”TURVALLINEN ARKI TIETOYHTEISKUNNASSA – EI TUURILLA VAAN TAIDOLLA”

VALTIONEUVOSTON PERIAATEPÄÄTÖS KANSALLISEKSI TIETOTURVASTRATEGIAKSI 4.12.2008

TOIMENPIDEOHJELMA

Sisältö:

1. JOHDANTO

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi hyväksyttiin joulukuussa 2008. Kansallisen tietoturvastrategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa.

Edellisen tietoturvastrategian aikana tietoturvatyö saatettiin käyntiin Suomessa laajalla rintamalla. Vuonna 2003 julkaistu tietoturvastrategia oli Suomessa ja Euroopassa ensimmäinen laatuaan. Uuden strategian ja siihen pohjautuvan toimenpideohjelman tavoitteena on keskittyä muutamiin alan asiantuntijoiden keskeisimpinä pitämiin kehittämiskohteisiin ja saada niissä aikaan mahdollisimman konkreettisia tuloksia.

Toimenpideohjelman valmistelu on tehty arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuus – ryhmässä. Ryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmään kuuluu yli 20 julkisen ja yksityisen sektorin tietoturvavaikuttajaa. Toimenpideohjelma on valmisteltu kansallisen tietoturvastrategian tavoitteiden saavuttamiseksi periaatepäätöksen painopisteiden pohjalta.

Toimenpideohjelman valmistelu on pyritty pitämään mahdollisimman avoimena prosessina. Toimenpideohjelman koostamisen pohjaksi järjestettiin laaja lausuntokierros uudesta tietoturvastrategiasta sekä avattiin asiasta julkinen keskustelu otakantaa.fi sivustolla. Tietoturvallisuus -ryhmä on valmistelun aikana kokoontunut neljä kertaa ja järjestänyt strategiaseminaarin ja työpajan tietoturvapäivänä 10.2.2009. Luonnos toimenpideohjelmaksi oli laajalla lausuntokierroksella 2009 aikana. Tietoturvallisuusryhmän sisällä on lisäksi toiminut erillinen toimenpideohjelmaa valmisteleva työvaliokunta.

Toimenpideohjelman keskeisenä ajatuksena on, että siinä toimeenpannaan muutamia keskeisiä hankkeita, joilla ratkaisevasti edistetään tietoturvaa Suomessa ja saadaan siten kansallinen tietoturvastrategia toteutettua tehokkaasti. Tarkoituksena on hakea synergioita ja miettiä tarkasti missä asioissa voidaan tuottaa lisäarvoa. Toimenpideohjelmalla on myös rajapintoja muiden ohjelmien kanssa, jotka otetaan työssä huomioon (mm. eräät sisäasiainministeriön sisäisen turvallisuuden ohjelmaan kuuluvat hankkeet). Valtionvarainministeriön strategiatyössä ja sen jalkauttamisessa keskitytään valtionhallinnon tietoturvallisuuteen.

Toimenpideohjelmaan on koottu strategian pohjalta 8 kärkihanketta, joissa paneudutaan uusiin ajankohtaisiin tietoturva-asioihin, parannetaan olemassa olevia toimintoja sekä vältetään päällekkäisten toimintojen tekemistä. Jokaiselle hankkeelle on nimetty vetäjä sekä muut osallistuvat tahot (mukana ainakin mainitut tahot). Hankkeille luodaan vetovastuullisten johdolla mittarit, joiden avulla hankkeen toteutumista seurataan. Toimenpideohjelman koordinointivastuu on arjen tietoyhteiskunnan tietoturvallisuus -ryhmällä.

