suomalaisten organisaatioiden CERT-tiimien kanssa. Ulkomailla hämmästellään usein sitä, miten hyvin oleellinen tieto kulkee CERT-Fin ja kaupallisten yritysten CERT-tiimien välillä Suomessa. Tämä näyttää olevan ainutlaatuista osaamista Suomessa. CERT-FI:llä on aktiivista yhteistyötä muunmuassa Yhdysvaltain US-CERTin kanssa ja teollisuusohjausjärjestelmiin erikoistuneen ICS-CERTin kanssa.

2.1.7 Johtopäätökset

Seuraavia toimenpiteitä tarvitaan suomalaisen tietoturvaosaamisen levittämiseksi:

- Tärkeintä on tehostaa pirstoutunut tietoturvan huippututkimus-, kehitys- ja koulutustoiminta yhdistämällä ne harkitun kehitysagendan mukaisesti. Toiminnan tulee tähdätä uuden liiketoiminnan synnyttämiseen ja olemassa olevan edistämiseen.
- On laajennettava ja syvennettävä suomalaisten tietoturvan tutkijoiden, asiantuntijoiden ja opettajien sekä suomalaisten organisaatioiden kansainvälisiä ja kansallisia yhteistyöverkostoja sekä suomalaisten mukanaoloa kansainvälisissä yhteistyöhankkeissa.
- On lisättävä suomalaisen tietoturvaosaamisen näkyvyyttä kansainvälisissä tieteellisissä julkaisuissa, konferensseissa ja sopivilla kansainvälisillä messuilla ja

näyttelyissä, sekä yhteistyöfoorumeissa. Eräät suomalaiset suuret yritykset ja tutkimusorganisaatiot näkyvät hyvin maailmalla, mutta varsinkin pk-yritysten pitäisi näkyä enemmän.
- Suomalaisten asiantuntijoiden pitää osata entistä paremmin hyödyntää maailmalla jo tuotettua materiaalia ja löytää sen avulla osa-alueita, joihin me yhteistyöllä voimme tuottaa uutta tietämystä ja kilpailuetua.

Tietoturvaan liittyvien teknologioiden merkitys globaalisti sekä liiketoiminnassa että yhteiskunnalle kriittisten perusrakenteiden ja liiketoiminnan näkökulmasta on suuri, ja tämä merkitys vahvistuu koko ajan. Tietoturvallisuudella on Suomelle suuri merkitys, koska:

- tarvitsemme kehittyneen tietoturvallisuustoimintakyvyn yhteiskunnan toimintojen varmistamiseksi, ja

- tietoturvaosaaminen luo merkittävän liiketoimintapotentiaalin, jota ei ole toistaiseksi täysimittaisesti hyödynnetty kansainvälisessä mittakaavassa.

On perusteltua todeta, että oikealla tavalla vahvistettu ja yhdistetty tietoturvaosaaminen luo liiketoimintapotentiaalia ja mahdollisuuksia olla globaali edelläkävijä. Suomessa on menetetty tilaisuuksia hyödyntää tietoturvaan liittyvää liiketoimintapotentiaalia. Suomessa on esimerkiksi kehitetty monia alan yksittäisiä teknologioita, mutta meillä on mittavia ongelmia erityisesti niiden integroinnissa ja laajamittaisessa käyttöönotossa. Tämä ongelma pitäisi korjata. Välttämättömänä vaatimuksena on myönteinen erottuminen muista, joka edellyttää innovatiivisia ja "käänteentekeviä" ratkaisuja. Erottuminen vaatii syvällistä pohtimista, mihin tietoturvaan liittyviin kärkiteemoihin panostetaan.

Vaikka tekninen osaaminen Suomessa on korkeaa tasoa, jäävät markkinointi ja tuotteistaminen usein vajaatehoisiksi. Kansallisissa tietoturvaosaamisen hyödyntämistoimenpiteissä pitäisi panostaa myös tietoturvaan liittyvään tuotteistamiseen ja kansainväliseen markkinointiin. Esimerkiksi Saksa on ollut vuonna 2010 hyvin esillä kansainvälisissä tapahtumissa.

Alun perin hankkeen 5 tavoitteenasettelu ei korostanut tietoturvan tutkimus- ja kehitystoiminnan tehostamista. Työryhmän työn aikana hankkeessa hahmottui kuitenkin vahvasti näkemys, että nimenomaan tähän pitäisi suunnata enemmän voimavaroja. Tietoturvaosaamisen kehittäminen Suomen kansainvälistä kilpailukykyä edistävään suuntaan on samalla mitä merkittävintä suomalaisten tietoturvaosaamisen kansainvälistä levittämistä.

