LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 93/2005
Viestintä

Tietoturvalliseen tietoyhteiskuntaan

Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 13.12.2005

Liikenne- ja viestintäministeriö
Helsinki, 2006

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä
13.12.2005

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Kansallisen tietoturvallisuusasioiden	Raportti
neuvottelukunnan sihteeristö,	Toimeksiantaja Kansallisen tietoturvallisuusasioiden nvk
pj. Tuire Saaripuu	Toimielimen asettamispäivämäärä 17.10.2003

Julkaisun nimi

Tietoturvalliseen tietoyhteiskuntaan. Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 13.12.2005

Tiivistelmä

Kansallinen tietoturvallisuusasioiden neuvottelukunta on luovuttanut liikenne- ja viestintäministerille toisen toimintavuotensa kertomuksen. Kansallinen tietoturvastrategia ja sen nojalla perustettu kansallisen tietoturvallisuusasioiden neuvottelukunta on tuottanut hyviä tuloksia, esimerkiksi roskapostin määrä välitetystä liikenteestä on pudonnut 80 prosentista kolmannekseen.

Tulevana vuonna 2006 Suomen EU-puheenjohtajuuskauden keskeinen teema on tietoturvallisuus. Suomella on mahdollisuus nostaa tietoturvaosaamisensa Euroopan ja muun maailman tietoisuuteen.

Tietoturvapolitiikalla on keskeinen merkitys tietoyhteiskunnan kehittämisessä. Liikenne- ja viestintäministeri Susanna Huovisen esille nostama vaatimus uuden arjen tietoyhteiskunnan strategiasta, ubiikkiajattelu tuo tekniikan antamat mahdollisuudet jokapäiväisen elämän osaksi. Esimerkiksi liikenneturvallisuus, logistiikka, kauppa, terveydenhuolto ja teollisuus ovat aloja, joissa verkottuminen takaa hyvän palvelutason ja tehostaa tuottavuutta. Neuvottelukunnan vuoden 2005 kertomuksessa kuvataan jo tehty työ ja hahmotellaan ensi vuoden painopisteet. Vuoden 2005 kertomuksessa painopisteet ovat supistuneet aiemmasta neljästä kolmeen, koska osa hankkeista on saatu valmiiksi. On myös ollut tarkoituksenmukaista organisoida työmuotoja uudelleen toisiaan tukeviksi. Työskentelyn painopisteet ovat Tietoturvalliset sähköiset palvelut, Kansallinen tietoturvatilannekuva sekä Tietoturvatietoisuus.

Tietoturvatietoisuus on lisääntynyt vuonna 2005. Tänäkin vuonna järjestetty Tietoturvapäivä sekä hyvin alkuun lähtenyt LUOTI-hanke ovat esimerkkejä onnistuneista hankkeista vuonna 2005. Uusina tietoturvallisuusongelmina ovat nousseet phishing eli väärän identiteetin käyttäminen tietoverkkopalveluissa. Samoin uusiin niin sanottuihin älypuhelimiin liittyvät haittaohjelmat ovat nousseet esiin tänä vuonna. CERT-Fi on onnistunut toiminnassaan erinomaisesti ja reagoi välittömästi tieto-turvallisuuden kannalta kriittisiin tapahtumiin.

Avainsanat (asiasanat)

Tietoturvallisuus, turvallinen verkkoasiointi, kansallinen tietoturvallisuusstrategia

Muut tiedot

Yhteyshenkilö/LVM: Tuire Saaripuu

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 93/2005	1457-7488 (painotuote) 1795-4045 (verkkojulkaisu)	952-201-484-2 (painotuote) 952-201-485-0 (verkkojulkaisu)

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
82	suomi	15 €	julkinen

Jakaja	Kustantaja
Edita Publishing Oy	Liikenne- ja viestintäministeriö

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum
13.12.2005

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Sekretariatet för den nationella delegationen	Rapport
för informationssäkerhet	Uppdragsgivare Delegationen för informationssäkerhet
ordf. Tuire Saaripuu	Datum för tillsättandet av organet 17.10.2003

Publikation

Mot ett säkert informationssamhälle. Rapport till statsrådet av den nationella delegationen för informationssäkerhet avgiven den 13 december 2005.

Referat

Den nationella delegationen för informationssäkerhet har överlämnat en rapport om sitt andra verksamhetsår till kommunikationsministern. Den nationella informationssäkerhetsstrategin och den nationella delegationen för informationssäkerhet som grundats med stöd av strategin har nått goda resultat, t.ex. mängden skräppost av all förmedlad e-postkommunikation har sjunkit från 80 procent till en tredjedel.

Under Finlands EU-ordförandeskap 2006 är informationssäkerhet ett centralt tema. Finland har nu en chans att fokusera Europas och den övriga världens uppmärksamhet på sitt kunnande inom informationssäkerhet.

Informationssäkerhetspolitiken är av central betydelse för samhällsutvecklingen. Den tanke som kommunikationsminister Susanna Huovinen har fört fram om en strategi för den nya vardagen i informationssamhället och allestädes närvarande datorer (*ubiquitous computing*) gör tekniska tillämpningar till en del av vår vardag. Trafiksäkerhet, logistik, handel, hälsovård och industri är exempel på branscher där nätverk borgar för en god servicenivå och ökad produktivitet.

I delegationens rapport beskrivs det arbete som gjorts under 2005 och skisseras riktlinjerna för 2006. I rapporten har antalet prioritetsområden sjunkit från fyra till tre, eftersom en del projekt redan har slutförts. Dessutom har det varit ändamålsenligt att omorganisera vissa arbetsformer som stöder varandra. De tre prioritetsområdena är säkra elektroniska tjänster, den nationella lägesbilden av informationssäkerhet samt medvetenhet om informationssäkerhet.

Medvetenheten om informationssäkerhet har ökat under 2005. Informationssäkerhetsdagen som arrangerades också i år och det nystartade LUOTI-projektet är exempel på framgångsrika projekt under det gångna året. Dessvärre har nya informationssäkerhetsproblem såsom phishing, dvs. identitetsstöld i nättjänster, dykt upp. Också skadliga program som angriper s.k. smarta mobiltelefoner har blivit vanligare. Lyckligtvis har CERT-FI (Computer Emergency Response Team) vid Kommunikationsverket arbetat föredömligt och omedelbart reagerat på alla kritiska säkerhetsincidenter.

Nyckelord

informationssäkerhet, säkra e-tjänster, den nationella informationssäkerhetsstrategin

Övriga uppgifter

Kontaktperson vid kommunikationsministeriet är Tuire Saaripuu.

Seriens namn och nummer	ISSN	ISBN
Kommunikationsministeriets publikationer 93/2005	1457-7488 (trycksak) 1795-4045 (nätpublikation)	952-201-484-2 (trycksak) 952-201-485-0 (nätpublikation)

Sidoantal	Språk	Pris	Sekretessgrad
82	finska	15 €	offentlig

Distribution	Förlag
Edita Publishing Ab	Kommunikationsministeriet

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication
13 December 2005

Authors (from body; name, chairman and secretary of the body)	Type of publication
Secretariat of the National Information Security	Report
Advisory Board;	Assigned by National Information Security Advisory Board
chair: Tuire Saaripuu	Date when body appointed 17 October 2003

Name of the publication

Creating a safer information society. National Information Security Advisory Board report submitted to the Government on 13 December 2005

Abstract

The National Information Security Advisory Board has submitted to the Government a report on its second term. The National Information Security Strategy and the Advisory Board established by its virtue have produced good results; for example spam email has reduced from 80 per cent to one third of transmitted messages.

A focal theme in Finland's EU Presidency in 2006 will be information security. Finland will have an opportunity to raise awareness in Europe and in the rest of the world of its information security competence.

In the development of the information society information security policy plays an important role. Ms Susanna Huovinen, Minister of Transport and Communications of Finland, has called for a strategy on the theme of information society in everyday life, ubiquitous thinking, that integrates the technological opportunities into our daily lives. For example traffic safety, logistics, trade and commerce, health care and industry are sectors in which networking ensures a high level of service and increases productivity.

The Advisory Board report of 2005 describes the work that has been done and gives guidelines for the coming year. The number of priority projects has been reduced from four to three, because some of the projects have already been completed. The three priorities will be Information-secure electronic services, Analysis of national information security, and Information security awareness. Furthermore, working methods have been reorganised so that they reasonably support one another.

Information security awareness increased in 2005. The National Information Security Day and the good start of the LUOTI project are examples of successful projects in 2005. A new information security problem is phishing, i.e. using a wrong identity in information network services. The year also marked the emergence of malicious software related to the new, so-called smart phones. CERT-FI was very successful in reacting immediately to critical information security incidents.

Keywords

Information security, safe on-line service, national information security strategy

Miscellaneous

Contact person at the Ministry: Tuire Saaripuu

Serial name and number	ISSN	ISBN
Publications of the Ministry of Transport and Communications 93/2005	1457-7488 (printed version) 1795-4045 (electronic version)	952-201-484-2 (printed version) 952-201-485-0 (electronic version)

Pages, total	Language	Price	Confidence status
82	Finnish	€15	Public

Distributed by	Published by
Edita Publishing Ltd	Ministry of Transport and Communications

SISÄLLYSLUETTELO

Liikenne- ja viestintäministeri Susanna Huovinen neuvottelukunnan kertomuksen luovutustilaisuudessa 13.12.2005

Vuonna 2004 kansallisen tietoturvallisuusasioiden neuvottelukunnan ensimmäisen vuosikertomuksen luovutustilaisuudessa liikenne- ja viestintäministeri Leena Luhtanen korosti suomalaisen tietoyhteiskunnan turvallisuutta ja kilpailukykyä, jota ei voi saavuttaa ilman kansalaisten ja yrityselämän luottamusta sähköisten asiointikanavien ja palveluiden turvallisuuteen. Tietoturvallisuuteen liittyvät uhat ovat uhkaamassa koko tietoyhteiskunnan perustaa.

Kansainvälistäkin huomiota saaneen kansallisen tietoturvallisuusstrategian nojalla perustettu kansallisen tietoturvallisuusasioiden neuvottelukunnan toinen toimintavuosi käynnistyi ensimmäisen toimintavuoden aikana saavutettujen ansiokkaiden selvitysten ja tulosten pohjalta. Kansallisen tietoturvallisuusasioiden neuvottelukunnan työn taustalla on yhteiskunnan kaikkien toimijoiden, hallinnon, palveluiden käyttäjien ja elinkeinoelämän edustajien yhteinen näkemys siitä, että tietoturvalliset palvelut ovat uuden arjen yhteiskunnan keskeinen kaikkeen toimintaan vaikuttava perusvaatimus.

Vuonna 2005 neuvottelukunta on jatkanut aloittamaansa työtä ansiokkaasti, painopisteitä uusien haasteiden myötä tarkistaen. Erityisesti tämän vuoden loppupuolella esiintyneet identiteettiin kohdistuvat hyökkäykset phishingin muodossa ovat asettaneet palveluntarjoajille uusia haasteita. Erinomainen esimerkki tietoturvallisuusstrategian merkityksestä Suomessa on ollut roskapostin määrän putoaminen 80 prosentista noin kolmannekseen välitetystä liikenteestä strategian käynnistämisestä lähtien syksyllä 2003. Palveluiden turvallisen käytön takaaminen yhdistettynä helppokäyttöisyyteen ovat avaintekijät sähköisten viestintäpalveluiden lisääntymiseen. Jotta sähköisten viestintävälineiden kehittäminen ja käyttäminen voisivat jatkua ja lisääntyä entisestään, haasteet on voitava ratkaista luotettavalla tavalla. Jos tämä luottamus rikollisten ja haitallisten toimijoiden vuoksi menetetään, menetetään paljon.

Kansainvälistyminen vaikuttaa myös tietoturvahankkeisiin entistä enemmän, esimerkiksi Euroopan verkko- ja tietoturvaviraston aloitettua toimintansa elokuussa odotukset ovat innokkaat. Virastolta odotetaan paljon tukea eurooppalaisen tietoturvatietoisuuden nostamiseksi. Virasto joutuu lunastamaan lupauksensa ja tarjoamaan jäsenvaltioille ja yksittäisille kuluttajille parhaita käytäntöjä tietoturvallisuuden eri osa-alueilla. Toimialat tietoturvariskien hallinta, tietoturvatietoisuuden jakaminen erityyppisille käyttäjäryhmille ja CERT-toiminta koskettavat kaikkia toimijoita. Viraston onkin löydettävä se tapa, joka palvelee alan toimijoita parhaiten jokapäiväisessä elämässä ja liiketoiminnassa.

Uusi arjen yhteiskunta ja sen taustalla vaikuttava ubiikkiajattelu ei ole vain tulevaisuutta, vaan jo tätä päivää verkottuvassa maailmassa. On välttämätöntä, että eurooppalainen kehitys ja kilpailukyky pystyvät haastamaan muut maailman kehittyneet tietoyhteiskunnat. Suomi toteuttaa laajamittaisesti Euroopan komission i2010-ohjelmaa, mutta markkinatilanteen murroskautena emme voi jäädä vain seuraamaan tätä päivää. Meidän on pystyttävä näkemään entistä pitemmälle tulevaisuuteen turvataksemme asemamme tietoyhteiskunnan kärkimaana ja voidaksemme taata kansalaisillemme tehokkaat, laadukkaat ja luotettavat palvelut.

Vuonna 2006 Euroopan unionin Suomen puheenjohtajuuskaudella liikenne- ja viestintäministeriön keskeinen teema on tuoda esiin arjen yhteiskunnan sovellusalueita. Tietoturvallisuuden merkitys kasvaa entisestään, kun eri alustavaihtoehtojen tuoma verkottuminen tuo uusia mahdollisuuksia

älykkäiden ja helppokäyttöisten palveluiden rakentamiselle. Uudet palvelumuodot eivät voi kehittyä, elleivät tietoturvalliset ratkaisut ole arkipäivää. Tämän vuoksi on saavutettava yhteisesti hyväksyttäviä ratkaisuja standardien ja regulaation keinoin, kuitenkaan luomatta jäykkää sääntelykoneistoa. On jaettava tietoturvallisuustietoisuutta ja -osaamista, jolloin eri toimijoiden sekä palveluiden käyttäjien välinen yhteistoiminta helpottuu.

Puheenjohtajuuskaudellaan Suomi järjestää yhdessä Euroopan komission ja Euroopan verkko- ja tietoturvaviraston kanssa kutsuvieraskonferenssin ”i2010 – Towards a Ubiquitous European Information Society”, joka on tarkoitettu alan johtaville asiantuntijoille ja päättäjille. Kunnianhimoisena tavoitteena on saada konferenssille myös kansainvälistä huomiota sekä kuulla maailman johtavien toimijoiden puheenvuoroja. Konferenssin painopiste on suunnattu erityisesti tietoyhteiskunnan sovelluksiin ja ratkaisuihin painottaen arjen yhteiskunnan asettamia haasteita. Kohteena on eurooppalainen i2010-ohjelma sovellusalueineen siten, että tietoyhteiskunnan kehityksen myötä tarkastellaan liiketoiminnan kehittymistä vuosina 1996 – 2006 – 2016 ja sitä, mitä vaikutuksia nopealla teknologian kehittymisellä on koko alan liiketoimintaan.

Haluan tuoda valtioneuvoston tervehdyksen kansallisen tietoturvallisuusasioiden neuvottelukunnalle sekä sen vastuusihteeristölle sen erinomaiseen työhön liittyen. Neuvottelukunnan työ on tullut puolitiehen hankkeena ja edelleen voin nähdä, että paitsi jo saavutetusta erinomaisesta materiaalista ja hyvistä tuloksista olette kehittämässä työssänne uusia toimintatapoja. Työnne on todellinen menestystarina siitä, mitä yhteiskunnan eri tahot, sekä julkinen sektori että kehittyvät teollisuudenalat voivat yhdessä tehdä demokratian kehittymisen, perusoikeuksien toteutumisen, helppokäyttöisten palveluiden tuottamisen sekä kansallisen kilpailukyvyn saavuttamiseksi. Olette työskennelleet yhdessä uusien ajatusten äärellä, mutta kuitenkin jalat tukevasti maan pinnalla hallinnon vaatimusten ja liike-elämän lainalaisuuksien todellisuudessa. Samalla haastatte olemassa olevat näkemykset tietoturvallisuuden peruskysymyksistä. Olette tuoneet arvokkaan kokemuksenne yhteiseen pöytään ja todella edistäneet yhteistyötä eri toimijoiden välillä. Kiitos teille kaikille siitä!

Suomalainen tietoyhteiskunta on maailman kärkeä. On yhteinen poliittinen tahto, että meillä on kansallinen tietoturvastrategia. Se on neuvottelukunnan jokaisen toimijan vahvuus ja työkalu. Sähköiset palvelut eivät kehity, ellemme ole kaikki luomassa yhteisiä pelisääntöjä niiden rakentamiseen. Ilman luottamusta ei ole olemassa sähköisiin viestintäpalveluihin liittyvää liiketoimintaa eikä kansalaisen arkea helpottavia asiointipalveluita.

Arvoisa kansallisen tietoturvallisuusasioiden neuvottelukunta sekä vastuusihteeristö työryhmineen, toivon näiden kiitoksen sanojen myötä teille ja läheisillenne oikein hyvää ja rauhallista joulunaikaa sekä onnellista ja menestyksellistä vuotta 2006.

Helsingissä joulukuun 13. päivänä 2005

Susanna Huovinen
Liikenne- ja viestintäministeri

Neuvottelukunnan näkemys tavoitteiden toteutumisesta ja ehdotukset valtioneuvostolle

Kansallisen tietoturvallisuusasioiden neuvottelukunnan työ on vakiintunut ja kansallinen tietoturvastrategia on tuottanut hyviä tuloksia. Esimerkiksi roskapostin määrä välitetystä liikenteestä on pudonnut 80 prosentista kolmannekseen. Tulevana vuonna Suomen EU-puheenjohtajuuskauden keskeinen teema on tietoturvallisuus. Suomella on mahdollisuus nostaa tietoturvaosaamisensa Euroopan ja muun maailman tietoisuuteen.

Suomalainen tietoyhteiskunta puolustaa paikkaansa maailman huippuyhteiskuntien joukossa. Tietoturvapolitiikalla on siinä keskeinen merkitys. Suomessa laadittu maailman ensimmäinen tietoturvakatsaus sekä Euroopan ensimmäinen koko yhteiskunnan tietoturvastrategia on huomioitu kaikkialla. Tietoyhteiskuntastrategiamme on palkittu kansainvälisen tietoturvallisuusalan RSA-konferenssissa parhaana eurooppalaisena turvallisuustoiminnan periaatteena. Suomen aloitteesta myös Euroopan komissio suunnittelee eurooppalaista tietoturvastrategiaa.

Liikenne- ja viestintäministeri Susanna Huovisen esille nostama vaatimus uuden arjen tietoyhteiskunnan strategiasta ja ubiikkiajattelu yleisestikin sopii erinomaisesti kansallisen tietoturvallisuusasioiden neuvottelukunnan ohjenuoraksi. Suomen on syytä ottaa oppia muiden kokemuksista, erityisesti Japanista ja Koreasta, voidakseen säilyttää asemansa maailman tietoyhteiskuntien kärkijoukossa. Neuvottelukunnan työn tarkoituksena on löytää keinot, joilla eri viestintäratkaisuja voidaan hyödyntää mahdollisimman saumattomasti, monipuolisesti ja turvallisesti. Tämä on juuri sitä työtä, jota neuvottelukunta on tehnyt perustamisestaan lähtien.

Uusi arjen yhteiskunta tuo tekniikan antamat mahdollisuudet jokapäiväisen elämän osaksi. Esimerkiksi liikenneturvallisuus, logistiikka, kauppa, terveydenhuolto ja teollisuus ovat aloja, joissa verkottuminen takaa hyvän palvelutason ja tehostaa tuottavuutta. Toteutuessaan ihmisten luottamuksen arvoisena arjen yhteiskunta edistää demokratiaa, tasa-arvoa ja kansalaisten elämän laatua.

Neuvottelukunta tuntee vastuunsa tietoturvallisuusalan suunnannäyttäjänä. Siksi se hakee uusia toimintamuotoja löytääkseen tietoturvallisuusalan vielä kartoittamattomat ongelmakohdat. Tavoitteena on entisestään terävöittää työtä valtioneuvoston asettamien tavoitteiden täyttämiseksi. Neuvottelukunnan työtapoja ja painopisteitä uudistetaan. Havaituista tietoturvauhkista tiedotetaan selkeästi niin, että viesti rohkaisee käyttämään tarjolla olevia välineitä ja palveluita turvallisesti.

Neuvottelukunnan kertomuksessa kuvataan jo tehty työ ja hahmotellaan ensi vuoden painopistealueet. Vuoden 2005 kertomuksessa painopistealueet ovat supistuneet aiemmasta neljästä kolmeen, koska osa hankkeista on saatu valmiiksi. On myös ollut tarkoituksenmukaista organisoida työmuotoja uudelleen toisiaan tukeviksi.

Neuvottelukunnan vuoden 2006 työssä otetaan huomioon tähän saakka tehty työ ja siitä opitut muutostarpeet. Työskentelyn painopisteet ovat Tietoturvalliset sähköiset palvelut, Kansallinen tietoturvatilannekuva sekä Tietoturvatietoisuus. Vuoden 2006 aikana järjestetään neuvottelukunnan työn terävöittämiseksi ryhmätyömuotoinen harjoitus, jossa pureudutaan vielä selvittämättömiin tietoliikenteen, prosessien ja organisaatiostrategian aukkopaikkoihin tietoturvallisuuden alan tutkimuskohteiden löytämiseksi. Lisäksi seurataan uusia hankkeita esimerkiksi Helsingin Kauppakamarin, Keskuskauppakamarin sekä sisäasiainministeriön yhteishanketta yritysten tietoturvallisuuden paranta-

miseksi, jotta saadaan kokonaiskuva eri toimijoiden yhteistyön tuloksista. Neuvottelukunnan rooli on näkyvä myös sen osahankkeiden, kuten Tietoturvapäivän ja PK-yritysten koulutuskiertueen aikana. Samoin kansainvälisen tietoturvalainsäädännön kartoittaminen käynnistyy osana LUOTI -hanketta. Kansainvälisen yhteistyön merkitys kasvaa Euroopan verkko- ja tietoturvaviraston aloitettua toimintansa. Tätä toimintaa neuvottelukunta seuraa ja ottaa vaikutteita omaan toimintaansa, toisaalta vie viestiä Eurooppaan kansallisten edustajiensa kautta. On myös käyty neuvotteluja siitä, että saamme kokoukseemme vierailevan luennoitsijan kansainväliseen tietoturvalainsäädäntöön liittyen. Neuvottelukunta seuraa myös Euroopan komission tietoturva-aloitteita ja ottaa ne huomioon osana toimintaansa.

Tietoturvallisissa sähköisissä palveluissa toimintaa ohjaava ajatus on rohkaista palveluntarjoajia luomaan uusia tietoturvallisia palveluita käyttäen laajasti eri alustavaihtoehtoja, kuten tietokonetta, matkaviestimiä sekä digitaalista televisiota. Tavoitteena on edistää uuden arjen tietoyhteiskunnan ajattelua hyödyntää aitoa verkkojen yhteiskäyttöä. Painopistealueen sisällä seurataan edelleen tietoturva-alaan liittyvää lainsäädäntöä, aluksi kotimaassa, mutta jo alkuvuodesta 2006 Suomen yritysten kannalta keskeisissä Euroopan maissa. Painopisteen tukihankkeena on raportoitu biometrisen tunnistamisen tietoturva, joka noussee omaksi hankkeekseen vuonna 2006.

Kansallisen tietoturvallisuuden tilannekuvan ylläpidon tarkoituksena on jakaa asiallista ja tietoturvallisuusasioihin keskittynyttä oikeaa tietoa kuluttajille, organisaatioille ja yrityksille. Keskeinen toiminta-alue on kriittinen infrastruktuuri. Uhkakuvilla pelottelua on vältettävä ja alan toimijoita on rohkaistava puhumaan oikeista asioista oikealle yleisölle niin, että sähköisen viestinnän tuomat edut voidaan hyödyntää täysimääräisesti kuitenkin välttäen siihen liittyvät rikolliset ja haitalliset ilmiöt. Painopisteeseen ovat sulautuneet tietoturvallisuusriskien arviointi, verkkorikoksien tutkimus, roskapostin välttäminen sekä lainsäädännöllisin että teknisin keinoin ja tietoturvahaavoittuvuuksien analysointi. Painopistealueelle on sulautunut myös kansallisen tietopääoman suoja-hanke, joka on luovuttanut loppuraporttinsa loppuvuodesta 2004.

Tietoturvatietoisuuden edistämisen keskeinen keino on tietoturvapäivä. Vuoden 2005 tietoturvapäivä oli suurmenestys kuten aiemminkin. Peräti 98 prosenttia peruskoulun opettajista tunsi tapahtuman ja 2/3 kouluista käytti aktiivisesti hankkeen tuottamaa materiaalia. Hankkeen kotisivuilla käytiin yli 900 000 kertaa ja 20 000 koululaista otti osaa tietoturva-aiheiseen kilpailuun. Myös vuonna 2006 järjestetään tietoturvapäivä, jonka kohderyhmänä ovat koululaiset, heidän vanhempansa sekä PK-yritykset. Useampikin työryhmä kartoittaa tietoturvaongelmia, ja tätä työtä hyödynnetään neuvottelukunnan työssä vuonna 2006. Omana tukihankkeenaan raportoi myös yritysten tietoturvatietoisuus-hanke, joka toimii yhteistyössä Helsingin kauppakamarin, Keskuskauppakamarin sekä sisäasiainministeriön yritysturvallisuushankkeen kanssa. Erityisesti tietoturvatietoisuuden osa-alue on voimakkaassa kehitysvaiheessa ja tuottaa lisäarvoa myös kansallisen tietoturvallisuusasioiden neuvottelukunnan työlle. Painopistealueella on sovellettu myös Tilastokeskuksen ”Viestintävälineiden käyttö 2005” -tutkimusta.

Varsinaisten painopistealueiden ulkopuolella on toiminut omana hankkeenaan Tietoturvastrategian vaikuttavuus -ryhmä. Se on arvioinut kansallisen tietoturvastrategiahankkeen ja sen hankeryhmien etenemistä ja hankeryhmien toimien vaikutuksia tietoturva-alan kehittymiseen keväällä 2005. Sen tehtävänä on myös laatia suositukset jatkotyön suuntaamiseen ja esittää menetelmiä strategiahankkeen lopullisen tuloksellisuuden mittaamiseen vuonna 2007. Hankeryhmän kanssa laadittiin osahankkeiden jatkotyövaihtoehdot, arvioitiin tehostamis- ja tarkentamisehdotusten vaikutuksia sekä tehtiin ehdotukset mahdollisesta muusta yhteistyöstä ja uusista kehittämishankkeista.

