LIIKENNE- JA VIESTINTÄMINISTERIÖ
VPO/VVE

MUISTIO
1.12.2008

VALTIONEUVOSTON PERIAATEPÄÄTÖKSEN PERUSTELUMUISTIO KANSALLISESTA TIETOTURVASTRATEGIASTA *"Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –"*

Strategian tausta

Kansallisessa tietoyhteiskuntakehityksessä eletään vaihetta, jossa aikaisemmin erillisenä toimintalohkona ollut tieto- ja viestintäteknologia on muuttunut osaksi kansalaisten jokapäiväistä arkea. Arjen tietoyhteiskunnassa (ns. ubiikkiyhteiskunta) tietotekniset ratkaisut monipuolistuvat ja muuttuvat käyttäjien kannalta kiinteäksi osaksi ihmisten ja yritysten normaalitoimintaa. Tämän takia on oleellista, että kansalaiset voivat käyttää tietoyhteiskunnan palveluita vaivatta ja että sähköiset palvelut koetaan luotettaviksi. Tämä on kaikkien vastuulla ja siksi tietoturvaosaaminen ja -tiedostaminen ovat oleellisen tärkeitä asioita. Tavoitteena on turvallinen arki tietoyhteiskunnassa, ei tuurilla vaan taidolla. Tietojen luottamuksellisuuden, eheyden ja käytettävyyden merkitys on suuri tämän päivän arjen tietoyhteiskunnassa.

Edellinen valtioneuvoston periaatepäätös kansalliseksi tietoturvallisuusstrategiaksi hyväksyttiin vuonna 2003 ja se kokosi lähes ainutlaatuisella tavalla sekä yksityisen että julkisen sektorin toimijat saman pöydän ääreen. Ennen kaikkea strategia nosti tietoturvan merkittäväksi aiheeksi yhteiskunnalliseen keskusteluun. Tietoturvatietämyksemme ja ymmärryksemme on kasvanut ja Suomi on voinut edustaa eturivin maita tietoturva-asioissa sekä EU:ssa että kansainvälisillä foorumeilla. Tietoturvallisuusstrategia oli ensimmäinen Euroopassa ja mahdollisesti ensimmäinen maailmassa. Tietoturvallisuusstrategian ja sen toteutusta koordinoivan kansallisen tietoturvallisuusasioiden neuvottelukunnan toimikausi loppui keväällä 2007. Tätä työtä tehtiin hyvin vahvasti julkisen ja yksityisen sektorin välisenä yhteistyönä. Tietoturvallisuusstrategian suurimmat tulokset olivat tietoturvatietoisuuden lisääntyminen, mm. kansallisen tietoturvapäivän luomisella, kansallisen tietoturvatilannekuvan muodostaminen sekä "Luottamus ja tietoturva sähköisissä palveluissa" –kehittämisohjelman puitteissa saavutetut tulokset.

Toimintaympäristö muuttuu nopeasti ja sen takia on tarve päivittää tietoturvastrategia. Tärkeää on saada realistinen ja fokusoitu kansallinen tietoturvastrategia, jossa on muutamia priorisoituja tavoitteita. Tietoturvasta on tehtävä olennainen ja luonteva osa jokapäiväistä elämää. Strategiaa ei tämän takia kirjoiteta vain alan asiantuntijoille. Strategialla ei vain passiivisesti reagoida vaan vaikutetaan aktiivisesti tulevaisuuteen, uskalletaan olla aktiivisia ja rohkeita edelläkävijöitä. Strategia ei vaikuta tietoturvallisuuteen liittyvään vastuunjakoon eikä olemassa oleviin organisaatiorakenteisiin. Tämä strategia ja valtiovarainministeriön koordinoima

valtionhallinnon tietoturvalinjaukset tukevat toisiaan. Strategialla on linkkejä myös hyväksyttyyn sisäisen turvallisuuden toimintaohjelmaan.