2.2 Kehittämissuunnitelma: Suomeen tarvitaan tietoturvan huippuosaamiskeskittymä

2.2.1 Huippuosaamiskeskittymän tarve ja hyödyt

Panostukset tulee ohjata nimenomaan suomalaisen tietoturvaosaamisen kehittämiseen niin, että Suomeen syntyy globaalisti tunnettu tietoturvan huippuosaamiskeskittymä. Tällä hetkellä suomalainen tietoturvaosaaminen on pirstoutuneena ja laajan hyödyntämisen kannalta vaikeasti saavutettavissa yrityksissä, tutkimusorganisaatioissa ja valtionhallinnon organisaatioissa. Osaamisen tehokas hyödyntäminen vaatii suurempien kokonaisuuksien käsittelyä, kuin yksittäisillä toimijoilla on Suomessa mahdollisuuksia. Pelkkä keskusteluyhteistyö ei riitä, vaan asiantuntijoiden osaamista tulee yhdistää erityisen kehittämisagendan mukaisesti. Suomeen tulee synnyttää uutta liiketoimintaa ideoiva tietoturvan osaamiskeskittymä, jossa kotimaiset tuotekehitysverkostot ja kansainvälisen tason tutkimusverkostot risteävät ruokkien uutta luovaa tuotekehitystä, tietoturvallisuuden parantamista ja osaamispääomamme kehittämistä. On tärkeää, että tällainen toiminta rakentuu kaikenkokoisten yritysten, tutkimusmaailman ja valtionhallinnon yhteistyölle. Keskittymän kehitysagendaan tulee valita rajallinen määrä todellisia kärkialueita, joihin suunnataan panostusta.

Suomen tietoturvan huippuosaamiskeskittymän toimintaan kuuluu myös oleellisesti yhteistyö kansainvälisesti merkittävien asiantuntijoiden kanssa ja tähän liittyvä Suomen osaamispääomaa kartuttava toiminta, kuten vaihtotutkimusvierailut. Osana kehitysagendaa pitää tunnistaa kansainväliset tahot, joiden kanssa yhteistyötä tehdään ensisijaisesti.

Työryhmä arvioi Suomen tietoturvan huippuosaamiskeskittymällä saavutettavan seuraavia kansallisia hyötyjä:

- Suomi profiloituu nykyistä selkeämmin kansainvälisesti johtavana tietoturvamaana ja suunnannäyttäjänä. On huomattava kuitenkin että tämä status täytyy ansaita toiminnan onnistumisella.
- Syntyy uutta innovaatiopotentiaalia, jos nykyisin hajallaan oleva kapea ja syvällinen tietoturvan eri osa-alueiden asiantuntijaosaaminen yhdistetään. Yhdistämistä kannattaa tehdä myös erityisesti liiketoimintaosaamisen suhteen.
- Suomeen syntyy uutta liiketoimintaa ja työpaikkoja varmistaen osaltaan hyvinvointiyhteiskuntamme kehittymistä ja jatkuvuutta.
- Suomesta tulee houkutteleva tietoturva-alan sijoituskohde kansainvälisesti.
- Huippuosaamiskeskuksen osaamispääoma parantaa kansallista turvallisuuttamme ja kriittisiin perusrakenteisiin liittyvää tietoturvallisuustoimintakykyämme.
- Osaamispääoma parantaa myös kansalaisten tietoturvatietoisuutta.
- Verkottunut malli tarjoaa sekä liiketoiminnan ketteryyttä että skaalautumiskykyä laajoihin järjestelmätoimituksiin.

- Keskittymä mahdollistaa yhteisiä markkinointi- ja tuotteistusponnistuksia.

Tietoturvaan liittyvä tehokkaasti toteutettu osaamista järjestelmällisesti yhdistävä yhteistyö on kansainvälisesti harvinaista, ja Suomessa on siihen hyvät mahdollisuudet. Suomen asemoituminen globaalisti tietoturvan mallimaana ja houkuttelevana sijoituskohteena tietoturvaosaamisen suhteen on sidoksissa siihen, panostetaanko huippuosaamiskeskittymään riittävästi. Panostamistoimenpiteillä on kiire.

2.2.2 Oulun tietoturvaklusterista Suomen huippuosaamiskeskittymään

Nykyisillä Oulun tietoturvaklusterin toimijoilla on pienessä mittakaavassa huippuosaamiseen tarvittavat perusvalmiudet ja potentiaali, mutta resurssit toiminnan kehittämiseksi globaalisti vahvasti näkyvään suuntaan puuttuvat. Oulun tietoturvaklusterin toimijoista koottava yhteenliittymä on tällä hetkellä potentiaalisin osapuoli toimimaan esiasteena suomalaiselle tietoturvaosaamisen huippuosaamiskeskittymälle. Toimintaa tulee ryhtyä kehittämään kuitenkin valtakunnallisesti. Oulun klusterin toimintaan nykyistä järeämpi panostaminen toimii alkusysäyksenä koko Suomen tietoturvaosaamisklusterin synnyttämiselle, joka on varsinainen tavoite. Paikkakuntakohtaista toimintaa pitää koordinoida, mutta koordinaatio ei saa olla liian raskasta. On myös huomattava, että nykyinen Oulun klusteri ei kata kaikkia tietoturvan sovellusalueita. Esimerkiksi kriittisten perusrakenteiden tietoturvaosaamisen osalta on aiheellista hyödyntää Huoltovarmuuskeskuksen ja CERT-FI:n jo luomaa CIIP-verkostoa. Suomen tietoturvan huippuosaamiskeskittymällä tulee olla tarvittava yhteistyö jo olemassa olevien verkostojen kanssa.