2. PERUSTAIDOT ARJEN TIETOYHTEISKUNNASSA

*Ensimmäisen painopisteen toimenpiteissä kehitetään kansallista tietoturvapäivä-hanketta, lisätään tietoturvatietoisuutta, seurataan tietoisuuden tasoa ja kehitetään tietoturvaosaamista, laaditaan aktiivinen ja ennakoiva viestintäsuunnitelma. Lisätään tietoturvavaatimukset osaksi jokaista tarjouspyyntöä, ml. ratkaisujen ja palvelujen suunnitteluvaiheet, edistetään tietoturvaratkaisujen laajempaa käyttöä, selvitetään mahdollisuutta kehittää turvallisille palveluille myönnettävää erillistä sertifikaattia, edistetään sertifioitujen tietoturva-ammattilaisten määrän lisäämistä Suomessa. **

HANKE 1: Tietoturvatietoisuuden lisääminen

Tausta/ toimenpiteen sisältö:

Toimiva tietoyhteiskunta edellyttää, että sen tarjoamien palveluiden turvallisuus pystytään takaamaan. Tietoturva on kaikkien tietoyhteiskuntaan osallistuvien vastuulla ja jokaisen tahon on ymmärrettävä oma osuutensa tästä vastuunjaosta. Tämän takia on erityisen tärkeää kasvattaa tietoturvaymmärrystä kaikkialla yhteiskunnassa.

Hankkeessa arvioidaan, mitä tietoturvan perustaidot arjen tietoyhteiskunnassa tarkoittavat ja tämän pohjalta valmistellaan tietoturvaviestejä kaikille keskeisille väestöryhmille. Viestien jalkauttamiseksi valmistellaan erillinen viestintäsuunnitelma.

Hankkeessa arvioidaan lisäksi Tietoturvapäivä -konseptin kehittämistarpeet, joista keskeisimpänä on tietoturvapäivän laajentaminen koko maata koskevaksi. Tietoturvapäivähankkeessa pyritään saamaan tietoturvapäivän tilaisuuksia pääkaupunkiseudun lisäksi myös alueelliselle ja paikalliselle tasolle. Vuosittain helmikuussa järjestettävä tietoturvapäivä on julkishallinnon, elinkeinoelämän ja järjestöjen yhteinen hanke ja sen tarkoituksena on kansalaisten tietoturvatietoisuuden lisääminen.

Hankkeessa tulee huomioida erityisesti pk-sektori siten, että selvitetään mahdollisuudet luoda oma tietoturvahanke pk-sektorille. Pk-yrityksille suunnatussa tietoturvaviestinnässä tulee ottaa huomioon nykyistä paremmin yritysten tarpeet teknisten näkökohtien korostamisen sijaan. Tietoturvaviestit tulee liittää tiiviiksi osaksi yritysten liiketoimintanäkökulmaa.

Suomalainen koulujärjestelmä on pohja kansalliselle tietoturvaosaamiselle. Tietoturvaopetus tulee varmistaa kaikille koululaisille ja opiskelijoille ja se pitää laajentaa myös ATK-opetuksen ulkopuolelle. Hankkeessa pyritään vaikuttamaan siihen, että tietoturvavalmiuksia kehitetään jokaisella koulutusasteella.

Tulos /vaikuttavuustavoite:

Yleistavoitteena on kansallisen tietoturvatietoisuuden parantuminen sekä tietoturvaan liittyvien vastuiden, oikeuksien ja velvollisuuksien selkeytyminen. Tietoyhteiskunta on mahdollistanut useiden arjen askareiden ja toimien hoitamisen monipuolisesti verkossa, joten siellä tulee noudattaa samoja sääntöjä ja turvallisuusajattelua kuin

muussa arkielämässä verkon ulkopuolella. Läpileikkaus hankkeen viesteissä tulee olemaan internetin ja tietoturvan maallistaminen pois sen teknisestä luonteesta. Viestit toteutetaan kohderyhmän mukaan kansantajuisesti opastaen ja turhien uhkakuvien luomista viesteissä vältetään. Lisäksi hankkeen yhtenä pitkän aikavälin tavoitteena on saada tietoturvaopetus osaksi koulujen opetussuunnitelmia.

Hankkeen tuloksena tietoturvapäivän jo hyvin toimiva konsepti paranee entisestään samalla kuin pk-sektorin erityistarpeet otetaan huomioon. Tietoturvapäivän sisällöt ja viestit leviävät laajemmin ja kohdentuvat entistä paremmin. Tietoturvatietoisuus kasvaa koko maassa.

