15.12.2015

Suomen tietoturvallisuusstrategian luonnosversion 9.12.2015 kommentointi

SAMLINK

Kiitän mahdollisuudesta kommentoida Suomen tietoturvallisuusstrategian luonnosta.

Pidän tietoturvallisuusstrategiassa erityisen hyvänä seuraavia toimenpiteitä:

- Tietoturvallisuuden perustavoitteen – luottamuksen – korostamista
- Kansalaisten yksityisyyden suojan korostamista tietoturvallisuutta kehitettäessä
- Tilannekuvan muodostamista tietoturvariskien aiheuttamista vahingoista sekä niiden ja ennaltaehkäisyn kustannusvaikutuksista

Tietoturvallisuusstrategian suhde Suomen kyberturvallisuusstrategiaan toimeenpano-ohjelmineen on epäselvä. Suosittelen selventämään heti dokumentin alussa, miten kyberturvallisuus- ja tietoturvallisuusstrategia liittyvät toisiinsa – vai liittyvätkö.

Esitän seuraavia huomioitani strategian toimenpiteisiin liittyen liittyen:

- Strategian toimenpiteitä voisi vielä konkretisoida. Melko paljon on mainittu selvityksiä, kartoituksia ja huomiointeja. Mitä vaikutuksia näillä käytännössä tavoitellaan?
- Yhtenä toimenpiteenä on parantaa luottamusta sähköisiin transaktioihin sähköisen tunnistamisen kansallisen luottamusverkoston avulla. Käsittääkseni luottamusverkoston pääasiallinen tavoite on helpottaa käyttäjien ja tunnistamispalveluja tarvitsevien tahojen toimintaa. Tunnistuspalvelut ovat jo aiemminkin olleet vahvoja, toimivia ja luotettuja (pankkitunnisteet, mobiilivarmenteet).
- Toimenpiteenä on sertifiointien merkityksen selvitys. Yritysten ja kuluttajien näkökulmasta ongelma on, että palvelujen ja tuotteiden tietoturvatason arviointi ja vertailu on erittäin hankalaa ilman erityisasiantuntemusta (ns. ”market for lemons” – ongelma). Suosittelen miettimään keinoja, kuinka palvelujen ja tuotteiden laatu tietoturvan osalta voidaan tuoda näkyväksi – ilman raskaita auditointi- tai sertifiointiponnistuksia.
- Toimenpiteenä mainitaan anonymisointi henkilötietojen käsittelyyn liittyvien riskien pienentämiseksi. Sähköisissä palveluissa käytetään nykyään aivan liian laajasti henkilötunnusta (HETU). Tietääkseni myös nykyiset suunnitelmat sähköisen tunnistamisen luottamusverkostoon liittyen perustuvat vahvasti HETU:n käsittelyyn ja jakamiseen. On mahdollistettava sähköisen asiointitunnuksen (SATU) käyttö palveluissa ja kannustettava sen käyttöön.

Lisäksi haluan esittää muutamia mielestäni varteenotettavia, uusia näkökohtia:

- Perusteluosassa tuodaan esiin tietoturvan huomioimisen tarve jo ohjelmistokehityksen alkuvaiheessa. Tätä ei kuitenkaan mielestäni tuoda riittävästi esille varsinaisessa strategiassa. Digitalisoinnin ytimessä on sovelluskoodi. Tarvitaan toimenpiteitä tietoturvan rakentamiseksi sisään sovelluksiin ja sovellusarkkitehtuureihin.
- Perusteluosassa korostetaan salausmenetelmiin liittyvää osaamista. Tällaista erikoisosaamista toki Suomessa tarvitaan lisää, mutta tietoturvallisissa kokonaisratkaisuissa salaus on vain yksi ratkaisuelementti muiden joukossa. Suurimmalle osalle liiketoimintaa harjoittavia yrityksiä riittää salausteknologioiden perusosaaminen ratkaisujen tuottamiseksi hyvien, luotettavien salaustuotteiden avulla.

- Suomessa on toteutettu kansallisia tietoturvallisuusvaatimuskokonaisuuksia, kuten Valtionhallinnon tietoturvatasot ja KATAKRI. Suuri osa yrityksistä tukeutuu kuitenkin kansainvälisiin IT- ja tietoturvallisuusstandardeihin, kuten ISO 27001, ISF Standard of Good Practice for Information Security, ITIL ja COBIT. On varmistettava, että suomalaisia yrityksiä ei laeilla ja määräyksillä pakoteta kansallisten standardien käyttöön. Näin on mahdollisesti tapahtumassa esim. sähköisen tunnistamisen kansallisen luottamusverkostoon liittyen, jossa KATAKRIa esitetään toimijoille vaatimuksena.
- Tietoturvavastuiden sopiminen eri osapuolten välillä on yrityksille haastavaa ilman tietoturvan erityisosaamista. Suosittelen arvioimaan, olisiko mahdollista tuottaa tietoturvasopimusmallit ja –mallilausekkeet esim. samaan tyyliin kuin HVK SOPIVA toiminnan jatkuvuuden takaamisen alueella.

Lopuksi haluan tuoda esille yhteiskuntamme tietoturvallisuusasenteisiin liittyvän kypsymättömyyden. Palvelun tietoturvasta ei useinkaan olla halukkaita maksamaan, mutta tietoturvaloukkaustilanteessa palveluntarjoajaa moititaan julkisuudessa – joskus jopa kohtuuttomasti. Täydellinen tietoturva on mahdotonta ja yleinen asenneilmapiiri olisi saatava sellaiseksi, ettei tietoturvaloukkauksen ilmoittanut taho ole automaattisesti syyllinen. Eri palveluilla on erilaiset tietoturvavaatimukset ja luonnollisesti on suhtauduttava vakavasti esim. henkilötietojen vuotoon, mutta satunnaisen verkkosivun ”hakkerointi” automaattisella työkalulla ei ole yhtä vakava onnettomuus. Yleistä kansalaisten tietoutta tietoturvasta ja digitaalisen maailman riskeistä on siis syytä edistää. Tällöin myös palveluntarjoajien halukkuus informoida käyttäjiä tietoturvaratkaisuistaan ja –poikkeamistaan lisääntyy.

Kunnioittavasti,

Jari Pirhonen
turvallisuusjohtaja
Oy Samlink Ab