Valtion tieto- ja viestintätekniikkakeskus Valtori

Lausunto

29.12.2020 Valtori/1636/00 05 00/2020

Asia: VN/24348/2020

# Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

## Lausunnonantajan lausunto

**Ehdotukset poliittisiksi linjauksiksi, kommentit:**

Valtion tieto- ja viestintätekniikkakeskus Valtori kiittää mahdollisuudesta lausua selvityksen väliraporttiin tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla.

Digitalisaation edetessä yhteiskunnan toimintakyvyn kannalta tärkeiden tietojen ja toimintojen riippuvuus tietoteknisten palvelujen ja verkkojen toiminnasta korostuu. Panostukset kyber- ja tietoturvallisuuden sekä varautumisen kehittämiseen ja resursointiin ovat tärkeitä uhkavektoreiden hallinnassa. Valtori näkee, että lausuntopyynnössä kuvattujen linjausten laatiminen on tärkeää, ja edesauttaa tilanteen kehittymistä oikeaan suuntaan.

Väliraportissa kuvattuihin linjauksiin esitämme seuraavat kommentit:

Linjaus 10: Kriittisille toimialoille säädetään velvoite määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot.

Linjaus on erittäin kannatettava. Ensiarvoisen tärkeää on tietää mitä tulee suojata, ja millä tavoin. Suojattavat tiedot on tunnistettava ja luokiteltava, jotta suojaustoimenpiteet kohdistuvat oikeisiin paikkoihin ja oikeamittaisina. Kun yksityinen yritys käsittelee valtiohallinnon tietoja, on tietojen luokittelu val-tiohallinnon toimijan vastuulla, mutta mm. niiden yksityishenkilöihin liittyvien tietojen osalta, jotka yritys kerää tai tuottaa itse, vastuu luokittelusta on yrityk-sellä itsellään. Yritysten kykyä tunnistaa ja luokitella oikein tällaisia tietoja voisi olla tarpeen tukea ja vahvistaa esimerkiksi tarkennetulla ohjeistuksella. Val-tiohallinnon osalta Yhteiskunnan turvallisuusstrategiassa (YTS) on tunnistettu yhteiskunnan toiminnan kannalta elintärkeät toiminnot, mutta niiden tunnista-minen ei ole riittävää ilman toimintojen selkeää priorisointia ja kriittisyysluokittelua, joka mahdollistaisi kunkin toiminnon kannalta keskeisten tietojen tunnistamisen ja luokittelun, sekä näiden avulla riittävän ja oikeasuhtaisen suojaamisen. Elintärkeiden toimintojen tunnistamisen jälkeen olisi

tärkeää myös tunnistaa toimintoihin liittyvien häiriöiden tarkat vaikutukset, toimintoihin liittyvät prosessit sekä niiden tueksi tarvittavat tiedot ja tietotekniset järjestelmät, sekä näiden keskinäiset riippuvuudet.

Linjaus 11, kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot

Tietojen suojauksen tulee perustua niiden luottamuksellisuuden ja kriittisyyden pohjalta määräytyviin vaatimuksiin, ei niitä käsittelevän organisaation kokoon, toimialaan tai osaamiseen. Tämä toki myös edellyttää, että vaatimukset ovat selkeitä, oikeasuhtaisia, kustannustehokkaita ja yksiselitteisesti todennettavissa. Vaatimusten todentamisessa ulkoisen toimijan toteuttama auditointi ei ole kuitenkaan ainoa vaihtoehto, esimerkiksi maksukorttitietojen suojaamiseen laadittu PCI-DSS -standardi käyttää pienempien toimijoiden kohdalla säännöllistä organisaation itsearviointia todentamiskeinona tilanteissa, joissa kattavan ja kalliin ulkoisen auditoinnin vuosittainen toteuttaminen olisi taloudellisesti kohtuutonta. Vastaavaa mallia voitaisiin harkita myös esim. pienempien terveysalan toimijoiden vaatimustenmukaisuuden todentamisessa.

Linjaus 23 (sekä linjaus 24), Arvioidaan tarve säätää Valtorin tietosuojaa ja tietoturvaa koskevista vastuista ja velvoitteista vastaavasti kuin on jo tehty Valtion talous- ja henkilöstöhallinnon palvelukeskuksen (Palkeet) osalta. Lähtökohtana on, että Valtorin tarjoamien ja välittämien kriittisten palveluiden on täytettävä voimassa olevan viranomaisten auditointi-työkalun (Katakri) TL IV -tason vaatimukset.

Linjauksen 23 ensimmäisen osan osalta Valtori näkee, että mahdollisten uusien tehtävien vaatimien lisäresurssien tarkastelu on huomioitava ja siten linjauksen 24 sanamuoto on kannatettava. Valtori näkee lisäksi, että mahdollinen tehtävä-kokonaisuuksien siirto on suunniteltava huolellisesti ja tarvittaessa varattava suunnittelun pohjalta riittävä siirtymäaika.

Linjauksen 23 toisen osan osalta tulkintamme mukaan sanamuoto TL IV -tason vaatimusten täyttämisestä edellyttäisi kriittisten palvelujen sijaintia ja tuotta-mista vain Suomen rajojen sisäpuolelta. Käsityksemme mukaan kriittisille palve-luille ei ole olemassa yksiselitteistä määrittelyä. Valtori esittää, että linjauksen kirjausta tarkennettaisiin niin, että asiakohdan vaikutukset selvitetään ennen toimeenpanoa.

Turvallisuusjohtaja Hannu Naumanen

Valtion tieto- ja viestintätekniikkakeskus, Valtori

**Väliraportin muut osat, kommentit:**

-

Tallinen Anna
Valtion tieto- ja viestintätekniikkakeskus Valtori - Lausunnon kirjoittanut
Hannu Naumanen