

Valtiovarainministeriö
PL 28
00023 VALTIONEUVOSTO

VN/36127/2023

Lausunto

Suomen Erillisverkot Oy kiittää mahdollisuudesta lausua Lausuntopyyntöön ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta.

Huomiot ehdotetusta soveltamisalan laajenemisesta varautumisen arviointiin sekä muutoksen mahdollisista vaikutuksista:

Esityksessä ehdotettu varautumisen arviointi osana tietojärjestelmien ja tietoliikennejärjestelyjen arviointia on kannatettava ja tarpeellinen lisä, joka tukee viranomaisten toiminnan jatkuvuutta häiriö- ja poikkeustilanteissa.

Jotta varautumisen arvioinnilla saavutetaan tavoiteltu vaikuttavuus, on kuitenkin jatkotyössä tärkeää kiinnittää huomiota käytettäviin arviointikriteeristöihin. Yhtenäisten, selkeiden ja riskiperusteisten varautumisen arviointikriteerien kehittäminen ja kansallinen ohjeistus ovat edellytys arviointien vertailtavuudelle ja laadulle.

Huomiot ehdotetuista arviointimenettelyjä koskevista muutoksista sekä uusista viranomaisia koskevista arviointivelvollisuuksista ja niiden vaikutuksista organisaation toimintaan (3–3 c §):

Esityksen tavoitteena on ajantasaistaa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskeva sääntely sekä selkeyttää arviointimenettelyjä ja toimijoiden rooleja. Tavoitteet ovat perusteltuja ja vastaavat toimintaympäristön muutoksiin, erityisesti lisääntyneisiin kyberturvallisuusuuhkiin ja monimutkaistuneisiin järjestelmäkokonaisuuksiin.

Pidämme myönteisenä, että esityksessä pyritään riskiperusteiseen lähestymistapaan ja arviointien oikeasuhtaisuuteen sekä keventämään menettelyjä erityisesti matalamman turvallisuusluokan järjestelmissä.

Esityksessä korostetaan viranomaisen vastuuta oman toimintansa ja järjestelmiensä tietoturvallisuuden arvioinnista vähintään itsearviointin keinoin. Itsearviointivelvollisuus on lähtökohtaisesti perusteltu, sillä se tukee viranomaisten omaa tietoisuutta tietoturvallisuuden ja varautumisen tilasta. Käytännön

vaikutusten osalta on kuitenkin huomioitava, että itsearviointien laatu ja kattavuus voivat vaihdella merkittävästi toteuttajien välillä. Ilman riittävää ohjeistusta ja yhteisiä arviointikriteerejä itsearvioinnit voivat muodostua muodollisiksi eikä niillä välttämättä saavuteta esityksen tavoitteita tietoturvallisuuden tosiasiallisesta parantamisesta. Itsearviointivelvollisuus tulee lisäämään myös viranomaisten asiantuntijaresurssien tarvetta. Kokemuksemme mukaan itsearvioinnit kuormittavat erityisesti arvioitavan kohteen vastuuhenkilöitä ja edellyttävät heiltä merkittävää ajankäyttöä, usein enemmän kuin varsinaista arviointityötä tekevältä taholta.

Muut arviointilakia koskevat huomiot (yksilöitynä pykälittäin):

Pidämme perusteltuna, että luotettavia palveluntarjoajia voidaan hyödyntää julkisten, salassa pidettävien sekä TL IV -tietojärjestelmien arvioinnissa (3 §). Jotta menettely olisi hallittu ja ennakoitava, olisi kuitenkin syytä:

- täsmentää laissa tai muussa sääntelyssä, mitä vähimmäisvaatimuksia luotettavalle palveluntarjoajalle asetetaan vähintäänkin niiltä osin, kun arviointi kohdistuu turvallisuusluokiteltuihin kohteisiin;
- arvioida, tulisiko luotettavien palveluntarjoajien käytöstä antaa yhtenäistä kansallista ohjeistusta;
- ohjata luotettavien palveluntarjoajien keskitettyyn hankintaan ja valintaan, esimerkiksi Hanselin yhteishankintasopimusten kautta, jolloin palveluntarjoajalta voitaisiin edellyttää vähimmäisvaatimusten täyttymistä jo sopimukseen liittymisen yhteydessä.

Palveluntarjoajien käyttäminen TL IV -arvioinneissa tulee todennäköisesti lisäämään arvioitujen kohteiden kattavuutta ja näin ollen parantaa tietoturvallisuuden tilannetta. Kuitenkin ilman palveluntarjoajiin kohdistuvia yhtenäisiä vaatimuksia on olemassa riski, että arviointitoiminnan laatu tulee vaihtelevaan merkittävästi. Tietoturvallisuuden taso voi jopa heikentyä nykytilanteesta, jossa TL IV -arviointeja tekevät tietoturvallisuuden arviointilaitokset vakiintuneilla ja ohjatuilla toimintatavoilla.

Ystävällisin terveisin

Markku Järvinen

Johtaja, Asiakkaat, Palvelut ja Varautuminen
markku.jarvinen@erillisverkot.fi

This documents contains 2 pages before this page
Dokumentet inneholder 2 sider før denne siden

Tämä asiakirja sisältää 2 sivua ennen tätä sivua
Dette dokument indeholder 2 sider før denne side

Detta dokument innehåller 2 sidor före denna sida

authority to sign
representative
custodial

asemavaltuus
nimenkirjoitusoikeus
huoltaja/edunvalvoja

ställningsfullmakt
firmateckningsrätt
förvaltare

autoritet til å signere
representant
foresatte/verge

myndighed til at underskrive
repræsentant
frihedsberøvende