2.2.3 Jatkotoimenpiteet

Konkreettisena jatkotoimenpiteenä tälle mietinnölle esitetään projektisuunnitelman laatimista Suomen tietoturvan huippuosaamiskeskittymän toiminnan järjestelmälliseksi organisoinniksi. Suunnitelman tulee identifioida myös vastuullinen taho, joka voi olla esimerkiksi tutkimusorganisaatioiden (Oulun yliopisto, Aalto-yliopisto, Tampereen teknillinen yliopisto, Lappeenrannan teknillinen yliopisto, Lapin yliopisto ja VTT) yhteenliittymä tai valtionhallinnon yksikkö. Yrityksillä tulee olla keskittymässä merkittävä ohjaava ja osallistuva rooli. Myös tutkimusmaailman, valtionhallinnon ja yritysten yhteenliittymä voi toimia vastuullisena tahona. Työryhmä ei ehdota tässä vaiheessa kuitenkaan mitään tiettyä vastuullista tahoa, vaan tämä keskustelu on käytävä erikseen.

Keskittymän perustaminen edellyttää arviolta 3–5 miljoonan euron kertaluontoisen rahoituksen, joka jakautuu mm. seuraaviin kohteisiin noin kolmen vuoden ajanjaksolla:

- henkilökustannukset
- projektivalmistelukustannukset
- verkottumistilaisuuksiin osallistuminen ja niiden järjestäminen
- tutkijavierailujen kustannukset
- tilakustannukset

Toiminta pitää kuitenkin suunnitella riittävän yksityiskohtaisesti, jolloin tämä arvio voi muuttua. Rahoituksen avulla huippuosaamiskeskittymän toiminnan pitäisi noin kolmen vuoden kuluessa pystyä varmistamaan jatkuvuutensa hankkimalla omaa projektirahoitusta. Suunnitelmaan tulee kuulua myös rahoitussuunnitelma. Keskustelut rahoitusmahdollisuuksista potentiaalisten rahoitustahojen kanssa täytyy aloittaa mahdollisimman pian.

Osaamiskeskittymän hallinnon pitää olla kevyttä ja pääpaino olla harkitulla projektityöskentelyllä. Toimintaa ei saa linjata pelkäksi keskustelufoorumiksi, ja sen jatkuvuuteen tulee kiinnittää erityistä huomiota.

3. Painopiste 2: Suomalainen osallistuminen tietoturvastandardisointiin

3.1 Nykytilanne

3.1.1 Standardien merkitys liiketoiminnalle

Standardit ovat välttämättömiä liiketoiminnalle. Ilman niitä tuotteet, palvelut ja tekniset ratkaisut olisivat yhteen toimimattomia ja vertailukelvottomia ja organisaatioiden olisi hyvin hankalaa pärjätä pitkäjänteisesti kansainvälisillä liiketoiminta-areenoilla. Standardisointitoiminta koostuu standardien laadinnasta ja niiden soveltamisesta. Tietoturvastandardisoinnissa on suomalaisilla kummankin toiminnan suhteen paljon kehittymisen tarvetta ja mahdollisuuksia. Työssä tulisi varmistaa, että suomalaiset innovaatiot tulevat huomioiduiksi standardeissa. Standardien soveltamiseksi standarditietoutta tulisi levittää niin, että hyviksi havaitut ja standardisoidut ratkaisut ja menetelmät olisivat kehittäjille ja päättäjille tuttuja ja niitä osattaisiin vaatia.

Osallistuminen standardisointityöhön on merkittävä ennakointikeino liiketoiminnan jatkuvuudelle ja kehittämiselle. Standardisoinnin peruspyrkimys on tuotannon tai toiminnan osatekijöiden yhteensovittaminen lisäarvon tuottamiseksi: kaikkea ei kannata tehdä itse. Kuitenkin standardisointityössä käsiteltävästä tiedosta vain osa tulee julkiseksi, ja sekin viiveellä. Osallistumisen myötä tietoa saadaan tuotekehitykseen oikea-aikaisesti parantamaan tuotteiden kilpailukykyä. Lisäksi osallistuminen avaa liiketoimintaa tukevia asiantuntijaverkostoja. Kilpailluilla markkinoilla on kyse kilpailukyvyn säilyttämisestä. Tietoturvaan liittyvällä standardisointityöllä on vaikutus edelläkävijyyteen, kilpailuetuun ja kasvun ja menestyksen saavuttamiseen.