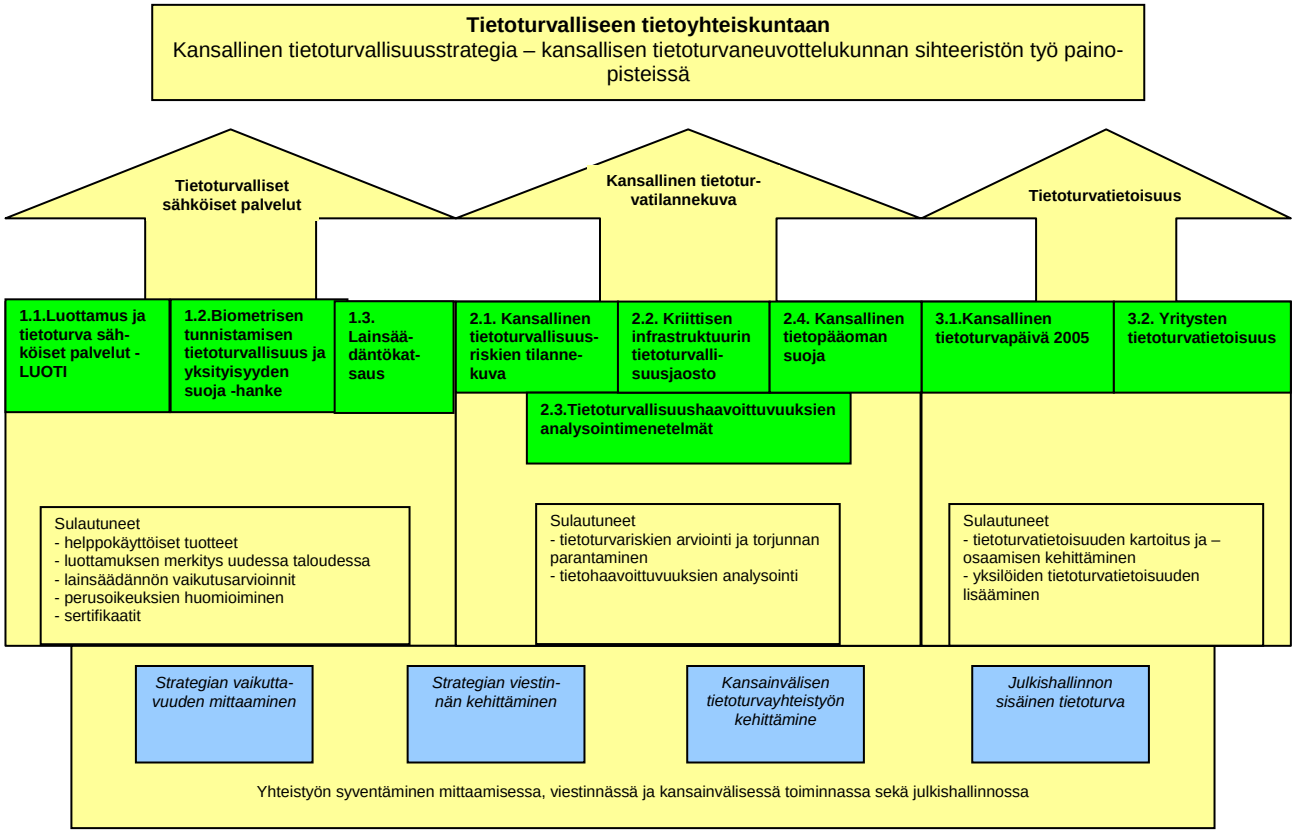
Strategiahanke esittää loppuraporttinaan tutkimuksen tuloksen kansalliselle tietoturvallisuusasioiden neuvottelukunnalle.

Kansallisen tietoturvallisuusasioiden neuvottelukunnan työ on lähtenyt hyvin käyntiin ja voimme kokea onnistuneemme työssämme tulosten perusteella. Muun muassa roskapostiviestin määrä on pudonnut kolmannekseen alun 80 prosentista syksystä 2003 lähtien. Tämän vuoksi olemme saaneet lisää verkkokapasiteettia hyötyohjelmien käyttöön. Hyvän tulokseen on vaikuttanut sekä sähköisen viestinnän tietosuojalain säännösten velvoittavuus että suodatusohjelmien käyttäminen. Roskapostien määrä on vähentynyt myös kansainvälisessä viestinnässä.

Yhteistyö läpi yhteiskunnan sekä normaali- että poikkeusoloissa toteuttaa parhaalla mahdollisella tavalla kansallista tietoturvallisuusstrategiaa. Työ tietoturvallisuuden parantamiseksi jatkuu kaikilla aloilla. Liikenne- ja viestintäministeriö seuraa teknisiä tietoturvallisuusuhkia sekä itsenäisesti että Viestintäviraston erinomaisesti hoidetun CERT-FI:n toiminnan kautta ja reagoi niihin välittömästi yhteistyössä muiden toimijoiden kanssa sekä nostamalla näiden haavoittuvuuksien ratkaisuehdotuksia esiin työryhmissään.

Tietoturvallisuus on taloudellinen ja poliittinen haaste, jonka merkitys määrittyy siitä saataviin hyötyihin tai sen laiminlyömisestä aiheutuviin haittoihin. Kansallinen tietoturvallisuusasioiden neuvottelukunta haluaa tarjota kaiken sen tuen, minkä Suomen johtavat toimijat voivat yhdessä tarjota, jotta tietoturvallisuuden kehittämiseen tässä maassa panostetaan vahvasti jatkossakin.

Tavoitteena tietoturvallinen tietoyhteiskunta



Neuvottelukunnan jäsenten allekirjoitukset 13.12.2005

Harri Pursiainen, pj, ylijohtaja
Liikenne- ja viestintäministeriö

Kristiina Pietikäinen, vpj,
vt. apulaisosastopäällikkö

Timo Kekkonen, osastopäällikkö
Kauppa- ja teollisuusministeriö

Arvo Jäppinen, ylijohtaja
Opetusministeriö

Marco Krogars, ylijohtaja
Puolustusministeriö

Markku Salminen, poliisiylijohtaja
Sisäasiainministeriö

Jorma Karjalainen, ylijohtaja
Valtiovarainministeriö

Mika Purhonen, ylijohtaja
Huoltovarmuuskeskus

Marita Wilska, kuluttaja-asiamies
Kuluttajavirasto

Kyösti Halonen, osastopäällikkö
Puolustusvoimat

Reijo Aarnio, tietosuojavaltuutettu
Tietosuojavaltuutetun toimisto

Rauni Hagman, pääjohtaja
Viestintävirasto

Kalevi Tiihonen, toimistopäällikkö
Elinkeinoelämän keskusliitto EK ry

Reijo Svento, toimitusjohtaja
Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry

Jouni Keronen, tietohallintojohtaja
Fortum Oyj

Risto Siilasmaa, toimitusjohtaja
F-Secure Oyj

Leena Linnainmaa, osastopäällikkö
Keskuskauppakamari

Martti Mehtälä, toimitusjohtaja
Microsoft Oy

Elise Lepinsalo-Harju, senior manager
Nokia Oyj

Bo Harald, johtaja
TietoEnator Oyj

Arto Vainio, toimitusjohtaja
SSH Communications Security Oy

Ilkka Hiidenheimo, toimitusjohtaja
Stonesoft Oyj

Lauri Virkkunen, toimitusjohtaja
Vattenfall Oy

Tuire Saaripuu, pääsihteeri
ylitarkastaja
Liikenne- ja viestintäministeriö

Valtioneuvoston periaatepäätös kansalliseksi tietoturvallisuusstrategiaksi 4.9.2003

Strategian tausta

Tietoyhteiskunta perustuu uuteen teknologiaan, uusiin toimintatapoihin ja uuteen osaamiseen. Näiden hyödyntäminen parantaa kansalaisten hyvinvointia, muuttaa vuorovaikutuksen ja yhteiskunnallisen osallistumisen tapoja sekä lisää tasa-arvoa ja demokratiaa. Samalla ne parantavat yritysten tuottavuutta ja kilpailukykyä sekä avaavat uusia markkinoita ja liiketoimintamahdollisuuksia. Julkiselle hallinnolle tietoyhteiskunta antaa mahdollisuuden uudistaa toimintatapoja, parantaa asiakaspalvelua ja säästää voimavaroja.

Tietoyhteiskunnan mahdollisuuksien hyödyntäminen ja uhkien torjunta edellyttävät kaikkien toimijoiden luottamusta kehityksen suuntaan. Kansalaisten ja yritysten luottamusta tietoyhteiskuntaan voidaan lisätä erityisesti tietoturvallisuutta ja yksityisyyden suojaa parantamalla. Tietoturvallisuudella tarkoitetaan eri muodoissa olevien tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturvallisuus sisältää tekniseen turvallisuuteen, yksilöiden käyttäytymiseen, organisaatioiden toiminatatapoihin ja yhteiskunnallisiin olosuhteisiin liittyviä ulottuvuuksia.

Tietoturvallisuutta uhkaavat mm. henkilökohtaisen yksityisyyden loukkaukset, roskaposti, teollisuusvakoilu, piratismi, tietokonevirukset, verkkoterrorismi ja elektroninen sodankäynti. Nämä voivat ulottua tietoverkkojen avulla silmänräpäyksessä kaikkialle. Samanaikaisesti tietoturvallisuus antaa mahdollisuuksia. Oikein toteutettuna se lisää yksilöiden toimintavapautta, antaa elinkeinoelämälle uusia liiketoimintamahdollisuuksia ja alentaa liiketoiminta- ja vuorovaikutuskustannuksia kaikkialla yhteiskunnassa.

Kansallinen tietoturvallisuusstrategia on keskeinen osa hallituksen tietoyhteiskuntapolitiikkaa. Sen avulla torjutaan tietoturvallisuuden uhkia ja hyödynnetään siihen liittyviä mahdollisuuksia sekä normaali- että poikkeusoloissa. Strategia antaa valtioneuvoston, elinkeinoelämän, järjestöjen ja yksittäisten kansalaisten tietoturvallisuusponnisteluille yhteisen suunnan. Strategia ei kuitenkaan vaikuta tietoturvallisuuteen liittyvään vastuunjakoon eikä olemassa oleviin organisaatiorakenteisiin.

Strategiset tavoitteet

Kansallisen tietoturvallisuusstrategian avulla Suomesta pyritään rakentamaan tietoturvallinen tietoyhteiskunta. Strategian tavoitteena on:

1. edistää kansallista ja kansainvälistä tietoturvallisuusyhteistyötä

2. edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia

3. parantaa tietoturvallisuusriskien hallintaa

4. turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma

5. lisätä tietoturvallisuustietoisuutta ja -osaamista

Strategiset tavoitteet ja niihin liittyvät toimenpiteet esitellään tarkemmin alla. Esittelyjärjestys ei heijastele tavoitteiden ja toimenpiteiden keskinäistä tärkeysjärjestystä.

Tavoitteiden saavuttaminen

Kansallisen tietoruvallisuusstrategian tavoitteet saavutetaan seuraavin toimenpitein.

1. Edistetään kansallista ja kansainvälistä tietoturvallisuusyhteistyötä

Tiedon tuottaminen ja hyödyntäminen uuden tieto- ja viestintäteknologian avulla maantieteellisen etäisyyden rajoittamatta on globalisaation perusvoima. Uusiin toimintamahdollisuuksiin liittyvä turvallisuus on suuri haaste viranomaisille, yrityksille, kansalaisille ja muille toimijoille. Kansallisen tietoturvallisuusstrategian avulla vaikutetaan tietoturvallisuutta edistävien standardien, toimintalinjausten ja yhteistyöfoorumien muodostumiseen ja varmistetaan, että tietoturvallisuutta koskeva työnjako eri toimijoiden kesken on selkeä.

2. Edistetään kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia

Tiedon tuottamisen ja hyödyntämisen maailmanlaajuiset markkinat tekevät tiedosta yhä arvokkaampaa pääomaa. Kansallisen tietoturvallisuusstrategian avulla varmistetaan tiedon avoin saatavuus ja turvallinen käyttö. Nämä antavat uusia liiketoimintamahdollisuuksia ja vakaan toimintaympäristön tietoa tuottaville, hyödyntäville ja turvaaville yrityksille. Tämä puolestaan parantaa Suomen kilpailukykyä ja tuottaa voimavaroja myös muihin yhteiskunnan kehityskohteisiin.

Tietoturvallisuusalan yritysten liiketoiminnallisten toimintaedellytysten kehittämisellä edistetään kansallista kilpailukykyä ja uusien monipuolisten tietoturvallisuuspalveluiden saatavuutta.

3. Parannetaan tietoturvallisuusriskien hallintaa

Tiedon turvallinen hyödyntäminen on yhä suurempi haaste kaikille toimijoille, sillä tunnetut riskit muuttuvat ja uusia uhkakuvia syntyy jatkuvasti. Kansallisen tietoturvallisuusstrategian avulla pyritään edistämään riskien ennakoivaa tunnistamista ja hallintaa yksilön, yrityksen ja yhteiskunnan tasolla. Riittävän ennakoinnin avulla voidaan taata paras mahdollinen turvallisuus ja minimoida siitä aiheutuvat kustannukset.

4. Turvataan perusoikeuksien toteutuminen ja kansallinen tietopääoma

Tietoturvallisen tietoyhteiskunnan rakentaminen ei voi tapahtua yksilöiden ja muiden toimijoiden perusoikeuksien ja vapauksien kustannuksella. Tietoturvallisessa tietoyhteiskunnassa kaikkien toimijoiden tulee voida luottaa siihen, että hänen tietonsa ja viestinsä välitetään, käsitellään ja tallennetaan luottamuksellisesti ja etteivät ne joudu vääriin käsiin. Lisäksi jokaisella on oltava mahdollisuus päästä helposti käsiksi niihin

tietoihin, joita hänellä on oikeus käyttää. Yrityksillä keskeistä turvattavaa pääomaa ovat yrityssalaisuuden piirin luettavat asiat, asiakastiedot ja tuotekehitystiedot.

5. Lisätään tietoturvallisuustietoisuutta ja -osaamista

Tietoturvallisuusasioiden osaaminen on noussut uudeksi kansalaistaidoksi. Tietoturvallisessa yhteiskunnassa kaikkien toimijoiden tulee olla tietoisia oman toimintansa tietoturvallisuusriskeistä sekä omasta roolistaan niiden ehkäisemisessä. Kansallisen tietoturvallisuusstrategian avulla kohotetaan osaamisen tasoa panostamalla sekä tietoturvallisuusammattilaisten erityisosaamiseen että kaikkien toimijoiden yleiseen tietoturvallisuustietoisuuteen.

Strategian toimeenpano

Tietoturvallisuustyön toteuttaminen ja tietoturvallisuuden kehittäminen kuuluu voimassaolevan lainsäädännön perusteella usean toimijan vastuulle. Yleinen tietoturvallisuuden normaaliajan ohjaus ja kehittäminen kuuluu lähinnä liikenne- ja viestintäministeriön (LVM), LVM:n alaisen Viestintäviraston sekä kauppa- ja teollisuusministeriön toimialaan. Julkishallinnon osalta tietoturvallisuuden ohjauksesta ja kehittämisestä on säädetty erikseen. Julkishallinnon tietoturvallisuuden kehittäminen kuuluu lähinnä valtiovarainministeriön (VM) ja sisäasiainministeriön (SM) toimialaan. LVM:n toimivaltaan kuuluu valtioneuvoston ohjesäännön (262/2003) mukaan sähköinen viestintä ja viestintäpalvelujen tietoturvallisuus. LVM:n tehtävänä on myös teletoiminnan ohjaus ja kehittäminen viestintämarkkinalain 119 §:n ja televiestinnän tietosuojalain (565/1999) 23 §:n mukaisesti. Viestintäviraston tehtävänä on toimia kansallisena tietoturvallisuusviranomaisena, joka teletoiminnan tietosuojalain 21 §:n mukaan harjoittaa CERT-toimintaa ja valvoo sekä teletoiminnan tietosuojalain että viestintämarkkinalain noudattamista. Viestintävirasto harjoittaa myös tietoliikenneturvallisuuden valvontaa (COMSEC, communications security) ja se voi antaa teknisiä määräyksiä teletoiminnan tietosuojalain ja viestintämarkkinalain tietoturvallisuutta koskevista säännöksistä. Viestintähallinnosta annetun valtioneuvoston asetuksen (697/2001) 1 §:n mukaan Viestintäviraston tehtäviin kuuluu myös televiestinnän ja siihen liittyvän tietoturvallisuuden standardoinnin koordinointi ja kehittäminen. KTM:n tehtävänä on valtioneuvoston ohjesäännön mukaan teknologiapolitiikka ja tekninen turvallisuus.

Valtioneuvoston ohjesäännön mukaan VM:n toimialaan kuuluu valtion tietohallinnon, tietojenkäsittelyn ja tietoturvallisuuden yleiset perusteet, hallinnon sähköinen asiointi ja valtioneuvoston yhteinen tietohallinto. VM:n tehtävänä on myös sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) 22 §:n mukaisesti antaa tarkempia ohjeita hallinnon sähköisen asioinnin tietoturvallisuuden järjestämisestä. Valtioneuvoston ohjesäännön mukaan SM:n toimivaltaan kuuluu valtion ja kuntien välinen verkkoasiointi ja tietohallinto. VNK:n toimialaan kuuluu valtioneuvoston ohjesäännön mukaan valtioneuvoston yleisten toimintaedellytysten ja palvelujen järjestäminen.

Tietosuojaviranomaisten tehtävänä on valvoa henkilötietolain (523/1999) tietoturvallisuussäännösten noudattamista ja edistää hyvää tiedonhallintatapaa, mihin sisältyy myös tietoturvallisuutta koskevia vaatimuksia. Arkistolaitoksen tehtävät tietoturvallisuuden alalla keskittyvät arkistolain (831/1994) perusteella pysyvästi säilytettävien

asiakirjojen säilyvyyden turvaamiseen ja sen tehtävänä on sähköisestä asioinnista viranomaistoiminnassa annetun lain 22 §:n mukaan antaa tarkempia määräyksiä hallinnon sähköisen asioinnin kirjaamisesta ja rekisteröimisestä. Muita keskeisiä ja aktiivisia toimijoita tietoturvallisuuden alalla ovat poliisin hallinnosta annetun lain (110/1992) perusteella keskusrikospoliisi, suojelupoliisi ja muut poliisiviranomaiset sekä mm. Funet CERT ja TIEKE. Lisäksi yksityisten yritysten itsesääntelyllä samoin kuin erilaisilla yritysten käytännön tietoturvallisuustoimenpiteillä on keskeinen merkitys tietoturvallisuuden kehittämisen ja toteutumisen kannalta

Tietoturvallisuusalan yhteistyötä tehdään mm. Yritysturvallisuuden neuvottelukunnassa, joka on Teollisuuden ja Työantajain Keskusliiton, Palvelutyönantajat ry:n sekä näiden jäsenyritysten yhteistyöorganisaatio. Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) on valtion ja kuntien tietohallinnon yhteisten hankkeiden kehittämisfoorumi. JUHTA pyrkii sovittamaan yhteen valtion ja kuntien tietotekniikan, tietohallinnon ja sähköisten asiointipalvelujen kehittämistä ja laatii toimialaansa liittyviä, myös tietoturvallisuutta koskevia, suosituksia ja ohjeita. VM:n asettama valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) antaa valtionhallinnon tietoturvallisuutta koskevia ohjeita.

Poikkeusoloihin varautumista koskevien säännösten perusteella tehtävällä tietoturvallisuustyöllä on keskeinen merkitys myös rauhanajan tietoturvallisuuden kehittymisen ja toteutumisen kannalta. Varautumistoimien ylin johto kuuluu kauppa- ja teollisuusministeriölle, jonka hallinnonalaan kuuluu puolustustaloudellinen suunnittelukunta (PTS). PTS:n tietojärjestelmäjaoston tehtäviin kuuluu edistää yhteiskunnan, erityisesti elinkeinoelämän tietoturvallisuutta. Lisäksi varautumista koskevia erityistehtäviä on mm. lääninhallituksilla ja niitä avustavilla sähköisen viestinnän valmiusryhmillä.

Kaikilla edellä mainituilla tahoilla tehdään sektorikohtaista yhteistyötä ja tietoturvallisuutta edistäviä kehittämishankkeita, mutta laajempi yhteistyö ja toimenpiteiden koordinointi on tällä hetkellä vähäistä. Kansallisen tason koordinaation puute saa aikaan tarpeetonta päällekkäisyyttä ja johtaa rajallisten resurssien tehottomaan käyttöön. Alalla ei myöskään ole olemassa toimivia kanavia, joiden kautta tietoturvallisuusasioista kertyneitä kokemuksia ja käytäntöjä voitaisiin välittää eri toimijoille.

Toimeenpanon organisointi

Todellisessa tietoyhteiskunnassa uusi tieto, osaaminen ja teknologia sekä uudet toimintatavat ulottuvat kaikille elämänaloille. Tietoturvallisuus on välttämätön osa tietoyhteiskuntaa ja myös sen tulee ulottua kaikkialle yhteiskunnassa. Tämä edellyttää entistä tiiviimpää yhteistyötä kaikkien toimijoiden kesken. Kansallinen tietoturvallisuusstrategia luo perustan paremmalle yhteistyölle, sillä se ohjaa tietoturvallisuusponnisteluita kohti yhteisiä tavoitteita ja edistää tietoturvallisuushankkeiden yhteistä suunnittelua ja toteutusta sekä niitä koskevaa tietojenvaihtoa. Strategian toimeenpano ei kuitenkaan muuta tietoturvallisuuteen liittyvää vastuunjakoa eikä olemassa olevia organisaatiorakenteita.

Valtioneuvostolla on kokonaisvastuu tietoturvallisuusstrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriö asettaa kansallisen tietoturvallisuusasioiden neuvottelukunnan, joka tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Kansallinen tietoturvallisuusasioiden neuvottelukunta antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategiaa. Neuvottelukunta tarjoaa laaja-alaisen foorumin eri toimijoiden ja organisaatioiden yhteistyön tehostamiseksi tietoturvallisuuteen liittyvissä kysymyksissä, mutta se ei muuta olemassa olevaa vastuunjakoa eikä organisaatiorakenteita.

Strategian toimeenpanon tehostamiseksi neuvottelukunta voi perustaa erityiskysymyksiin tai tiettyihin toimialoihin keskittyviä työryhmiä.

Taloudelliset ja yhteiskunnalliset vaikutukset

Periaatepäätöksessä asetetut tavoitteet voidaan toteuttaa kehyspäätösten sekä vuosittain talousarvion yhteydessä tehtävien päätösten puitteissa.

Samalla strategia tuottaa merkittävää lisäarvoa. Se lisää eri viranomaisten tietoturvallisuusyhteistyötä ja ehkäisee päällekkäisiä toimenpiteitä ja tehostaa siten julkisten varojen käyttöä. Strategia rakentaa yrityksille parempaa toimintaympäristöä ja edistää uusien ja helppokäyttöisten tuotteiden ja palveluiden kehittämistä ja lisää näin suomalaisyritysten kansainvälistä kilpailukykyä. Lisäksi strategian avulla lisätään kaikkien käyttäjien tietoturvallisuustietoisuutta ja parannetaan alan asiantuntijoiden osaamista ja vahvistetaan näin kaikkien toimijoiden mahdollisuuksia hyödyntää täysimääräisesti tietoyhteiskunnan tarjoamia mahdollisuuksia.

Kommunikationsminister Susanna Huovinens tal vid överlämnandet av delegationens rapport den 13 december 2005

När den nationella delegationen för informationssäkerhet år 2004 överlämnade sin första rapport till kommunikationsminister Leena Luhtanen betonade hon att det finska informationssamhället präglas av säkerhet och konkurrenskraft. Detta är möjligt endast om medborgarna och affärslivet har förtroende för att de elektroniska kommunikationerna och tjänsterna är säkra att använda. Varje hot mot informationssäkerheten utgör ett hot mot grunderna för hela informationssamhället.

Den nationella delegationen för informationssäkerhet som grundades med stöd av den internationellt uppmärksammade nationella informationssäkerhetsstrategin inledde sitt andra verksamhetsår mot bakgrund av de goda resultaten av de utredningar som gjorts under det första verksamhetsåret. Delegationens arbete bygger på en gemensam syn som alla samhällsaktörer, förvaltningen, de som använder tjänsterna samt näringslivet, delar om att säkra e-tjänster är ett grundläggande villkor för all verksamhet i den nya vardagen i informationssamhället.

År 2005 har delegationen fortsatt sitt förtjänstfulla arbete och justerat sina prioriteringar för att bemöta nya utmaningar. I synnerhet de angrepp som mot slutet av året riktats mot Internetanvändarnas identitet i form av s.k. phishing ställer nya krav på alla tjänsteleverantörer. Att andelen skräppost av alla förmedlade e-postmeddelanden har sjunkit från 80 procent till ca en tredjedel sedan informationssäkerhetsstrategin antogs hösten 2003 är ett utmärkt exempel på hur kraftfull strategin har varit i Finland. För att utbudet av elektroniska kommunikationstjänster skall öka måste tjänsterna vara säkra och lätta att använda. För att utvecklingen av elektroniska medier skall fortsätta och användningen av dem ytterligare öka måste de utmaningar som gäller säkerheten lösas på ett tillförlitligt sätt. Om vi på grund av brottslig och skadlig verksamhet förlorar detta förtroende, förlorar vi mycket.

Idag inverkar internationaliseringen mer än någonsin också på olika projekt som gäller informationssäkerheten. Nu ställs t.ex. stora förväntningar på den Europeiska byrån för nät- och informationssäkerhet (ENISA). Byrån väntas göra en stor insats för att öka medvetenheten om informationssäkerhet i Europa. ENISA måste infria sina löften och visa såväl medlemsstaterna som de enskilda konsumenterna exempel på bästa praxis inom olika områden av informationssäkerhet. Samtliga aktörer berörs t.ex. av hur risker som hotar informationssäkerheten hanteras, hur medvetenheten om informationssäkerhet ökas bland olika användargrupper samt hur CERT-samarbetet (Computer Emergency Response Teams) för att förebygga, upptäcka och utreda kränkningar av informationssäkerheten framskrider. Därför måste byrån finna en metod för att på ett optimalt sätt tillgodose användarnas behov i deras dagliga liv och affärsverksamhet.

Den nya vardagen i informationssamhället som bygger på tanken om allestädes närvarande datorer (*ubiquitous computing*, förkortat *ubicomp*) är inte bara en framtidsbild, utan redan verklighet i vår nätverksbyggande värld. Den europeiska utvecklingen och konkurrenskraften måste vara i nivå med de utmaningar som de övriga avancerade IT-samhällena i världen ställer. Finland genomför Europeiska kommissionens i2010-program på bred front, men eftersom marknadssituationen befinner sig i en brytningstid kan vi inte bara vänta och se vad som händer. Vi måste försöka se allt längre in i framtiden för att trygga vår position bland de ledande informationssamhällena och för att garantera våra medborgare effektiva och tillförlitliga tjänster av god kvalitet.

För Finlands EU-ordförandeskap 2006 har kommunikationsministeriet valt IT-tillämpningar i vår vardag till ett centralt tema. Betydelsen av informationssäkerhet växer i takt med att de alternativa plattformarna bildar nätverk som öppnar nya möjligheter för att skapa intelligenta och lätthanterliga tjänster. De nya e-tjänsterna kan inte utvecklas om inte lösningar som är datatekniskt tillförlitliga är en del av vår vardag. Därför är det viktigt att vi kan komma överens om gemensamt accepterade standarder och regler, utan att vi behöver införa ett tungt och svårhanterligt regelverk. Vi måste sprida medvetenhet och kunskap om informationssäkerhet för att underlätta samarbetet mellan olika aktörer och tjänsteanvändare.