Kansallinen tietoturvastrategia on keskeinen osa hallituksen tietoyhteiskuntapolitiikkaa. Arjen tietoyhteiskunnan neuvottelukunnan toiminta-ohjelmassa 2008-2011 todetaan, että

> *”Luottamus on tietoyhteiskunnan tärkeimpiä asioita. Luottamus tietoyhteiskuntaan edellyttää teknisesti toimivia ja turvallisia palveluita. Laajasti ymmärrettynä luottamus on käyttäjän kokemus tai näkemys palvelun laadusta. Tavoitteena on luottamuksen ylläpitäminen ja vahvistaminen.*
>
> *Luottamusta vahvistavat palveluiden helppokäyttöisyys, riittävä kuluttajansuoja, varmuus sisältöjen aitoudesta sekä kuluttajan yksityisyyden ja muiden etujen suojelusta. Kuluttajan aseman parantaminen edellyttää kaikilta toimijoilta vastuullisuutta, myös kuluttajalta itseltään.*
>
> *Yhteiskunnan toiminnot riippuvat lähes täysin tietoverkkojen ja tietojärjestelmien toimintavarmuudesta. Järjestelmät ovat haavoittuvaisia erilaisille tietoturvauhille ja tietoverkkorikollisuudelle. Toimintaympäristön tietoturvallisuuteen on siten alati kiinnitettävä huomiota, jotta kriittisen infrastruktuurin toiminta ja tietoturvallisuus varmistetaan.”*

Strategia luotiin arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuusryhmässä vuoden 2008 aikana lukuisilla työpajoilla, kokouksilla ja haastattelukierroksella. Arjen tietoyhteiskunnan tietoturvallisuusryhmä tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi.

Strategiset 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

Tietoturva on muutakin kuin tekniikkaa. Arjen tietoyhteiskunnassa kansalaiset tarvitsevat uudenlaisia perustaitoja, joita heillä ei aiemmin ollut. Tietoturva nähdään edelleen liiaksi irrallisena osana viestintä- ja tietojärjestelmien kehittämistä. Tietoa on erilaista ja siitä johtuen tulisi miettiä mitä riskejä tiedon turvaamiseen liittyy. Luottamus tietoyhteiskuntaa kohtaan syntyy, kun sekä palveluiden käyttäjät että

tuottajat ymmärtävät omat vastuunsa, oikeutensa ja velvollisuutensa. Myös yrittäjien ja yritysten tietoturvasta vastaavien osaamisen kehittäminen on tärkeää.

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. 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 identiteettivarkaustapauksissa.

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Suomi elää globaalissa tietoverkkotaloudessa, joten merkittävä osa tietoturvauhista ja –hyökkäyksistä (mm. palvelunestohyökkäykset) kohdistuu meihin maamme rajojen ulkopuolelta. Suomen tulee toimia aktiivisesti kansainvälisessä viranomaisyhteistyössä verkkorikollisuuden ennaltaehkäisemiseksi sekä siitä aiheutuvien haittojen vähentämiseksi. Suomen tulee paitsi kehittää omaa kansallista sääntely-ympäristöään yritysten kannalta yksinkertaisempaan ja ennustettavaan suuntaan myös pyrittävä aktiivisesti vaikuttamaan kansainväliseen sääntelyyn.

Toimenpiteet

1.1. Tietoturvatietoisuuden ja -osaamisen vahvistaminen

Turvallinen toiminta edellyttää perustaitoja niin palveluiden tuottajilta kuin niiden käyttäjiltäkin. Strategialla pyritään varmistamaan, että kansalaisilla on 2000-luvun kansalaistaitoon rinnastettava osaaminen, so. tietoyhteiskunnassa vaadittava tietoturvan lukutaito liittyen verkkopalveluiden käyttöön, omien luottamuksellisten tietojen (salasanat, luottokortti- ja pankkitiedot, henkilötiedot) säilyttämiseen, yleisten verkkohuijausten tunnistamiseen sekä oman päätelaitteen turvallisuudesta huolehtimiseen. Konkreettisia keinoja väestön tietoturvatietoisuuden ja –osaamisen vahvistamiseksi tulisi kehittää.