Monet tekniset tietoturvastandardit mahdollistavat liiketoimintaa – niitä voidaan kutsua *liiketoiminnan mahdollistajastandardeiksi*. Nykyisellään suomalaiset eivät hyödynnä teknisten mahdollistajastandardien potentiaalia. Standardeilla on myös tärkeä rooli toimijoiden välisen luottamuksen lisääjinä. Toimittamalla standardin vaatimusten mukaisia ratkaisuja yritykset voivat saada kilpailuetua etenkin kansainvälisissä julkishallintojen tarjouskilpailuissa. Etenkään pk-yrityksillä ja tutkimusorganisaatioilla ei ole käytössään riittävästi taloudellisia resursseja liiketoiminnan mahdollistajastandardisointiin. Liiketoimintahyödyn tunnistaminen on usein hankalaa, jos standardisointi ei ole yrityksen ydinosaamista eikä siihen ole resursseja osallistua. Syynä tähän on se, että usein liiketoimintahyödyt syntyvät pitkällä aikavälillä. Mahdollisuuksia osallistua liiketoiminnan mahdollistajastandardisointiin pitää edistää.

3.1.2 Tietoturvaan liittyvä standardisointi

Kuten tietoturvaosaamista yleensä, voidaan tietoturvastandardisointia tarkastella kahdesta fokusalueesta: tekniset tietoturvaratkaisut ja organisaatioiden tietoturvanhallinta. Suomalaisten osallistumisaktiivisuus tietoturvastandardisointiin näissä fokusalueissa eroaa toisistaan: osallistuminen teknisten standardien

kehittämiseen on laajempaa kuin hallinnan standardien. Tietoturvanhallintastandardeissa ovat käsite- ja vastuumäärittelyt hyvin keskeinen asia, kun taas teknisissä tietoturvastandardeissa fokuksessa ovat tekniset tietoturvamekanismit ja erityisesti tietoturvaan liittyvät protokollat, algoritmit tai järjestelmäarkkitehtuurit. Tietoturvallisuuden standardisoinnin koko alue on hyvin laaja, epäyhtenäinen ja hajanainen sekä vaikeasti ymmärrettävä jopa asiantuntijoille saati standardien hyödyntäjille.

Virallisia kansainvälisiä standardeja laativat organisaatiot ovat ISO (International Organization for Standardization) [35], IEC (International Electrotechnical Commission) [36] ja ITU (International Telecommunication Union) [37]. Vastaavanlaisia eurooppalaisia standardisointiorganisaatioita ovat CEN (Comité Européen de Normalisation) [38], ETSI (European Telecommunications Standards Institute) [39] ja CENELEC (Comité Européen de Normalisation Electrotechnique) [40]. Kaikilla näillä standardisointiorganisaatioilla on myös tietoturvallisuuden alan standardisointia.

Tietoturvan kokonaisvaltaisessa standardisoinnissa ISO/IEC on tunnetuin organisaatio. Erityisesti tärkeässä roolissa ovat komitean JTC1/SC 27 ISO/IEC 27000 -sarjan standardit, jotka muodostavat tietoturvaan keskittyvän kokonaisuuden. ISO/IEC 27000-sarja sisältää sekä tietoturvanhallintastandardeja että teknisiä standardeja, kuten salaustekniikkaan ja tietoturvaevaluointiin liittyvät standardit.

Tietoturvanhallinnan kansainväliseen standardisointiin osallistuminen keskittyy Suomessa ISO/IEC 27000-sarjan aktiviteetteihin. Kuitenkin siinäkin toiminnassa ollaan sekä kotimaisella että kansainvälisellä tasolla heikosti mukana. Suomalaiset asiantuntijat ja standardien käyttäjät, organisaatiot, tutkimuslaitokset ja yliopistot, ovat passiivisia, ts. eivät osallistu kokouksiin eivätkä paljoa kommentoikaan esillä olevia tekstejä. Syitä tähän ovat matkakustannukset, ajan puute, saavutettujen hyötyjen epäsuora luonne ja vähäisen kansainvälisen osallistumisen perinne. Kyse on myös siitä, että hallintastandardit ovat varsin yleisiä johdon työkaluja, eivätkä toimi niin suoraan mahdollistajina lisäarvon tuotannolle kuin monet tekniset tietoturvaan liittyvät standardit. Tietoturvanhallinnan standardisointiin osallistuminen Suomessa nojaa suurelta osin asiantuntijoiden omaan harrastuneisuuteen, ja on selvästi vähäisempää, verrattuna esimerkiksi Ruotsiin tai joihinkin muihin kehittyneisiin maihin.

