Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Lausunto

05.01.2021

TRAFICOM/543179/04.04.05.03/2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Liikenne- ja viestintävirasto pitää väliraportissa esitettyjä ehdotuksia kannatettavina. Ehdotettujen toimenpiteiden toteuttaminen vaatii viranomaisten talous- ja henkilöstöresurssien lisäämistä, ja on tärkeää, että toimenpiteistä päätettäessä, pidetään huolta riittävistä resursseista ja toimenpiteiden toteuttamiseksi viranomaisten nykyisiä resursseja kasvatetaan. Resurssoinnissa on hyvä jo tässä vaiheessa huomioida myös parhaillaan käynnissä oleva EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) uudistuksen mahdollisesti aiheuttamat lisäresurssitarpeet. Liikenne- ja viestintävirasto ehdottaakin, että toimenpide-ehdotuksissa vielä yhdeksi toimenpiteeksi selkeästi nostettaisiin esille kriittisten toimialoja valvovien viranomaisten resurssien kasvattaminen vastaamaan nykyisten tietoturva- ja tietosuojavaatimusten valvontaan ja raportissa esitettyjen uusien toimenpiteiden toteuttamiseksi ja vaatimusten valvontaan vaadittavia resursseja. Ilman näitä resursseja ei tietoturvallisuuden valvontaa ja ehdotettuja toimenpiteitä saada tehokkaasti toteutettua eikä tietoturvallisuuden ja tietosuojan tasoa nostettua kyseisillä kriittisillä toimialoilla.

Liikenne- ja viestintäviraston ehdottaa uudeksi toimenpiteeksi myös pilvipalveluiden ja -palveluntarjoajien kartoittamista osana kriittisten toimialojen toiminnan varmistamista. Kriittiset organisaatiot käyttävät pilvipalveluita entistä enemmän ja tehokkaan ohjauksen ja valvonnan kannalta olisi tärkeää, että Suomessa valvovalla viranomaiselle olisi tiedossa keskeiset pilvipalveluiden tarjoajat ja vastaavasti palveluntarjoajat olisivat tietoisija niitä koskevista vaatimuksista ja velvoitteista. Pilvipalvelut kuuluvat myös NIS-direktiivin soveltamisalaan ja ovat direktiivissä määriteltyjä Digitaaliset palvelut -kokonaisuutta. Tämä toimenpide tulee käytännössä tehtäväksi muutoinkin, jos NIS-direktiivin uudelleen tarkastelussa komission ehdotus pilvipalveluiden tarjoajien määrittämisestä keskeisten palveluntarjoajien joukkoon hyväksytään.

Liikenne- ja viestintävirasto ehdottaa myös, että yhtenä toimenpiteenä liikennetoimialan merkittävimmät toimijat arvioitaisiin ja tunnistettaisiin uudelleen ja arviointi tehtäisiin

kokonaisvaltaisemmin huoltovarmuuden ja yhteiskunnan toimivuuden näkökulmasta. Nykyisin NIS-direktiivin mukaisen lainsäädännön

sovelmistala on kapea ja moni huoltovarmuuden ja yhteiskunnan kannalta merkittävä toimija jää soveltamisalan ulkopuolle. Arvioinnissa voitaisiin huomioida

komission muutosehdotukset NIS-direktiivin arviointikriteereihin soveltamisalaan kuuluvien toimijoiden arvioimiseksi.

Liikenne- ja viestintävirasto pitää tärkeänä, että kriittisille toimialoille tietoturvavaatimuksia määriteltäessä arvioidaan ja säädetään tarvittaessa myös valvoville viranomaisille määräyksenantovaltuuksien lisäksi selkeät valvontavaltuudet, tiedonsaantioikeudet sekä mahdollisuus velvoittaa korjaaviin

toimenpiteisiin ja määrätä seuraamuksia merkittävistä lainsäädännön rikkomuksista. Tulisi myös harkita säädettäväksi valvovalle viranomaiselle mahdollisuus käyttää ulkopuolisia asiantuntijoita arvioimaan tietojärjestelmien vaatimustenmukaisuutta. On myös tärkeää, että kriittisille toimialoille tietoturvavaatimuksia määriteltäessä käytetään hyväksi se kansallinen liikkumavara, jonka kansainvälisen lainsäädäntö, mukaan lukien EU-lainsäädäntö mahdollistaa, jotta riittävä tietoturvallisuuden taso saavutetaan.

