Eduskunta
Liikenne- ja viestintävaliokunta
Asia: E 83/2017 vp Valtioneuvoston selvitys: Kyberturvallisuus; strategia; puolustus; digitaaliset sisämarkkinat

Viite: Pyydetty asiantuntijalausunto 13.11.2017

Viittaan tässä lausunnossa antamaani lausuntoon U 58/2017 vp Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi ("kyberturvallisuusasetus"), koska siinä esitetyt kommentit koskevat myös tätä laajempaa tiedonantoa.

Kyberturvallisuudessa, laajemmassa yhteydessä digitaalisessa turvallisuudessa tulee varmistua esimerkiksi seuraavien osa-alueiden toteutumisesta

a) Kyvykkyys puolustautua digitaalisia uhkia vastaan
   - Hallinnolliset ja tekniset prosessit ja teknologiat

b) Havainnointikyky
   - Kyvykkyys tunnistaa toimintaan liittyviä uhkia ja poikkeamia
     - Riskienhallinta ja muut hallinnolliset keinot
     - Tekninen turvallisuus ja seuranta

c) Reagointikyky
   - Tieto- tai kyberturvallisuuspoikkeaman, tietoturva- tai sietosuojaloukkauksen osalta kyvykkyys käynnistää tarvittavat toimenpiteet näiden arvioimiseksi ja tähän reagoimiseen

d) Kyky palautua normaaliin toimintaan poikkeaman jälkeen
   - Toiminnan jatkuvuuteen ja varautumiseen liittyvät prosessit, joilla organisaation toiminta saadaan palautettua häiriö- tai poikkeamatilanteen jälkeen sen toimintavaatimusten (tärkeys, kriittisyys) mukaisesti

e) Ohjeistus, koulutus ja aktiivinen viestintä
   - Organisaation henkilöstön sekä sen alihankkijoiden ja sidosryhmien osalta

Suomessa tätä kokonaisuutta edistetään muun muassa Suomen kyberturvallisuusstrategian (2013) sekä siihen liittyvän toimeenpano-ohjelman avulla (2017-2020). Tämän ohella valtiovarainministeriö vastaa julkisen hallinnon digitaalisen turvallisuuden kehittämisestä, julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) toimiessa kehittämisen ja yhteistyön elimenä.

Nyt tässä lausunnolla olevassa kokonaisuudessa katetaan useimmat edellä olevat osa-alueet sekä nostetaan esille uusia menetelmiä kyberturvallisuuden vahvistamiseksi Euroopan Unionissa. Tässä yhteydessä tulee korostaa sitä, että vaikka usein esille nostetaan tietoturvauhkien merkitys kyberturvallisuudelle (tietojen tai toiminnan luottamuksellisuus, saatavuus ja eheys) alue, vielä suurempi riski syntyy normaalissa ICT-palvelutuotannossa esiintyvistä häiriöistä. Tämän takia tulisi huomata, että sekä uhat että keinot kehittää toimintaa näitä uhkia vastaan vaihtelevat merkittävästi riippuen siitä, kehitetäänkö toimintaa ja kyvykkyyksiä tietoturvauhkia vai muita ICT-palvelutuotantoon liittyviä uhkia vastaan. Nykyinen pitkälle kehittynyt yhteiskunta edellyttää molempien osa-alueiden huomioimista ja kehittämistä.

Uhkatilanne tulee joka tapauksessa molempien osalta merkittävästi muuttumaan, koska toiminnan digitalisaation määrä ja luonne (digitalisaatio, automatisaatio, keinoäly ja robotisaatio) sekä tätä toimintaa uhkaavat tekijät (tietoverkko- ja kyberrikollisuus, riippuvuus sähköstä sekä muista kriittistä infrastruktuuria suojelevista rakenteista) ovat myös valtavassa muutoksessa.

Esimerkki uudenlaisesta uhkatilanteen muutoksesta ovat viimeisen parin vuoden aikana kyvykkäiltä valtiollisilta toimijoilta varastetut kybertoimintaympäristöön kehitetyt tiedustelu- ja hyökkäystyökalut, joita melkein kuka tahansa osaava asiantuntija tai organisaatio voi nyt valjastaa omaan käyttöönsä.

Näiden seikkojen johdosta nyt luotavien rakenteiden tulee olla joustavia ja skaalautuvia samalla tavalla, mitä teknologiamuutos, toimintarakenteiden ja nopeasti kehittyvä uhkatilanne niiltä edellyttävät. Tässä yhteydessä tulisi myös selkeästi nostaa esille sellaiset keinot, joilla digitaalista turvallisuutta kehitetään yhä enemmän hyödyntämään automatisaatiota (esimerkiksi ohjelmistorobotit) sekä keinoälyä, koska muilla keinoilla ero näitä keinoja hyödyntävien tietoverkko- ja kyberrikollisten ja yhteiskunnan ja yritysten suojautumiskeinojen välillä kasvaa kriittisen suureksi. Tämä voi pahimmillaan johtaa kansalaisten ja yritysten luottamuspulaan digitaalisessa toimintaympäristössä toimittaessa.

Digitaalinen turvallisuus edellyttää kehittämistä kaikilla yhteiskunnan tasolla, poliittisesta päätöksenteosta ja kyberdiplomatiasta kyberpuolustuksen kehittämiseen sekä kansalaisten tietoisuuden kasvattamiseen myös hybridiuhkien, erityisesti informaatiovaikuttamisen osalta. Tässä kansainvälinen yhteistyö ja tiedonvaihto ovat entistä tärkeämmässä roolissa, koska digitaalisessa toimintaympäristössä tapahtuvat ilmiöt ja uhat ovat yhä globaaleimpia, toisaalta ne voivat olla myös entistä alueellisempia ja kohdistetumpia. Tämän johdosta esitys ENISAn toiminnan vakiinnuttamisesta ja kehittämisestä sekä vaikutustenarviointi kyberturvallisuuden osaamiskeskusten verkoston perustamisesta ovat keskeisiä keinoja yhteistyön, asiantuntijuuden sekä osaamisen kehittämiseksi.

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