Tietoturvallisuuden hallinnan standardisoinnissa ISO/IEC 27000 -standardit ovat vain yksi osa-alue. Muita merkittäviä osa-alueita ovat esimerkiksi yksityisyydensuojastandardit (ISO/IEC 29100). Toiminta yksityisyydensuoja-alueen standardisoinnissa on Suomessa aktiivisempaa kuin ISO/IEC 27000 -standardisoinnissa. Tähän on osaltaan syynä se, että ko. ala on huomattavasti alikehittynyt tietoturva-alaan verrattuna ja yritykset painivat parhaillaan käytännössä paljon yksityisyydensuojakysymysten parissa kuluttajamarkkinoille suunnatuissa tuotteissa.

Suomen Standardisoimisliitto SFS on organisoinut noin 60 suomalaisesta asiantuntijasta koostuvan kansallisen tason seurantaryhmän ISO/IEC-tietoturvastandardisoinnin seurantaa ja siihen vaikuttamista varten. SFS:llä on käytössään tätä varten vain minimaalisia rahoitusmahdollisuuksia, kuten työ- ja elinkeinoministeriön myöntämät toimialayhteisöavustukset kansainväliseen standardisointityöhön osallistumiseen liittyvien matkojen rahoittamiseksi. Nämä resurssit eivät mahdollista sitä liiketoimintapotentiaalin hyödyntämistä, mitä standardeihin liittyy, ja varsinkin pienet ja keskisuuret suomalaiset yritykset menettävät tilaisuuksia.

Virallisten standardisointiorganisaatioiden lisäksi on monia toimialakohtaista, alueellista tai *de facto* -standardisointia toteuttavia muita organisaatioita. Esimerkiksi tietoliikenteen kansainvälistä tietoturvastandardisointia toteutetaan kansainvälisessä insinöörijärjestössä IEEE (Institute of Electrical and Electronics Engineers) [41], joka on maailman laajin kansainvälinen tekniikan alan ammattilaisten järjestö, ja sillä on noin puoli miljoonaa jäsentä 150 maassa. Suuri määrä standardisointityöstä tehdään erilaisissa teollisuusfoorumeissa, joista työ viedään hyvin valmisteltuna virallisiin standardeihin. Eri toimialoilla, kuten tietoliikenteessä, teollisuusautomaatiossa, pankkialalla ja terveydenhoitoalalla on omaa tietoturvaan liittyvää toimialakohtaista standardisointia. Internet-teknologioihin liittyvää tietoturvaa standardoidaan lukuisissa IETF:n (Internet Engineering Task Force) [42] työryhmissä. Suomessa toimivat suuret yritykset osallistuvat erittäin aktiivisesti tietoliikennealan teknisten tietoturvaratkaisujen standardisointiin ETSIssä, IETF:ssä ja 3GPP:ssä. Tällä osallistumisella yritykset varmistavat liiketoimintaympäristönsä tarkoituksenmukaisuutta ja jatkuvuutta. Mobiiliverkkojen tietoturvastandardisointia toteutetaan mm. 3GPP:ssä (3rd Generation Partnership Project) [43]. Kriittisten perusrakenteiden tietoturvaan liittyviä standardeja on hyväksytty ja on valmisteilla ISAssa (International Society of Automation) [44] ja IEC:ssä: ISAn *Industrial Automation and Control System Security* ISA99 ja IEC:n *Industrial communication networks – Network and system security* IEC 62443. Nämä standardit vaikuttavat jatkossa merkittävästi varsinkin teollisuusautomaatioalan toimijiin. Terveydenhoitoalalla THL on toiminut aktiivisesti ISO TC 215:n ja CEN TC 251 Health informatics -komiteoiden tietoturva- ja tietosuojaryhmissä. Teollisuusautomaatioalalla on pitkä historia turvallisuuden (*safety*) standardisoinnissa, ja pyrkimyksenä on integroida tietoturva-asioita yleisiin turvallisuusstandardeihin. Kriittisten perusrakenteiden tietoturvan standardisointiin pitäisi Suomessa myös panostaa nykyistä enemmän.

Monet suuret suomalaiset yritykset pitävät ISF:ssä tehtävää tietoturvan ohjeistustyötä hyödyllisenä ja käyttävät ohjeistuksia oman toimintansa suunnittelussa. On näköpiirissä, että osa ISF:n tuloksista tulee lähitulevaisuudessa avoimesti saataviksi. Tämä saattaa aukaista uusia standardisointiaktiviteetteja virallisissa standardisointijärjestöissä.

On tärkeää osallistua virallisen standardisointityön lisäksi työryhmiin, jotka valmistelevat esityksiä virallisiksi standardeiksi.