Väliraportin muut osat, kommentit:

Liikenne- ja viestintävirasto jakaa väliraportissa esitetyn nykytilan kuvauksen nykyisestä tietoturvallisuuden ja -suojan tilanteesta kriittisillä toimialoilla ja niitä valvovien viranomaisten resursseista. Tällä hetkellä pääosalle kriittisistä toimialoista asetetut tietoturvavaatimukset ovat hyvin ylätasoisia, minkä

seurauksena tietoturvallisuuden taso eri toimijoiden kuin myös eri toimialojen välillä on suuri. Nykyisin monella kriittistä toimialaa valvovalla sektoriviranomaisella ei myöskään ole riittäviä talous- ja henkilöstöresursseja valvoa nykyisiä kriittisille toimialoille asetettuja ylätason tietoturvavaatimuksia saati tulevaisuudessa mahdollisesti asetettavia tarkemman tason tietoturvavaatimuksia. Resurssivajeesta johtuen valvoville sektoriviranomaisille ei myöskään ole kertynyt riittävää osaamista tietoturvallisuudesta ja siihen liittyvästä ohjaus- ja valvontatyöstä. Erilaisiin toteutuneisiin tietoturvauhkiin ja -loukkauksiin

joudutaankin reagoimaan kriittisillä toimialoilla jälkijättöisesti ja kehittämistoimenpiteitä aletaan tekemään tulevaisuuden varalla vasta siinä vaiheessa, kun jokin merkittävä tietoturvauhka tai -loukkaus on jo realisoitunut, mistä Vastaamo-tapaus on esimerkki.

Liikenne- ja viestintävirasto pitää tärkeänä, että vastaavanlainen arviointi ja toimenpide-ehdotuksien kartoitus tehtäisiin myös muille kriittisille toimialoille kuin nyt raporttia laativan työryhmän toimeksiannossa määritellyille ja väliraportissa käsitellyille NIS-direktiivin mukaisille kriittisille toimialoille. Esimerkiksi

Huoltovarmuuskeskuksen julkaisemassa Kyberturvallisuuden nykytila eri toimialoilla – Kartoituksen keskeiset havainnot -julkaisussa on osoitettu selkeitä tietoturvallisuuden kehitystarpeita muun

muassa logistiikka-, media- ja elintarvikesektoreilla ja nämä tehdyt havainnot vastaavat myös Liikenne- ja

viestintäviraston käsitystä kyseisten toimialojen tietoturvallisuuden ja laajemmin kyberturvallisuuden tilasta. Monia näistä toimialoista ollaan digitalisoimassa tulevina vuosina, ja on olennaista, että tietoturvallisuudesta ja -suojasta huolehditaan alusta lähtien. Digitalisoinnin myötä esimerkiksi logistiikkasektorin huoltovarmuus- ja turvallisuuskriittisten kuljetusten tietojen digitalisoinnissa, tiedon käytettävyydessä ja jakamisessa tietoturvan merkitys korostuu entistä enemmän. Logistiikassa esillä oleva koko kuljetusketjun kattava tiedon virtaus ja muu digitalisaatiokehitys edellyttää aiempaa vahvempaa tieturvan ja tietosuojan toteuttamista.

Liikenne- ja viestintävirasto on julkaissut useita ohjeita ja oppaita orgnisaatioille tietoturvallisuuden kehittämisen tueksi. Nämä ohjeet ja oppaat ovat saatavilla viraston internetsivuilta (https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeetja-oppaat-organisaatioille-ja-yrityksille). Liikenne- ja viestintävirasto on parhaillaan valmistelemassa ohjetta (Verkkotunnusten turvallinen hallinta) verkkotunnusvälittäjille ja verkkotunnusten käyttäjille verkkotunnusten turvallisesta hallinnasta, missä esitetään suosituksia verkkotunnusten turvaamiseksi ja turvallisen käytön mahdollistamiseksi. Ohje käytännössä tulee koskemaan kaikkia kriittisten toimialojen ja julkishallinnon toimijoita. Liikenne- ja viestintäviraston on myös kehittänyt organisaatioiden käyttöön niin sanotun Kybermittarin (www.kybermittari.fi) tukemaan organisaatioiden kyberturvallisuuden kypsyystason arviointia ja kehittämistä. Virasto esittää, että raportissa viitattaisiin näihin edellä mainittuihin ohjeisiin ja oppaisiin sekä Kybermittariin ja kannustettaisiin kriittisten toimialojen ja julkisen sektorin toimijoita tutustumaan niihin ja hyödyntämään niitä omassa kyber- ja tietoturvallisuuden kehitystyössä.

Juutinen Jukka-Pekka
Liikenne- ja viestintävirasto