Cyber Security
JYVÄSKYLÄ - FINLAND

Tietoturvastrategian kuulemistilaisuus 14.12.2015

Mika Kataikko,
Kyberturvallisuusjohtaja,
Jykes & Kyber INKA

Cyber Security
JYVÄSKYLÄ - FINLAND

Yleiset kommentit tietoturvastrategialuonnokseen (1/3)

1.1. Koska kyseisessä strategialuonnoksessa todetaan strategian keskittyvän elinkeinoelämän tietoturvallisuuden ja kilpailukyvyn edistämiseen, on strategialuonnoksen nimi harhaanjohtava, kyseessä on pikemmin ”Suomalaisen elinkeinoelämän tietoturvallisuusstrategia.

1.2. Jotta dokumentti voisi olla Suomen tietoturvallisuusstragia, tulisi dokumentissa ottaa vahvemmin kantaa myös julkisen sektorin järjestelmien ja ratkaisujen turvallisuuteen, ja yhtä lailla, huomioida selvemmin akateemisen maailman rooli ja tarvittavat toimenpiteet tietoturvallisuuden huomioon ottamiseksi Suomessa.

Cyber Security
JYVÄSKYLÄ - FINLAND

Yleiset kommentit tietoturvastrategialuonnokseen (2/3)

1.3. On hyvä asia, että tämä strategialuonnos ottaa kantaa suomalaisen elinkeinoelämän tietoturvallisuuteen ja sen kehittämiseen. Mutta olisi tärkeätä huomioida strategiassa suomalaisen elinkenoelämän moninaisuus, ottaen huomioon ainakin seuraavat elinkeinoelämän toimijoita luokittelevat attribuutit:

i) Globaali (vievä) – Kansallinen
ii) Julkinen toimija – yksityinen yritys
iii) PK-yritykset (ja mikro-yritykset) – Suuryritykset
iv) Tietoturvallisuuden tilaaja – tietoturvallisuuden toimittaja
v) Tietoturvallisuuden soveltaja – tietoturvallisuuden toteuttaja

Cyber Security
JYVÄSKYLÄ - FINLAND

Yleiset kommentit tietoturvastrategialuonnokseen (3/3)

1.4. Strategialuonnoksessa mainitaan useasti tarve yhteistyölle, mutta pelkän maininnan lisäksi strategiassa olisi tarpeellista tuoda esille konkreettisia yhteistyötapoja, jota strategian toimeenpanolla tavoitellaan. Strategian (ja sen toimeenpanosuunnitelman) pitäisi vastata kysymykseen ”Mistä suomalainen (tietoturvaa soveltava) PK-yritys saa apua ja tukea omalle toiminnalleen?”

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (1/X)

Sivu 2, kolmas kappale: Kyseinen strategialuonnos ottaa kantaa EU:n verkko- ja tietoturvallisuusdirektiivin toimeenpanosta, mutta olisi ehdottoman tärkeätä myös kirjoittaa strategialuonnoksessa auki ko. strategian suhde tulevaan EU:n tietosuoja-asetukseen (siihen kuitenkin viitataan tässä strategialuonnoksessa)

Sivu 2, kuva: Tarkoitetaanko kuvassa oikealla alhaalla olevassa tekstissä ”Tietoturvaklusteri” jotakin olemassa olevaa suomalaista tietoturva-organisaatioita tai yhteistoimintaelintä ?

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (1/X)

Sivu 6, Toimenpide #3: On ehdottoman tärkeä ja kannatettava toimenpide, erityisesti suomalaiset yksityiset ihmiset ja pk- ja mikroyritykset tarvitsevat tähän liittyen apua

Sivu 6, Toimenpidelista : Koska kyseisen toimenpidekokonaisuuden tarkoituksna on edistää suomalaisten käyttämien ja myös tuottamien ja toimittamien ratkaisujen tietoturvaa ”sisäänrakennettuna” ominaisuutena, tähän kohtaan tulisi lisätä myös tuotteiden ja palvelujen tietoturvan todentaminen (testaaminen). Suomessa on useita tieto- ja kyberturvallisuuden tutkimus-, testaus- ja harjoitteluympäristöjä, joita yksityisten toimijoiden pitäisi enenevässä määrin käyttää suomalaisten digitaalisten palvelujen turvallisuuden todentamiseksi. Näitä ympäristöjä ovat esim.