Under sitt EU-ordförandeskap ordnar Finland tillsammans med Europeiska kommissionen och Europeiska byrån för nät- och informationssäkerhet (ENISA) en konferens under namnet ”i2010 – Towards a Ubiquitous European Information Society”, där de inbjudna gästerna är ledande experter och beslutsfattare inom området. Det ambitiösa målet är att konferensen skall väcka internationell uppmärksamhet och utgöra ett forum med anföranden av världens toppexperter. Konferensens huvudtema är tillämpningar och lösningar i informationssamhället med särskild tonvikt på IT i vardagen. Fokus ligger på det europeiska i2010-programmet med dess tillämpningsområden och på att följa upp utvecklingen i IT-samhället i bredd med utvecklingen av affärsverksamheten åren 1996–2006–2016. Samtidigt studeras konsekvenserna av den snabba tekniska utvecklingen på affärsverksamheten inom hela branschen.

Jag vill framföra statsrådets hälsning till den nationella delegationen för informationssäkerhet samt dess sekretariat med anledning av er föredömliga arbetsinsats. Delegationens projektarbete har nu kommit halvvägs och jag kan med glädje konstatera att ni utifrån det utmärkta material och de goda resultat som ni hittills nått har vidareutvecklat nya arbetsmetoder för den återstående projekttiden. Ert framgångsrika arbete är ett exempel på hur olika delar av samhället, den offentliga sektorn och nydanande industribranscher, tillsammans kan bidra till en demokratisk utveckling, tillgodose grundläggande fri- och rättigheter, skapa lätthanterliga tjänster samt stärka den nationella konkurrenskraften. Ni har samarbetat för att ta fram och föra vidare nya idéer, men ändå behållit fotfästet i den verklighet och lagbundenhet som förvaltningen och näringslivet ställer. Samtidigt har ni ifrågasatt förhärskande synsätt på informationssäkerhet. Ni har sammanfört värdefulla erfarenheter och verkligen främjat samarbetet mellan olika aktörer. Ett stort tack till er alla som deltagit i arbetet!

Det finländska informationssamhället hör till den absoluta världstoppen. Vår nationella informationssäkerhetsstrategi är ett uttryck för en gemensam politisk vilja. Strategin är en tillgång och ett verktyg för alla aktörer inom branschen. De elektroniska tjänsterna kan inte utvecklas om vi inte alla tillsammans deltar i skapandet av gemensamma spelregler. Om det inte finns något förtroende för elektroniska kommunikationstjänster kan det inte heller finnas affärsverksamhet inom området eller e-tjänster som underlättar människornas vardag.

Ärade nationella delegation för informationssäkerhet samt dess sekretariat och arbetsgrupper, jag ber att få framföra er ett varmt tack och önskar er alla en fridfull jul samt ett gott och framgångsrikt år 2006.

Helsingfors den 13 december 2005

Susanna Huovinen
Kommunikationsminister

Delegationens syn på måluppfyllelse med förslag till statsrådet om fortsatta åtgärder

Den nationella delegationen för informationssäkerhet har etablerat sin verksamhet och den nationella informationssäkerhetsstrategin har gett goda resultat. Ett exempel på detta är att mängden skräppost av all förmedlad e-postkommunikation har sjunkit från 80 procent till en tredjedel. Under Finlands EU-ordförandeskap nästa år är informationssäkerhet en av prioriteterna. Finland har nu en chans att fokusera Europas och den övriga världens uppmärksamhet på sitt kunnande inom informationssäkerhet.

Det finländska informationssamhället försvarar sin plats bland världens toppsamhällen. Informationssäkerhetspolitiken är en viktig framgångsfaktor för vårt land. Finland har uppmärksammats internationellt som det första land i världen med en nationell informationssäkerhetsöversikt och det första land i Europa med en informationssäkerhetsstrategi som omfattar hela samhället. Vår strategi för informationssamhället har belönats som den bästa europeiska säkerhetsprincipen vid RSA, en av de största IT-säkerhetskonferenserna i världen. På initiativ av Finland bereder också Europeiska kommissionen nu en europeisk informationssäkerhetsstandard.

Den tanke som kommunikationsminister Susanna Huovinen har fört fram om en strategi för den nya vardagen i informationssamhället och om en smart närmiljö med datorsystem överallt, är ett utmärkt rättesnöre också för delegationen. För att säkra sin position som ett av de ledande informationssamhällena i världen bör Finland ta fasta på erfarenheter från annat håll, i synnerhet från Japan och Korea. Syftet med delegationens arbete är att finna medel för att utnyttja olika kommunikationslösningar så helgjutet, varierat och säkert som möjligt. Det är precis vad delegationen gjort sedan den tillsattes.

I den nya vardagen i informationssamhället är tekniken en del av det alldagliga livet. Trafiksäkerhet, logistik, handel, hälsovård och industri är exempel på områden där nätverk borgar för en god servicenivå och ökad produktivitet. När den nya vardagen i informationssamhället lever upp till människornas förtroende främjar den allmänna mål såsom demokrati, jämställdhet och livskvalitet.

Delegationen känner sitt ansvar som vägvisare inom informationssäkerhet. Därför söker delegationen nya verksamhetsformer för att finna svar på olösta problem som hänför sig till informationssäkerhet. Arbetet skärps ytterligare för att de mål som statsrådet har ställt skall nås. Delegationens arbetsmetoder och tyngdpunkterna i arbetet förnyas. Information om observerade hot mot informationssäkerheten sprids på ett klart och entydigt sätt och människorna uppmuntras att följa angivna säkerhetsåtgärder då de använder e-kommunikationer och e-tjänster.

I delegationens rapport beskrivs det arbete som gjorts hittills och skisseras riktlinjerna för nästa år. I rapporten från 2005 har antalet prioritetsområden minskat från fyra till tre eftersom en del projekt redan har slutförts. Dessutom har det också varit ändamålsenligt att omorganisera vissa arbetsformer som stöder varandra.

Delegationens arbete för 2006 läggs upp mot bakgrund av det arbete som gjorts hittills samt konstaterade ändringsbehov. Arbetet är indelat i tre prioriteringar: säkra elektroniska tjänster, en nationell lägesbild av informationssäkerhet samt ökad medvetenhet om informationssäkerhet. Under 2006 gör delegationen som grupparbete en övning för att finna nya undersökningsobjekt och för att inrik-

ta arbetet på outforskade områden beträffande datakommunikation, processer och organisationsstrategier. Dessutom tar delegationen hänsyn till resultaten av aktuella undersökningar, såsom samarbetsprojektet mellan Helsingfors handelskammare, Centralhandelskammaren samt inrikesministeriet i syfte att öka informationssäkerheten i företag, för att på så sätt skapa sig en helhetsbild av de senaste rönen inom området. Delegationen har också en synlig roll i olika delprojekt, såsom den nationella informationssäkerhetsdagen och utbildningen av små och medelstora företag. Som en del av LUOTI-projektet inleds en utredning av den internationella lagstiftningen i fråga om informationssäkerhet. Det internationella samarbetet har blivit allt viktigare i och med att Europeiska byrån för nät- och informationssäkerhet (ENISA) har inlett sin verksamhet. Dels anpassar delegationen sin egen verksamhet efter det internationella samarbetet, dels förmedlar den sitt budskap till Europa genom de nationella representanterna i samarbetet. I enlighet med etta har delegationen dryftat möjligheten att bjuda in en utländsk gästföreläsare för att berätta om den internationella lagstiftningen på området. Delegationen tar också del av Europeiska kommissionens initiativ i fråga om informationssäkerhet och anpassar sin verksamhet enligt dem.

Inom prioritetsområdet ***säkra elektroniska tjänster*** är den ledande tanken att uppmuntra tjänsteleverantörerna att ta fram nya, datatekniskt sett säkra e-tjänster som bygger på alternativa plattformar, såsom datorer, mobiltelefoner och digital television. Målet är att främja IT i vardagen och effektiv samanvändning av näten. En av uppgifterna är att följa hur lagstiftningen i fråga om informationssäkerhet utvecklas i Finland, och efter ingången av 2006 också i de länder i Europa som är viktiga med tanke på finländska företag. Ett av stödprojekten går ut på att kartlägga informationssäkerhetsfrågor i samband med biometrisk identifikation, vilket troligen blir ett separat projekt 2006.

Den nationella lägesbilden av informationssäkerheten skall sprida saklig och objektiv information om informationssäkerhet till konsumenter, organisationer och företag. Inom denna prioritet är kritisk infrastruktur ett centralt verksamhetsområde. Avskräckande hotbilder bör ersättas med satsningar på att få aktörerna inom branschen att rikta sin information till rätt målgrupp. På detta sätt kan de fördelar som den elektroniska kommunikationen erbjuder utnyttjas fullt ut och eventuella skadliga och brottsliga fenomen undvikas. Denna prioritet omfattar även utvärdering av säkerhetsrisker, undersökning av Internetbrottslighet, skydd mot skräppost med antingen lagstiftningsmässiga eller tekniska medel samt analys av sårbarheter. I prioriteten ingår även projektet för att skydda det nationella informationskapitalet vars slutrapport överlämnades i slutet av 2004.

Informationssäkerhetsdagen är en ett viktigt verktyg för att öka ***medvetenheten om informationssäkerhet***. Informationssäkerhetsdagen 2005 var en lika stor succé som dess föregångare. Hela 98 procent av grundskollärarna kände till temadagen och två tredjedelar av dem använde aktivt det material som producerats för evenemanget. Evenemangets webbplats besöktes över 900 000 gånger och 20 000 skolelever deltog i webbtävlingen om informationssäkerhet. Målgruppen för Informationssäkerhetsdagen 2006 består av skolelever, deras föräldrar samt små och medelstora företag. Problem som hänför sig till informationssäkerhet utreds av flera arbetsgrupper och resultaten utnyttjas i delegationens arbete 2006. Ett separat stödprojekt med rapporteringsskyldighet tar sikte på att öka medvetenheten om informationssäkerhet bland företag. Projektet genomförs i samarbete med ett företagssäkerhetsprojekt under ledning av Helsingfors handelskammare, Centralhandelskammaren och inrikesministeriet. Delområdet som går ut på att öka medvetenheten befinner sig i en speciellt kraftig utvecklingsfas och skapar mervärde för delegationens arbete. Arbetet inom denna prioritet bygger delvis på den undersökning om användningen av kommunikationsmedel som Statistikcentralen gjort 2005.

Som ett fristående projekt utanför de egentliga prioritetsområdena har en undergrupp studerat verkningarna av informationssäkerhetsstrategin. Gruppen gjorde våren 2005 en bedömning av hur den

nationella informationssäkerhetsstrategin och dess olika delprojekt har framskridit och utvärderade vilka effekter de genomförda åtgärderna har haft på utvecklingen av informationssäkerhetsbranschen. Vidare skall gruppen utarbeta rekommendationer för inriktningen av det fortsatta arbetet och föreslå metoder för hur de slutliga resultaten av strategin skall mätas 2007. Delegationen utarbetade i samråd med projektgruppen förslag till fortsatta åtgärder för de olika delprojekten, bedömde verkningarna av de föreslagna åtgärderna för att effektivisera och precisera arbetet samt lade fram förslag för eventuellt övrigt samarbete och nya utvecklingsprojekt.

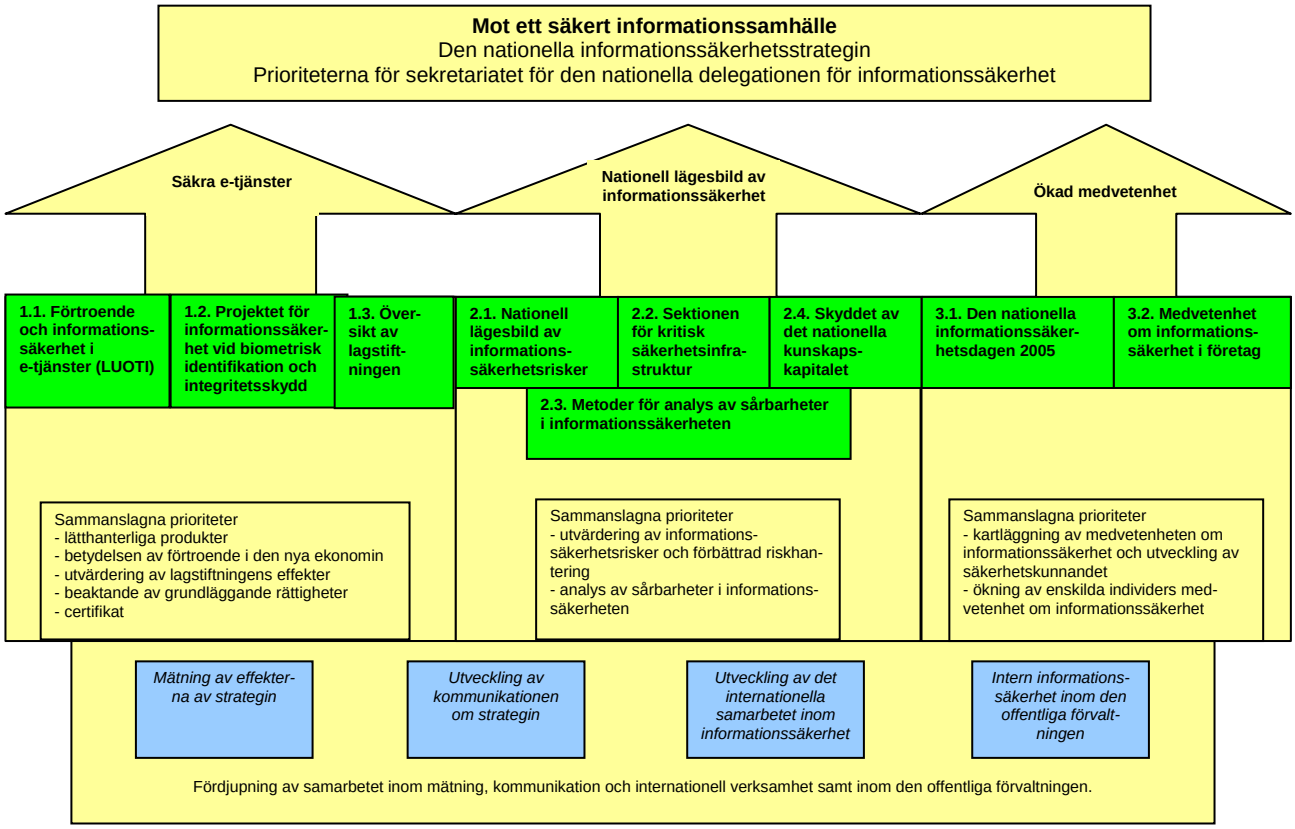
Projektgruppen som ägnar sig åt att undersöka verkningarna av informationssäkerhetsstrategin skall redogöra för resultaten i en slutrapport som överlämnas till delegationen.

Den nationella delegationen för informationssäkerhet har kommit ordentligt igång med sitt arbete och på basis av de goda resultaten kan den anses ha lyckats med sin uppgift. Bland annat andelen skräppost av alla e-postmeddelanden har sjunkit från 80 procent till en tredjedel sedan hösten 2003. Tack vare detta har vi fått mer ledig nätkapacitet för nyttoprogram. Bidragande orsaker till det goda resultatet har varit de bindande bestämmelserna i lagen om dataskydd vid elektronisk kommunikation samt den ökade användningen av filterprogram. Mängden skräppost har minskat också i den internationella kommunikationen.

Ett samarbete genom hela samhället såväl under normala förhållanden som under undantagsförhållanden är det bästa tänkbara sättet för att genomföra den nationella informationssäkerhetsstrategin. Arbetet för att förbättra informationssäkerheten fortsätter på alla områden. Kommunikationsministeriet håller ständig uppsikt över tekniska hot mot informationssäkerheten, dels självständigt, dels genom den utmärkta CERT-FI-verksamhet som Kommunikationsverket leder. Ministeriet reagerar omedelbart på eventuella hot i samverkan med andra aktörer och de olika arbetsgrupperna vid ministeriet framför förslag om hur konstaterade sårbarheter kan elimineras.

Informationssäkerheten är en ekonomisk och politisk utmaning, vars betydelse definieras utifrån den nytta den ger eller de olägenheter som försummelsen av den leder till. Den nationella delegationen för informationssäkerhet och dess medlemmar som företräder de ledande aktörerna inom branschen i Finland ger sitt helhjärtade stöd till alla initiativ i syfte att fortsätta den kraftig satsningen på att utveckla informationssäkerheten i vårt land.

Med sikte på ett säkert informationssamhälle



Helhetsbild av informationssäkerheten

Situationen för informationssäkerhet har utvecklats i många avseenden under 2005. Medvetenheten om informationssäkerhet ökar alltjämt samtidigt som programuppdateringar, antivirusprogram och brandväggar blir allt vanligare. Under den senare delen av året har användningen av datanättjänster störts av nya typer av skadliga koder, särskilt phishing och virus i smarttelefoner.

Medvetenheten om informationssäkerhet har ökat markant under 2005. Programuppdateringar, antivirusprogram och personliga brandväggar är redan allmänt kända metoder för att höja informationssäkerheten i datanättjänster. Även i år har den nationella informationssäkerhetsdagen framgångsrikt banat väg för en ökad medvetenhet om informationssäkerhet. Ett annat initiativ i samma anda är det nystartade LUOTI-projektet i syfte att sporra aktörerna inom branschen att skapa nya, innovativa och säkra nättjänster. Ett nytt hot mot informationssäkerheten som blivit vanligare under 2005 är phishing eller identitetsstöld via tjänster i datanät. Under det gångna året har också många skadliga program som angriper multifunktionella mobiltelefoner eller s.k. smarttelefoner påträffats. CERT-FI har otroligt snabbt lyckats reagera på kritiska incidenter som äventyrat informationssäkerheten och informerat konsumenter, tjänsteleverantörer och potentiellt sårbara organisationer om hoten och om olika sätt att skydda sig mot dem.

Informationssäkerhetsdagen

Informationssäkerhetsdagen 2005 var riktad till skolor och skolelever. Informationssäkerhetsdagen fick ett gott mottagande i finska grundskolor och dess tema utnyttjades aktivt i undervisningen under hela vårterminen. Enlig en undersökning som Taloustutkimus Oy gjorde bland lärarna kände 98 procent till Informationssäkerhetsdagen och två skolor av tre hade utnyttjat temadagens material i undervisningen. Inemot 500 grundskollärare deltog i förfrågningen som utfördes i maj 2005.

Majoriteten av dem som svarade på frågorna ansåg att Informationssäkerhetsdagen är nyttig och att den behövs. Också den elektroniska informationssäkerhetsskolan som finns på webbplatsen www.tietoturvakoulu.fi ansågs vara till nytta för undervisningen.

Största delen av lärarna som deltog i förfrågningen ansåg att eleverna tack vare Informationssäkerhetsdagen använder Internet på ett säkrare sätt än förr.

Vid utgången av oktober 2005 hade webbplatsen www.tietoturvakoulu.fi haft över 39 300 besökare. Också webbplatsen www.tietoturvaopas.fi har varit populär: från början av november 2004 till slutet av oktober 2005 hade webbplatsen besökts över 77 500 gånger.

Informationssäkerhetsprogrammet LUOTI

LUOTI-programmet inleddes 2005 för att främja utvecklingen av säkra elektroniska produkter och -tjänster samt för att utveckla den omgivande verksamhetsmiljön, dvs. lagstiftning, forskning och utbildning. Målet är också att skapa visioner om framtida hot mot informationssäkerheten och att finna lösningar på dem och att sporra nytänkande produkt- och serviceutveckling för digitalt innehåll som kan distribueras via en

mängd olika plattformar. LUOTI-programmet främjar informationssäkerheten med hjälp av praktiskt inriktade tjänster och användningssituationer. Målet är att skapa en gynnsam verksamhetsmiljö för utvecklingen av varierande e-tjänster. En del av programmet går ut på att granska eventuella behov att utveckla lagstiftning, forskning och utbildning och att framföra förbättringsförslag.

Centrala aktörer i programmet är data- och kommunikationsföretag och de anställda vid dem.

Som en del av LUOTI-programmet startades en öppen projektsökning i juni 2005. Till programmet har valts tre pilotprojekt som syftar till att kommersialisera innovativa underhållstjänster i vilka hanteringen av informationssäkerhet intar en central roll.

Säkerheten i datanät

I fråga om informationsintrång är ökningen fortfarande kraftigast i fråga om sådana kränkningar som siktar på ekonomisk vinning. Ett nytt hot mot informationssäkerheten som blivit vanligare under 2005 är phishing eller identitetsstöld via tjänster i datanät. Under det gångna året har också många skadliga program som angriper smarttelefoner påträffats. Kommunikationsministeriet stödjer spridningen av information om säkra förfaranden för att på så sätt förebygga skadlig användning av näten. Det är viktigt att konsumenterna har tillgång till anvisningar och information om hur man kan skydda sig för t.ex. phishing, virusangrepp i smarttelefoner och skräppost samt om hur man uträttar ärenden elektroniskt och säkert i trådlösa lokala nät (WLAN). Också i fråga om trådlösa nät betonas betydelsen av informationssäkerhet. Kommunikationsministeriet öppnar också en särskild webbplats ägnad åt skräppostskydd. Flera grupper arbetar med att utreda vilka informationssäkerhetsproblem som drabbar företag. På detta område samarbetar Helsingfors handelskammare, Centralhandelskammaren och en strategigrupp för företagssäkerhet vid inrikesministeriet för att öka företagens beredskap att motarbeta brottslighet. Den nationella delegationen för informationssäkerhet håller sig noggrant à jour med arbetet och föreslår att det utnyttjas i någon form av samarbete i delegationens arbete 2006.

Phishing eller fiske

Phishing är illegal verksamhet som går ut på att bedragaren försöker fiska information om mottagarens Internetbankkoder, kreditkortsnummer eller andra personuppgifter som kan användas i hopp om ekonomisk vinning. Vanligen skickar bedragaren falsk e-post som ser ut att komma från en legitim avsändare och ber mottagaren uppge personliga koder för e-kommunikation eller kreditkort. Problemet har blivit allmänt känt under 2005 särskilt till följd av de angrepp som bankernas webbplatser utsatts för och där mottagarna av phishing-meddelanden har uppmanats uppge sina personliga Internetbankkoder för utomstående.

Skräppost

Mängden skräppostmeddelanden av all e-postkommunikation har minskat uppskattningsvis med 25 procent jämfört med året innan. På så sätt har den nätkapacitet som kan användas för nyttig e-postkommunikation vuxit betydligt. Minskningen av skräppost beror bl.a. på de lagstiftningsmässiga medel som lagen om dataskydd vid elektro-

nisk kommunikation tillåter samt på rent tekniska metoder såsom filtrering. Den relativa andelen skräppost av all e-postkommunikation har sjunkit en aning också på andra håll i världen.

Det målinriktade arbete som gjorts för att minska mängden skräppost har utan tvivel gett resultat. I fråga om bekämpningen av skräppost har Finland procentuellt sett nått bättre resultat än resten av världen. År 2003 var skräppostens andel av den totala mängden e-postkommunikation 80 procent, 2004 hade siffran sjunkit till 45 procent och 2005 utgjorde skräpposten endast c. en tredjedel av alla e-postmeddelanden. Den motsvarande siffran i resten av världen var 90 procent år 2003, 60 procent år 2004 och ca hälften av all e-postkommunikation år 2005.

Skadliga program och virus i smarta telefoner

Spionprogram och andra skadliga program som angripit en hemdator ger sig till känna som problem som stör Internetanvändningen, bl.a. så att datorn blir långsam eller så att en stor del av den lediga kapaciteten försvinner. De skadliga programmen kan också störa användningen av Internet så att de utan att användaren märker det styr honom eller henne till en viss webbplats med t.ex. reklam eller vuxenunderhållning. I Finland har ett fåtal organisationers intranät utsatts för allvarliga angrepp av skadliga program. I ett enskilt fall infekterades dock flera hundra olika datasystem. I samtliga fall som CERT-FI fått kännedom om har viruset kommit in i organisationen via en bärbar dator som smittats utanför organisationen och sedan kopplats till intranätet.

Beträffande skadliga program som angriper mobiltelefoner har situationen tills vidare hållits rätt lugn. Virusskrivarnas intresse har koncentrerats främst till terminaler i mobilkommunikationsnät som använder operativsystemet Symbian. Stora publikevenemang är särskilt riskbenägna för att sprida skadliga program i mobiltelefoner.
Under 2005 har problemet drabbat speciellt användningen av s.k. smarta telefoner.
Sårbarheter i program

Förekomsten av sårbarheter i program har närmast begränsat sig till olika webbläsare. Sårbarheter har drabbat bl.a. Microsoft Internet Explorer (IE) samt Mozilla, Firefox och Netscape. Vissa problem förekommit också i program för säkerhetskopiering. Eftersom säkerhetskopieringar i datasystem vanligen fungerar med administratörsrättigheter har sårbarheterna en benägenhet att bli mycket allvarliga. De skadliga programmen försöker passera såväl antivirusprogram som brandväggar. Därför accentueras vikten av programuppdateringar med tanke på informationssäkerheten.

Trådlösa lokala nät (WLAN) och skyddet av dem

I sina årsrapporter har CERT-FI fäst uppmärksamhet bl.a. vid olovlig användning av trådlösa lokala nät, bristfällig definition av nätet, blockeringsattacker som riktas till nätet och avlyssning av datakommunikation. Missbruk av trådlösa WLAN-nät och avlyssning av kommunikationerna kan hindras genom att man i nätet använder kryptering och kräver användaridentifikationer, vilka skyddar nätet från utomstående. Det finns flera alternativa och kompletterande lösningar både för att kryptera förbindelsen och för att identifiera användarna, och utbudet kan variera något enligt leverantör.

Statistik om informationssäkerhet

Enligt en utredning som kommunikationsministeriet låtit göra om finländarnas kunskaper i fråga om informationssäkerhet är det fortfarande många som använder datorer och Internet utan att känna till ens de mest grundläggande och vanligaste problemen. Enligt utredningen upplever 39 procent av dem som använder Internet hemma att de har tillräckliga eller utmärkta kunskaper och färdigheter om informationssäkerhet. Hela 10 procent anser dock att de inte besitter denna kompetens. Delegationen vill råda bot på denna situation genom att öka medvetenheten om frågor som gäller informationssäkerhet. Syftet är att skapa lätthanterliga och säkra tjänster som är tillgängliga för alla och som förverkligar de mål som vardagen i IT-samhället ställer. Informationssäkerhetsdagen är ett av verktygen. Det arbete som Europeiska byrån för nät- och informationssäkerhet (ENISA) gör för att öka medvetenheten följs aktivt för att vi ska kunna ta del av bästa praxis i fråga om informationssäkerheten.

Enligt utredningen har 92 procent av Internetanvändarna ett program för filtrering av virus på sin hemdator. Av hemdatorerna är 78 procent försedda med en brandvägg, medan endast 36 procent av datorerna i hemmen är skyddade mot spion- och skadeprogram. Totalt 26 procent av svararna visste inte om de har ett skydd mot spion- och skadeprogram på sin dator.

Virusinfektioner är en del av Internetanvändarnas vardag. Av finska hemdatorer har 44 procent någon gång drabbats av ett virus. Sammanlagt 56 procent av användarna hade lyckats avlägsna viruset på egen hand med hjälp av ett virusskyddsprogram.

Den nationella delegationen för informationssäkerhet

Kommunikationsministeriet tillsatte den nationella delegationen för informationssäkerhet för att stödja de mål och åtgärder som fastställts med stöd av principbeslutet om den nationella informationssäkerhetsstrategin. Den nationella delegationen för informationssäkerhet skall främja samordningen av de åtgärder som verkställigheten av strategin förutsätter, följa upp genomförandet av strategin samt göra framställningar till statsrådet om uppdateringen av strategin. Delegationen och styrgrupperna för de olika delprojekten har hittills haft intill 200 medlemmar som företräder de finska aktörerna inom branschen.

