LIIKENNE- JA VIESTINTÄMINISTERIÖ
VPO/VVE

1.12.2008

VALTIONEUVOSTON PERIAATEPÄÄTÖS KANSALLISESTA TIETOTURVA-STRATEGIASTA *"Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –"*

Strategian tavoitteet

Kansallisen tietoturvastrategian avulla pyritään luomaan 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. Yleinen tietoturvaosaamisen pitää olla korkealla tasolla ja yhteiskunnan eri tahot toimivat saumattomassa yhteistyössä tietoturvan edistämiseksi. Suomi on tietoturvan edelläkävijämaa maailmassa vuonna 2015.

Painopiste 1: Perustaidot arjen tietoyhteiskunnassa

Painopiste 2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Toimenpiteet

Painopiste 1: Perustaidot arjen tietoyhteiskunnassa

Jokainen tietoyhteiskunnan toimija vaikuttaa teoillaan sekä omaan että muiden tietoturvallisuuteen. Siksi on tärkeää, että kaikilla on tietoturvallisuudesta riittävät perustiedot ja -taidot. Luottamus tietoyhteiskuntaa kohtaan syntyy, kun sekä palveluiden käyttäjät että tuottajat ymmärtävät vastuunsa, oikeutensa ja velvollisuutensa.

Palveluiden käyttäjien tulee kyetä tunnistamaan ja tiedostamaan turvallisen ja luotettavan palvelun lähtökohdat. Sähköisen asioinnin kansalaistaidot ja verkkolukutaito ovat edellytyksiä turvalliselle liikkumiselle verkossa. Riskien ennakointi, tunnistaminen ja niihin varautuminen säästää monelta ikävältä yllätykseltä. Erityisesti **palvelun tarjoajan** tulee varmistaa palveluiden käytön turvallisuus sekä osaltaan huolehtia luottamuksellisten tietojen tunnistamisesta ja suojaamisesta. Palvelun tarjoajalla on myös velvollisuus huolehtia palvelun turvallisuuden jatkuvasta ylläpitämisestä palvelu- ja toimintaympäristön muuttuessa.

Avoin ja selkeä viestintä palvelun turvallisuudesta ja mahdollisista riskeistä luo perustan sille luottamukselle, jota arjen tietoyhteiskunnassa toimimisessa tarvitaan.

Palvelun tarjoajan vastuuta ei voi ulkoistaa. Käytännössä palvelun tarjoaja vastaa palvelun tuottamiseen osallistuvien toimijoiden kanssa palvelun tietoturvallisuudesta. Strategian tehtävänä on integroida tietoturva kiinteäksi osaksi tietoyhteiskunnan perusrakenteita. Tämä edellyttää paitsi yleisen tietoturvatietoisuuden ja –osaamisen vahvistamista myös tietoturvanäkökohtien huomioon ottamista järjestelmähankinnoissa ja sopimusprosesseissa.

- **Tietoturvatietoisuuden ja -osaamisen vahvistaminen**
    - Kehitetään kansallista tietoturvapäivä-hanketta
    - Lisätään tietoturvatietoisuutta, seurataan tietoisuuden tasoa ja kehitetään tietoturvaosaamista
    - Laaditaan aktiivinen ja ennakoiva viestintäsuunnitelma

- **Turvallisten sähköisten palveluiden tarjoaminen ja luottamuksellisuuden varmistaminen**
    - 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

Painopiste 2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Sähköiset palvelut ja asiointi muodostavat yhä keskeisemmän osan niin julkisen kuin yksityisen sektorin palvelujärjestelmää. Samalla riippuvuus tietotekniikasta tekee palveluista entistä haavoittuvaisempia. Erilaisia viestintäpalveluita käyttävien kansalaisten on voitava luottaa, että palveluiden käyttö on turvallista ja että luottamuksellisia tietoja ei joudu vääriin käsiin. Kansalaisille ja yrityksille tulee taata riittävä viranomaistuki, jos tietoturvaa on loukattu esimerkiksi identiteettivarkaus-tapauksissa.