Toteutus- ja seurantavastuu:

Päävastuu: Anna Lauttamus-Kauppila /**Viestintävirasto**
Mukana; Liikenne- ja viestintäministeriö, Keskuskauppakamari, EK, Microsoft, Suomen yrittäjät, Opetusministeriö, Opetushallitus, Sisäasiainministeriö, Kuluttajavirasto, Työ- ja elinkeinoministeriö, VTT

Aikataulu: Viestintäsuunnitelma sekä suunnitelma tietoturvapäivähankkeen kehittämisestä tulevat olla valmiit keväällä 2010.

HANKE 2: Palveluntarjoajan vastuut, oikeudet ja velvollisuudet

Tausta/ toimenpiteen sisältö:

Yhteiskunnan palvelut siirtyvät yhä voimakkaammin verkkoon, jonka tähden kansalaisten turvallinen siirtyminen palveluiden käyttäjiksi on varmistettava. Luottamuksen puute on yksi keskeisimmistä sähköisten palveluiden käyttöönoton esteistä. Kansalaisten on voitava luottaa, että verkko- ja viestintäpalveluiden käyttö on turvallista. Tässä työssä korostetaan erityisesti yhteistyön tärkeyttä ja yritysten johdon roolia ja vastuuta.

Hankkeessa selvitetään tämän hetken tilanne palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista. Selvityksen pohjalta tehdään suositusluonteinen ehdotus parhaiksi käytännöiksi.

Tulos /vaikuttavuustavoite:

Hankkeen tavoitteena on lisätä palveluiden ja tuotteiden tietoturvaominaisuuksien vertailukelpoisuutta, tehdä tietoturvallisia palveluita näkyväksi sekä lisätä kansalaisten luottamusta.

Palveluntarjoajan vastuut, oikeudet ja velvollisuudet selkiintyvät ja luotettavien tietoturvaratkaisujen käyttö laajenee. Hanke edistää tietoturvan integroimista kiinteäksi osaksi tietoyhteiskunnan perusrakenteita. Yritysten valveutuneisuus tietoturva-asioista paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Jaakko Turunen /**Keskuskauppakamari**
Mukana: Tietotekniikan liitto, Liikenne- ja viestintäministeriö, Oikeusministeriö, Tieto, Microsoft, Teliasonera, Kuluttajavirasto, Kesko, Valtiovarainministeriö, Työ- ja elinkeinoministeriö, Tietosuojavaltuutetun toimisto, EK, Viestintävirasto, HIIT, VTT

Aikataulu: Hanke aloittaa keväällä 2010.

3. TIETOIHIN LIITTYVIEN RISKIEN HALLINTA JA TOIMINTAVARMUUS

Toisen painopisteen toimenpiteissä tuetaan yritysten käyttöön tarkoitettujen riskienhallintamallien laajempaa käyttöönottoa, järjestetään riskienhallintaan liittyvää koulutusta. Selvitetään mitä menetelmiä ja varautumismalleja tulee kehittää entistä monimutkaisempien verkkojen ja verkostojen hallintaan, selvitetään mahdollisuutta tukea yritysten varautumis- ja riskienhallintatoimintaa, tuetaan lainsäädännöllisin keinoin yhteiskunnan elintärkeiden toimintojen tarvitsemien viestintäverkkojen ja viestintäpalvelujen toiminnan varmistamista. *

HANKE 3: Tietoihin liittyvien riskien tunnistaminen ja tietojen suojaamiseen liittyvien vaatimusten tunnistaminen (riskienhallintaa)

Tausta/ toimenpiteen sisältö:

Hankkeessa kartoitetaan tarkoituksenmukaisia riskienhallintatyökaluja ja edistetään niiden käyttöönottoa. Hankkeessa pohditaan myös miten riskienhallintaan ja palvelujen jatkuvuuteen liittyvää koulutusta voitaisiin edistää erityisesti pk-yrityksille. Lisäksi pyritään edistämään yrittäjäjärjestöjen roolia riskienhallintaan liittyvässä opastuksessa. Hankkeessa pyritään auttamaan organisaatioita selkeyttämään tietoriskien ohjausta ja hallintaa. Riskitietoisuutta lisätään tiedottamalla valikoiduista toteutuneista tietoriskeistä.