Tuire Saaripuu
generalsekreterare
överinspektör
Kommunikationsministeriet
PB 31, 00230 Statsrådet
Tfn (09) 160 28305, 040 761 5406
fornamn.efternamn@mintc.fi

Tietoturvan kokonaiskuva

Tietoturvallisuustilanne on kehittynyt vuonna 2005 usealla taholla. Tietoturvatietoisuus on edelleen kasvavamassa ja ohjelmistopäivitykset, virustorjuntaohjelmistot sekä henkilökohtaiset palomuurit ovat jo yleisesti käytössä. Uudet tietoverkkopalveluiden häiriötekijät, erityisesti phishing ja älypuhelinvirukset ovat aiheuttaneet haittaa vuoden loppupuoliskolla.

Tietoturvatietoisuus on lisääntynyt huomattavalla tavalla vuonna 2005. Ohjelmistopäivitykset, virustorjuntaohjelmat sekä henkilökohtaiset palomuurit ovat jo yleisesti tunnettuja keinoja nostaa tietoturvallisuutta tietoverkkopalveluissa. Menestyneitä hankkeita tietoturvallisuuden ja tietoturvatietoisuuden kannalta ovat olleet tänäkin vuonna järjestetty Tietoturvapäivä sekä hyvin alkuun lähtenyt LUOTI-hanke, jossa tarkoituksena on rohkaista alan toimijoita kehittämään uusia innovatiivisia ja tietoturvallisia verkkopalveluita. Vuonna 2005 uusina tietoturvallisuusongelmina ovat nousseet phishing eli väärän identiteetin käyttäminen tietoverkkopalveluissa. Samoin uusiin niin sanottuihin älypuhelimiin liittyvät haittaohjelmat ovat nousseet esiin tänä vuonna. CERT-Fi on onnistunut reagoimaan tietoturvallisuuden kannalta kriittisiin tapahtumiin lyhyimmässä mahdollisessa ajassa ja tiedottamaan uhkista ja niiltä suojautumisesta kuluttajille, palvelun tarjoajille sekä haavoittumisille alttiille organisaatioille.

Tietoturvapäivä

Tietoturvapäivä vuonna 2005 oli suunnattu kouluille ja koululaisille. Tietoturvapäivä otettiin hyvin vastaan suomalaisissa peruskouluissa, ja tietoturvapäiväteemaa hyödynnettiin kevätlukukauden aikana aktiivisesti. Taloustutkimus Oy:n peruskoulujen opettajille tekemän kyselyn mukaan 98 prosenttia kyselyyn vastanneista tunsi Tietoturvapäivän ja kaksi kolmesta koulusta oli hyödyntänyt opetuksessaan teemaan liittyvää materiaalia. Toukokuussa 2005 tehtyyn kyselyyn vastasi lähes 500 peruskoulun opettajaa.

Valtaosa kyselyyn vastanneista opettajista piti Tietoturvapäivää tarpeellisena. Lisäksi opetuksen tueksi tehtyä tietoturvakoulu.fi-sivustoa pidettiin erittäin hyödyllisenä.

Kyselyyn vastanneista opettajista suurin osa katsoi, että Tietoturvapäivällä on ollut vaikutusta oppilaiden turvallisempaan internetin käyttöön.

Tietoturvakoulu.fi-sivustolla on käynyt vuoden 2005 lokakuun loppuun mennessä yli 39 300 kävijää. Myös tietoturvaopas.fi-sivustolla on ollut runsaasti kävijöitä: marraskuusta 2004 alkaen tietoturvaopas.fi-sivuilla oli vieraillut yli 77 500 kävijää lokakuun 2005 loppuun mennessä.

Luoti

Vuonna 2005 alkaneen LUOTI-ohjelman tavoitteena on edistää turvallisten sähköisten palveluiden tuote- ja palvelukehitystoimintaa sekä kehittää siihen liittyvää toimintaympäristöä - lainsäädäntöä, tutkimusta ja koulutusta. Ohjelman tavoitteena on myös lisätä näkemyksellisyyttä tulevaisuuden tietoturvariskeistä ja niihin liittyvistä ratkai-

sumahdollisuuksista sekä tuoda uutta näkökulmaa tuote- ja palvelukehitykselle käyttäen digitaalisen sisällön monikanavaista jakelualustaa. LUOTI -ohjelmassa tietoturvaa pyritään edistämään käytännön palveluiden ja käyttötilanteiden kautta sekä kehittää toimintaympäristöä siten, että se olisi mahdollisimman suotuisa turvallisten sähköisten palveluiden kehitystyölle. Ohjelman tehtävänä on arvioida lainsäädännön, tutkimuksen ja koulutuksen mahdollisia kehitystarpeita sekä esittää parannusehdotuksia.

Ohjelman keskeisimpiä toimijoita ovat tieto- ja viestintäalan yritykset ja niissä toimivat henkilöt.

Ohjelmassa on käynnistetty kesäkuun 2005 alussa avoin hankehaku. Ohjelmaan on valittu kolme uuden innovatiivisen viihdepalvelun kaupallistamiseen tähtäävää pilottihanketta, joissa tietoturvan käsittelyllä on selkeä rooli.

Tietoverkkoturvallisuus

Tietoturvallisuuteen liittyvissä loukkauksissa erityisesti taloudellista hyötyä tavoittelevat loukkaukset jatkavat voimakasta lisääntymistä. Vuonna 2005 uusina tietoturvallisuusongelmina ovat nousseet phishing eli väärän identiteetin käyttäminen tietoverkkopalveluissa. Samoin uusiin niin sanottuihin älypuhelimiin liittyvät haittaohjelmat ovat nousseet esiin tänä vuonna. Liikenne- ja viestintäministeriö edistää kuluttajille suunnatun tiedon antamista turvallisista toimintatavoista verkkoihin liittyvän haitallisen käytön ehkäisemiseksi. Kuluttajanäkökulmasta julkaistaan ohjeita ja tiedotteita, miten voidaan suojautua muun muassa phishingiltä, älypuhelinviruksilta sekä roskapostilta sekä kuinka voidaan asioida turvallisesti langattomassa lähiverkossa (WLAN). Myös langattoman verkon tietoturvaa korostetaan. Liikenne- ja viestintäministeriö avaa niin ikään erityisesti roskapostin torjumiseen tarkoitetut sivustot. Yritysten tietoturvaongelmia kartoitetaan useamman ryhmän toimesta. Esimerkiksi Helsingin kauppakamari, Keskuskauppakamari sekä sisäasiainministeriön yritysturvallisuusstrategiaryhmä työskentelevät yhdessä yritysten rikosturvallisuuden lisäämiseksi. Kansallisen tietoturvallisuusasioiden neuvottelukunta seuraa kiinnostuneena tätä työtä ja ehdottaa hyödynnettäväksi sitä yhteistyön puitteissa neuvottelukunnan työssä vuonna 2006.

Phishing eli kalastelu

Phishing on taloudellisesti hyödynnettävän tiedon, kuten verkkopankkitunnusten, luottokorttinumeroiden tai henkilötietojen laitonta hankkimista siten, että rikollinen pyrkii selvittämään sähköisen asioinnin tunnisteita tai maksuvälinetietoja kysymällä niitä tunnusten haltijalta palveluntarjoajan nimissä lähetetyllä väärennetyllä sähköpostiviestillä. Ongelma on tullut yleiseen tietoisuuteen vuonna 2005 erityisesti pankkien verkkosivuille kohdistetuilla hyökkäyksillä, joissa kuluttajaa on yritetty erehdyttää antamaan henkilökohtaiset pankkitunnuksensa väärien henkilöiden käyttöön.

Roskaposti

Roskasähköpostiviestien määrä on vähentynyt vuonna 2005 arviolta 25 prosenttia edellisen vuoden roskapostien määrästä. Näin ollen viestinnän hyödylliseen käyttöön jäävä verkon kapasiteetti on olennaisesti lisääntynyt. Roskapostin vähentymiseen ovat

vaikuttaneet muun muassa lainsäädännölliset keinot sähköisen viestinnän tietosuojalain mukaisesti sekä tekninen suodatus. Myös maailmanlaajuisesti roskapostiviestien suhteellinen määrä on hieman pienentynyt.

Työ, jota on määrätietoisesti tehty roskapostin vähentämiseksi, on selvästi tuottanut tulosta. Suomessa on saavutettu muuta maailmaa paremmat prosentuaaliset tulokset roskapostin torjunnassa. Vuonna 2003 Suomessa välitetyn viestinnän osuudesta 80 prosenttia oli roskapostia, vuonna 2004 roskapostin määrä oli pudonnut 45 prosenttiin ja vuonna 2005 se oli enää noin kolmannes välitetystä liikenteestä. Vastaavat ulkomaiset luvut olivat vuonna 2003 90 prosenttia, vuonna 2004 60 prosenttia sekä vuonna 2005 noin puolet kokonaisliikenteestä.

Haittaohjelmat ja älypuhelinvirukset

Vakoilu- ja haittaohjelmien pääsy kotikoneelle aiheuttaa internetin käyttöä haittaavia ongelmia siten, että haittaohjelmat hidastavat tietokoneen toimintaa sekä vievät tietokoneelta käyttökapasiteettia. Lisäksi haittaohjelmat saattavat häiritä internetin käyttöä myös siten, että ne ohjaavat käyttäjää tämän huomaamatta tietyille verkkosivuille, kuten mainossivustot sekä tai aikuisviihde. Suomessa on havaittu muutamia huomattavia haittaohjelmatartuntoja organisaatioiden sisäverkoissa. Yksittäisessä tartunnassa saastui jopa satoja tietojärjestelmiä. Kaikissa CERT-FI:n tietoon tulleissa tapauksessa tartuntareitti organisaatioon oli kannettava tietokone, joka saastui organisaation ulkopuolella ja kytkettiin saastuneena sisäverkkoon.

Mobiilihaittaohjelmatilanne on pysynyt toistaiseksi varsin rauhallisena. Haittaohjelmakirjoittajien kiinnostus on keskittynyt erityisesti Symbian-käyttöjärjestelmällä varustettuihin matkaviestinverkkojen päätelaitteisiin. Erityisiä riskialueita mobiilihaittaohjelmien leviämisen suhteen ovat suuret yleisötapahtumat.
Tämä ongelma on näkynyt vuonna 2005 erityisesti niin sanottujen älypuhelinten käyttöongelmien yhteydessä.

Ohjelmistohaavoittuvuudet

Ohjelmistohaavoittuvuudet ovat keskittyneet jonkinasteisesti selainohjelmistoihin. Haavoittuvuuksia on löydetty sekä Microsoft Internet Explorer (IE) että Mozilla-, Firefox- ja Netscapeselaimissa. Ongelmia on havaittu myös varmuuskopiointiohjelmissa. Koska varmuuskopio-ohjelmistot toimivat tietojärjestelmissä tyypillisesti pääkäyttäjän oikeuksilla, se tekee haavoittuvuuksista varsin vakavia. Ilmiöllä on pyrkimyksenä ohittaa virustorjuntaohjelmistot sekä palomuurit. Tämän vuoksi ohjelmistopäivitysten merkitys kasvaa tietoturvallisuudesta huolehtimisen osalta.

Langattomat lähiverkot (WLAN) ja niiden suojaaminen

Langattomien lähiverkkojen luvattomaan käyttöön, verkon puutteelliseen määrittelyyn, verkkoa vastaan suunnattaviin palvelunestohyökkäyksiin sekä verkkoliikenteen salakuunteluun ja muuttamiseen liittyviin on kiinnitetty huomiota muun muassa CERT-FI -tilannekatsauksissa. Langattomien WLAN-verkkojen väärinkäytökset ja yhteyksien salakuuntelu voidaan estää käyttämällä verkossa salausmenetelmää ja estämällä ulkopuolisilta pääsy verkkoon käyttäjien tunnistuksen avulla. Sekä yhteyden

salaamiseen että käyttäjien tunnistamiseen on useita vaihtoehtoisia ja toisiaan täydentäviä ratkaisuja, jotka saattavat jonkin verran vaihdella laitetoimittajakohtaisesti.

Tietoturva tilastoissa

Liikenne- ja viestintäministeriön teettämän selvityksen mukaisesti suomalaisten tietoturva-asioihin liittyvä osaaminen on vielä sellaisella tasolla, että läheskään kaikki tietokoneiden ja internetin käyttäjät eivät tunne tyypillisimpiä perusongelmia. Tutkimuksen mukaan 39 prosenttia internetin kotikäyttäjistä kokee omat tietoturvaan liittyvät tietonsa ja taitonsa riittäviksi tai erinomaisiksi. Jopa 10 prosenttia kokee, että heiltä ei löydy tämän tyyppistä osaamista. Tähän osuuteen tietoturvallisuuden lisäämisessä neuvottelukunnan työ pyrkii vastaamaan tietoturvatietoisuuden lisäämisellä. Pyrkimyksenä on luoda helppokäyttöiset ja kaikkien saavutettavissa olevat turvalliset palvelut, jotka toteuttavat arjen yhteiskunnan tavoitteet. Työkaluna on esimerkiksi Tietoturvapäivä. Myös Euroopan verkko- ja tietoturvaviraston työtä tietoisuuden lisäämiseksi seurataan aktiivisesti, jotta voitaisiin saavuttaa tietoturvatietoisuuden parhaat käytännöt.

Tutkimuksen mukaan 92 prosentilla internetin käyttäjistä on kotikoneellaan virustorjuntaohjelma. Palomuuri on asennettu 78 prosenttiin kotikoneista, mutta vakoilu- ja haittaohjelmien torjuntaohjelma on vain 36 prosentilla. 26 prosenttia vastaajista ei osannut kertoa, onko heidän kotitietokoneessaan vakoilu- tai haittaohjelmien torjuntaohjelmaa.

Virustartunnat ovat arkipäivää internetin käyttäjien keskuudessa. 44 prosenttia suomalaisista kotikoneista oli joskus saanut virustartunnan. 56 prosenttia käyttäjistä oli onnistunut poistamaan virustartunnan omatoimisesti tietokoneelta torjuntaohjelman avulla.

Kansallisen tietoturvallisuusasioiden neuvottelukunta

Liikenne- ja viestintäministeriö asetti kansallisen tietoturvallisuusasioiden neuvottelukunnan, jonka on tuettava kansallisen tietoturvallisuusstrategian periaatepäätöksen nojalla tehtyjä tavoitteita ja toimenpiteitä. Kansallisen tietoturvallisuusasioiden neuvottelukunnan tehtävänä on tukea tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista, seurata strategian toteutumista ja tehdä valtioneuvostolle ehdotuksia strategian päivittämisestä. Neuvottelukuntaan ja sen eri hankkeiden ohjausryhmiin on osallistunut lähes kaksisataa suomalaista alan toimijaa.

Neuvottelukunnan näkemykset toiminnastaan on esitelty edellä.

Tuire Saaripuu
pääsihteeri
ylitarkastaja
liikenne- ja viestintäministeriö
PL 31, 00230 Valtioneuvosto
puh. (09) 160 28305, 040 761 5406
etunimi.sukunimi@mintc.fi

1. TIETOTURVALLISET SÄHKÖISET PALVELUT

Tietoturvallisten sähköisten palveluiden kehittämisessä toimintaa ohjaavana ajatuksena on rohkaista palveluntarjoajia luomaan uusia tietoturvallisia palveluita helposti ja tehokkaasti, käyttäen laajasti digitaalisen sisällön monikanavaista jakelualustaa. Tavoitteena on edistää Arjen yhteiskunnan Ubiquitous-ajattelua ja hyödyntää aitoa verkkojen yhteiskäyttöä.

1.1. Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelma

Tavoite ja tausta

Liikenne- ja viestintäministeriö teetti vuoden 2003 lopussa esiselvityksen tietoturvallisuutta koskevan tutkimus- ja kehittämisohjelman mahdollisuuksista edistää suomalaisten tieto- ja viestintäalan yritysten kilpailukykyä ja toimintamahdollisuuksia.

Tietoturvaohjelman valmistelu käynnistettiin esiselvityksen johtopäätösten pohjalta loppukeväällä 2004. Esiselvitys- ja valmistelutyössä on kuultu suomalaisten tai Suomessa toimivien tieto- ja viestintäalan yritysten asiantuntijoita, liiketoiminnan kehittäjiä sekä yritysten johtohenkilöitä.

Helmikuussa 2005 käynnistyneen kaksivuotisen Luoti-ohjelman tavoitteena on edistää uusien monikanavaisten sähköisten palveluiden tietoturvaa ja niihin liittyvän toimintaympäristön -lainsäädännön, tutkimuksen ja koulutuksen - kehittymistä. Ohjelmassa luodaan näkemyksellisyyttä siitä, millaisia tietoturvaan liittyviä haasteita sähköisten palveluiden kehitystyö tulee lähivuosien aikana kohtaamaan, miten niihin tulisi varautua, millaisia ratkaisumahdollisuuksia on olemassa ja miten niitä tulisi kehittää. Ohjelman perimmäisenä tavoitteena on lisätä kuluttajien luottamusta uusia sähköisiä palveluita kohtaan.

Luoti-ohjelmassa tietoturvaa pyritään kehittämään käytännön palveluiden ja käyttötilanteiden kautta. Ohjelman tavoitteena on löytää kaupallisia pilottiprojekteja, joissa uusien sähköisten palveluiden tietoturvaa koskevia ratkaisuja ja toimintamalleja päästään viemään eteenpäin.

Vuonna 2005 palvelunkehitystoimintaa tarkasteltiin viihdepalveluiden näkökulmasta. Tässä työssä odotetaan syntyvän sellaista tietoa ja osaamista, jota voidaan hyödyntää myös muissa käyttöympäristöissä sekä julkisella että yksityisellä sektorilla. Ohjelman kuluessa arvioidaan erikseen mahdollisuutta laajentaa tarkastelua myös muihin käyttöympäristöihin.

Ohjelman keskeisimpinä toimijoina ovat tieto- ja viestintäalan yritykset ja niissä toimivat henkilöt. Liikenne- ja viestintäministeriön budjetti ohjelmalle on noin 400 000 €/vuosi.

Lisätietoa Luoti-ohjelmasta ja sen etenemisestä löytyy ohjelman verkkosivuilta www.luoti.fi. Ohjelman esiselvitys sekä valmistelun loppuraportti ovat saatavilla sähköisesti osoitteesta www.mintc.fi/tietoturvallisuusstrategia.

Käynnistettyjen toimien tilanne vuonna 2005 ja etenemistavoitteet vuonna 2006

Liikenne- ja viestintäministeriö on asettanut ohjelmalle ohjausryhmän. Ohjausryhmän tehtävänä on suunnata ohjelman toimintaa ja luoda edellytyksiä sen onnistumiselle. Ohjausryhmä määrittelee ohjelman tavoitteet ja niille sopivat mittarit sekä seuraa ohjelman tavoitteiden toteutumista. Ohjausryhmä on kokoontunut vuonna 2006 neljä kertaa.

Ohjelmaan potentiaalisesti osallistuville yrityksille ja medialle kohdennettu ohjelman käynnistystilaisuus pidettiin 18.3.2005 Säätytalolla. Paikalla oli noin 100 ohjelmasta kiinnostunutta kuulijaa.

Ohjelmalle on perustettu omat verkkosivut osoitteeseen: www.luoti.fi. Verkkosivuilla välitetään tietoa ohjelman toiminnasta ja tuloksista ja niiden välityksellä on mahdollisuus ilmoittautua ohjelmaan. Ilmoittautuneita on noin 160 henkilöä yli sadasta yrityksestä tai julkisen sektorin organisaatiosta. Näistä enemmistö on yritysten asiantuntijoita.

Ohjelmassa on teetetty erilliset taustaselvitykset sekä mobiilimaailman että digi-tv-ympäristön tietoturvauhkista ja niiden ratkaisumahdollisuuksista. Toukokuun 2005 alussa valmistuneet selvitykset on kirjoitettu palvelunkehittäjien näkökulmasta. Selvitykset teetettiin VTT:n ja Oulun yliopisto yhteistyönä. Lisäksi selvitysten kommentointiin osallistui joukko aktiivisia yrityksiä. Selvitykset on saatavilla ohjelman verkkosivuilta, joista suomenkielistä mobiili-selvitystä on ladattu 1 400 kertaa ja digi-tv-selvitystä 800 kertaa. Taustaselvitykset purettiin auki kesäkuun 2005 alussa järjestettävissä LUOTI-seminaareissa, joihin osallistui reilut 80 pääosin yritysten asiantuntijaa.

Luoti-ohjelma on valinnut kahdeksan tietoturvakonsultointia tarjoavaa yritystä ohjelman asiantuntijapooliin. Asiantuntijapoolin yrityksillä on mahdollisuus päästä tarjoamaan asiaintuntijapalveluita ohjelman pilottihankkeisiin ja/tai osallistumaan hankkeiden workshop-työskentelyyn.

Ohjelmassa on käynnistetty kesäkuun 2005 alussa avoin hankehaku. Ohjelmaan on valittu kolme uuden innovatiivisen viihdepalvelun kaupallistamiseen tähtäävää pilottihanketta, joissa tietoturvan käsittelylle löytyy selkeä rooli. Luoti-ohjelman pilottihankkeissa kehitetään digitaalisen sisällön monikanavaista jakelualustaa, vuorovaikutteista draamatelevisiosarjaa sekä yhteisöllistä verkkopeliä monikanavaympäristöön. Osa pilottihakkeissa tehtävästä työstä siirtyy vuodelle 2006. Pilottihankkeiden tulokset esitellään yhteisessä Luoti-seminaarissa huhti/toukokuussa 2006.

Vuonna 2006 ohjelmaan pyritään valitsemaan kolme pilottihanketta miltä tahansa toimialalta tai käyttöympäristöstä. Lisäksi ohjelmaan valitaan uusi 3-5 yrityksen tietoturva-asiantuntijapooli. Vuoden 2006 pilottihankkeiden tulokset esitellään Luoti-seminaarissa marraskuussa 2006.

Ohjelman lainsäädäntöryhmän työn suunnittelu on käynnistynyt loppusyksystä 2005 ja käytännön työ pyritään aloittamaan keväällä 2006. Lainsäädäntöryhmän tavoitteena on käytännöllisistä lähtökohdista ja pilottihankkeissa tehtyä työtä hyödyntäen arvioida, miten nykyinen lainsäädäntö vaikuttaa uusien sähköisten palveluiden kehitystoimintaan sekä miten lainsäädäntöä tulisi kehittää. Parhaillaan on käynnissä kilpailutus vertailututkimuksesta, jossa peilataan Suomen tietoturvaa koskevaa lainsäädäntöä tiettyjen EU-maiden vastaavaan.

Ohjelmassa teetetään 2006 aikana pienimuotoinen selvitys EU:n tutkimuksen 7. puiteohjelmien tarjoamista tutkimusyhteistyö- ja rahoitusmahdollisuuksista tietoturvan alalla. Ohjelman pilottihankkeissa kerätään tietoa siitä, millaisia tarpeita sähköisten palveluiden kehittäjillä on tietoturvaosaamisen suhteen. Erillistä tietoturvan tutkimukseen ja koulutukseen perehtyvää ryhmää ei ohjelmassa ole katsottu tarpeelliseksi perustaa.

Luoti-ohjelmassa tuotetaan vuoden 2006 aikana opas sähköisten palveluiden kehittäjille. Oppaan tarkoituksena on mahdollisimman kansankielisesti esittää, mitä palvelukehityksessä tulee ottaa huomioon, jotta tietoturvallisuus on riittävällä tasolla ratkaistu. Oppaassa kiinnitetään erityistä huomiota uusien ja monikanavaisten palveluiden tietoturvavaatimuksiin. Lisäksi oppaassa pyritään selvittämään, miten kuluttajien luottamusta sähköisiä palveluita kohtaan voidaan edistää. Ohjelman taustaselvityksissä ja pilottiprojekteissa syntyvä aineisto toimivat taustamateriaalina palvelunkehittäjän oppaan laadinnassa. Palvelunkehittäjän opas julkaistaan Luoti- ohjelman päätöstilaisuudessa joulukuussa 2006.

Ohjelmasta ja sen aktiviteeteista on viestitetty aktiivisesti ja ne ovat saaneet hyvin tilaa alan lehdistössä ja verkkomedioissa. Verkkosivustojen lataukset ovat aktiivikuukausina olleet noin 30 000–40 000 kertaa.

Arvio toimien vaikuttavuudesta hankkeeseen yhdistettävien ja tukihankkeiden kanssa vuonna 2005

Painopistehankkeen vaikuttavuus

Luoti-ohjelma lisää yritysten tietoisuutta tietoturvan roolista sähköisten palveluiden kehitystyössä. Ohjelma lisää näkemyksellisyyttä monikanavaisuuden (internet, digi-tv, mobiili) luomista tietoturvahaasteista ja niiden ratkaisumahdollisuuksista uusissa palvelunkehityshankkeissa. Ohjelmassa kehitetään käytännön hankkeiden avulla uutta toimintamallia, jossa tietoturva otetaan sähköisten palveluihin mukaan jo niiden kehittämisen alkuvaiheessa. Uusien toimintatapojen ja menetelmien uskotaan kehittävän tietoturvakonsultointia sekä lisäävän sähköisiä palveluita kehittävien yritysten osaamista ja kilpailukykyä. Pilottihankkeissa syntyvää tietämystä ja osaamista voidaan monistaa vastaaviin palvelunkehityshankkeisiin sekä eri toimialueille.

Luoti-ohjelma edistää verkostoitumista ja uusien kontaktien syntymistä alan keskeisiin toimijoihin. Koska ohjelma tavoittaa uusia sähköisiä palveluita kehittäviä keskeisiä tahoja, siinä luodut toimintamallit ja hyvät käytännöt voivat levittäytyä mm. alihankintaverkostojen kautta laajalti suomalaisiin yrityksiin. Ohjelma saattaa lainsäätäjien ja regulaattoreiden tietoon sähköisten palveluiden kehittäjien näkemyksiä tietoturvaa

ja uusia digitaalisia palveluita koskevan lainsäädännön kehittämistarpeita. Näitä näkemyksiä voidaan hyödyntää mm. uuden lainsäädännön valmistelussa.

Tukihankkeiden vaikuttavuus yhdessä painopisteen kanssa

Biometria-hanke raportoi tuloksistaan itsenäisesti yhdessä Sertifikaatit–hankkeen kanssa.

Yhdistettävien hankkeiden yhdistämisen aikataulu ja jo tehdyn työn sekä mukana olevien tahojen kytkeminen painopistehankkeen työhön

Luoti-ohjelma hyödyntää yhdistettävissä hankkeissa jo tehtyä työtä ja sen tuloksia. Ohjelmaan yhdistyneiden Luottamuksen ja tietoturvallisuuden merkitys uudessa taloudessa sekä Helppokäyttöisiä ja yhteensopivia tuotteita sekä innovatiivisia kehittämisalueita -hankkeiden tavoitteet ja työ sisältyvät sellaisenaan Luoti-ohjelmaan ja sen tavoitteisiin.

Lainsäädännön vaikutusarvioinnit ja Perusoikeuksien huomioonottaminen -hankkeissa mukana olevat tahot voivat osallistua Luoti-ohjelman lainsäädäntöryhmään ja sen valmisteluun.