1.2 Turvallisten sähköisten palveluiden tarjoaminen ja luottamuksellisuuden varmistaminen

Tavoitteena on tehdä kotimaisista verkkopalveluista mahdollisimman turvallisia koko palveluiden elinkaaren aikana (alkaen suunnitteluvaiheesta). Näin tietoturva tulee olennaiseksi osaksi palveluiden laatua. Tämä tarkoittaa käytännössä tietoturvanäkökohtien huomioonottamista myös hankintaprosessien yhteydessä ja palvelusopimuksia tehtäessä. Tietoturvan kehittäminen ei saa olla vain IT-osaajien asia. Johdon rooli on ensi arvoisen tärkeää integroitaessa tietoturva osaksi liiketoiminta- ja hallintoprosesseja. Tietoturvallisuus on huomioitava koko palvelutuotantoketjuun liittyvässä koulutuksessa. Palveluista on tehtävä yksinkertaisia, konkreettisia ja helposti ymmärrettäviä unohtamatta kuitenkaan luottamuksellisten tietojen suojaamista. Yksinkertaisuus tuottaa jo itsessään turvallisuutta.

2.1 Riskienhallinnan ja toimintavarmuuden kehittäminen

Riskien hallinta muodostaa tietoyhteiskunnan tiedon varmistamisen perustan ja takaa järjestelmän toimintavarmuuden ja yritysten liiketoiminnan jatkuvuuden. Riskienhallintanäkökulma tulee aina sisällyttää uusien tuotteiden ja palveluiden suunnitteluun. Yrityksissä riskienhallinta ei ole pelkästään it-asiantuntijoiden tehtävä, vaan se on kyettävä integroimaan kiinteäksi osaksi liiketoiminnan suunnittelua, johtamista ja toteutusta. Yritysten riskienhallintajärjestelmän luominen on johdon asia. Riskien arviointi ja minimointi kuuluu jokaiseen palveluiden kehittämisvaiheeseen. Strategian tehtävänä on edistää riskienhallintamenettelyjen käyttöä. Tämän toiminnan on tapahduttava saumattomassa yhteistyössä viranomaisten, yritysten ja kansalaisten kanssa.

2.2 Yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa tilanteissa

Yhteiskunnan riippuvuus tieto- ja viestintäjärjestelmistä on hyvin kokonaisvaltaista ja syvenee entisestään. Samalla kuitenkin kilpailu ja pyrkimys kustannustehokkuuteen saattaa vähentää käytettävyyden turvainvestointeja. Arjen tietoyhteiskunnassa yhä suuremmaksi haasteeksi muodostuu entistä monimutkaisempien verkkoja toimintavarmuus ja niiden riskien hallinta. Jo pelkästään internetin kautta tapahtuvaan sähköisten laitteiden ohjaamiseen (esim. katuvalaistuksen ja liikennevalo-ohjauksen siirtyminen internetiin) liittyy suuria riskejä häiriötilanteiden osalta. Yhteisillä harjoituksilla parannetaan varautumista häiriöihin normaalioloissa sekä turvaamaan toiminnan jatkuvuus poikkeusoloissa. Harjoituksissa panostetaan yhteistyömallien luomiseen ja testaukseen. Harjoituksia kehitetään konkreettisen toiminnan suuntaan.

3.1 Suomen houkuttelevuuden ja kilpailukyvyn vahvistaminen ennustettavuutta lisäämällä

Sääntely-ympäristön selkeys ja ennustettavuus on keskeinen tekijä yrityksille. Suomen tulee kehittää lainsäädäntöään siten, että tietoturvakysymyksiin sääntely on mahdollisimman kevyttä ja samalla kattavaa. Viranomaisten tulee lainsäädäntöä kehittäessä kriittisesti tarkastella sen vaikutuksia yritysten toimintaedellytyksiin ja kansalaisten/kuluttajien oikeuksiin (mahdolliset ristiriitanäkökohdat on otettava huomioon). Yhä useampi yritys on monikansallinen ja toimii globaaleilla markkinoilla. Ongelmaksi käytännössä on osoittautunut se, että kansalliset säädökset sekä EU-direktiivien toimeenpano eri maissa eroavat toistaan. Tämä osaltaan vaikeuttaa myös suomalaisten, monessa maassa toimivien, yritysten toimintaedellytyksiä.