Tietojen turvallisuudesta ei kyetä enää entiseen tapaan huolehtimaan fyysisen turvallisuuden keinoin. Yritysten tulee olla perillä ajankohtaisista tietoturvallisuusvaatimuksista. Tietojen ja tietopalvelujen turvaamisen perusta syntyy erilaisien suojausvaatimusten tunnistamisesta. Vaatimuksia on asetettu mm. lainsäädännössä, sopimuksissa sekä organisaation itselleen luomissa toimintapolitiikoissa. Organisaatioissa ei välttämättä kuitenkaan osata tai pystytä tunnistamaan näitä vaatimuksia kattavasti ja systemaattisesti, mikä vaikeuttaa tavoitteellista ja tarkoituksenmukaista tietoturvallisuustyötä.

Lisäksi hankkeessa arvioidaan sellaisen menetelmän kehittämistä, jonka avulla erilaiset tietojen turvaamiseen liittyvät vaatimukset pystyttäisiin tunnistamaan ja hallitsemaan tehokkaasti. Menetelmän avulla toimijat pystyisivät kohdistamaan tietojen turvaamiseen liittyvät toimensa tehokkaammin ja tarkoituksenmukaisemmin oikeisiin asioihin.

Tulos /vaikuttavuustavoite:

Tuloksena on, että riskienhallintaosaaminen lisääntyy ja riskien ennakointi paranee. Yritysten liiketoiminnan kannalta keskeisten riskien tunnistaminen ja torjuminen vahvistuu. Riskienhallintamallien käyttöönotto lisääntyy erityisesti sellaisten yritysten keskuudessa, joilla ei ole mahdollisuutta riskienhallinnan ammattilaisten palkkaamiseen. Tietojen ja tietopalveluiden turvaaminen tulee pysyväksi osaksi yritysten riskienhallintaa.

Toteutus- ja seurantavastuu:

Päävastuu: Sauli Savisalo /**Huoltovarmuuskeskus**
Mukana: EK, Liikenne- ja viestintäministeriö, Suomen Yrittäjät, Keskuskauppakamari, Nordea, Luottokunta, VTT, FiCom, Finanssialan Keskusliitto, Keskusrikospoliisi, Puolustusministeriö, Puolustusvoimat

Aikataulu: Kartoitus aloitetaan syksyllä 2009 ja ehdotukset käyttöönoton edistämiseksi keväällä 2010

HANKE 4: Yritysten toiminnan jatkuvuuden ja kansalaisten palveluiden saatavuuden varmistaminen (toimintavarmuus)

Tausta/ toimenpiteen sisältö:

Yhteiskunnan toimintojen siirtyessä yhä suuremmassa määrin verkkoon, on tietoliikenteen häiriötön toiminta kaikissa oloissa erityisen tärkeää. Hankkeessa selvitetään, miten tieto- ja viestintäpalveluiden toimivuuden turvaamista voitaisiin edistää.

Lisäksi varautumisen ja huoltovarmuuden kannalta on olennaista selvittää vaihtoehtoiset mallit Suomen kansainvälisten tieto- ja viestintäliikenneyhteyksien turvaamiseksi mm. merikaapelissa, operaattoriyhteistyöllä, kansainvälisellä yhteistyöllä sekä satelliittiyhteyksin. Hankkeessa selvitetään mahdollisuutta rakentaa merikaapeli Suomesta Keski-Eurooppaan.

Tulos /vaikuttavuustavoite:

Tavoitteena on edistää tietoyhteiskunnan häiriönsietokykyä ja huoltovarmuutta erityisesti kasvavan viestiliikenteen tarpeisiin tulevaisuudessa. Yritysten toiminnan jatkuvuus ja kansalaisten palveluiden saatavuus tulevat paremmin varmistetuiksi. Hankkeella pyritään myös parantamaan Suomen ja suomalaisten yritysten houkuttelevuutta.