3.2 Kehittämissuunnitelma: Standardisointityöhön tarvitaan lisää tukirahoitusta

3.2.1 Aktiivisen kansainvälisen osallistumisen malli

Työryhmä esittää tavoitteeksi aktiivisen kansainvälisen osallistumisen mallin rakentamisen tietoturvallisuuden standardisointiin. Tietoturvastandardisointiin osallistumisen mahdollistamiseksi ja edistämiseksi esitetään tietoturvallisuuden standardisointiin suuruusluokaltaan noin 160 000 € vuosittaista tukirahoitusta, jolla voitaisiin rahoittaa suomalaisten asiantuntijoiden osallistumista kansainvälisiin kokouksiin.

SFS:n IT-standardisoinnin yksikkö on tunnistanut myöntämiensä suorien kokousmatkojen rahoituksien tehokkaimpana välineenä osallistumisen edistämiseen. Standardisointityössä tarvitaan laajamittaista asiantuntijoiden vapaaehtoistoimintaa ja standardisointityön kokousmatkarahoitus toimii mahdollistajana tälle työlle. On huomattava, että tässä ehdotettu rahoitus ei kata standardisointityötä kuin kokousmatkojen osalta. Työ edellyttää lisäksi suuren määrän vapaaehtoistyötä kokouksiin osallistuvilta asiantuntijoilta. Kokousmatkarahoitus mahdollistaa laajan vapaaehtoistyön hyödyntämisen tietoturvastandardisoinnissa. Aktiivisen kansainvälisen osallistumisen mallissa on kuitenkin myös tärkeää, että standardisointiin osallistuvien asiantuntijoiden omissa organisaatioissa on toimintaan motivoivia tekijöitä, kuten liiketoimintahyödyn syntymisen potentiaali.

Arvio 160 000 €:n vuosirahoituksen suuruudesta perustuu seuraavaan laskelmaan:

- rahoitus Eurooppaan suuntautuvaa matkaa varten 40 asiantuntijalle maksaa noin 1500 euroa / asiantuntija
- rahoitus muualle kuin Eurooppaan suuntautuvaa matkaa varten 40 asiantuntijalle maksaa noin 2500 euroa / asiantuntija.

3.2.2 Jatkotoimenpiteet

Ensimmäisenä jatkotoimenpiteenä tälle mietinnölle esitetään laadittavaksi suunnitelma edellä esitetystä tukirahoituksesta.

Toisena jatkotoimenpiteenä esitetään selvitettäväksi kansainvälisen standardisoinnin kenttä tietoturvallisuuden alueelta ja päätetään niistä alueista, joihin on Suomen kannalta tarkoituksenmukaisinta aktiivisesti osallistua. Tässä työssä kartoitetaan myös toimintaan käytettävissä olevat resurssit. Kansainvälisessä standardisoinnissa ei riitä, että vain kommentoidaan tai vain osallistutaan satunnaisesti kokouksiin, vaan työssä edellytetään pitkäjänteistä ja johdonmukaista osallistumista. Ehdotetaan erityiseksi toimenpiteeksi selvittää, miten tietoturvallisuuden tekniset ratkaisut ja organisaatioiden tietoturvallisuuden hallintaratkaisut saataisiin nivoutumaan paremmin toisiinsa ja tukemaan toinen toisiaan luonnollisella ja tehokkaalla tavalla standardisointia apuna käyttäen.

4. Muut toimenpiteet

Seuraavassa esitetään muita strategisia ja tärkeitä toimenpiteitä tietoturvallisuuden parantamiseksi Suomessa, jotka ovat välillisesti yhteydessä hankkeen tavoitteisiin.

4.1 Tietoturvakoulutus

Asiantuntijatason tietoturvaosaamisen lisäksi yhteiskunnan tietoturvallisuuteen liittyy kansalaisten tietoturvatietoisuus, jonka kehittämisen lähtökohtana ovat yhteiskunnan toiminnot ja toimijat. Yhteiskunnallinen tietoturvallisuustarkastelu riippuu oleellisesti yleisestä tietoyhteiskuntakehityksestä. Koulutukseen pitäisi panostaa nykyistä huomattavasti enemmän: tietoyhteiskuntavalmiuksien ja tietoturvatietoisuuden oppiminen alkaa peruskoulusta, ellei jo aiemmin.

