Eduskunta
Liikenne- ja viestintävaliokunta
Asia: U 58/2017 vp Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi ("kyberturvallisuusasetus")

Viite: Pyydetty asiantuntijalausunto 13.11.2017

Riskienhallinnasta, tieto- ja kyberturvaturvallisuudesta, toiminnan jatkuvuudesta ja varautumisesta häiriötilanteisiin sekä henkilötietojen käsittelyyn liittyvästä tietosuojasta (”digitaalinen turvallisuus”) on muodostunut sitä kriittisempi kokonaisuus, mitä enemmän yhteiskunnat ja organisaatiot ovat aluksi sähköistäneet 1990–2010 -luvuilla ja nyt digitalisoineet 2010-luvulla omia toimintaprosesseja. Teknologian jatkaessa kehittymistä ns. Mooren lain mukaisesti, se tulee tarjoamaan jatkossa kiihtyvällä vauhdilla uudenlaisia, entistä kehittyneempiä mahdollisuuksia toiminnan kehittämiseen uudelleenmuotoiltujen palveluiden, päätelaitteiden sekä muiden uutta teknologiaa (keinoäly, robotisaatio) hyödyntävien laitteiden muodossa.

Valitettavasti tämä sama mahdollisuus koskee valtioiden ja organisaatioiden ohella myös tietoverkko- ja muita rikollisia sekä tiedusteluorganisaatioita. Tämän johdosta on erittäin tärkeää, että digitaalista turvallisuutta kehitetään laaja-alaisena kokonaisuutena, jossa a) vahvistetaan ja kehitetään ENISAn toimintaa ja b) edistetään tieto- ja viestintäteknologiahyödykkeiden sertifiointia.

a) Vahvistetaan ja kehitetään ENISAn toimintaa

Euroopan unionin verkko- ja tietoturvavirasto ENISAn rooli on näkynyt toistaiseksi esimerkiksi Suomessa varsin vähän. Mikäli sen roolia kasvatetaan ja vahvistetaan, Suomen tulisi varmistaa sen toiminnasta saatava hyöty kasvattamalla ENISAn kanssa tehtävää yhteistyötä siten, että ENISAn toteuttamat hankkeet, tuottamat materiaalit, tiedot ja julkaisemat palvelut voidaan entistä paremmin saada koko yhteiskunnan digitaalisen turvallisuuden kehittämisen tueksi. Tämä tulisi toteuttaa varmistamalla Suomen osalta tarvittava vaikuttamis - ja asiantuntijatyö ENISAn kanssa ja huolehtimalla myös riittävästä resurssoinnista kansallisesti tämän työn hyödyntämiseksi.

b) Edistetään tieto- ja viestintäteknologiahyödykkeiden sertifiointia

Digitaalisessa turvallisuudessa tulisi tunnistaa sekä nykyinen toimintaympäristö että toiminnan muuttuminen seuraavan vuosikymmenen vuoden aikana. Tällä hetkellä keskeinen huolenaihe liittyy esineiden-internet-laitteiden (Internet of Things, IoT) muodostamaan uhkaan. Tässä suomalaisella osaamisella (palvelumuotoilu ja sovelluskehitys, digitaalinen turvallisuus, turvallisten laitteiden valmistus) on merkittävä liiketoimintamahdollisuus erikoistua ja tarjota palveluita entistä globaalimmin myös EU-alueelle haluaville toimijoille.

Todennäköisesti IoT-laitteita merkittävämpi uhka tulee pitemmällä aikavälillä muodostumaan erilaisten keinoälyjärjestelmien kehittymisestä niiden saavuttaessa syväoppimisen kautta kehitysvaiheen, jonka seuraaminen ja valvominen ihmisten toimesta voi olla täysin mahdotonta. Tällainen keinoäly luo merkittävän, nykyistä digitalisaatio-vaihetta suuremman mahdollisuuden laaja-alaiseen rakennemuutokseen koko Euroopan Unionin tasolla, mutta samalla se luo erittäin suuren uhkan, johon liittyvät riskit tulisi tunnistaa ja ottaa hallintaan.

Tässä yhteydessä luotava sertifiointijärjestelmän tulisi olla tarvittaessa monipuolisesti skaalautuva ja riittävän laaja ottamaan huomioon teknologian nopea kehittyminen. Samassa yhteydessä tulisi kuitenkin ottaa huomioon, että laadittava sertifiointiohjelma tukee digitaalisten laitteiden ja palveluiden turvallista kehittämistä tarkoituksenmukaisesti liiketoiminnan osana eikä siten, että se näyttäytyy lähinnä hallinnollisena rasitteena, jolloin se kääntyy itseään vastaan ja aiheuttaa vain lisääntyviä kustannuksia.

Lisäksi tulisi huolehtia siitä, että riskienhallinta toimii entistä keskeisemmässä roolissa organisaatioissa niin digitaalisten laitteiden ja palveluiden käyttöönottamisessa kuin niiden kehittämisessä. Mikäli organisaatio ei tunnista käyttämäänsä teknologiaan ja palveluun liittyviä uhkia, on sen mahdotonta hyödyntää tätä teknologiaa tarkoituksenmukaisesti ja kustannustehokkaasti.

Sertifiointiohjelman kolme tasoa tulisi kytkeä myös siihen, kuinka kriittisestä toiminnasta on kyse. Tällöin laitteet ja palvelut voisivat jakautua kolmeen käyttötarkoitukseen niiden turvallisuuden näkökulmasta, jolloin organisaatioiden ja osin myös kansalaisten olisi myös paremmin mahdollista hankkia laitteita ja palveluita paremmin heidän tarvitsemaan käyttötarkoitukseen.

Yhteenveto

Koska digitaalista turvallisuutta koskevat uhat kasvavat nopeammin kuin siihen liittyvät keinot suojautua, ehdotuksessa kuvatut toimenpiteet oikealla tavalla toteutettuna ovat sellaisia toimenpiteitä, joiden avulla Euroopan Unionin alueesta voidaan vahvistaa globaalina turvasatamana digitaaliselle liiketoiminnalle niin jo siellä toimiville tai sinne haluaville yrityksille kuin kansalaisille. Samanaikaisesti käynnissä olevat EU:n yleisen tietoturva-asetuksen soveltaminen 25.5.2018 alkaen sekä verkko- ja tietoturvadirektiiviin kansallinen täytäntöönpano luovat Euroopalle mahdollisuuden saavuttaa kilpailukykyä digitaalisessa toimintaympäristössä kun nämä toimenpiteet on saatu käyttöön ja vaikuttamaan. Näitä vaikutuksia on kuitenkin kunnolla mahdollista arvioida vasta 2020-luvulla.

Tämän kaiken vastakohtana on se, että nyt EU:n suunnittelemat toimenpiteet toteutetaan tai kohdistetaan väärin, joka aiheuttaa pahimmillaan sellaisen tilanteen, joka karkottaa nykyisiä Eurooppalaisia toimijoita muualle sekä vähentää myös EU:n ulkopuolelta tänne kiinnostuneiden yritysten kiinnostusta. Tasapaino tarvittavan turvallisuuden ja sen toteuttamisen sekä ylisääntelyn ja hallinnollisen työn välillä on siten keskeisessä roolissa, jotta tässä luotavat toimintarakenteet toimivat mekanismeina suuremman kansalaisten ja yritysten luottamuksen ja sitä kautta menestymisen ja liiketoiminnan mahdollistajina.

Kimmo Rousku
Erityisasiantuntija, VAHTI-pääsihteeri
kimmo.rousku@vm.fi, puh. 050 566 2996