Muut hankkeeseen osallistuneet henkilöt

Kimmo Lehtosalo
Luoti-ohjelman ohjelmapäällikkö
Eera Finland Oy
Itämerenkatu 5
00180 Helsinki
puh 0201 588 588
etunimi.sukunimi@eera.fi

Tuire Saaripuu
lainsäädäntöryhmän vastuuhenkilö
ylitarkastaja
liikenne- ja viestintäministeriö
PL 31, 00023 Valtioneuvosto
puh. (09) 160 28305, 040 761 5406
etunimi.sukunimi@mintc.fi

Ohjelman ohjausryhmä

Päivi Antikainen, liikenne- ja viestintäministeriö, *siht.*
Pauli Heikkilä / Sirpa Ojala, Digita Oy
Ari Hyppönen, F-Secure Oyj
Pirkko Jokinen, SWelcom Oy
Lotta Lautsuo, Starcut Ltd.
Kari Oksanen, Nordea Oyj
Kristiina Pietikäinen, liikenne- ja viestintäministeriö, *pj.*

Eero Silvennoinen, Tekes
Carina Stenvall, MTV Oy Interactive
Janne Uusilehto, Nokia Oyj
Teemupekka Virtanen, Teknillinen korkeakoulu
Janne Yli-Äyhö, TeliaSonera Oyj

Ohjelman työvaliokunta

Päivi Antikainen, liikenne- ja viestintäministeriö
Keith Bonnici, Tekes
Kimmo Lehtosalo, Eera Finland Oy
Kristiina Pietikäinen, liikenne- ja viestintäministeriö
Juhapekka Ristola, liikenne- ja viestintäministeriö
Tuire Saaripuu, liikenne- ja viestintäministeriö

1.2. Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -hanke

Tavoite ja tausta

Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -hankkeen keskeisenä tavoitteena on lisätä luottamusta biometrian käyttöön myös kaupallisissa sovelluksissa ja palveluissa. Luottamus on välttämätön edellytys biometrisen tunnistamisen yleistymisen kannalta. Biometrisessa tunnistamisessa käytettävien järjestelmien tietoturvasta huolehtiminen on olennainen tekijä näitä menetelmiä koskevan luottamuksen rakentamisessa. Palveluntarjoajat ja muut toimijat, jotka biometriaa hyödyntävät tarvitsevat selkeätä ja helposti omaksuttavaa tietoa siitä, mitä tietoturvaan liittyviä seikkoja niiden tulisi ottaa huomioon biometriaa hyödyntävissä palveluissaan ja järjestelmissään.

Luottamuksen edistämiseksi hankkeessa pyrittiin arvioimaan biometrisen tunnistamisen käyttöön liittyviä tietoturvakysymyksiä, keskeisimpiä riskejä ja ongelmia. Tietoturvakysymysten selvittämisellä ja analysoinnilla pyritään edistämään suomalaisten yritysten liiketoimintamahdollisuuksia ja biometrista tunnistamista hyödyntävää palvelukehitystä. Hankkeen näkökulmana oli yksityisen sektorin kaupalliset palvelut ja sovellukset. Viranomaistarpeisiin käytettävät sovellukset eivät siten kuuluneet hankkeen piiriin.

Tavoitteena oli tuottaa työryhmän suositusten ja näkemysten kautta helposti omaksuttavaa, käytännön läheistä ja riittävän yleisen tason tietoa biometrisen tunnistamisen edellyttämästä tietoturvasta alan toimijoille, ja toisaalta muodostaa selkeä näkemys jatkotoimenpiteiden tarpeesta ja sisällöstä voimassa olevan lainsäädännön kehittämistarpeiden arviointia varten. Hankkeen toteuttamisella pyritään omalta osaltaan vaikuttamaan myös siihen, että biometrisessa tunnistamisessa otetaan Suomessa huomioon perustuslain turvaamat tietoturvaan ja yksityisyyden suojaan liittyvät oikeudet ja varmistetaan biometriaan liittyvien tietoturvariskien riittävä hallinta.

Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -hanke tukee strategian painopistehankkeista hanketta LUOTI – Luottamus ja tietoturva sähköisissä palveluissa.

Työryhmä kokoontui vuoden 2005 aikana yhteensä kuusi kertaa.

Tilanne vuonna 2005

Hankkeessa toteutettiin selvitys, jossa arvioitiin ja koottiin yhteen yksityisyyden suojan toteutumiseksi keskeisimmät tietoturvavaatimukset. Selvityksessä pyrittiin arvioimaan vaatimuksia lähtien muutamasta erilaisesta case–tyyppisestä palvelutyyppikuvauksesta, ns. järjestelmätason tietoturvavaatimuksista sekä eri biometrisen tunnistamisen menetelmien ominaispiirteistä yksityisyyden suojan ja tietoturvan osalta, ja pyrittiin näiden pohjalta muodostamaan kokonaisuus biometrisen tunnistamisen tietoturvavaatimuksista yksityisyyden suojan näkökulmasta. Tietoturvavaatimusten arvioinnissa pidettiin lähtökohtana voimassa olevan lainsäädännön asettamia vaatimuksia tietoturvan toteuttamisen osalta.

Selvitykseen sisältyy oheistus biometrista tunnistamista hyödyntäville palveluntarjoajille tietoturvan ja yksityisyyden suojan osalta. Laadittu selvitys ”Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja” julkaistiin liikenne- ja viestintäministeriön Julkaisuja-sarjassa 80/2005.

Nykyinen henkilötietojen käsittelyä koskeva sääntely on joustavaa eikä estä biometriaa hyödyntävien palvelujen kehittämistä ja käyttöönottoa. Voimassa oleva sääntely on toisaalta yleisluonteista ja perustuu pitkälti erilaisten periaatteiden soveltamiseen, mikä vaikeuttaa lainsäädännön käytännön soveltamista ja tulkintaa. Nimenomaista biometriaa koskevaa sääntelyä ei ole.

Biometria tarjoaa mahdollisuuksia, mutta siihen liittyy sen kaltaisia yksityisyyden suojaan liittyviä riskejä, että voimassa oleva sääntely ei tarjoa riittäviä eväitä palvelujen toteuttamiseen ja biometrian hyödyntämiseen. Palvelujen kehittäjien on käytännössä hyvin vaikeaa päätellä voimassa olevasta sääntelystä, miten ja mihin biometriaa saa käyttää ja miten biometriaa hyödyntävät palvelut tulisi toteuttaa. Tästä syystä voimassa oleva lainsäädäntö ei biometrian kohdalla kykene täyttämään myöskään tehtäväänsä biometria-tietojen kohteiden yksityisyyden suojaamiseksi riittävällä tavalla. Näin ollen on selvää, että on olemassa tarve laatia biometrista tunnistamista koskevat perustason oikeudelliset säännökset.

Biometriaa koskevan sääntelyn tarkempi toteuttamistapa ja sisältö tulisi kuitenkin arvioida erikseen. Biometriaa koskevan sääntelyn osalta tulisi etsiä sellainen minimitaso, jolla turvattaisiin yksityisyyden suojan huomioon ottaminen biometrisen tunnistamisen kohdalla Suomessa. Sääntelyn avulla voitaisiin karsia pahimmat epäkohdat, jotka saattaisivat ilman esitetyn kaltaista kontrollia viedä biometriaa hyödyntäviä palveluja ja ylipäätään näitä menetelmiä koskevan luottamuksen pahimmassa tapauksessa peruuttamattomasti.

Sääntelystä olisi hyötyä suomalaisille palvelukehittäjille, koska se lisäisi selkeiden pelisääntöjen ja mahdollisen viranomaisvalvonnan kautta luottamusta palveluihin, rajoittamatta kuitenkaan uusien innovaatioiden ja palvelumallien kehittämistä. Tietoturvastrategian biometriahankkeen kantavana ajatuksena on ollut nimenomaan biometriaa hyödyntävän palvelukehityksen edistäminen. Yksityisyyden suojaaminen ja palveluntarjoajien intressit eivät ole vastakkaisia, vaan päinvastoin palvelujen menestyminen edellyttää välttämättä riittävän määrän luottamusta, ja tässä tarkoituksessa nimenomaan tietoturvasta huolehtimista mm. yksityisyyden suojaamiseksi. Tietoturvan ja yksityisyyden suojaaminen on tiettyyn rajaan asti nimenomaan biometriaa hyödyntävien tahojen etujen mukaista ja intressissä.

Sääntelyllä annettaisiin selkeä viesti palvelukehittäjille, että biometriaa saa käyttää, mutta sitä tulee käyttää harkiten ja suunnitelmallisesti sekä riittävät tietoturvaratkaisut huomioonottaen. Pelisääntöjen selkeys edistäisi suomalaisten palvelukehittäjien toimintamahdollisuuksia verrattuna muiden maiden yrityksiin ja antaisi kotimaisille toimijoille selkeän ajallisen etumatkan.

Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -työryhmä esittää, että liikenne- ja viestintäministeriö käynnistäisi mahdollisimman pian erillisen hankkeen biometrisen tunnistamisen sääntelyntarpeen arvioimiseksi ja tarvittavien oikeudellisten säännösten laatimiseksi sähköisistä allekirjoituksista annettuun lakiin

14/2003. Hankkeen tulisi keskittyä yksityisen sektorin palveluihin ja laadittava sääntely tulisi rajata siten, että viranomaisten käyttötarpeet jäisivät sääntelyn ulkopuolelle.

Hankkeessa tulisi yllämainittujen kysymysten lisäksi arvioida, miltä osin ns. passiivisesta biometrisestä tunnistamisesta, eli ilman tunnistettavan eri toimenpiteitä tapahtuvasta tunnistamisesta, joka voi tapahtua myös tunnistettavien kohteiden tietämättä, tulisi laatia erillistä oikeudellista sääntelyä. Biometriseen tunnistamiseen liittyvän monenlaisen kameravalvonnan ja erilaisen teknisen valvonnan lisääntyminen sekä tähän käytettävien teknisten ratkaisujen kehittyminen edellyttää myös näiden asioiden arviointia oikeudelliselta kannalta. Arvioinnissa tulisi ottaa huomioon tunnistettavien itsemääräämisoikeuden toteutuminen ja arvioida esimerkiksi informointivelvollisuuden ja suostumuksen merkitystä tämänkaltaisissa sovelluksissa.

Hankkeessa syntyvän tiedon ja ymmärryksen levittämisessä pyritään hyödyntämään mahdollisimman pitkälle kansallisen tietoturvastrategian ja Luoti-hankkeen resursseja. Molemmilla hankkeilla on erilliset verkkosivut ja mm. Luoti-hankkeen tiedotteet ja seminaarit tavoittavat varsin laajan joukon sähköisten palvelujen kehittäjiä.

Vaikutukset ja muutostarpeet

Hankkeessa on pyritty lisäämään tietämystä biometrisen tunnistamisen tietoturvavaatimusten ja biometriaan liittyvien yksityisyydensuoja -kysymysten osalta. Hanke päättyy alkuperäisen aikataulun mukaisesti vuoden 2005 lopussa ja työryhmä laati loppuraporttinsa marraskuussa 2005. Raportti ja edellä mainittu selvitys ovat molemmat saatavilla tietoturvastrategian verkkosivuilta osoitteesta: www.mintc.fi/tietoturvallisuusstrategia. Työryhmän esittämän lainsäädäntöä koskevan jatkotyön osalta tullaan keväällä 2006 arvioimaan, tullaanko työtä tältä osin jatkamaan tietoturvastrategian yhteydessä vai strategiasta erillisenä hankkeena.

Juha Perttula
neuvotteleva virkamies
liikenne- ja viestintäministeriö
PL 31, 00023 VALTIONEUVOSTO
puh. (09) 160 28617
etunimi.sukunimi@mintc.fi

Muut hankkeeseen osallistuneet henkilöt:
Ailisto Heikki, VTT
Karvonen Kaarlo, Finnair Oyj
Karppinen Lauri, Tietosuojavaltuutetun toimisto
Kivinen Tuomas, Nordea Pankki Suomi Oyj
Rakshit Tommi, Sisäasiainministeriö
Saapunki Ari, Aldata Solution Finland Oy
Pösö Päivi, Väestörekisterikeskus (hankkeen alkuvaiheessa Tuire Saaripuu, Väestörekisterikeskus)
Salminen Helvi, Setec Oy

1.3. Lainsäädäntökatsaus

Tavoite ja tausta

Kansallisen tietoturvallisuusasioiden neuvottelukunnan työalueet lainsäädännön vaikutusarvioinnit sekä perusoikeuksien huomioonottaminen olivat vuoden 2004 neuvottelukunnan sihteeristön painopistealueina. Hankeryhmät saivat raporttinsa valmiiksi joulukuussa 2004. Raportit ovat saatavilla sähköisesti osoitteesta www.mintc.fi/tietoturvallisuusstrategia.

Lainsäädännön vaikutusarvioinnit -hankkeen tavoitteena on arvioida säännöllisesti tietoturvallisuuteen ja tietoyhteiskuntaan liittyvän lainsäädännön ja kansainvälisten sopimusten vaikutuksia viestintäpalvelujen, verkkopankkipalvelujen, sähköisten tunnistamispalvelujen, sähköisen kaupankäynnin ja hallinnon sähköisten asiointipalveluiden kehittämisen ja käytön kannalta. Oikeudellinen tietoturvallisuuden tutkimus on varsin uusi ilmiö.

Kansalliseen lainsäädäntöön on viime aikoina tullut huomattavia määriä tietoturvallisuuslainsäädännöksi luokiteltavaa sääntelyä. Vaikka sääntely ei suoraan viittaa tietoturva–sanaan, erityisesti yksityisyyden suojaa koskeva ja sitä kautta myös tietoturvallisuutta koskevaa lainsäädäntöä on runsaasti.

Hankeryhmä kartoitti erillisen selvityksen pohjalta, miten hyvin tietoturvallisuutta koskeva lainsäädäntö palvelee yrityksiä ja muita yhteisöjä tietoturvallisuuteen liittyvien kysymysten ja ongelmien kanssa ja kuinka hyvin tietoturvallisuutta koskevaa lainsäädäntöä tunnetaan. Selvityksen päämääränä oli saada tietoa tietoa alan toimijoilta siitä, miten he näkevät lainsäädännön pureutuvan jokapäiväisessä työssä tietoturvallisuuden parissa eli mitkä ovat yritysten tämänhetkiset tietoturvaongelmat ja uhat sekä, millä tavoin voimassaoleva lainsäädäntö on vaikuttanut yrityksen tietoturvallisuutta koskeviin ratkaisuihin.

Perusoikeuksien merkityksen kasvu on johtanut uuteen tarkasteluun sen, toteutuvatko perusoikeudet uuden informaatioinfrastruktuurin puitteissa ja onko uuden normiston luominen tarpeen uutta digitaalista toimintaympäristöä varten. Tarkastelun kohteena ovat erityisesti sananvapauden, viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen. Perusoikeuksien toteutumista tarkastellaan erityisesti tietoturvallisuutta koskevissa säännöksissä, viranomaisohjeissa, standardeissa sekä viranomaisten sähköisissä asiointipalveluissa.

Perusoikeuksien huomioon ottaminen -työryhmä on käynnistänyt kaksi selvitystyötä, joissa kartoitetaan, miten sananvapaus, yksityiselämän suoja ja muut perusoikeudet huomioidaan tietoyhteiskunnan palveluita, sähköistä viestintää ja turvallisuutta käsittelevissä säännöksissä, viranomaisohjeissa sekä viranomaisten sähköisissä asiointipalveluissa. Toinen käynnistetyistä selvityksistä pureutuu konkreettiseen tietoturvallisuuslainsäädännön analyysiin perusoikeuksien kannalta, kun toinen puolestaan lähestyy asiaa teoreettisemmalla viitekehyksellä. Perusoikeuksien vaikutusta tietoturvallisuuden alalla ei ole aiemmin tutkittu. Asian haasteellisuutta lisää se, että perusoikeuksien ja samalla tietoturvallisuuden asiantuntijoita on maassamme erittäin vähän.

Hankeryhmän alkuperäisenä tarkastelun kohteena oli myös standardien selvittäminen perusoikeuksien toteutumisen kannalta. Hankeryhmä huomasi, että standardien käsittely on oma iso kokonaisuutensa, minkä vuoksi ne jätettiin perusoikeusselvityksestä pois ja niiden käsittely siirrettiin Sertifikaatit-hankkeen yhteyteen.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Lainsäädännön vaikutusarviointi jatkaa työtään LUOTI-hankkeen yhteydessä. Hankkeen tavoitteena on konkretisoida, mistä tietoturvallisuuslainsäädännön isoimmat haasteet tietoturvallisuuden alalla ovat. Samalla voidaan kartoittaa isoimmat kysymykset, joihin pyritään hankkeen yhteydessä hakemaan vastaukset. Näin voidaan saavuttaa tasapaino lainsäädännön ja tietoturvatoiminnan välillä. Liikenne- ja viestintäministeriö on lähtenyt selvittämään Suomen yrityselämän kannalta keskeisimpiä tietoturvallisuuteen liittyviä säännöksiä palvelunkehittäjän ja loppukäyttäjän näkökulmasta. Lainsäädäntöselvitys on tarkoitus kohdentaa Suomeen, Ruotsiin, Norjaan, Tanskaan, Saksaan, Venäjään ja Viroon.

Vaikutukset ja muutostarpeet

Työryhmät eivät ole kokoontuneet raporttien valmistumisen jälkeen. Työryhmien raportit ovat valmistuneet joulukuussa 2004 ja ne ovat saatavilla sähköisesti osoitteesta www.mintc.fi/tietoturvallisuusstrategia.

Hankkeen vastuusihteeri on vuonna 2004 ollut neuvotteleva virkamies Sanna Helopuro liikenne- ja viestintäministeriöstä sekä erityisasiantuntija Kirsi Miettinen liikenne- ja viestintäministeriöstä.

Tuire Saaripuu
pääsihteeri
ylitarkastaja
liikenne- ja viestintäministeriö
PL 31, 00230 Valtioneuvosto
puh. (09) 160 28305040 761 5406
etunimi.sukunimi@mintc.fi

2. KANSALLINEN TIETOTURVATILANNEKUVA

Tavoitteena on tunnistaa tietoturvallisuutta vaarantavat uhkatekijät ja jakaa asiallista ja tietoturvallisuusasioihin keskittynyttä oikeaa tietoa kuluttajille, organisaatioille ja yrityksille. Painopisteen keskeinen toiminta-alue on kriittinen infrastruktuuri. Uhkakuvilla pelottelua on vältettävä ja alan toimijoita on rohkaista puhumaan oikeista asioista oikealle yleisölle niin, että sähköisen viestinnän tuomat edut voidaan hyödyntää täysimääräisesti kuitenkin välttäen siihen liittyvät rikolliset ja haitalliset ilmiöt.

2.1. Kansallinen tietoturvallisuusriskien tilannekuva

Tavoite ja tausta

Hankkeen tavoitteena on luoda tarkoituksenmukainen kansallinen tietoturvallisuusriskien tilannekuva, jota ylläpidetään Viestintävirastossa, päivittää sitä jatkuvasti ja huolehtia siitä, että tilannekuva on keskeisten toimijoiden käytössä.

Tilannekuvan tulee olla ajantasainen ja antaa toimijoille tietoa tietoturvallisuuden kehityksestä ja ajankohtaisista uhkista. Tilannekuvan tulee palvella osaltaan asiakaskuntaa päätöksenteossa tietoturvallisuusratkaisujen toteuttamisessa. Tietoturvallisuuden tilannekuvan tavoitteena on auttaa eri asiakassegmenttejä vastaamaan tietoturvallisuuteen liittyviin uhkiin sekä palvella tietoturvallisuuskulttuurin kehittymistä ja seurantaa. Tavoitteena on tietoturvallisuuden kokonaiskuvan näkeminen ennen ongelmatilanteita.

Tavoitteena on myös levittää tietoa eri toimialoja koskevista ongelmista laajempaan tietoisuuteen ongelmatilanteiden välttämiseksi – useat toiminnot ovat hyvin riippuvaisia toisistaan. Tavoitteena on muodostaa tilannekuva sekä dynaamisesti että staattisesti. Tilannekuvan jakelusta on huolehdittava useita eri kanavia käyttäen ja myös media huomioiden. Yhteistoiminta tilannekuvan luomisen ja jakelun osalta on tarkoitus toimia sekä normaali- että poikkeusoloissa. Erityinen painopiste tilannekuvan muodostamisessa on sähköisen viestinnän toimivuuden ja viestintäverkkojen tietoturvallisuustilanteen osalta. Lisäksi uhkat kriittisen infrastruktuurin osalta ovat tärkeässä asemassa.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Kansallisena CERT-toimijana Viestintäviraston CERT-FI ryhmä on muodostanut kansallista tietoturvallisuusriskien tilannekuvaa vuoden 2002 alusta lähtien. Tämän tilannekuvan CERT-FI on koonnut eri tietolähteiden perusteella, joista esimerkkeinä voidaan tuoda esille mm. CERT-FI-ryhmälle ilmoitetut tietoturvaloukkaustapaukset ja niiden yritykset sekä julkiset ja ei julkiset postituslistat ja foorumit, joissa käsitellään mm. ohjelmistohaavoittuvuuksiin sekä haittaohjelmiin liittyviä asioita. Tätä eri lähteistä muodostettua tietoturvallisuusriskien tilannekuvaa on raportoitu eri tahoille mm. CERT-FI:n julkaisemien varoitusten ja ohjeiden muodossa. Julkaisukanavina ovat toimineet muun muassa Viestintäviraston www-sivusto, postituslistapalvelu sekä YLE:n teksti-tv. Kansallisten tietoverkkojen toimintaa vaarantavista sekä loppukäyttäjiä koskettavista uhkista Viestintäviraston CERT-FI on julkaissut myös lehdistötiedotteita.

Työryhmätyöskentelyn seurauksena Viestintäviraston prosesseja on tehostettu toimivan ja kaikkia osapuolia palvelevan tietoturvallisuusriskien tilannekuvan muodostamiseksi ja jakelemiseksi. Tilannekuvaprosessin kehittämiseksi tehty tutkimustyö on saatu päätökseen ja seuraavana työvaiheena on käynnistetty tietojen keräämiseen ja julkaisuun liittyvä automatisointihanke. Tilannekuvan julkaisun osalta merkittävin käynnistynyt hanke on julkaisujärjestelmän määrittely ja toteutus yhdistettynä viraston www-sivuston uusimiseen.

Dynaamisen tilannekuvatiedon jakelua on tehostettu CERT-FI:n www-sivuston välityksellä "tietoturva nyt" -osion muodossa sekä omien, teknisten tilannekuvan muodostamiseen liittyvien tietojärjestelmien määritys- ja testaustyön avulla. Tietoturvallisuuden dynaamisen tilannekuvatiedon jakelua on tehostettu myös ottamalla käyttöön RSS-feed -kanavat CERT-FI:n julkaisemien varoitusten ja tietoturva nyt -osion osalta sekä SMS-varoituspalvelut. Tietoturvauhkatilanteen kehittyminen ja uhkatilanteiden nopeus edellyttää jakelukanavien laajentamista myös mobiiliviestintään. Viranomaisyhteyksien reaaliaikaisen ylläpidon osalta on otettu käyttöön salaava videoneuvottelujärjestelmä sekä Virve-puhelimet. Virve-puhelimien puheryhmien hallinnointiin ja käyttöpaikan muodostamiseen on hankittu tarvittavat laitteet ja ohjelmistot.

Tilannekuvatiedon jakelu on käynnistetty myös Viestintäviraston www-sivuilla julkaistavan tilannekatsauksen muodossa. Tilannekatsauksessa tarkastellaan edellisen vuosineljänneksen tai vuoden aikana esille tulleita tietoturvallisuuteen vaikuttavia asioita, kuten haittaohjelmia ja niiden vaikutuksia Suomessa, roskapostitukseen liittyviä ilmiöitä, ongelmatietojärjestelmien lukumääriä sekä tietomurtoihin ja haavoittuvuuksiin liittyvää kehitystä. Tilannekatsauksessa analysoidaan myös seuraavan vuosineljänneksen aikana tietoturvan tulevaisuuden näkymiä. Tieto ilmestyneestä tilannekatsauksesta toimitetaan tiedotteena myös lehdistölle. Tilannekuvakatsausten osalta Viestintävirasto tuottaa myös erillistä valtionjohdon turvallisuustilannekuvaa.

Tietoturvallisuuden tilannekuvan muodostamisen osalta työryhmätyöskentely on saavuttanut pisteen jossa uusia kehityskohteita tai yhteistyötarpeita ei työryhmätoiminnan muodossa ole nähtävissä. Vuonna 2006 hanke jatkuu Viestintäviraston normaalina tietoturvatyötä edistävänä projektina käynnistettyjen kehittämishankkeiden eteenpäin saattamiseksi. Käynnistettyjen kehityshankkeiden loppuvaiheessa on myös huolehdittava tilannekuvatiedon markkinoinnista ja tunnettuuden lisäämisestä.

Vaikutukset ja muutostarpeet

Kansallisen tietoturvallisuusriskien tilannekuva -hankkeen vaikutukset näkyvät eritoten tietoturvallisuuden tietoisuuden kasvuna ja tätä kautta kansallisen tietoturvallisuuskulttuurin kehittymisenä. Yksittäisenä esimerkkinä tietoisuuden tasosta voidaan mainita Suomeen kohdistuvien phishing-hyökkäysten ennakointi Viestintäviraston tilannekuvaraporteissa sekä uuden uhkan välttäminen myös kuluttajarajapinnassa. Kun tietoturvallisuuden tilannekuvaa kyetään viestimään eri asiakassegmenteille tehokkaasti ja heidän tarpeidensa mukaisesti, kyetään tietoturvallisuutta vaarantavia uhkatilanteita välttämään oikein tehtyjen ja tehokkaasti ajoitettujen vastatoimien avulla kaikissa asiakassegmenteissä aina teleyrityksistä kuluttaja-asiakkaisiin. Vika- ja häiriötilanteisiin liittyviä ongelmatilanteita kyetään myös tehokkaammin hallitsemaan ja riski toiminnan

keskeytymiseen pienenee. Kriittiseen infrastruktuuriin kohdistuvia uhkatilanteita kyetään myös paremmin havaitsemaan ja hallitsemaan. Hankkeella on myös selviä vaikutuksia tietoturvallisuusyhteistyön, kilpailukyvyn, toimintamahdollisuuksien sekä riskien hallinnan osa-alueilla, sillä kansallinen tietoturvallisuusriskien tilannekuva palvelee tehokkaasti myös näitä osa-alueita.

Oikean ja oikea-aikaisen tilannekuvatiedon avulla voidaan ennaltaehkäistä tai rajoittaa tietoturvallisuutta uhkaavia tilanteita. Hankkeen tuloksena tuotetaan mahdollisimman tarkkaa tilannekuvatietoa eri asiakassegmenteille tietoturvauhkien analysoimiseksi. Uhkista aiheutuvat tietoturvallisuusriskit on aina arvioitava eri tahojen toimesta itse pitäen mielessä kunkin eri tahon toiminnan jatkuvuudelle kriittiset toiminteet. Tietoturvallisuusriskien tilannekuvan tehokkaasta muodostamisesta ja jakelusta huolimatta on eri tahojen aina itse tiedostettava ne uhkatekijät, jotka ovat kriittisiä eri tahojen toiminnan jatkuvuudelle. Tilannekuvan on tarkoitus palvella näiden uhkatekijöiden havaitsemista, mutta ei tunnistaa niitä eri toimijoiden puolesta.