Tietoturvan perus- ja asiantuntijatason koulutus on laajuudeltaan riittämätöntä Suomessa. Riittävä tietoturvakoulutus toimii sekä ammatillisen tietoturva-asiantuntijuuden lähtökohtana että kuluttajan tietoturvatietoisuuden mahdollistavana tekijänä. Tietoturvan ammattilaisten koulutustasossa on merkittäviä puutteita kansallisella tasolla. Yliopistojen ja korkeakoulujen koulutusohjelmissa ei ole riittävässä laajuudessa huomioitu tietoturvallisuutta. Monissa yliopistoissa ja korkeakouluissa tällä hetkellä suuri osa tietoturvaa opiskelevista on ulkomaalaisia vaihto-opiskelijoita. Tämä toisaalta edistää tietoturvan vientiä ulkomaille, mutta toisaalta herättää kysymyksen, miten suomalaisia opiskelijoita voisi houkutella enemmän alalle. Ongelma ei ole pelkästään kansallinen: esimerkiksi Iso-Britanniassa vain alle 20 % kandidaattivaiheen opiskelijoista on saanut opetusta tietoturvallisuudesta [45]. Eroavaisuudet tietoturvan opetusohjelmien sisällön ja laajuuden välillä ovat suuria ja joissain yliopistoissa ja korkeakouluissa tietoturvallisuuden perustutkinto-opetus puuttuu kokonaan tai lähes kokonaan. Perus- ja asiantuntijakoulutuksen lisäksi haasteena on kouluttaa myös julkisten organisaatioiden ja yritysten henkilöstö riittävän tietoturvatietoiseksi. Eri toimialoilla toimivan henkilöstön tehokas ja motivoiva tietoturvakoulutus edellyttää uusia toimintamalleja.

Koulutuksella saadaan aikaan merkittäviä tuloksia tietoturvallisuuden parantamisessa. Monien tutkimusten mukaan yksilöiden tietoturvakäyttäytymistä on mahdollisuus parantaa tietoturvatietoisuuden lisääntyessä.

Konkreettisena toimenpiteenä esitetään tehtäväksi selvitys erillisessä asiantuntijaryhmässä tietoturvallisuuden kouluttamisesta ja koulutusohjelmista sekä niiden sisällöistä ja osallistujista yliopistoissa, ammattikorkeakouluissa ja muissa oppilaitoksissa. Koulutusselvityksen pohjalta esitetään luotavaksi toimivat yhteydet koulutuksen ja tietoturvaosaamisen tarpeiden välille.

4.2 Avoin verkostoyhteistyö

Suoran innovaatiopanostuksen lisäksi kansainvälisen yhteistyön ja vaikuttamisen välttämättömänä edellytyksenä on luova, aktiivinen ja monipuolinen suomalainen verkostoyhteistyö alueella. Verkostojen tulisi olla erityisesti laaja-alaisia,

monipuolisia ja avoimia kommunikointiverkostoja eikä yksinomaan viranomaisjohdettuja. Verkostoja syntyy erityisesti kansainvälisissä tutkimus- ja kehitysprojekteissa sekä yhteistyöfoorumeille osallistumisen myötä.

Verkostoyhteistyöhön liittyy myös tarve uuden, avoimen, tietoturvaan liittyvän yhteistyö- ja keskustelukulttuurin edistämisestä. Verkostoissa eri vaikuttajien määrää ei pidä supistaa eikä toiminnan päällekkäisyydestä ole haittaa, koska laaja verkoston ulottuvuus auttaa hyviä ideoita leviämään ja jalostumaan tehokkaimmin. Oleellista on vuorovaikutteinen kommunikaatio ja sen tukeminen esimerkiksi avoimilla interaktiivisilla sosiaalisen median ratkaisuilla. Tällä hetkellä avoin keskustelu tietoturvallisuuden kysymyksissä Suomessa on vähäistä. Yksi syy siihen, että merkittävää kommunikaatiota ei ole aiheessamme saatu aikaan, on ihmisten kiire ja osaamisen pirstoutuneisuus. Ei ole myöskään olemassa verkostoitumista edistäviä suomalaisia keskustelufoorumeja aiheesta. Keskustelufoorumeihin pitäisi saada mukaan yritysten ja julkisten organisaatioiden edustajia, asiantuntijoita, tutkijoita ja kouluttajia sekä myös tavallisia tiedon hyödyntäjiä ja tietotekniikan käyttäjiä. Konkreettisena toimenpiteenä esitetään avoimen sosiaalisen median teknologiaa hyödyntävän tietoturvan asiantuntijoiden ja soveltajien verkostoitumiseen kannustavan keskustelualustan luomista.

Suomessa nykyisessä tietoturvaan liittyvässä mediakeskustelussa on ongelmana reaktiivisen tietoturvallisuuden ylikorostuminen. Medianäkyvyys on valtavoittoisesti sattuneiden tietoturvaloukkausten läpikäyntiä, eikä tietoturvauhkiin etukäteen varautuminen ole riittävästi esillä.

4.3 Tietovarastoinnin potentiaali

Kansainvälinen tietovarastointi saattaa olla Suomelle myös varteenotettava mahdollisuus. Suomalainen laadukas tietosuoja ja mahdollistaa turvallisen ja laajamittaisen tietovarastoinnin ja siihen liittyvän palvelutoiminnan maassamme. Suomalainen yhteiskunta on toimiva länsimainen demokratia, jossa toimintatavat ovat varsin läpinäkyviä. Tällainen toiminta luo myös erinomaisen pohjan tietosuojaan liittyvän lainsäädännön edelleen vahvistamiseksi ja sen ylläpitämiseksi kansainvälisellä huipputasolla. Tietosuojaosaamisemme on kansallisen tietoturvallisuuden strateginen näkökulma, joka täytyy ottaa myös huomioon jatkopohdinnoissa. Eräissä maissa on viranomaisilla ja yksityisilläkin tahoilla valtuuksia urkkia maassa säilytettävää tietoa. Meidän lakimme ja käytäntömme ovat tässä suhteessa korkealla eettisellä tasolla ja suomalaiset koetaan laajalti luotettavina yhteistyökumppaneina. Voimme oikeutetusti olla ylpeitä yhteiskuntamme toimintaperiaatteista.