3.2 Ennakoivan ja vaikuttavan kansainvälisen yhteistyön terävöittäminen

Ennakoiva ja vaikuttava kansainvälinen toiminta edellyttää hyvää kansallista koordinaatiota ja toimintojen priorisointia. On tärkeää, että kansainvälinen vaikuttaminen aloitetaan riittävän varhaisessa vaiheessa (esim. osallistumalla aktiivisesti valmisteluvaiheen työryhmiin ja epävirallisiin verkostoihin). On tärkeää kartoittaa kansainvälisiä hyviä käytäntöjä sekä kyetä viemään suomalaista tietoturvaosaamista ulkomaille. Lisäksi suomalaisen lainsäädännön ja sääntely-ympäristön edistyksellisyyttä tulee riittävästi ”markkinoida” kansainvälisessä yhteistyössä. Tätä kautta Suomen on mahdollista vaikuttaa muiden maiden

regulaatiokäytäntöihin tavalla, joka palvelee suomalaisten yritysten toimintaa globaaleilla markkinoilla.

Menestyminen kansainvälisen yhteistyössä edellyttää myös aktiivista vaikuttamista EU:n tietoyhteiskuntapolitiikan ja kansainvälisten järjestöjen tietoturvaa koskeviin linjauksiin. Toimivan ja tuloksekkaan NCSA-toiminnon (kansallinen tietoliikenneturvallisuusviranomainen, National Communications Security Authority) perustaminen edistäisi Suomen osallistumista kansainväliseen yhteistyöhön sekä suomalaisten tietotekniikka-alueen toimijoiden osallistumista kansainvälisiin tarjouskilpailuihin. Tietoliikenneturvallisuusviranomaisen rooli kansainvälisen yhteistyön edistäjänä toisi näkyvyyttä suomalaiselle tietoturvaosaamiselle niin viranomais- kuin yritysmaailman kannalta.

Strategian toimeenpano

Lähtökohdat

Nykyisen työjaon mukaan tietoturvallisuus ja tietoturvallisuuden kehittäminen kuuluu voimassa olevan lainsäädännön mukaan usean toimijan vastuulle, sekä yksityisen sektorin että julkisen sektorin vastuulle. Valtioneuvoston ohjesääntöön (262/2003, muutettu 1.1.2008) on kirjattu ministeriöiden työnjako.

Toimeenpanon organisointi

Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriön asettaman Arjen tietoyhteiskunnan tietoturvallisuus –ryhmä tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Arjen tietoyhteiskunnan tietoturvallisuus –ryhmässä on laaja-alaisesti toimijoita sekä yksityisen sektorin että julkisen sektorin osalta. Työryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategiaa sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä.

Arjen tietoyhteiskunnan tietoturvallisuusryhmä perustettiin 31.8.2007 ministeri Suvi Lindénin päätöksellä vuosiksi 1.9.2007 - 28.2.2011. Ryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmä käsittelee tietoturvaan liittyviä laajoja ja eri sektoreita ylittäviä kysymyksiä läheisessä yhteistyössä muiden tietoturvallisuutta edistävien tahojen kanssa.

Taloudelliset ja yhteiskunnalliset vaikutukset

Periaatepäätöksessä asetetut tavoitteet voidaan toteuttaa kehyspäätösten sekä vuosittain talousarvioin yhteydessä tehtävien päätösten puitteissa. Strategian avulla lisätään kaikkien käyttäjien tietoturvaosaamista ja –tietoisuutta. Strategian avulla lisätään ja vahvistetaan kansallista yhteistyötä tietoturvan osalta.