Toteutus- ja seurantavastuu:

Päävastuu: Kari Wirman /**FiCom**
Mukana: Huoltovarmuuskeskus, Liikenne- ja viestintäministeriö, Microsoft, Teliasonera, Tieto, Viestintävirasto, operaattorit, tietotekniikkatalot,

Teknologiateollisuus/tietotekniikka-ala, Tekes, Puolustusvoimat, toimihenkilöunioni, Kesko, VTT, Finanssialan keskusliitto

Aikataulu: Merikaapeli esiselvitys aloitetaan syksyllä 2009. Selvitys tietoliikennepalveluiden toimivuuden turvaamisesta valmis keväällä 2010

4. KILPAILUKYKY JA KANSAINVÄLINEN VERKOSTOYHTEISTYÖ

*Kolmannessa painopisteessä korostuu kansainvälisten standardien käyttöönoton edistäminen sekä aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön, vaikutetaan EU-yhteistyön kautta siihen, että tietoturvaan liittyvät direktiivit toimeenpannaan mahdollisimman yhdenmukaisesti, joka edistää useassa maassa toimivien suomalaisten yritysten toimintaa. Harkitaan kansallisen kv-yhteistyöverkoston perustamista, jossa tieto ja kokemukset kv-työryhmistä leviävät, selvitetään Suomen kansallisen tietoliikenneturvallisuusviranomaisen (NCSA) perustamisen tarvetta. **

HANKE 5: Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön

Tausta/ toimenpiteen sisältö:

Suomi on useilla osa-alueilla tietoturvaosaamisen edelläkävijä, mutta sitä ei ole tarpeeksi hyvin osattu markkinoida kansainvälisesti. Suomessa ei pidä pelkästään seurata kansainvälistä kehitystä, vaan on myös pyrittävä aktiivisesti viemään maailmalle omaa tietoturvaosaamistamme. Viranomaisten ja yritysten tulisi aktiivisemmin välittää ajankohtaista tietoa muihin maihin (mm. kääntämällä uudet lait ja tärkeät säädökset englanniksi). Hankkeessa laaditaan suunnitelma Suomi-kuvan parantamiseksi tietoturvamaana.

Kansainvälisen yhteistyön avulla pystytään vaikuttamaan Suomelle oleelliseen eurooppalaisen tietoturvan kehittämiseen ja suomalaisen tietoturvatietämyksen kasvattamiseen. Hankkeessa selvitetään lisäksi miten edistetään Suomen mahdollisuuksia vaikuttaa aktiivisesti kansainvälisten standardien kehittämistyöhön sekä miten edistetään kansainvälisten standardien laajamittaista hyödyntämistä.

Tulos /vaikuttavuustavoite:

Tavoitteena on vaikuttaa yhteiseen EU politiikkaan omaehtoisen aktiivisuuden kautta ja toisaalta parantaa tiedonvaihtoa näyttämällä muille esimerkkiä. Tavoitteena on myös luoda parempia edellytyksiä kansainvälisille toimijoille tulla tai investoida Suomeen. Viranomaisten ja yritysten aktiivisuus viestiä ajankohtaisista asioista Suomen rajojen ulkopuolelle kasvaa ja Suomen maine tietoturvamaana paranee.

Kansainvälisten standardien ja parhaiden käytäntöjen noudattaminen ja siten tietoturvallinen palveluympäristö edistää Suomen kansainvälistä kilpailukykyä ja

vaikuttaa yritysten halukkuuteen investoida Suomeen. Kansallisten toimijoiden yhteistyö standardointikysymyksissä paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Reijo Savola /**VTT**
Mukana: Liikenne- ja viestintäministeriö, Viestintävirasto, SFS, Nokia, Teliasonera, Teknologiateollisuus, Ulkoasiainministeriö, Sisäasiainministeriö, Tekes, Puolustusvoimat

Aikataulu: Suunnitelma valmis keväällä 2010

HANKE 6: Yritysten kilpailukyky ja NCSA

Tausta/ toimenpiteen sisältö:

Hankkeen tarkoituksena on vauhdittaa kansallisen tietoliikenne-turvallisuusviranomaisen (National Communications Security Authority, NCSA) perustamista Suomeen sekä löytää tähän tarvittava rahoitus erityisesti jatkon osalta. Virallisen NCSA:n puuttuminen vaikuttaa siten, että Suomelle luovutetaan turvaluokiteltua tietoa pidättyvästi ja toisaalta suomalaisten yritysten toimintaedellytykset kansainvälisillä markkinoilla ovat heikentyneet. Ilman NCSA:n lausuntoa suomalaiset toimijat eivät mm. voi osallistua tasavertaisesti kansainvälisiin tarjouskilpailuihin. Tietoturvallisuusviranomaistehtävien järjestämisellä on siten myös kaupallinen ja vientiteollinen intressi.

Tulos /vaikuttavuustavoite:

Suomen sisäisen ja ulkoisen turvallisuuden kannalta täysipainoinen osallistuminen turvaluokiteltua tietoa edellyttävään kansainväliseen yhteistyöhön on ensiarvoisen tärkeää. NCSA-tehtävien suorittamiseksi perustetaan riittävillä ja uskottavilla resursseilla varustettu kansallinen toimija. Kansallisen tietoliikenneturvallisuuden taso nousee Suomessa vastaamaan kehittyneeltä teollisuusvaltiolta edellytettäviä vaatimuksia sekä Suomen mahdollisuudet osallistua tasavertaisella pohjalla kansainväliseen tietoturvallisuusyhteistyöhön tulee turvatuksi.

Toteutus- ja seurantavastuu:

Päävastuu: Timo Lehtimäki /**Viestintävirasto**
Mukana: Valtiovarainministeriö, Ulkoasiainministeriö, Liikenne- ja viestintäministeriö, VTT

Aikataulu: Kansallisen tietoliikenneturvallisuusviranomaisen rahoitus jatkon osalta varmistetaan vuoden 2010 aikana

HANKE 7: Kansallisen yhteistyön tehostaminen ja aktivointi kansainvälisissä tietoturva-asioissa

Tausta/ toimenpiteen sisältö:

Suomen vähäiset resurssit kansainvälisessä vaikuttamisessa tulee suunnata tehokkaammin. Hankkeessa perustetaan kansallinen foorumi tiedonvaihdon parantamiseksi ja pohditaan myös muita toimenpiteitä kansallisen yhteistyön tehostamiseksi. Olemassa olevia hyviä kansainvälisiä foorumeita pyritään myös käyttämään aktiivisemmin vaikuttamiseen. Foorumia hyödynnetään tiedonvaihtokanavana erityisesti EU:ssa tapahtuvan tietoturvapolitiikan ja Euroopan verkko- ja viestintäviraston (ENISA) osalta.

Tulos /vaikuttavuustavoite:

Tavoitteena on tehostaa kansainvälistä yhteistyötä tarjoamalla kansallinen foorumi alan toimijoille. Tavoitteena on kokonaiskuvan parantuminen suomalaisten viranomaisten ja yksityisen sektorin edustajien kansainvälisestä toiminnasta. Tuloksena on kansallisten resurssien tehostuminen, tiedonvaihdon parantuminen sekä Suomen vaikutusmahdollisuuksien lisääntyminen.

Toteutus- ja seurantavastuu:

Päävastuu: **LVM**
Mukana: Valtiovarainministeriö, Teliasonera, Ulkoasiainministeriö, Sisäasiainministeriö, Tekes, Puolustusvoimat, Viestintävirasto

Aikataulu: Foorumin ensimmäinen tilaisuus järjestetään syksyllä 2009

5. MUUT HANKKEET

HANKE 8: Tutkimushanke lähitulevaisuuden tietoturvatrendeistä

Tausta/ toimenpiteen sisältö:

Hankkeessa kartoitetaan lähitulevaisuuden tietoturvauhkia, jotka liittyvät mm. uusiin teknologioihin, palveluihin, tuotantomalleihin ja yritysrakenteisiin. Hankkeessa pyritään identifioimaan uusia trendejä ja niihin liittyviä riskejä ja mahdollisuuksia. Kartoituksen jälkeen mahdollisia tietoturvauhkia arvioidaan erityisesti Suomen näkökulmasta. Lisäksi arvioidaan erillisen tietoturva-ohjelman perustamista.