Kehitystyön on oltava jatkuvaa Viestintäviraston tietoturvatilannekuvan kehitystyötä. Tavoitteena on edelleen kehittää yhteistyötä eri toimijoiden kanssa sekä tehostaa tilannekuvatiedon muodostamista ja jakelua.

Timo Lehtimäki
johtaja
Viestintävirasto
PL 313, 00181 Helsinki
puh. (09) 6966 815, 050 514 8286
etunimi.sukunimi@ficora.fi

Muut hankkeeseen osallistuneet henkilöt

Arnell Jani, Viestintävirasto
Hakola Tuomo, Ficix
Kajantie Sari, Keskusrikospoliisi
Kuparinen Veli-Pekka, Huoltovarmuuskeskus
Perttula Juha, liikenne- ja viestintäministeriö
Rintanen Terho, puolustusvoimat
Viitasaari Mikko, TeliaSonera Finland Oyj

2.2. Kriittisen infrastruktuurin tietoturvallisuusjaosto

Tavoite ja tausta

Kriittisen infrastruktuurin tietoturvallisuusjaoston tavoitteena on alueen yhteistyön tehostaminen. Jaoston tehtävänä on kartoittaa kriittisen infrastruktuurin toimijat ja keskeiset toimenpiteet tietoturvallisuuden ja yhteistyön lisäämiseksi. Tavoitteena on lisätä proaktiivista toimintaa, mutta toisaalta turvata liiketoiminnan jatkuvuus myös häiriöiden kohdatessa. Tavoitteena on luoda yhteistyö toimijoiden kesken tietoturvatietoisuuden lisäämiseksi, parhaiden käytäntöjen luomiseksi ja niiden levittämiseksi. Yhteiskunnan toimivuuden kannalta kriittisten toimijoiden tietoturvallisuudesta huolehtimalla voidaan merkittävästi lisätä yhteiskunnan toimivuutta erilaisissa häiriötilanteissa ja siten lisätä luottamusta yhteiskunnan toimivuuteen. Sähkönjakelun ja sähköisen viestinnän voimakkaan riippuvuussuhteen vuoksi yhtenä tavoitteena on hallita teknologiariskien vaikutuksia viestintäpalveluihin ja sähkönjakeluun sekä laatia toimenpide-ehdotuksia. Jaoston tavoitteena on myös Viestintäviraston CERT-toiminnan kehittäminen paremmin kriittistä infrastruktuuria palvelevaksi.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Jaoston toiminta on hyvin pitkäjänteistä johtuen laajasta ja monimutkaisesta tehtäväkentästä. Toimijoiden ja toiminnan kartoituksen osalta on tullut voimakkaasti esille toiminnan laajuus - jo nykyisellään toimintaa ja yhteistyötä on monella taholla olemassa. Kansainvälinen yhteistyö on koettu välttämättömäksi ongelmien globaalin luonteen vuoksi. Yhteistyön osalta Suomi on mukana NISCC:n (National Infrastructure Security Coordination Centre) CIIP listalla, jossa hakemistoon kerätään eri maiden kriittisen infrastruktuurin vastuutahojen yhteystiedot. Yhteisten osa-alueiden listaa laajennetaan kattamaan mm. toiminnanohjausjärjestelmät ja standardointi. Tiedonvaihtokanavat ovat kansainvälisellä tasolla vahvistumassa, ja myös EU:n toimet kriittisen infrastruktuurin suojelemiseksi ovat jaoston seurannassa. Jaoston kanta on erityisen positiivinen näitä hankkeita kohtaan. Euroopan tasolla on voimakkaita merkkejä toimien suuntaamiseksi terrorismin torjuntaan - kriittisen infrastruktuurin turvaamiseksi tulee kuitenkin korostuneesti tuoda esille toimien ulottaminen laajemmaksi esimerkiksi tietoverkkouhkien torjuntaan.

Toimijoiden ja toimintojen kartoitusta on tehty kansallisesti Huoltovarmuuskeskuksen kontaktien perusteella - tärkeysluokiteltuihin yrityksiin liittyvä kartoitustyö on jatkuvaa. Työn tuloksina saadaan ajantasainen kontaktilista tietoturvallisuusalueen tietojen vaihtoon. Kansainvälisen vertailukohdan osalta on tehty Huoltovarmuuskeskuksen toimesta selvitystyö. Raportissa tarkastellaan, miten eri länsimaat ovat määritelleet ja luokitelleet kriittisen infrastruktuurinsa, mitä suunnitelmia on sen turvaamiseksi sekä mitkä tekijät ovat vaikuttaneet suunnitelmien kehittämiseen. Tavoitteena on selventää kriittisen infrastruktuurin käsitettä, luoda yleiskuva suunnitelmista, joita eri maissa on tehty kriittisen infrastruktuurin turvaamiseksi, sekä selvittää miksi nämä eroavat toisistaan. Kriittistä tietoteknistä infrastruktuuria (Critical Information Infrastructure, CIIP) käsitellään osittain erikseen johtuen sen keskeisestä asemasta muiden infrastruktuurien toiminnalle.

Viestintäviraston CERT-toimintaa pyritään kehittämään myös kriittisen infrastruktuurin alueella. CERT-FI-ryhmän yhdelle tekniselle asiantuntijalle on allokoitu omaksi vastuualueeksi kriittisen infrastruktuurin toimijoiden kenttä. Haavoittuvuuskoordinaatio on toiminta-alue, jota Viestintävirastossa pyritään kehittämään paremmin kriittistä infrastruktuuria palvelevaksi. Toimijoille on tarve jakaa konkreettista tietoa esimerkiksi aluetta koskevista haavoittuvuuksista ja ennakkotiedoista haavoittuvuuksiin liittyen. Tietoturvauhkatilanteen kehittyminen ja uhkatilanteiden nopeus edellyttää jakelukanavien laajentamista mobiiliviestintään myös kriittisen infrastruktuurin järjestelmien osalta. Viestintävirasto on ottanut käyttöön palvelun, joka mahdollistaa varoituksen tilaamisen omakustannushintaan tekstiviestipalveluna. Viranomaisyhteyksien reaaliaikaisen ylläpidon osalta on otettu käyttöön salaava videoneuvottelujärjestelmä sekä Virve-puhelimet. Virve-puhelimien puheryhmien hallinnointiin ja käyttöpaikan muodostamiseen on hankittu tarvittavat laitteet ja ohjelmistot.

Kehitystyö yhteistyön lisäämiseksi ja tiedon jakamiseksi on myös käynnistynyt Viestintävirastossa. Tarkoituksena on uudistaa viraston www-sivusto ja samalla perustaa myös erillinen CIP-osio. Sivuilla esitetään valikoidusti esim. parhaita käytäntöjä, erilaisia tarkistustemplateja ja tietoturvaohjeita. Kriittisen infrastruktuurin tietojärjestelmiä uhkaavat samantyyppiset uhat kuin muitakin tietojärjestelmiä riippuen mm. niissä käytettävistä ohjelmistoista ja palveluista. Uhat liittyvät usein ohjelmistohaavoittuvuuksiin, joita hyödyntämällä mahdollinen hyökkääjä voi kohdistaa kohdejärjestelmään ei toivottuja toimia, joita voivat mm. olla tietomurrot ja palvelunestohyökkäykset. Palvelunestohyökkäyksillä voidaan hyökkääjän toimesta pyrkiä lamauttamaan elintärkeitä tietojärjestelmiä, joko kohdistamalla hyökkäys suoraan kohdejärjestelmään tai siihen tietoverkkoon tai tietoverkon osaan, johon kriittisen infrastruktuurin tietojärjestelmä on kytketty. Kriittisen infrastruktuurin tietojärjestelmien turvaamisessa on otettava huomioon sekä välittömät että välilliset uhat ja se, miten näitä molempia uhkatyyppejä vastaan voidaan varautua.

Vaikutukset ja muutostarpeet

Jaosto on toiminut yhteistyö- ja tiedonjakokanavana välittäen ajankohtaista tietoa ja parhaita käytäntöjä alueen toimijoille. Tätä kehitystä on syytä jatkaa siten, että jaostosta muodostuu yhteistyökanava ja parhaiden käytäntöjen jakoon soveltuva foorumi kriittisen infrastruktuurin toimijoille. Muutosten osalta merkittävin organisatorinen vaikutus on jaoston toimintaan sulautuvilla hankkeilla (tietoturvariskien arviointi ja tietoturvahaavoittuvuuksien analysointimenetelmät). Sulautuvat hankkeet tulevat toimimaan alaryhminä ja ne palvelevat hyvin jaoston tarkoitusta ja kohdeorganisaatioita. Työtä on jatkossa tarkoitus organisoida siten, että jaosto muodostaa alaryhmiä pienempien asiakokonaisuuksien hoitamiseksi tai vaihtoehtoisesti jaosto esittää toimenpide-ehdotuksia olemassa oleville organisaatioille havaittujen tarpeiden osalta. Jaoston itsensä tehtävänä on kartoittaa yhteistyötarpeita ja kriittisiä kehittämiskohteita sekä toimia asettamiensa alatyöryhmien ja hankkeiden ohjaajana. Tällaisista hankkeista voidaan mainita esimerkkinä syksyllä käynnistynyt yhteistyö mobiiliverkon käytettävyyden kasvattamiseksi sähkönsyöttöjä varmistamalla. Yhteistyötä tehdään Huoltovarmuuskeskuksen, energiayritysten ja teleyritysten kesken.

Timo Lehtimäki
johtaja
Viestintävirasto
PL 313, 00181 Helsinki
puh. (09) 6966 815, 050 514 8286
etunimi.sukunimi@ficora.fi

Muut hankkeeseen osallistuneet henkilöt

Arnell Jani, Viestintävirasto
Arnkil Lars, VR-Yhtymä Oy
Bergius Kimmo, Microsoft Finland Oy
Halkola Tapio, Finnet-liitto ry
Heliö Erkki, TietoEnator Oyj
Huopio Kauto, Viestintävirasto
Junnila Esko, Digita Oy
Kananen Ilkka, Huoltovarmuuskeskus
Keronen Jouni, Fortum Oyj
Lahti Juhani, Song Networks
Mellin Jorma, Ficix
Myllyniemi Heikki, Elisa Oyj
Saarela Pekka, liikenne- ja viestintäministeriö
Porthan Juhani, sisäasiainministeriö
Ristikankare Timo, Fingrid
Tassberg Antti, Nokia Oyj
Wirman kari, FiCom ry
Ylitalo Timo, Suomen Pankkiyhdistys ry

2.3. Tietoturvallisuushaavoittuvuuksien analysointimenetelmät

Tavoite ja tausta

Hankkeen tavoitteena on kartoittaa, mitä tietoturvallisuushaavoittuvuuksien analysointimenetelmiä on käytössä, ja sen pohjalta pyrkiä edistämään niiden kehittymistä. Tässä tarkoituksessa hanke tukee ja toteuttaa tutkimushankkeita, jotka parantavat tietoinfrastruktuurin haavoittuvuuksien hallintaa. Hankkeen alkuperäisenä tavoitteena oli myös levittää tutkimushankkeiden perusteella syntyvää tietämystä ja parhaita käytäntöjä keskeisten toimijoiden ja organisaatioiden käyttöön niiden tietoturvariskien hallinnan ja turvallisten tietojärjestelmien strategisen suunnittelun tueksi. Näin voidaan edistää tietoyhteiskunnan toimijoiden tietoturvallisuutta ja ennaltaehkäistä niihin kohdistuvia uhkia.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Hanke on kartoittanut ja edistänyt metodeja haavoittuvuuksien löytämiseen sekä pyrkinyt kehittämään koko em. prosessia tukevia toimintatapoja ja hyviä käytäntöjä.

ICT-alan yrityskartoitus

Vuonna 2005 hankkeen painopisteenä oli keskeisiin ICT-alan yrityksiin kohdistunut tietoturvallisuushaavoittuvuuksien analysointimenetelmien kartoitus. Kyselyyn vastasi 15 yritystä 25:stä. Kohteena olivat Suomessa toimivat merkittävät ohjelmistotoimittajat/palveluyritykset, tietoturvayritykset ja teleoperaattorit.

Vastauksista havaittiin, että ICT-alan keskeiset toimijat Suomessa saavat riittävästi, joskaan ei aina riittävän nopeasti tietoa tietoturvallisuushaavoittuvuuksista. Haavoittuvuuksia ilmenee jopa päivittäin. Näillä yrityksillä on runsas yhteistyökumppaniverkko haavoittuvuuksien analysoinnissa. Niillä on keinoja omien ohjelmistotuotteiden haavoittuvuuksien vähentämiseen sekä tilanteen hallintaan ja korjaamiseen, kun omissa tai ulkopuolisissa ohjelmistoissa ilmenee haavoittuvuus.

Haavoittuvuuksien analysointiin ja korjaamiseen käytetään merkittävästi resursseja, ei aina Suomessa, mutta ainakin ulkomaisen emoyhtiön organisaatiossa.

Selvityksen perusteella syntyi yleiskuva, että nopea ja hyvin organisoitu tiedonvaihto sekä yritysten sisällä että niiden välillä on avainasemassa kilpajuoksussa haavoittuvuuksien hyväksikäyttäjiä vastaan. Hallittu reagointi perustuu yrityksen omaan tai ulkopuoliseen analyysiin haavoittuvuuden kriittisyydestä.

Selvityksen mukaan on saatavissa analyysipalvelua ja ohjelmistotyökaluja haavoittuvuuksien (ja hyökkäysten) havaitsemiseksi ja analysoimiseksi. Näiden välineiden ja menetelmien yleistymistä ja edelleen kehittymistä kuitenkin toivotaan. Hanke 3.3 paneutui näihin tarkemmin keskustelemalla kahden tietoturvayritysten kanssa.

Haavoittuvuudet kätkeytyvät ohjelmarakenteisiin. Nyt kun haavoittuvuuksien vaarat ovat tulleet esille hyökkääjien käyttäessä niitä järjestelmällisesti hyväkseen, ymmärretään arkkitehtuurien ja ohjelmointimenetelmien keskeisyys haavoittuvuuksien vähentämisessä pitkällä aikavälillä. Selvityksen tuloksia esiteltiin ja käsiteltiin Kriittisen infrastruktuurin tietoturvallisuusjaoston kokouksessa.

Protos-Matine -projekti

Lisäksi vuonna 2004 käynnistynyt Oulun yliopiston tutkimushanke, Protos-Matine -projekti, jatkui. Se tutkii tietoinfrastruktuurin haavoittuvuuden hallintaa protokollariippuvuuksien näkökulmasta. Rahoittajat vuonna 2005 olivat liikenne- ja viestintäministeriö sekä Maanpuolustuksen tieteellinen neuvottelukunta. Projekti antoi raportin LVM:n asettamalle johtoryhmälle, joka koostui pääosin hankkeeseen 3.3. osallistuneista.

Protos-Matine-projekti etsi menetelmiä, jolla löydetään tietoliikenneprotokollien haavoittuvuuksia. Tutkimus kohdistui moniin saman protokollan toteuttaviin tuotteisiin sekä protokollaperheisiin. Tärkeä haavoittuvuuksien syntytapa on niiden periytyminen yhteisistä spesifikaatioista tai yhteisistä historiallisista ohjelmakoodin osista.

Toisena toimintavuotenaan 2005 projekti täydensi protokollakartoituksia asiantuntijahaastatteluin, eri käyttäjäryhmiin kohdistuvin haastatteluin sekä analysoimalla mediaaineistoa. Projekti jäsensi tuloksiaan tieteellisiksi artikkeleiksi ja loppukäyttäjälle tarkoitettuun muotoon sekä rakensi graafisen työkalun, jonka avulla tietoverkon protokollariippuvuuksia voidaan havainnollistaa.

Projekti osallistui myös liikenne- ja viestintäministeriön LUOTI-ohjelman (Luottamus ja tietoturva) mobiilimaailman ja digi-tv:n tietoturvauhkia ja niiden ratkaisemista koskevaan esiselvitykseen.

Hanke 2.3 *Tietoturvallisuushaavoittuvuuksien analysointimenetelmät* jatkaa painopistehankkeen 2.2. *Kriittisen infrastruktuurin tietoturvallisuus* alatyöryhmänä. Alatyöryhmä etsii tapoja soveltaa vuonna 2005 saatuja ICT-yrityskartoituksen ja Protos-Matine -projektin tuloksia kriittisen infrastruktuuriin suojaamiseen.

Vastuusihteeri
Ilkka Kananen
hankkeen puheenjohtaja
apulaisjohtaja
Huoltovarmuuskeskus
Pohjoinen Makasiinikatu 7 A
00130 Helsinki
puh. 040 5000 238
etunimi.sukunimi@nesa.fi

Muut hankkeeseen osallistuneet henkilöt
Hannu Sivonen
hankkeen sihteeri
Huoltovarmuuskeskus
Keith Bonnici
Teknologian kehittämiskeskus
TEKES
Arsi Heinonen
Viestintävirasto
Terttu Mellin
Valtiovarainministeriö
Juha Perttula
Liikenne- ja viestintäministeriö

2.4. Kansallisen tietopääoman suoja

Tavoite ja tausta

Kansallisen tietopääoman suoja -hankkeen tavoitteena on arvioida kansallisen tietopääoman suojaa kokonaisuudessaan huomioiden sekä yksityisen että julkisen sektorin tilanne ja kehitystarpeet. Tavoitteena on saada käytännönläheinen kuva siitä, millaista tietopääomaa pidetään kansallisesti tärkeänä, onko panostettu tietopääoman suojaan riittävästi ja mitä voitaisiin tietopääoman suojaksi tehdä tulevaisuudessa. Samoin hankkeen tavoitteena on kartoittaa mitkä ovat tulevaisuuden kannalta erityisen merkittäviä tietosuojariskejä tietopääoman kannalta, arvioida, miten tilannetta voitaisiin parantaa ja pyrkiä tätä kautta vähentämään tietoturvariskejä.

Kansallisen tietopääoman tulee olla suojattu siten, että ulkopuoliset tahot eivät voi päästä siihen käsiksi ja että ne tahot, jotka ovat oikeutettuja tietopääomaa käyttämään, voivat käsitellä tietopääomaa tietoisena siitä, että käsittely on turvallista. Hankkeella pyritään parantamaan organisaation tietoturvallisuustietoisuutta ja tietoturvallista toimintaa.

Tietopääoman käsite on hyvin laaja, minkä vuoksi työryhmä lähti rajaamaan sitä. Hankkeen osalta keskityttiin aineettomaan pääomaan, mikä koostuu datasta, informaatiosta, immateriaalioikeuksista ja itse organisaatiosta. Tämä tietopääoma koostuu nimenomaan systemaattisista luoduista käsitteellisistä tiedoista, jotka ovat organisaation toiminnan ja perustehtävienkannalta oleellisia, kuten innovaatioista, keksinnöistä, teknisistä kuvauksista ja piirustuksista, metodologioista, ohjelmistoista, sovelluksista, dokumenteista ja muista tieto-objekteista. Yrityksen toiminnan kannalta välttämätöntä tietopääomaa ovat edellisten lisäksi esimerkiksi yrityssalaisuudet, asiakastiedot sekä tuotekehitystiedot. Valtionhallinnon puolella aineettomana pääomana voitaisiin pitää esimerkiksi viranomaisten pitämiä perusrekistereitä, jotka sisältävät tietoja yhteiskunnan toiminnan kannalta merkittävistä asioista. Merkittävän osan tietopääomasta muodostaa myös yksityisten kansalaisten yksityisyyden suojan piiriin lukeutuva tietopääoma.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Hankeryhmä käynnisti selvitystyön, jonka tavoitteena on tuottaa arviointiryhmälle käytännönläheinen kuva muun muassa siitä, millaista tietopääomaa pidetään kansallisesti tärkeänä. Selvitettiin myös, onko tietopääoman suojaan panostettu riittävästi ja mitä tietopääoman suojaamiseksi voidaan tehdä tulevaisuudessa. Selvityksessä on otettu kantaa myös siihen, mitkä ovat tulevaisuudessa Suomen kannalta tietopääomaan kohdistuvia erityisen merkittäviä tietoturvariskejä. Samalla arvioidaan, miten tilannetta voitaisiin parantaa ja siten vähentää riskejä. Selvitys on saatavilla sähköisesti osoitteesta www.mintc.fi/tietoturvallisuusstrategia. Selvityksen valmistuttua hankeryhmä ei ole enää kokoontunut.

Vaikutukset ja muutostarpeet

Kansallinen tietopääoma on yksi kansallisen tietoturvallisuusstrategian painopisteistä. Kysymyksessä on keskeinen tietoturvallisen yhteiskunnan arvo, jonka turvaaminen koskee perusoikeuksia ja vapauksia. Kansallisen tietoturvallisuusasioiden neuvottelu-

kunnan työssä toteutuvat tämän hankeen päämäärän mukaiset toimenpiteet, mutta on olennaista, että kansallisen tietopääoman suojaaminen pysyy edelleen neuvottelukunnan työn keskeisenä tavoitteena.

Hankkeen vastuusihteeri on vuonna 2004 ollut neuvotteleva virkamies Sanna Helopuro liikenne- ja viestintäministeriöstä.

Tuire Saaripuu
pääsihteeri
ylitarkastaja
liikenne- ja viestintäministeriö
PL 31, 00230 Valtioneuvosto
puh. (09) 160 28305, 040 761 5406
etunimi.sukunimi@mintc.fi

3. TIETOTURVATIETOISUUS

Vuoden 2005 tietoturvapäivä oli suurmenestys kuten aiemminkin. Myös vuonna 2006 järjestetään tietoturvapäivä, jonka kohderyhmänä ovat tällä kertaa koululaiset, heidän vanhempansa sekä PK-yritykset. Yritysten tietoturvaongelmia kartoitetaan useamman ryhmän toimesta, muun muassa Helsingin Kauppakamari, Keskuskauppakamari sekä sisäasiainministeriön työn alla oleva yritysturvallisuusstrategiryhmä työskentelevät yhdessä yritysten rikosturvallisuudenlisäämiseksi. Tätä työtä ehdotetaan hyödynnettäväksi myös neuvottelukunnan työssä vuonna 2006.

3.1. Kansallinen tietoturvapäivä 2005

Tavoite ja tausta

Julkishallinnon, elinkeinoelämän ja järjestöjen yhteinen kansallinen tietoturvapäivä järjestetään vuosittain helmikuussa. Tietoturvapäivän keskeisenä tavoitteena on viestinnän ja markkinoinnin keinoin kohentaa kansalaisten tietoisuutta internetin mahdollisuuksista sekä tieturvauhista ja keinoista, joilla näiltä uhilta voidaan suojautua ja välttyä.

Vuoden 2005 tietoturvapäivä järjestettiin 8.2.2005 ja sen kohderyhmänä olivat erityisesti peruskoululaiset, heidän opettajansa ja vanhempansa. Päivän tavoitteena oli, että turvallinen internetin käyttö on kouluissa näkyvästi esillä koko kouluvuoden ajan ja tietoturvatieto kulkee oppilaiden mukana myös koteihin. Kuluvan vuoden hankkeessa korostettiin itsensä turvaamista, pelisääntöjen noudattamista ja tietokoneen suojaamista internetiä käytettäessä.

Tietoturvapäivän tukihankkeina ovat olleet Tietoturvatietoisuuden ja -osaamisen kartoitus sekä Yksilöiden tietoturvatietoisuuden lisääminen. Nämä hankkeet käynnistyivät 2004 erillisinä hankkeina, mutta ovat vuoden 2005 aikana täysin sulautuneet Tietoturvapäivähankkeeseen.

Tietoturvapäivä järjestetään jälleen vuonna 2006, jolloin erityisenä kohderyhmänä ovat pk-yritykset. Pienten ja keskisuurten yritysten lisäksi tulevan vuoden Tietoturvapäivässä huomioidaan edelleen myös peruskoululaiset. Vuoden 2005 tietoturvapäivä kouluissa oli hyvä alku lasten ja nuorten tietoturvatietoisuuden lisäämiselle, mutta kouluista saadun palautteen perusteella opettajat toivovat aiheen esille ottamista uudestaan vuoden 2006 Tietoturvapäivän yhteydessä.

Käynnistettyjen toimien tilanne vuonna 2005

Tietoturvapäivää vietettiin tänä vuonna 8. helmikuuta ensimmäistä kertaa koko Euroopan-laajuisesti. Tietoturvapäivänä eduskuntatalossa järjestettiin laaja huippuseminaari, johon oli kutsuttu eri alojen päättäjiä tietoturvapäivähankkeen yhteistyöyrityksistä, julkishallinnosta ja järjestöistä. Seminaaria isännöivät tulevaisuusvaliokunta ja liikenne- ja viestintävaliokunta. Puheenjohtajana oli tulevaisuusvaliokunnan puheenjohtaja Jyrki Katainen.

Euroopan unionin verkko- ja tietoturvavirasto ENISAn pääjohtaja Andrea Pirotti vieraili tietoturvapäivänä Suomessa ja osallistui kutsuseminaariin. Pääjohtaja Pirotti ja liikenne- ja viestintäministeri Leena Luhtanen vierailivat myös helsinkiläisessä Ressun peruskoulussa ja tutustuivat siellä käytännössä suomalaiseen tietoturvaopetukseen. Tietoturva oli nostettu monissa suomalaisissa kouluissa erityiseksi teemaksi tietoturvapäivänä.

Hankkeessa mukana olevat organisaatiot järjestivät Tietoturvapäivänä ja kevään aikana useita asiakkailleen, henkilöstölleen ja muille kohderyhmilleen suunnattuja tietoturva-aiheisia tempauksia.

Tietoturvapäivä lanseerattiin opettajille Opettaja-lehden kautta 15.10.2004 ilmestyvässä numerossa, jonka teemana olivat tietotekniikka ja uudet mediat. Lehden levikki on 91 157 (LT 2003) ja se tavoittaa tutkitusti yli 170 000 lukijaa.

Opettajille ja rehtoreille lähetettiin postitse materiaalia tietoturvapäivästä. Yhteensä kolmessa eri lähetyksessä jaettiin opetuksen tueksi ja koulujen käyttöön esittelykalvo Tietoturvapäivästä, tietoturva-aiheinen päivänavausteksti, esite Tietoturvakoulu.fi-sivustosta ja juliste. Lisäksi kouluille mainostettiin erityisesti kummitoimintaa ja Tietoturvakoulu-fi:n kummipankkia.

Maanlaajuinen markkinointikampanja aloitettiin vuoden 2005 alkupuolella. Televisiomainonnan kanavina käytettiin YLE:ä, SubTV:tä ja MTV3:a. Printtimainonnassa hyödynnettiin mahdollisuuksien mukaan etusivumainosta suurimmissa sanomalehdissä (Helsingin Sanomat, Huvudstadsbladet, Aamulehti, ja Kaleva). Kohderyhmää tavoiteltiin erityisesti Opettaja-lehdessä, Koululaisessa ja Suosikissa olleilla ilmoituksilla. Mediaa lähestyttiin tiedotustilaisuuksilla sekä laajasti median edustajien one-to-one-tapaamisilla. Lisäksi kaikki hankkeen yhteistyökumppanit toivat hanketta esiin omilla verkkosivuillaan.