Kun ulkoistetaan palveluita ja ketjutetaan hankintoja on varmistettava tietoturvan kokonaisvaltainen hallinta. Palveluita suunniteltaessa tulee koko verkon tietojen turvallisuus arvioida kokonaisvaltaisesti. Tässä palvelun tarjoajalla on keskeinen vastuu. Tietojen luottamuksellisuus, tietojen eheys ja käytettävyys ovat oleellisia asioita palvelussa.

Tietoyhteiskunnan kriittisen infrastruktuurin toimivuus ja tieto- ja viestintäjärjestelmien sekä viestintäpalveluiden turvallisuus tulee varmistaa kaikissa tilanteissa –normaalioloista poikkeusoloihin asti. Yritysten toiminnan jatkuvuus ja kansalaisten palveluiden saatavuus on varmistettava.

- **Riskienhallinnan ja toimintavarmuuden kehittäminen**

- Tuetaan yritysten käyttöön tarkoitettujen riskienhallintamallien laajempaa käyttöönottoa
- Järjestetään riskienhallintaan liittyvää koulutusta

- **Yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa tilanteissa**

  - Selvitettävä 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

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Suomen tulee kehittää omaa kansallista sääntely-ympäristöään yritysten kannalta yksinkertaisempaan ja ennustettavampaan suuntaan sekä pyrkiä aktiivisesti vaikuttamaan kansainväliseen sääntelyyn. Kansallisen lainsäädännön selkeys ja liiketoiminnan esteiden poistaminen vaikuttavat olennaisesti kansalliseen kilpailukykyyn ja yritysten haluun investoida Suomeen. Lisäksi on huolehdittava siitä, että erot tietoturvaan liittyvien EU-direktiivien kansallisessa toimeenpanossa eivät kohtuuttomasti vaikeuta useassa EU-maassa toimivien suomalaisten yritysten toimintaa. Kilpailukykyisen tietoyhteiskunnan kannalta on välttämätöntä, että sen keskeinen tietopääoma kuten teollisoikeudet ja yrityssalaisuudet on suojattu. Näillä toimenpiteillä voidaan turvata yritysten toiminta Suomessa ja suomalaisten yritysten toiminta ulkomailla sekä lisätä Suomen houkuttelevuutta yritysten sijoittautumisessa.

Suomi on osa globaalia tietoverkkotaloutta ja suurin osa tietoturvauhista ja -hyökkäyksistä kohdistuu meihin maamme rajojen ulkopuolelta. Näiden uhkien torjuminen edellyttää paitsi kattavaa varautumista ja toimivia kansainvälisiä yhteistyöverkostoja myös ennakoivaa toimintaotetta ja heikkojen signaalien tunnistamista. Suomen tulee toimia aktiivisesti kansainvälisessä viranomaisyhteistyössä tietoturvauhkien ennaltaehkäisemiseksi ja haittojen vähentämiseksi. Globalisaatio ei ole ainoastaan uhka, vaan myös mahdollisuus. Toimiakseen vaikuttavasti kansainvälisillä foorumeilla Suomen tulee kyetä priorisoimaan kansainvälistä toimintaansa ja kohdistamaan resurssinsa tietoturvan kannalta keskeisiin kysymyksiin. Vaikuttavaan toimintaan päästään ainoastaan hyvällä kansallisella yhteistyöllä ja etukäteisvaikuttamisen kautta.

- **Suomen houkuttelevuuden ja kilpailukyvyn vahvistaminen ennustettavuutta lisäämällä**

  - 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

- **Ennakoivan ja vaikuttavan kansainvälisen yhteistyön terävöittäminen**
    - Harkitaan kansallisen kv-yhteistyöverkoston perustamista, jossa tieto ja kokemukset kv-työryhmistä leviävät
    - Selvitetään Suomen kansallisen tietoliikenneturvallisuus-viranomainen (NCSA) perustamisen tarvetta

Strategian toimeenpano

Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriön asettama arjen tietoyhteiskunnan tietoturvallisuus –ryhmä tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Arjen tietoyhteiskunnan tietoturvallisuus –ryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategia sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä.

Tavoitteiden saavuttamiseksi periaatepäätöksen painopisteiden pohjalta tehdään toimenpide-ohjelma. Strategian toteutuksen kannalta tarpeelliset toimenpiteet, mittarit, ja seuranta sisältyvät toimenpide-ohjelmaan, joka valmistuu keväällä 2009.