Tulos /vaikuttavuustavoite:

Hankkeella pyritään ennakoimaan mahdollisia uusia tietoturvariskejä. Hankkeessa tuotettu tieto auttaa riskikartoitusten tekemistä eri toimialoilla. Hankkeen tavoitteena on arvoida voidaanko tuottaa pysyvä kehityksen seurannan malli ja mekanismi, jonka avulla Suomen varautuminen tulevaisuuden haasteisiin tulee paranemaan.

Toteutus- ja seurantavastuu:

Päävastuu: Ossi Kuittinen /**SITRA**
Mukana: VTT, Tekes, Liikenne- ja viestintäministeriö, Oikeusministeriö Keskusrikospoliisi, Puolustusvoimat, Huoltovarmuuskeskus, Työ- ja elinkeinoministeriö, SUPO, Viestintävirasto, VTT

Aikataulu: Projektisuunnitelma valmis syksyllä 2009

HANKE 9: Tietoturvallisuuden mittaaminen

Tausta/ toimenpiteen sisältö:

Tietoturvallisuuden mittaaminen on sateenvarjohanke, jossa mitataan sekä strategian onnistumista että tietoturvan kehitystä yleensä. Hankkeessa selvitetään, miten tällä hetkellä tietoturvallisuuden tasoa seurataan Suomessa ja tämän pohjalta tehdään ehdotus käytettäviksi menetelmiksi ja mekanismeiksi.

Tulos /vaikuttavuustavoite:

Hankkeella varmistetaan strategian mahdollisimman tehokas toteutuminen. Lisäksi hankkeessa sovitaan indikaattorit kansallisen tietoturva-asioiden seuraamiselle. Kansallinen käsitys tietoturvan tasosta selkeytyy ja vertailukelpoisuus kansainvälisesti paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Petri Puhakainen /**Oulun Yliopisto**
Mukana: Tilastokeskus, Viestintävirasto, Microsoft, Valtiovarainministeriö, VTT, Liikenne- ja viestintäministeriö, Puolustusvoimat, Tekes, Kesko, Nokia

Aikataulu: Indikaattorikartoitus on valmis keväällä 2010

6. TOIMEENPANON TOTEUTUS, SEURANTA JA RESURSSIT

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi toimeenpannaan tällä toimenpideohjelmalla. Toimenpideohjelman jokaisessa hankkeessa on yksi

organisaatio, joka on vetovastuussa kyseisestä hankkeesta (julkisen tai yksityisen sektorin taho). Strategian toteutuksen kannalta tarpeelliset toimenpiteet ja seuranta sisältyvät toimenpideohjelmaan. Tarkemmat ja yksityiskohtaisemmat toimenpiteet, mittarit ja seuranta laaditaan perustettavissa työryhmissä syksyn 2009 aikana.

Liikenne- ja viestintäministeriön asettama arjen tietoyhteiskunnan tietoturvallisuus –ryhmä tukee strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Toimenpideohjelman seuranta- ja ohjausvastuu toteutetaan siten, että hankkeiden puheenjohtajat muodostavat ”työvaliokunnan”. Valiokunta raportoi työn edistyksestä arjen tietoyhteiskunnan tietoturvallisuus –työryhmälle.

Arjen tietoyhteiskunnan tietoturvallisuus –ryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategia sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä. Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Hankkeiden loppuraportit valmistuvat 28.2.2011 mennessä, jolloin arjen tietoyhteiskunnan neuvottelukunnan alaisen tietoturvallisuus –ryhmän mandaatti loppuu.

Hankkeen vetovastuussa oleva taho vastaa toimenpideohjelman toteutuksen yhteydessä syntyneistä kuluista. Toimenpideohjelma toteutetaan virkatyönä. LVM:n T&K-rahaa voi käyttää pienimuotoisiin tutkimushankkeisiin eri päätöksellä.

* (teksti suoraan valtioneuvoston periaatepäätöksestä)