Viitteet

[1] Teknologiateollisuuden innovaatiopolitiikan työryhmän raportti. Teknologiateollisuus, 13.12.2010.

[2] Gartner, Inc., 3/2009.

[3] Frost & Sullivan. The 2011 $(ISC)^2$ Global Information Security Workforce Study, 2011.

[4] A. Gurtov. Host Identity Protocol (HIP): Towards the Secure Mobile Internet. Wiley and Sons, 2008.

[5] Cloud Software -TiViT SHOK –projekti. http://cloudsoftwareprogram.org/

[6] Oulu IT Security Cluster. http://security.ouluclusters.com/

[7] Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI, Valtiovarainministeriö. http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

[8] Kansallisen tietoturvastrategian toimenpideohjelma, Liikenne- ja viestintäministeriö. http://www.lvm.fi/web/fi/ministerio/strategiat/strategia/view/1127143

[9] CSC – Tieteen tietekniikan keskus. http://www.csc.fi/index.html

[10] Funet CERT. http://www.cert.funet.fi

[11] Tietoturva ry. http://www.ttlry.fi/yhdistykset/tietoturva/

[12] ISACA Finland. http://www.isaca.fi/

[13] FinnSecurity ry. http://www.finnsecurity.fi

[14] OWASP (Open Web Application Security Project) Helsinki Local Chapter. http://www.owasp.org/index.php/Helsinki

[15] International Information Systems Security Certification Consortium (ISC)2. https://www.isc2.org/

[16] SANS Institute. http://www.sans.org

[17] Yhdysvaltain NIST (National Institute of Standards and Technology). http://www.nist.gov/index.html

[18] Yhdysvaltain Department of Homeland Security. http://www.dhs.gov/index.shtm

[19] Build Security In. https://buildsecurityin.us-cert.gov/bsi/home.html

[20] ENISA (European Network and Information Security Agency). http://www.enisa.europa.eu/

[21] ISF (Information Security Forum). https://www.securityforum.org/

[22] SAFECode (Software Assurance Forum for Excellence in Code). http://www.safecode.org

[23] IAEA (International Atomic Energy Agency). http://www.iaea.org/

[24] ICASI (Industry Consortium for Advancement of Security on the Internet). http://www.icasi.org/

[25] FIRST (Forum of Incident Response and Security Teams). http://www.first.org/

[26] EU:n Komission 7. puiteohjelma (EU Commission Seventh Framework Programme). http://cordis.europa.eu/fp7/home_en.html

[27] NESSI (Networked European Software & Services Initiative). http://www.nessi-europe.com

[28] Net!Works (European Technology Platform for Communications Networks and Services). http://www.networks-etp.eu

[29] DigitalEurope. http://www.digitaleurope.org/

[30] Iso-Britannian CPNI (Centre for the Protection of National Infrastructure). http://www.cpni.gov.uk/

[31] ITEA2 (Information Technology for European Advancement) Eureka Cluster. http://www.itea2.org

[32] CELTIC Eureka Cluster. http://www.celtic-initiative.org
[33] WPISP (Working Party on Information Security and Privacy). http://www.oecd.org/dataoecd/20/2/36871394.pdf
[34] CERT-FI http://www.cert.fi
[35] ISO (International Organization for Standardization). http://www.iso.org/iso/home.html
[36] IEC (International Electrotechnical Commission). http://www.iec.ch/index.htm
[37] ITU (International Telecommunication Union). http://www.itu.int/en/pages/default.aspx
[38] CEN (Comité Européen de Normalisation). http://www.cen.eu/cen/pages/default.aspx
[39] ETSI (European Telecommunications Standards Institute). http://www.etsi.org/WebSite/homepage.aspx
[40] CENELEC (Comité Européen de Normalisation Electrotechnique). http://www.cenelec.eu/Cenelec/Homepage.htm
[41] IEEE (Institute of Electrical and Electronics Engineers). http://standards.ieee.org
[42] IETF (Internet Engineering Task Force). http://www.ietf.org
[43] 3GPP (3rd Generation Partnership Project). http://www.3gpp.org
[44] The International Society of Automation. http://www.isa.org
[45] UK Universities Neglect I Security Teaching: Survey. Computer Fraud & Security, Vol. 2008, Issue 6, s. 2-3.