Arvio toimien vaikuttavuudesta hankkeeseen yhdistettävien ja tukihankkeiden kanssa vuonna 2005

Painopistehankkeen vaikuttavuus

Tietoturvapäivä 2005 otettiin hyvin vastaan suomalaisissa peruskouluissa, ja tietoturvapäiväteemaa hyödynnettiin kevätlukukauden aikana aktiivisesti. Taloustutkimus Oy:n peruskoulujen opettajille tekemän kyselyn mukaan 98 prosenttia kyselyyn vastanneista tunsi Tietoturvapäivän ja kaksi kolmesta koulusta oli hyödyntänyt opetuksessaan teemaan liittyvää materiaalia. Toukokuussa 2005 tehtyyn kyselyyn vastasi lähes 500 peruskoulun opettajaa.

Valtaosa kyselyyn vastanneista opettajista piti Tietoturvapäivää tarpeellisena. Lisäksi opetuksen tueksi tehtyä tietoturvakoulu.fi-sivustoa pidettiin erittäin hyödyllisenä. Tutkimuksen mukaan noin puolet (52 %) kouluista on käyttänyt tietoturvakoulu.fi-sivustoa tietoturvaopetuksen tukena. Kolme neljästä (75 %) opettajasta on vieraillut sivustolla.

Kyselyyn vastanneista opettajista suurin osa katsoi, että Tietoturvapäivällä on ollut vaikutusta oppilaiden turvallisempaan internetin käyttöön. Tutkimuksen mukaan 63 prosenttia opettajista arvioi koululaisten internetin käytön muuttuneen vähintään hieman turvallisempaan suuntaan.

Tietoturvapäivälle näytetään vihreää valoa myös jatkossa: opettajista 84 % on sitä mieltä, että tietoturvapäivä on syytä järjestää myös ensi vuonna.

Tietoturvakoulu.fi-sivustolla on käynyt vuoden 2005 lokakuun loppuun mennessä yli 39 300 kävijää ja onnistuneita sivuhakuja on tehty lähes 984 800. Myös tietoturvaopas.fi-sivustolla on ollut runsaasti kävijöitä: marraskuusta 2004 alkaen tietoturvaopas.fi-sivuilla oli vieraillut yli 77 500 kävijää lokakuun 2005 loppuun mennessä. Opettajille tarkoitettuun Kummipankkiin oli ilmoittautunut 267 kummia, jotka edustavat hankkeessa mukana olevia yhteisöjä.

Tietoturvapäivänä avatun, koululaisille suunnatun kilpailun voittajat palkittiin koluvuoden päätteeksi. Kilpailuun oli kuukauden vastausaikana rekisteröitynyt yhteensä lähes 18 000 koululaista. Kilpailukysymykset ja -vastaukset tietoturvakoulu.fi-sivustolla ovat nyt kaikille avoimena tietoturvatestinä.

Tietoturvatietoisuutta ja -osaamista on kartoitettu Tilastokeskuksen keväällä 2005 toteuttamien haastattelututkimusten avulla sisällyttämällä haastatteluihin tietoturvakysymyksiä. Tämän Suomalaiset viestintävälineiden käyttäjinä 2005 -tutkimuksen tulokset julkaistaan vuoden 2005 lopulla osana Tilastokeskuksen laajempaa suomalaisten tietoyhteiskunnallistumista koskevaa raportointia. Saatujen ennakkotietojen mukaan kotikäyttäjien tekninen tietoturva (palomuurit, virustorjunta, varmuuskopiointi) on pysynyt suhteellisesti edellisen vuoden tasolla. Palomuuri on yli 80 prosentilla ja automaattinen virustarkastus noin 75 prosentilla internetyhteyksistä kotikoneista. Varmuuskopioita ei ota lainkaan lähes 40 prosenttia käyttäjistä. Tietoturvapäivä 2005 -hankkeen näkyvyyttä kysyttiin koululaisilta ja 30–40 prosenttia eri kouluasteiden oppilaista ilmoitti tietoturvaa käsitellyn oppitunneilla.

Hankkeelle julkista tunnustusta

Kansallisen tietoturvapäivähankkeen tietoturvakoulu.fi palkittiin Suomen eOppimiskeskuksen järjestämässä eEemeli 2005 -laatukilpailussa. Finaaliin asti pääsi kaikkiaan 12 e-oppimistuotetta. Tietoturvakoulu.fi sijoittui kilpailussa jaetulle toiselle sijalle.

Yhteiskuntaviestinnän yhdistys YVY on palkinnut Tietoturvapäivän Vuoden 2005 Yhteiskuntaviestintäteko -kilpailussa. Tietoturvapäivä 2005 -hanke jakoi toisen palkinnon Helsingin Sanomien ja Suomen Mielenterveysseuran yhteiskampanjan kanssa. Tietoturvapäivä on tuomariston mukaan hieno esimerkki siitä, miten erilaiset organisaatiot voivat yhdistää voimansa tärkeän asian puolesta edistääkseen yhteistä hyvää.

Tietoturvakoulu.fi on herättänyt kiinnostusta myös ulkomailla. Hankkeen toteuttamaa sivustoa eri-ikäisille koululaisille suunnattuine tarinoineen on hyödynnetty myös muiden Euroopan maiden tietoturvapäivähankkeissa, muun muassa Tanskassa ja Ruotsissa. Suunnitteilla on toteuttaa vastaavanlaiset sivustot myös Sveitsiin, Iso-Britanniaan ja Irlantiin.

Tukihankkeiden vaikuttavuus yhdessä painopisteen kanssa

Yksilöiden tietoisuuden lisääminen -hanke on toteutunut hyvin Kansallisen tietoturvapäivän aktiviteeteissa. Vuoden 2005 tietoturvapäivä toteutettiin samalla tavalla kuin ensimmäinen tietoturvapäivä vuonna 2004 sillä erotuksella, että painettua ”Joka kodin tietoturvaopasta” ei jaettu vuonna 2005. Mainonta ja viestintä ovat olleet samalla tasolla ja jopa runsaampia, kuin ensimmäisenä tietoturvapäivänä.

Painopistehankkeen vastuuhenkilöt ovat tehneet yhteistyötä nyt sulautuvien tukihankkeiden Tietoturvallisuustietoisuuden ja -osaamisen kartoittaminen sekä Yksilöiden tietoturvatietoisuuden lisääminen vastuuhenkilöiden kanssa. Esimerkiksi hanke Tietoturvallisuustietoisuuden ja -osaamisen kartoittaminen tulee osaltaan vaikuttamaan siihen, että kansalaisten tietoturvatietoisuuden lisääntymistä seurataan tilastollisesti myös jatkossa. Hankkeen työn tuloksena on Tilastokeskuksen haastattelututkimuksiin lisätty tietoturvaan liittyviä kysymyksiä. Tilastokeskuksen toteuttaman kyselytutkimuksen tulosten perusteella voidaan tehdä johtopäätöksiä ja antaa suosituksia esim. seuraavan tietoturvapäivän sisältöön. Hanke Yksilöiden tietoturvatietoisuuden lisääminen on ollut monilta osin päällekkäinen painopistehankkeen kanssa. Sen tavoitteet on joko jo saavutettu (esimerkiksi tietoturvasanasto vuonna 2004) tai tulevat katetuiksi painopistehankkeen ja muiden toimenpiteiden yhteydessä.

Yhdistettävien hankkeiden yhdistämisen aikataulu ja jo tehdyn työn sekä mukana olevien tahojen kytkeminen painopistehankkeen työhön

Kansallinen tietoturvapäivä -hankkeeseen yhdistettävät tukihankkeet ovat Tietoturvallisuus-tietoisuuden ja -osaamisen kartoittaminen sekä Yksilöiden tietoturvatietoisuuden lisääminen. Tukihankkeen Tietoturvallisuustietoisuuden ja -osaamisen kartoittaminen sisältö ja tavoitteet yhdistyvät painopistehankkeeseen kansalaisten tietoturvatietoisuuden ja -osaamisen osalta hankeryhmän kartoitustyön valmistuttua vuoden 2005 loppuun mennessä. Hankkeen työn tuloksena saadaan Tilastokeskuksen haastattelututkimuksiin liitettyjen tietoturvakysymysten tulokset syksyllä 2005. Hankkeen oppilaitoksiin kohdistuvat toimenpiteet jatkuvat osana opetusministeriön omaa toimintaa. Osa hankkeen työryhmän jäsenistä jatkaa työskentelyä Kansallinen tietoturvapäivä -hankkeen työryhmissä.

Tukihankkeen Yksilöiden tietoturvatietoisuuden lisääminen tavoitteet ja työ sisältyvät sellaisenaan Kansallisen tietoturvapäivän tavoitteisiin, ja hankkeet ovat olleet tavoitteiltaan monin tavoin päällekkäisiä. Tukihanke on jo käytännössä yhdistynyt painopistehankkeeseen.

Kristiina Klemetti
vastuusihteeri
viestintäpäällikkö
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry

Tietoturvapäivä 2005 -hankkeen vastuuhenkilöt

Johtoryhmä
Anna Lauttamus-Kauppila, Viestintävirasto (puheenjohtaja 8.11.2004 alkaen)
Nora Elers, FiCom ry (puheenjohtaja, vastuusihteeri 8.11.2004 asti)

Kristiina Klemetti, Ficom ry (vastuusihteeri 8.11.2004 alkaen)
Sari Salmela, Viestintävirasto (projektikoordinaattori, sihteeri)
Pirjo Immonen-Oikkonen, Opetushallitus
Suvi Kuikka, Pelastakaa Lapset
Anita Ovaska, Elisa Oyj
Timo Saxén, TeliaSonera Finland Oyj
Jaana Sirkiä, F-Secure Oyj
Tiina Vuorio, Microsoft Oy

Tietoturvapäivä 2006 -hankkeen vastuuhenkilöt

Johtoryhmä

Anna Lauttamus-Kauppila, Viestintävirasto (puheenjohtaja)
Kristiina Klemetti, FiCom ry (vastuusihteeri, pk-ryhmä)
Heli Alanko, Viestintävirasto (projektikoordinaattori, sihteeri)
Kimmo Bergius, Microsoft Oy
Pirjo Immonen-Oikkonen, Opetushallitus
Suvi Kuikka, Pelastakaa Lapset
Tero Kuitunen (varalla Jaana Lappi), kauppa- ja teollisuusministeriö
Leena Linnainmaa (varalla Tuula Tiihonen), Keskuskauppakamari
Nina Lundahl, Elisa Oyj
Timo Saxén, TeliaSonera Finland Oyj
Jaana Sirkiä, F-Secure Oyj
Erkki Hallavo, Hewlett-Packard Oy
Sari Salmela (koululaisryhmä)

Tietoturvapäivä 2005 -hankkeessa mukana olevat organisaatiot:

Tietoturvapäivä 2005 on valtioneuvoston alaisen tietoturvallisuusasioiden neuvottelukunnan päähanke. Muita päähankkeita ovat tietoturvallisuusohjelma, tietoverkkorikollisuus tietoturvallisuusongelmana ja kansallinen tietoturvallisuusriskien tilannekuva. Lisätietoja neuvottelukunnasta ja hankkeista osoitteessa http://www.mintc.fi/tietoturvallisuusstrategia.

Tietoturvapäivä 2005 -hankkeen järjestävät Elisa Oyj, Finnet-liitto ry, F-Secure Oyj, Hewlett-Packard Oy, Helsinki Televisio Oy, liikenne- ja viestintäministeriö, Mannerheimin Lastensuojeluliitto, Microsoft Oy, Nokia Oyj, Nordea Pankki Suomi Oyj, Opetushallitus, opetusministeriö, Pelastakaa Lapset ry, Song Networks Oy, Suomen Kuntaliitto, TeliaSonera Finland Oyj, TIEKE Tietoyhteiskunnan kehittämiskeskus, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Tietosuojavaltuutetun toimisto, Tietoturva ry, Tietoyhteiskuntaohjelma ja Viestintävirasto.

3.2. Yritysten tietoturvatietoisuus

Tavoite ja tausta

Yritysten tietoturvatietoisuus -työryhmän keskeisenä tavoitteena on parantaa elinkeinoelämän ja erityisesti pk-yritysten tietoturvatietoisuutta ja -toimintaa. Työryhmän tavoitteena on kartoittaa muita yritysten tietoturvatietoisuutta edistäviä toimijoita ja toimenpiteitä sekä koordinoida yrityksiin kohdistuvia toimenpiteitä. Lisäksi työryhmä antaa tarvittaessa suosituksia toimenpiteistä, joilla parannetaan yritysten tietoturvatietoisuutta.

Käynnistettyjen toimien tilanne vuonna 2005 ja etenemistavoitteet vuonna 2006

Vuoden 2005 helmikuussa valmistui Yritysten tietoturvatietoisuus -työryhmän raportti (www.mintc.fi/tietoturvallisuusstrategia). Siinä analysoitiin tietoturvatietoisuuden nykytilaa pk-yrityksissä sekä kartoitettiin yritysten tietoturvatietoisuutta edistäviä toimijoita ja toimenpiteitä. Lisäksi raportissa esitettiin malli koulutukseen perustuvasta tietoturvallisuusohjelmasta.

Vuoden 2005 aikana on monin eri tavoin pyritty parantamaan pk-yritysten tietoturvatietoisuutta ja -osaamista. Lisäksi vuonna 2006 käynnistyy uusia toimenpiteitä. Yritysten tietoturvatietoisuus -työryhmä pyrkii koordinoimaan vuonna 2006 toteutettavia lukuisia yritysten tietoisuutta ja osaamista lisääviä hankkeita. Lisäksi työryhmä pyrkii tunnistamaan tarpeita, joita nykyisillä toimenpiteillä ei ratkaista.

Yritysten tietoturvatietoisuus -työryhmä kokee ongelmalliseksi sen, että nykyisin ei ole saatavilla koko maan kattavaa tietoa pk-yritysten tietoturvatietoisuuden ja osaamisen tasosta ja kehityksestä. Kauppa- ja teollisuusministeriö toteuttaa vuonna 2006 valtakunnallisen kyselytutkimuksen, jossa kartoitetaan pk-yritysten tietoturvatasoa sekä inhimillisten että teknisten ratkaisujen osalta.

Seuraaviin kappaleisiin on koottu esimerkkejä yritysten tietoturvatietoisuutta edistävistä toimenpiteistä.

Seminaarikiertue Tietotekniikka Menestystekijäksi (TiMe) – Tietoturvaa pk-yrityksille

Vuonna 2005 käynnistyi Tietotekniikka Menestystekijäksi –Tietoturvaa pk-yrityksille -seminaarikiertue. Seminaarisarja kattaa yhteensä 10 tilaisuutta eri puolella Suomea ja sen tavoitteena on antaa pk-yrityksille puolueetonta ja käytännönläheistä tietoa tietoturvasta ja sen merkityksestä liiketoiminnalle. Puolen päivän kestoisissa tilaisuuksissa käsitellään tietoturvaa monipuolisesti mm. lainsäädännön, teknisten ja inhimillisten ratkaisujen sekä yritysten omien kokemusten näkökulmasta. Seminaarikiertueen rahoittaa kauppa- ja teollisuusministeriö, TE-keskukset sekä liikenne- ja viestintäministeriö. Toimintaa tukemassa ja järjestelyissä ovat mukana myös Viestintävirasto, Elinkeinoelämän keskusliitto, Ficom ry, TIEKE ry ja PKT-säätiö sekä tietoturva-alan yritykset. Seminaarikiertue päätyy toukokuussa 2006. Lisätietoa seminaarikiertueesta: www.verkkokaveri.fi.

Tietoturvakartoitus -palvelu

TIEKE ry on julkaissut pk-yrityksille suunnatun maksuttoman tietoturvakartoituspalvelun lokakuussa 2005. Palvelulla kannustetaan pk-yrityksiä parantamaan tietoturvansa tasoa. Palvelussa keskitytään pk-yritysten näkökulmasta tietoturvan keskeisimpiin ongelmiin ja annetaan ohjeita ongelmien ratkaisemiseksi. Linkit ohjaavat käyttäjiä tietoturvapalveluja tarjoavien yritysten ja organisaatioiden internetsivuille. Kysymykset ja ohjeet on muotoiltu mahdollisimman selkeiksi ilman lyhenteitä tai vaikeasti ymmärrettäviä ammattitermejä. Tietoturvakartoituspalvelu löytyy osoitteesta http://tietoturvakartoitus.tieke.fi. Kysymysten ja ohjeiden valmisteluun on osallistunut tietoturva- ja pk-yrityksiä.

Lyhytkestoiset tietoturva-seminaarit

Tieke ry järjestää vuonna 2006 yrittäjäjärjestöjen ja tietoturvayritysten kanssa pk-yrityksille myös pienimuotoisempia tietoturvaseminaareja. Niissä keskitytään tietoturvan peruskysymyksiin.

Yritysturvallisuusprojekti

Helsingin kauppakamarin ja Uudenmaan liiton Yritysturvallisuusprojekti tukee Uudenmaan alueen yrityksiä yritysturvallisuuden eri osa-alueilla. Seminaariluennoilla lisätään osallistujien riskienhallinnan ja turvallisuuden kehittämisessä tarvittavaa tietoutta ja valmiuksia. Projektiin osallistuminen on maksutonta. Vuoden 2005 aikana toteutettiin yhdeksän yritysturvallisuuden seminaaria, joista kuudessa käsiteltiin erityisesti tietoturvallisuuteen liittyviä aiheita. Projekti jatkaa toimintaansa saman laajuisena ensi vuonna.

Yritysten rikosturvallisuus 2005 -selvitys

Helsingin kauppakamari teki yhdessä Keskuskauppakamarin kanssa tutkimuksen, joka käsittelee yrityksiin kohdistuvia rikosriskejä. Selvitys käsittelee suomalaisten yritysten rikosturvallisuutta ja yrityksiin kohdistuvien rikosten ja väärinkäytösten torjuntaa. Selvitys perustuu 463 suomalaisen yrityksen sähköpostivastauksiin. Osana selvitystä kartoitettiin tietoturvaan liittyviä riskejä. Lisätietoa: http://www.helsinki.chamber.fi/chapter_images/2155_Yritysten_rikosturvallisuus_2005.pdf

e-Edistäjä -projekti

e-Edistäjä-projektissa (2004–2005) laadittiin aineistoa pk-yritysten verkko- ja tietoturvallisuuskoulutuksia varten. Aineisto on maksutonta ja vapaasti käytettävissä. Materiaali on saatavilla Elinkeinoelämän keskusliiton ja Tieke ry:n verkkosivuilla, joilla esitellään kunkin koulutusjakson tavoitteet ja sisältö. e-Edistäjä on EU:n Leonardo da Vinci -ohjelman hanke. Lisätietoa: http://www.e-facilitator.net/index.php/formation/default/ Theme/Verkko---ja-tietoturvallisuus-/3?.

Vaikutukset ja muutostarpeet

Kaikkien aikaisemmin mainittujen toimenpiteiden tavoitteena on lisätä mahdollisimman monen pk-yrityksen tietoturvatietoisuutta ja -osaamista. On arvioitu, että vuosina 2005–2006 pidettävillä Tietotekniikka Menestystekijäksi - tietoturvaa pk-yrityksille -

tilaisuuksilla tavoitetaan noin 700 pk-yrityksen edustajaa. Tieke ry:n vuonna 2006 järjestämällä seminaarisarjalla pyritään tavoittamaan noin 500 pk-yrittäjää. Helsingin kauppakamarin vuonna 2005 järjestämiin tilaisuuksiin osallistui 300 henkilöä ja tavoitteena on saavuttaa vuonna 2006 vastaava osallistujamäärä. Lisäksi Tieke ry:n tavoite on, että vuodessa tehdään noin 6000 Tietoturvakartoitus palvelun testiä.

Toimenpiteiden näkyvyyttä tukee helmikuussa 2006 järjestettävä Kansallinen tietoturvapäivä, jonka toisena kohderyhmänä on pk-yritykset. Kansallinen tietoturvapäivä edistää yritysten yleistä tietoturvatietoisuutta valtakunnan tasolla ja sen toimesta kootaan tietoturvaopas.fi –sivustolle selkeä pk-yrityksille tarkoitettu paketti tietoturvasta. Alueelliset tilaisuudet ja muut toimenpiteet tukevat Tietoturvapäivähanketta vastaamalla niihin haasteisiin, joita se nostaa esille.

Yritysten tietoturvatietoisuus -toimenpide oli vuonna 2004 sijoitettu painopistealueeseen 2 ”Edistetään kansallista kilpailukykyä ja suomalaisen tieto- ja viestintäalan yritysten toimintamahdollisuuksia”. Toimenpide siirrettiin vuoden 2005 aikana ”Tietoturvatietoisuus” -painopisteeseen, jolloin hanke tukee ja täydentää Kansallinen tietoturvapäivä -toimenpidettä.

Jaana Lappi
vastuusihteeri
ylitarkastaja
kauppa- ja teollisuusministeriö
PL 32, 00023 Valtioneuvosto
puh. (09) 1606 2658, 050 308 8143
etunimi.sukunimi@ktm.fi

Muut hankkeeseen osallistuneet henkilöt

Joni Halmelahti, Suomen Yrittäjät
Marja Heinonen, liikenne- ja viestintäministeriö
Kari Keskitalo, kauppa- ja teollisuusministeriö, 1.4.2005 → VNTHY
Tuija Kyrölä, Tietoturvakoulutus Oy, 1.3.2005 → Neste Oil Oyj
Terttu Mellin, Valtiovarainministeriö
Petri Puhakainen, Laurea-ammattikorkeakoulu
Helvi Salminen, Setec
Timo Simell, TIEKE Tietotekniikan kehittämiskeskus ry
Kalevi Tiihonen, Elinkeinoelämän keskusliitto ry.

4. KANSAINVÄLINEN YHTEISTYÖ

Tavoite ja tausta

Kansainvälisen yhteistyön huomioon ottaminen kansainvälisen tietoturvallisuuden alalla on osa kansallista tietoturvallisuusstrategiaa. Tietoturvallisuutta edistävien standardien, toimintalinjausten ja yhteistyöfoorumien muodostumiseen ja varmistetaan, että tietoturvallisuutta koskeva työnjako eri toimijoiden kesken on selkeä. Strategian mukaisesti kansainvälisen yhteistyön turvaamiseksi kansallisen tietoturvallisuusasioiden neuvottelukunnalla on keskeinen rooli tässä yhteistyössä. Neuvottelukunta tukee strategian toimeenpanon edellyttämien toimien yhteensovittamista, seuraa strategian toteutumista ja tekee valtioneuvostolle ehdotuksia strategian päivittämisestä. Strategiassa velvoitetaan osallistumaan aktiivisesti lainsäädännön ja standardien valmisteluun sekä muuhun tietoturvallisuusyhteistyöhön keskeisissä tietoturvallisuusalan vaikuttajaryhmissä Euroopan unionissa, muissa kansainvälisissä järjestöissä ja elinkeinoelämän yhteistyöforumeilla.

Tilanne vuonna 2005 ja eteneminen vuonna 2006

Hankeryhmä lähti selvittämään kansainvälisen tietoturvallisuusvaikuttamisen mahdollisuuksia ja käynnisti kartoituksen, jonka avulla pyritään selvittämään nykyistä kansainvälistä yhteistyötä ja vuorovaikutusta turvallisuusalalla sekä kartoittamaan tietoturvallisuusalankansainväliseen yhteistyöhön osallistuvien henkilöiden tarpeita yhteistyön suhteen. Kartoituksessa selvitettiin kokemuksia osallistumisen merkityksestä sekä näkemyksiä kansainvälisen yhteistyön hoitamisesta. Tarkoituksena on myös löytää keskeisesti toimivat henkilöt. Myös yhteistyön rakenne ja mahdolliset aukkopaikat ovat analysoinnin kohteena samoin kuin identifioinnin ongelmat ja haasteet kansainvälisen yhteistyön alalla. Selvityksessä arvioitiin myös kansainvälisen vaikuttamisen tarpeellisuutta.

Hankeryhmän työn valmistuttua ryhmä ei ole enää kokoontunut. Selvityksen loppuraportti ”Kartoitus vaikutusmahdollisuuksista kansainvälisessä yhteistyössä tietoturvallisuussektorilla” valmistui joulukuussa 2004 ja on saatavilla sähköisesti osoitteesta www.mintc.fi/tietoturvallisuusstrategia.

Vaikutukset ja muutostarpeet

Kansainvälinen yhteistyö on tietoturvallisuusstrategian mukaisesti yksi tietoturvallisuuden alan seurattavista kohteista. Hankkeen piirissä pyritään edelleen seuraamaan tietoturvallisuuden alan keskeisiä kansainvälisiä hankkeita sekä edistämään ja aktivoimaan yhteistyötä. Euroopan verkko- ja tietoturvallisuusviraston aloitettua toimintansa elokuussa 2005 Kreetalla Herakleionissa tietoturvallisuuden alalla on yksi keskeinen tekijä lisää, jonka työtä tietoturvallisuuden alan parhaiden käytänteiden levittämisessä on syytä seurata aktiivisesti. ENISAn johtokunnan puheenjohtaja sekä kansallinen yhteyshenkilö ovat liikenne- ja viestintäministeriöstä, joten ENISAn työstä raportoidaan sopivin keinoin tämän hankkeen yhteydessä. Suomen puheenjohtajuuskauden yksi teemoista on tietoturvallisuus, joten Euroopan unionin hankkeet ja linjaukset ovat erityisesti ajankohtaisia vuonna 2006.

Hankkeen vastuusihteeri on vuonna 2004 ollut ylitarkastaja Mari Herranen liikenne- ja viestintäministeriöstä.

Tuire Saaripuu
pääsihteeri
ylitarkastaja
liikenne- ja viestintäministeriö
PL 31, 00230 Valtioneuvosto
puh. (09) 160 28305,040 761 5406
etunimi.sukunimi@mintc.fi

5. JULKISHALLINNON SISÄINEN TIETOTURVA

5.1. Julkishallinnon sisäinen tietoturvallisuus

Tausta ja tavoite

Tiedonvaihdon kannalta on tärkeää, että valtiovarainminsteriön ja Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn tietoturvatyön laajakäyttöiset tulokset ovat mahdollisimman laajasti eri sektorien tiedossa. Otsikon tehtäväaluetta johdetaan ja koordinoidaan toimivaltaisten organisaatioiden (erityisesti valtiovarainministeriö) toimesta ja toimialan koordinaatioelimissä (erityisesti VAHTI).

Valtiovarainministeriö ohjaa valtionhallinnon tietoturvallisuutta ja tietohallintoa sekä julkisen hallinnon sähköistä asiointia. Vastuuorganisaationa valtion tietoturvallisuuden ohjauksessa toimii valtiovarainministeriön hallinnon kehittämisosasto. Valtionhallinnossa on tehty yli 20 vuotta suunnitelmallista tietoturvallisuuden kehitys- ja yhteistyötä valtiovarainministeriön johdolla.

Valtiovarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) valtiohallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIn tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta tietoturvallisuutta kehittämällä sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTIssa ovat edustettuina kaikki hallinnonalat ja -tasot. Johtoryhmä on laajasti kansallisesti ja kansainvälisesti tunnettu tietoturva-julkaisuista ja ohjeista.

Valtiovarainminsteriö on käynnistänyt vuonna 2004 laajan kehitysohjelman valtion tietoturvallisuuden kehittämiseksi. Kehitysohjelmalla vastataan nykyisiin ja tuleviin tietoturvahaasteisiin sekä vahvistetaan tietoturvallisuuden kehitys- ja yhteistyötä.

Kehitysohjelmalla on pääministeri Vanhasen johtaman tietoyhteiskuntaohjelman ministeriryhmän tuki sekä ministeri Mannisen johtaman hallinnon ja aluekehityksen ministeriryhmän tuki.