i) VTT:n Cyber War Room (http://www.vtt.fi/medialle/uutiset/vtt-n-kyberlaboratorio-etsii-turva-aukot-luotettavasti)

ii) JAMK:n JYVSECTEC:n RGCE (http://jyvsectec.fi/fi/kyberymparisto/)

iii) VTT:n ja Aalto yliopiston SAICS (http://www.fisc.fi/hankkeet/)

iv) KYAMK:n kyberlaboratorio (http://www.ictlab.kyamk.fi/images/kyberturvallisuus/tekstit/Kyberlaboratorion_ja_osaamisen_tilanne_13022015.pdf)

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (3/X)

Sivu 7, Toimenpide #1: Tilannekuvan muodostaminen on ehdottoman kannatettava asia, olisi tärkeätä pyrkiä arvioimaan myös Resilience – kustannuksia (eli niitä kustannuksia, jotka koituvat yrityksen mahdollisesta toimintakyvyn heikkenemisestä siinä tilanteessa, kun yritys on hyökkäyksen / laittoman toimenpiteen vaikutuksessa.

Sivu 7, Toimenpide #2: Tässä tulisi korostaa myös Proaktiivisuutta Komission ja varsinkin DG CONNECT:n suuntaan, tavoitteellista on että Suomi on entistä enemmän sekä referenssien että osaamisen kautta suuntaamassa Eurooppalaista innovaatiota turvallisempaan suuntaan. Tällä alueella erityisesti referenssit ”Public – Private –partnership – alueella” erityisen tärkeitä.

Sivu 7, Toimenpidelista: Osaamisen kehittämisessä olisi tärkeätä tunnistaa niin kutsutut toimiala-osaajat, eli ne ihmiset, joiden syväosaaminen on jollakin digitalisaatiota soveltavalla toimialalla (esim. valmistava teollisuus, terveydenhuolto, jne.) ja joilla on riittävä ymmärrys tietoturvallisuudesta. Tunnettu tosiseikka on, että esim. automaatioinsinöörit ja tietoturvallisuuden osaajat eivät ”kasva samassa puussa”

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (4/X)

Sivu 8, Toimenpide #1: Onko tässä tavoitteena kansallinen vai kansainvälinen malli ? Onko tarkoituksena tehdä vain ”snapshot” nykyhetkeen, vai pyrkiä jatkuvaan toimintaan ?

Sivu 8, Toimenpide #5: Standardointi tietoturva-alueella on erittäin kannatettava asia, esim. IoT-alan standardointi laahaa, josta syystä meillä on turvattomia ”älytelevisioita”, ”älyjääkaappeja”, sairaanhoidon kuvantamislaitteita, teollisuuden PLC-laitteita, jne… Nämä kaikki laitteet ovat turvallisia omalla sovellusalueellaan, mutta niille ei ole vaatimuksia / standardia tiedonsiirron näkökulmasta.

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (5/X)

Sivu 12, luettelo #3: Tahattomien vahinkojen ja tahallisen toiminnan lisäksi on myös nk. ”force majeure”-tyyppisiä tilanteita, jotka on hyvä tunnistaa.

Sivu 12, luettelo #4: Tietoturvariskit aiheuttavat toteutuessaan tyypillisesti myös kustannuksia, jotka johtuvat yrityksen tai toimijan alenneesta toimintakyvystä = resilience.

Sivu 13, kappaleen 1: Tietoturvariskit voivat johtua jopa heikosti suunnitellusta arkkitehtuurista, joskus jopa heikosti mietitystä tuotteen tai ratkaisun konseptista. Siksi ei voi puhua pelkästää suunnittelusta ja toteuttamisesta koodausmielessä, vaan Privacy by design tarkoittaa myös esim. järjestelmäsuunnittelua / arkkitehtuurisuunnittelua, tästä hyvänä esimerkkinä OP Pohjolan ongelmat vuoden 2014-2015 vaihteessa.

Cyber Security
JYVÄSKYLÄ - FINLAND

Kommentit tietoturvastrategialuonnoksen sisältöön (6/X)

Sivu 18, Otsikko ”Tietoturvaan liittyvä osaaminen”: Teknisen tietoturvan osaaminen on todella tärkeä asia, mutta yhtälailla osaamista pitää kehittää tietoturvaan liittyvien prosessien ja menetelmien osalta, varsinkin sovellusalueeseen liittyen, ja myös tietoturvan johtamisen osalta.

Cyber Security
JYVÄSKYLÄ - FINLAND