Ruokavirasto

Lausunto

24.07.2024 3589/00.00.04/2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

1. Tämä kyberturvallisuusstrategian luonnos on varsin hyvä. Huomioitaessa kyberuhkien rajat ja toiminnot ylittävä luonne, niin strategiassa on riittävässä määrin huomioitu tämä ulottuvuus. Luonnoksesta jää myös varsin kattava kuva kokonaisuuden hahmottamisesta ja jäsentämisestä. Strategialuonnoksessa nostetaan vahvasti esille riittävä resursointi. Tällä hetkellä tämä heikentää strategian uskottavuutta, kun valtio ei ole resursoimassa esimerkiksi NIS2 toimeenpanoa, vaan NIS2 uudet tehtävät tulee toteuttaa nykyisillä resursseilla jostain muusta tinkien. Strategia ei kykene ohjaamaan toimijoiden resursointia, joten joiltain osin ohjaus jää tyhjän päälle. Resurssikysymys on tärkeä, mutta sitä voisi lähestyä jotenkin muutoin kuin nyt kirjatulla tavoin.

2. Yleisesti tässä oli hyvä asioita, kuten tunnistettu riittämättömät toimintaedellytykset. Myös julkisen sektorin osaamistarvetta tuotiin esille. Yleisesti ei ehkä täysin ymmärretä, että tämäkin tulee huomioida.

Varsinainen kommentti:

Kappale: Julkiset palvelut ovat turvallisia (mutta vaikea kohdistaa mihinkään yhteen kohtaan)

Dokumentista jäi yleisesti kuva, että keskeisiä keinoja ovat ennaltaehkäisy, tilannekuva ja yhteistoiminta. Ja usein nousee tavallaan luonnollisesti esille tietotekniset keinot. Tässä painotetaan kyberturvallisuudesta huolehtimista, joka on tärkeää, mutta pystyykö se täysin varmistamaan palveluiden jatkuvuuden ja saannin, kun jotakin kaikesta varautumisesti huolimatta tapahtuu. Dokumentissa mainitaan myös häiriönsietoky, mutta se jää hieman vähäiselle huomiolle. Häiriönsietokyvyn kehittämiseen ei kuitenkaan juuri kuvata keinoja (yhteistoiminnan lisäksi).

Nykyiset ratkaisut pohjautuvat käytännössä täysin digitalisaatioon, mutta ennaltaehkäisevien keinojen pettäessä voi toiminnan jatkuvuus ja palautuminen olla heikkoa. Miten jatkuvasti entistä enemmän digitalisoituihin palveluihin perustuvat palvelut tuotetaan häiriö yms. tilanteissa, joissa osa digitaalista toimitusketjua on vaurioitunut.

Yhtenä keinona dokumentissa on TKI-toiminta. Olisi hyvä olla myös tutkimustietoa miten nykyisessä digitaalisessa toimintaympäristössä suunnitellaan häiriönkestävä hajautunut toimintaketju. Tarvittaisiin siis enemmän tietoa miten suunnitella ja toteuttaa turvallinen palvelut (ei ainoastaan tietoteknisestä näkökulmasta, vaan toiminnan näkökulmasta). Mikäli ennaltaehkäisy pettää ja jos häiriönsietokyky ei ole toiminnan tasolla (nojataan pelkästään tietotekniikkaan), niin vaikutukset voivat olla hyvinkin haitallisia.

3. a. Pitäisikö ottaa kantaa kyberhyökkäyskyvykkyyteen? Vai ollaanko vain puolustuksen kehittämisen varassa? Hyökkäyskyvykkyyden kehittäminen loisi edellytyksiä myös laadukkaamman puolustuksen rakentamiseen. Ei ehkä tämän dokumentin asia ja edistynee PV:n sisäisenä toimintona, mutta lakiteknisesti mietintään.

3. b. Kriittisen infran myymisen lainsäädäntö tai sen puuttuminen. Jos tulee tilanne että joku tarjoaa kriittisestä infrasta, luonnon varannoista tai logistiikasta riittävän suuren preemion niin miten kyberstrategia huomio vastaavat tilanteet?

Pyysalo Raimo
Ruokavirasto

Tieksola Olli-Pekka
Ruokavirasto