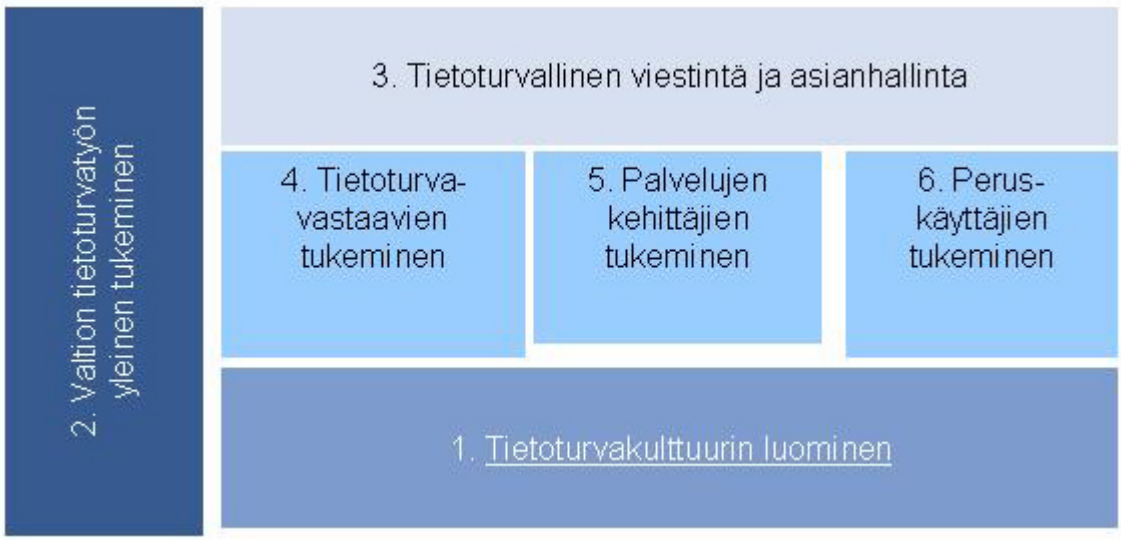
Valtiovarainministeriö johtaa valtion tietoturvallisuuden kehitysohjelmaa, joka valmistellaan, yhteensovitetaan ja koordinoidaan VAHTIssa. Tarkemmat tiedot hallinnon tietoturvatyöstä ja valtion tietoturvallisuuden kehitysohjelmasta löytyvät valtiovarainministeriön VAHTI-julkaisuista, jotka ovat saatavissa sekä painotuotteina että VM:n verkkosivuilta www.vm.fi.

Käynnistettyjen toimien tilanne vuonna 2005

Kehitysohjelman toimeenpano etenee hyvin ja laajalla osallistumispohjalla. Kehitysohjelman toimeenpanoon osallistuvat aktiivisesti kaikki hallinnonalat. Monissa hankkeissa on mukana myös kunnallishallinnon ja elinkeinoelämän edustajia.

Kehitysohjelmaan sisältyy yhteensä 28 kehityskohdetta, joista 23:ssa on tapahtunut merkittävää kehitystyötä vuosina 2004 ja 2005. Ohjelman hankealueet näkyvät ohei-

sesta kuvasta. Vuoden 2005 aikana on tapahtunut merkittävää kehitystyötä kaikilla hankealueilla. Useat hankkeet jatkuvat edelleen vuonna 2006.



Kuva: valtion tietoturvallisuuden kehitysohjelman hankealueet.

Tarkemmat tiedot kehitysohjelman etenemisestä löytyvät valtioneuvoston hankerekisteristä www.hare.vn.fi ja VAHTIn Internet-sivuilta www.vm.fi/vahti muun muassa VAHTIn ohjeista, toimintakertomuksista ja muista julkaisuista.

Arvio toimien vaikuttavuudesta

VM:n ja VAHTIn tietoturvatyö ja -ohjeet kattavat kaikki tietoturvallisuuden osa-alueet ja niihin sisältyvät tietojärjestelmiä ja -verkkoja koskevan turvallisuuden lisäksi myös hallinnollinen tietoturvallisuus, tietoaineistoturvallisuus sekä toimitilaturvallisuus ja tietosuoja.

VAHTIn tietoturvaohjeet ja toiminta sekä hallinnon yhteishankkeet, valtion tietoturvallisuuden kehitysohjelma ja muu yhteistyö ovat mitatusti tehostaneet hallinnon jatkuvaa ja ennakoivaa tietoturvatyötä.

Valtion tietoturvallisuuden yleisestä ohjauksesta ja kehittämisestä vastaa valtiovarainministeriön hallinnon kehittämisosasto, jonka keskeisinä toimintamuotoina ovat valtionhallintoa koskevat ohjeet, tietoturvayhteistyön koordinointi, hallinnon yhteishankkeet sekä ministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toiminta valtion tietoturvallisuuden koordinaatio- ja yhteistyöelimenä.

Valtionhallinnon lisäksi VAHTIn ja kehitysohjelman toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä tietoturvayhteistoiminnassa.

Valtiovarainministeriö osallistuu myös useisiin muihin kansallisen tietoturvastrategian hankkeisiin, joissa muutenkin on mukana osin samoja organisaatioita ja henkilöitä

kuin valtion tietoturvallisuuden kehitysohjelman toimeenpanossa, mikä on merkinnyt hyvää ja tehokasta yhteistyötä eri hankkeiden välillä.

Valtiovarainministeriö ja liikenne- ja viestintäministeriö ovat vuonna 2005 tiivistäneet monipuolisesti keskinäistä tietoturvayhteistyötään, mikä on merkinnyt valtion tietoturvallisuuden kehitysohjelman ja kansallisen tietoturvastrategian hankkeiden yhteistyön ja yhteensovittamisen paranemista entisestään.

Tietoturvallisuus ja sen osa-alueet muodostavat kattavasti dokumentoituina ja ohjeistettuina sekä hyvin johdettuina ja eri toimintojen yhteistyössä toimeenpantuina vahvan perustan organisaation toiminnan jatkuvuudelle, laadulle, luotettavuudelle, tehokkuudelle ja tuloksellisuudelle. Muun muassa tästä ja tietoturvakulttuurin vahvistumisesta on kyse julkishallinnon tietoturvallisuuden kehittämisessä ja sen vaikuttavuudessa.

Organisointi

Tehtäviä toteutetaan valtiovarainministeriön johdolla osana ministeriön laaja-alaista ohjaus- ja koordinointityötä.

Tehtävät valmistellaan, yhteensovitetaan ja koordinoidaan VAHTIssa, jonka toimintaan osallistuvat kaikki hallinnonalat. VM johtaa VAHTIn ja myös sen sihteeristön toimintaa sekä vastaa VAHTIn valmistelusta.

Mikael Kiviniemi
neuvotteleva virkamies
valtiovarainministeriö
hallinnon kehittämisosasto
PL 28, 00023 Valtioneuvosto
puh. (09) 160 33269
etunimi@sukunimi@vm.fi

6. TIETOTURVASTRATEGIAN VAIKUTTAVUUS

Tavoite ja tausta

Hankkeen ”Kansallisen tason toimijoiden toimintaedellytykset” tavoitteena oli arvioida kansallisen tietoturvastrategiahankkeen ja sen hankeryhmien etenemistä ja hankeryhmien toimien vaikutuksia tietoturva-alan kehittymiseen strategiahankkeen puolivälissä keväällä 2005 sekä laatia suositukset jatkotyön suuntaamiseen ja esittää menetelmiä strategiahankkeen lopullisen tuloksellisuuden mittaamiseen strategiahankkeen lopussa 2007. Strategiahankkeen tulokset on kirjattu Kansallisen tietoturvallisuusasioiden neuvottelukunnalle jätettyyn raporttiin.

Tilanne 2005

Hankeryhmän käyttämien JP-Epstarin konsulttien ja hankeryhmän yhteistyönä määriteltiin vuoden alussa osahankkeiden mittaamisessa käytettävät menettelytavat ja kyselylomakkeistot. Konsultit suorittivat tarvittavat osahankkeiden edustajien haastattelut ja kyselyt maalis-huhtikuussa 2005. Samalla tutkittiin tietoturvasta kerätyt tilastotiedot.

Tämän jälkeen yhdessä hankeryhmän kanssa laadittiin osahankkeiden jatkotyövaihtoehdot, arvioitiin tehostamis- ja tarkentamisehdotusten vaikutuksia sekä tehtiin ehdotukset mahdollisesta muusta yhteistyöstä ja uusista kehittämishankkeista.

Hankeryhmän raportti ”Tietoturvastrategian vaikuttavuus” valmistui toukokuun lopussa ja luovutettiin liikenne- ja viestintäministeriölle. Raportti on käsitelty Kansallisen tietoturvallisuusasioiden neuvottelukunnan kokouksessa 13.9.2005.

Hankeryhmä on saanut työnsä päätökseen eikä se enää jatka toimintaansa.

Ehdotukset

Hankeryhmän loppuraportissa on esitetty neuvottelukunnalle seuraavat kehittämisehdotukset.

Strategiahanke kattaa hyvin sille määritellyn tutkimusalueen. Strategiahankkeen näkökulmaa tulisi kuitenkin laajentaa sähköisten palveluiden tietoturvan kehittämisestä kattamaan myös kaikki ne yhteiskunnan muut prosessit, joihin liittyy tiedon turvaaminen.

Jotta laajentaminen voitaisiin tehdä strategiahanketta hyödyntäen, laajentamishankkeen aluksi tulisi käydä keskustelu, mitkä ovat sellaisia tietoja, joita tulee suojata. Tämän jälkeen on määriteltävä suojaamisen taso, eli se, millaisia riskejä voidaan ottaa. Vasta tämän jälkeen voidaan määrittää itse tiedon suojaamistapa. Näin voidaan saavuttaa kokonaiskuva strategiahankkeen roolista ja suunnata hankeryhmien toimintaa.

Näkökulman laajentaminen voidaan tehdä esimerkiksi lisäämällä strategiahankkeen ja muiden yhteiskunnan kehityshankkeiden yhteistyötä suojattavan tiedon tunnistamisessa.

Strategian painopisteitä tulisi jatkossakin tarkastella määräajoin, jotta päällekkäiseltä työltä voitaisiin välttyä ja voitaisiin löytää tietoturvallisuuden kannalta ongelmalliset aukkopaikat. Myös hankeryhmiä on voitava tarvittaessa yhdistää ja niiden tavoitteita on konkretisoitava. Tällä hetkellä strategiahankkeiden tavoitteet ovat liian yleisiä, jotta ne ohjaisivat riittävästi hankeryhmien toimintaa.

Tietoturvallisuus on voimakkaasti muuttuva ala, minkä vuoksi strategiahankkeen tulee tarkastaa määräajoin toimintansa. Hankeryhmien työ on myös jaettava osatavoitteisiin, joissa tarkastetaan hankeryhmän työn suuntaa. Tarvittaessa hankeryhmän työhön voidaan hakea uutta lähestymistapaa.

Osa strategiahankkeen hankeryhmien toimista on ollut toisistaan irrallisia, jolloin ryhmät kokevat vaikeaksi vaikuttaa riittävästi toimiensa tavoitteisiin ja sisältöön. Hankeryhmien välistä yhteistyötä on lisättävä kokoamalla hankeryhmät strategiahankkeiden uusien painopistealueiden ympärille ja koordinoimalla näiden toimia nykyistä tiiviimmin. Näin hankeryhmien yhteistyö lisääntyisi ja työ kattaisi entistä paremmin tutkimusalueen.

Pienistä resursseistaan huolimatta hanke on saavuttanut sille asetetut tavoitteet. Mikäli hankeryhmien tuloksia halutaan konkretisoida, on hankeryhmien käyttöön asetettava entistä enemmän resursseja. Strategiahankkeen resursseista on vastannut kutakin hankeryhmää vetävä ministeriö, minkä vuoksi neuvottelukunta ei ole voinut asettaa resursseja eri hankeryhmien käyttöön. Ratkaisu voisi olla esimerkiksi käytettävissä oleva resurssipooli, josta voitaisiin antaa tarvittaessa lisäresursseja eri hankeryhmiin. Erityisesti on huomattava, että kaikilla hankkeilla on oltava vastuusihteeri.

Tiedotuksen rooli on määriteltävä entistä selkeämmin, jotta sisäiset hankeryhmät saavat riittävästi tietoa muiden hankeryhmien toimista. Myös ulkoisesti strategiahankkeen tunnettuus ja tulosten julkaisu ovat jääneet vähäisiksi. Strategiahankkeelle tulee luoda sisäinen ja ulkoinen tiedotuspolitiikka ja mahdollisuuksien mukaan omat kotisivut. Ellei hanke näy riittävästi ulospäin, koko hankkeen vaikuttavuus kärsii.

Osa strategiahankkeen tehtävistä voitaisiin jättää muille organisaatioille. Eräiden hankeryhmien tulokset voidaan halutessa kaupallistaa. Tällaisten hankeryhmien toiminta olisi siirrettävä muille organisaatioille, kuten esimerkiksi Tekesille. Jo tällä hetkellä useat ryhmät käyttävät työnsä lähteenä esimerkiksi Tilastokeskuksen tutkimusmateriaalia.

Strategiahankkeen päätteeksi tulisi laatia vaikuttavuusarviointi, joka koostuu nykyisistä ja kehitettävistä Tilastokeskuksen mittareista, hankeryhmien omista mittareista ja hankkeen ulkopuolisille tahoille tehtävästä haastattelututkimuksesta. Vastuusihteeristö on jo nyt nostanut esiin ajatuksen, että kukin ryhmä lähtee arvioimaan oman työnsä tuloksia verrattuna hankkeen lähtötilanteeseen sekä edellisen vuoden tilanteeseen. Näin voidaan jo nyt hankkeen keskivaiheilla nähdä, mitkä hankkeet toimivat odotetusti ja voidaanko hankkeen jäsenten toimin asioita parantaa tietoturvallisuuden alalla.

Tavoitteena on, että kukin työryhmä tunnistaisi kolmesta viiteen työn osa-aluetta, jotka ovat selkeästi kehittyneet työn aikana. Tietoturvallisuuden mittariston kehittämistä

tulisi jatkaa niin, että tietoturvallisuuden mittaristo olisi myös kansainvälisesti käyttökelpoinen.

Strategiahanke on tuottanut arvokasta tietoa tietoturvasta ja strategiahankkeen toiminnasta. Tätä kokemusta hyödyntämällä Suomi voi edistää Euroopan laajuisen tietoturvallisuushankkeen kehittämistä omalla puheenjohtajakaudellaan vuonna 2006, erityisesti sen vuoksi, että tietoturvallisuus on yksi Suomen puheenjohtajuuskauden teema.

Kansallisen tietoturvallisuusstrategiahankkeen opeilla Suomi voisi tuoda konkreettisen ja johtavan panoksen EU:n tietoturvallisuustyön ohjaamiseen. Jos Suomi lähtee johtamaan tällaista Euroopan laajuista hanketta, tulisi Suomella olla valmiina esitys ohjelman rakenteeksi ja tietoturvan mittaristoksi. Tätä varten strategiahankkeessa saatu ohjelmallinen tietämys olisi voitava siirtää EU-tasolle ja tietoturvan mittaamiselle olisi kehitettävä toimiva mittaristo.

Hankeryhmä toivoo, että sen kehittämisehdotukset otetaan huomioon strategiahankkeen jatkotyössä.

Kaarlo Korvola
tietohallintojohtaja
sisäasiainministeriö
PL 26, 00023 Valtioneuvosto
puh. (09) 160 42796, 040 561 1649
kaarlo.korvola@intermin.fi

Tapio Virkkunen
Liikenne- ja viestintäministeriö

Keith Bonnici
Teknologian kehittämiskeskus TEKES

Ari Hyppönen
F-Secure Oyj

Kari Lehtinen
Elisa Oyj

Terttu Mellin
Valtiovarainministeriö

Pentti Saastamoinen
Tietotekniikan liitto ry

Markku Suvanen
Opetusministeriö

Teemupekka Virtanen
Teknillinen korkeakoulu

Kansallisia tietoturvatekijöitä

1. Aarnio Reijo, Tietosuojavaltuutetun toimisto
2. Ahola Ilkka, Sun Microsystems Oy
3. Ailisto Heikki, VTT
4. Alanko Heli, Viestintävirasto
5. Andersson Martin, viestintävirasto
6. Antikainen Päivi, liikenne- ja viestintäministeriö
7. Anttila Johanna, liikenne- ja viestintäministeriö
8. Arnell Jani, Viestintävirasto,
9. Arnkil Lars, VR-Yhtymä Oy
10. Arnö Kaj, MySQL AB
11. Aromaa Juha, Mannerheimin Lastensuojeluliitto
12. Autio Jussi, Finnet-liitto
13. Bergius Kimmo, Microsoft Finland Oy
14. Bonnici Keith, TEKES
15. Elers Nora, Tietoliikenteen ja tietotekniikan liitto FiCom ry
16. Haapaniemi Leena, SFS-Inspecta Sertifiointi Oy
17. Hagman Rauni, Viestintävirasto
18. Hakola Tuomo, Ficix
19. Halkola Tapio, Finnet-liitto ry
20. Hallavuo Erkki, Hewlett-Packard Oy
21. Hallikainen Aaro, Poliisin tietohallintokeskus
22. Halmelahti Joni, Suomen Yrittäjät
23. Halonen Kyösti, Puolustusvoimat
24. Hanski Mikko-Pekka, Idean Research Ltd.
25. Harald Bo, Nordea Oyj
26. Harjuhahto-Madetoja Katrina, Tietoyhteiskuntaohjelma
27. Heinonen Arsi, Viestintävirasto
28. Heinonen Marja, liikenne- ja viestintäministeriö
29. Heliö Erkki, TietoEnator Oyj
30. Helkamäki Tarja, Elisa Oyj
31. Helopuro Sanna, liikenne- ja viestintäministeriö
32. Herranen Mari, liikenne- ja viestintäministeriö
33. Hiidenheimo Ilkka, Stonesoft Oyj
34. Holopainen Sami, Elisa Oyj
35. Honkanen Jussi, Pelastakaa Lapset ry
36. Huhanantti Hellevi, Väestörekisterikeskus
37. Huhtiniemi Heikki, Tietosuojavaltuutetun toimisto
38. Huopio Kauto, Viestintävirasto
39. Huovinen Susanna, liikenne- ja viestintäministeriö
40. Hyppönen Ari, F-Secure Oy
41. Hyvärinen Pertti, puolustusvoimat
42. Hyytiä Kalevi, puolustusvoimat
43. Härkönen Juha, Fortum Oyj
44. Ilmonen Urho, Nokia Oyj
45. Immonen-Oikkonen Pirjo, Opetushallitus

46. Jokinen Pirkko, SWelcom Oy
47. Junnila Esko, Digita Oy
48. Jäppinen Arvo, opetusministeriö
49. Järvinen Antti, Kesko Oyj
50. Kaila Urpo, CSC Tieteen tietotekniikan keskus
51. Kajantie Sari, Keskusrikospoliisi
52. Kalinen Riku, Suojelupoliisi
53. Kallio Jani, Elisa Oyj
54. Kananen Ilkka, Huoltovarmuuskeskus
55. Kannisto Santeri, SOT Finnish Software Engineering Ltd.
56. Kara Eija, Tietosuojavaltuutetun toimisto
57. Kari H. Hannu, Teknillinen korkeakoulu
58. Karjalainen Jorma, valtiovarainministeriö
59. Karppinen Lauri, tietosuojavaltuutetun toimisto
60. Karvonen Kaarlo, Finnair Oyj
61. Keinälä Severi, elinkeinoelämän keskusliitto EK
62. Kekkonen Timo, kauppa- ja teollisuusministeriö
63. Keronen Jouni, Fortum Oyj
64. Keskitalo Kari, kauppa- ja teollisuusministeriö
65. Kilkkilä Sami, Viestintävirasto
66. Kivi Ritva, Opetushallitus
67. Kivinen Tuomas, Nordea Oyj
68. Kiviniemi Mikael, valtiovarainministeriö
69. Klemetti Kristiina, FiCom ry
70. Koivunen Erka, Elisa Oyj
71. Kokko-Herrala Riitta, Kuluttajavirasto
72. Koli Markku, Puolustusvoimat
73. Koponen Heikki, Symantec Finland
74. Korvola Kaarlo, sisäasiainministeriö
75. Koskinen Sami O, TKK
76. Krogars Marco, puolustusministeriö
77. Kuikka Suvi, Pelastakaa Lapset ry
78. Kuitunen Marjatta, TeliaSonera Finland Oyj
79. Kuitunen Tero, kauppa- ja teollisuusministeriö
80. Kuparinen Veli-Pekka, Huoltovarmuuskeskus
81. Kyrölä Tuija, Helsingin kauppakamari
82. Lahti Juhani, Song Networks
83. Laitala Riikka, Song Networks Oy
84. Laksola Tuula, Elisa Oyj
85. Lantto Eeva, Viestintävirasto
86. Lappi Jaana, kauppa- ja teollisuusministeriö
87. Lautsuo Lotta, Starcut Ltd.
88. Lauttamus-Kauppila Anna, Viestintävirasto
89. Lehtosalo Kimmo, Eera Finland Oy
90. Lepinsalo-Harju Elise, Nokia Oyj
91. Lavonen Maria, SSH Communications
92. Lehtimäki Timo, Viestintävirasto
93. Lehtinen Kari, Elisa Oyj
94. Lehtonen Sami, VTT
95. Lepinsalo-Harju Elise, Nokia Oyj

96. Lillberg Petri, SSH Communications Security Corporation
97. Linnainmaa Leena, Keskuskauppakamari
98. Luhtakanta Perttu, puolustusvoimat
99. Luhtala Riitta, Helsinki Televisio Oy
100. Luhtanen Leena, liikenne- ja viestintäministeri
101. Lundahl Nina, Elisa Oyj
102. Malkki Merja, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry
103. Markus Hannu, Nokia Oyj
104. Matikainen Jussi, Helsingin kaupungin opetusvirasto
105. Matthews Tia, Nokia Oyj
106. Mehtälä Martti, Microsoft Oy
107. Mellin Jorma, Ficix
108. Mellin Terttu, valtiovarainministeriö
109. Miettinen Kirsi, liikenne- ja viestintäministeriö
110. Mikkola Marko, Symantec Finland
111. Moilanen Usko, Keskusrikospoliisi
112. Mustonen Erkki, F-Secure Oyj
113. Mutanen-Pirttilä Päivi, Tietoyhteiskuntaohjelma
114. Myllyniemi Heikki, Elisa Oyj
115. Mäenpää Heikki, Kangasalan kunta
116. Mäenpää Markku, Kansallisarkisto
117. Mäki Pasi, Song Networks Oy
118. Naulapää Reijo, sisäasiainministeriö
119. Nenonen Markku, sisäasiainministeriö
120. Niemi Tapio, Kangasalan kunta
121. Nieminen Pete, Netsol Oy
122. Niittysalo Rami, MTV Interactive
123. Nikkilä Terhi, Song Networks Oy
124. Nurmela Juha, Tilastokeskus
125. Nurmi Tiina, TEKES
126. Ojajärvi Miina, kuluttajavirasto
127. Oksanen Kari, Nordea Pankki Suomi Oyj
128. Ovaska Anita, Elisa Oyj
129. Paananen Antti, Energiamarkkinavirasto
130. Palomäki Pirkka, F-Secure Corporation
131. Parmes Rauli, liikenne- ja viestintäministeriö
132. Partanen Heikki, Tietosuojavaltuutetun toimisto
133. Peltonen Mari, Elisa Oyj
134. Perttula Juha, liikenne- ja viestintäministeriö
135. Pietikäinen Kristiina, liikenne- ja viestintäministeriö
136. Pitkänen Olli, Helsinki Institute for Information Technology HIIT
137. Pohjola Hannele, Elinkeinoelämän keskusliitto EK ry
138. Porthan Juhani, sisäasiainministeriö
139. Puhakainen Petri, Laurea-ammattikorkeakoulu
140. Purhonen Mika, Huoltovarmuuskeskus
141. Pursiainen Harri, liikenne- ja viestintäministeriö
142. Pösö Päivi, Väestörekisterikeskus
143. Rakshit Tommi, sisäasiainministeriö
144. Rintala Suvi, Kangasalan kunta
145. Rintanen Terho, puolustusvoimat

146. Ristikankare Timo, Fingrid
147. Ristola Juhapekka, liikenne- ja viestintäministeriö
148. Rosendahl Mauri, Helsingin yliopisto ja Tietoturva ry
149. Rostedt Nils, Oy LM Ericsson Ab
150. Saapunki Ari, Aldata Solution Finland Oy
151. Saarela Pekka, liikenne- ja viestintäministeriö
152. Saaripuu Tuire, liikenne- ja viestintäministeriö
153. Saastamoinen Pentti, Tietotekniikan liitto ry
154. Salmela Sari, Viestintävirasto
155. Salminen Helvi, Setec Oy
156. Salminen Markku, sisäasiainministeriö
157. Salminen Oili, Tieke Tietoyhteiskunnan kehittämiskeskus ry
158. Saxén Timo, TeliaSonera Finland Oyj
159. Siilasmaa Risto, F-Secure Oyj
160. Silvennoinen Eero, Tekes
161. Simell Timo, Tieke Tietoyhteiskunnan kehittämiskeskus ry
162. Sirkiä Jaana, F-Secure Oyj
163. Sivonen Hannu, Huoltovarmuuskeskus
164. Stenvall Carina, MTV Oy Interactive
165. Ståhle Riittamaija, Finnet-liitto ry
166. Suhonen Mari, Tekniikan Sanastokeskus TSK ry
167. Summanen Kari, Patentti- ja rekisterihallitus
168. Suvanen Markku, opetusministeriö
169. Svento Reijo, Tietoliikenteen ja tietotekniikan liitto FiCom ry
170. Tamminen-Dahlman Anne, Tietosuojavaltuutetun toimisto
171. Tanner Simo, Kuntaliitto
172. Tarvainen Tapani, EFFI ry
173. Tassberg Antti, Nokia Oyj
174. Tassi Tiina, Finnet-ryhmä
175. Terho Arja, valtiovarainministeriö
176. Tiihonen Kalevi, Elinkeinoelämän keskusliitto EK ry
177. Tikkanen Leena, Mittatekniikan keskus
178. Tuurala Kati, Microsoft Oy
179. Typpö Anne, Oy LM Ericsson Ab
180. Tyry-Salo Satu, Suomen Kuntaliitto
181. Uusilehto Janne, Nokia Oyj
182. Vainio Arto, SSH Communications Security Oy
183. Vettenranta Leena, oikeusministeriö
184. Viitasaari Mikko, TeliaSonera Finland Oyj
185. Viljanen Maritta, Hewlett-Packard Oy
186. Wilska Marita, Kuluttajavirasto
187. Virkkunen Lauri, Vattenfall Oy
188. Virkkunen Tapio, liikenne- ja viestintäministeriö
189. Wirman Kari, Elisa Oyj
190. Virtanen Teemupekka, Teknillinen korkeakoulu
191. Vuorenmaa Ilkka, Tekijänoikeuden tiedotus- ja valvontakeskus ry
192. Vuorio Tiina, Microsoft Oy
193. Ylitalo Timo, Suomen Pankkiyhdistys ry
194. Yli-Äyhö Janne, TeliaSonera Oyj
195. Zilliacus Stefan, Symantec Finland