VALTIOVARAINMINISTERIÖ

Lausunto

VN/24348/2020-VN-saap-15

11.1.2021

Liikenne- ja viestintäministeriö

Viite: Liikenne- ja viestintäministeriön lausuntopyyntö 15.12.2020, VN/24348/2020

LAUSUNTO TYÖRYHMÄN VÄLIRAPORTTIIN SELVITYS TIETOTURVAN JA TIETOSUOJAN PARANTAMISEKSI YHTEISKUNNAN KRIITTISILLÄ TOIMIALOILLA

Liikenne- ja viestintäministeriö on 9.11.2020 asettanut työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla. Ryhmän toimikausi on 31.1.2021 saakka. Valtiovarainministeriöllä on ollut edustaja työryhmässä.

Raportissa on ansiokkaasti ja selkeästi kuvattu tietoturvallisuuden merkitystä digitaalisessa yhteiskunnassa sekä keskeisten merkittävien tietoturvallisuusviranomaisten toimintaa. Raportissa esitetään 35 ehdotusta poliittiseksi linjaukseksi, joista vähintään puoleen sisältyy joko suoraan lainsäädännön muuttamista tai lisäämistä koskeva linjaus tai sellaiseen toimeen ryhtyminen, joka edellyttää todennäköisesti lainsäädännön muuttamista.

Valtiovarainministeriön lausunto

Työryhmässä on päädytty ehdottamaan lainsäädäntöä ja määräyksiä parhaaksi keinoksi parantaa tietoturvaa. Lisäsääntelyn tarve ja sillä tavoiteltu toiminta on osin kuvattu melko yleisellä tasolla (esim. linjausehdotukset 1 ja 7). Uuden lainsäädännön suhdetta jo voimassa olevaan sääntelyyn ja lisäsääntelyn tarvetta tai oikeasuhtaisuutta ei ole arvioitu riittävällä tasolla. Esimerkiksi ohjauksen ja riittävien ohjaukseen ja toimeenpanoon osoitettujen resurssien merkitys varsinkin julkisella sektorilla olisi todennäköisesti varsin hyvä keino parantaa tietoturvallisuutta ja tietosuojaa.

Liikenne- ja viestintävirastolle ehdotetaan uusia tehtäviä ja resursseja, joiden suhdetta esimerkiksi muiden sektorikohtaisten valvontaviranomaisten tehtäviin ja resursseihin ei ole arvioitu tai perusteltu. Muut sektorikohtaiset valvontaviranomaiset eivät ole olleet edustettuna työryhmässä.

Jotkin poliittisista linjausehdotuksista ovat hyvin laajoja tai niitä ei ainakaan ole selvästi kohdistettu pelkästään kriittisiin toimialoihin. Pääosin linjaukset kuitenkin kohdistuvat ns. yhteiskunnan kriittisiin toimialoihin. Lähtökohtana työryhmän työssä on ollut, että se tarkastelee kriittisinä toimialoina terveydenhuoltoa, rahoitusmarkkinoita, energiahuoltoa, vesihuoltoa, liikennettä ja digitaalista infrastruktuuria sekä viestintäverkkoja. Lisäksi tarkasteltavana ovat olleet julkisen hallinnon merkittävät tietojärjestelmät (pois lukien turvallisuusviranomaisten verkot ja järjestelmät). Koko valtioneuvoston yhteinen asia on määritellä ja rajata kriittiset toimialat. Haasteena on, miten kriittisten toimialojen määritelmä tehdään, jotta se on kattava mutta oikeasuhtainen. Vastaava pohdinta on tullut esiin esim. tekoälyn riskiperustaisen sääntelyn arvioimisessa. Esimerkiksi jos terveydenhuolto määritellään riskialttiiksi/kriittiseksi toimialaksi, niin toimialan

kaikki toiminnot eivät kuitenkaan ole riskialttiita. Mikäli kaikkiin toimintoihin ulotetaan hyvin tiukkoja vaatimuksia ja valvontaa, voi siitä tulla suhteetonta ja kallista. Voidaankin kysyä, onko työryhmän lähtökohtainen arvio yhteiskunnan kriittisistä toimialoista ja siitä näkökulmasta tehdyt selvitykset olleet tarkoituksenmukaisia ja riittäviä.

Väliraportin tarkastelu kohdistuu lähinnä valtion viranomaisiin. Julkisessa hallinnossa merkittävimmät tietoturvallisuushaasteet ovat kuitenkin kunnissa, kuten raportissakin todetaan. Kuntiin on suoraan kohdennettu vain yksi linjaus (27), jossa on mainittu 15 suurinta kuntaa. Lisäksi linjauksia ei ole kohdennettu lainkaan kuntien ja kuntayhtymien ICT-yhtiöille. Suomen 310 kunnasta suurin osa järjestää tarvitsemansa ICT-palvelut yhden tai useamman yhdessä omistamansa palvelutuotantoyhtiön kautta tai yhteistyössä naapurikuntien kanssa. Kuntien omistamia ICT-palvelutuotantoyhtiöitä on useita (n. 20) ja niiden palvelutarjoama sekä rooli kuntien palvelutuotannossa vaihtelee tehtävä-aloittain sekä maantieteellisesti. Esimerkiksi kuntaomisteisten ICT-yhtiöiden rooli sosiaali- ja terveydenhuollon palvelutuotannossa on perinteisesti ollut muita kunnan toimialoja merkittävämpää. Nämä yhtiöt hoitavat merkittävissä määrin kuntien ja kuntayhtymien ICT-palveluiden toteuttamisesta ja ylläpitoa.

Valtiovarainministeriö pitää raportissa ehdotettuja poliittisia linjauksia rahoitussektorin kriittisten toimijoiden osalta pääosin hyväksyttävinä, mutta kiinnittää huomiota seuraaviin tarkennuksia vaativiin asiakokonaisuuksiin. Raportissa ehdotettujen linjausten tulisi työryhmän toimeksiannon mukaisesti kohdistua kriittisten alojen tietoturvaan ja tietosuojaan. Ehdotettujen linjausten muotoilussa tulisi käyttää erityistä tarkkuutta, jotta sanamuodot eivät ulotu kokonaisuudessaan sellaiseen rahoitussektorin operatiiviseen riskienhallintaan, jolla ei ole liityntää tietoturvaan tai tietosuojaan. Viranomaisten välisen yhteistyön ja tiedonkulun tehostaminen on tärkeä tavoite tietoturvan ja tietosuojan parantamiseksi. Raportissa tulisi kuitenkin kiinnittää erityistä huomiota viranomaisten välisiin toimivaltasuhteisiin ja tiedonkulkuun, jotka nykyisissä muotoiluissa jäävät epätäsmällisiksi. Valtiovarainministeriö pitää tärkeänä sitä, että kriittisten alojen sektoriviranomaiset säilyvät toimivaltaisina viranomaisina myös jatkossa. Sektoriviranomaisilla on paras osaaminen ja tieto toimialan erityispiirteistä. Kyberturvallisuuskeskuksen roolin tulee olla sektoriviranomaisia tosiasiallisesti tukeva. Kriittisten alojen valvonta- tai ohjausvastuuta ei tule siirtää Kyberturvallisuuskeskukselle. Viranomaisten toimivaltasuhteita koskeva mainintoja raportissa on muun muassa ehdotettujen poliittisten linjausten kohdissa 1-4 sekä raportin sivulla 20, jotka tulisi tältä osin selventää. Linjausten muotoiluissa tulee huolehtia myös siitä, että lähtökohtana rahoitussektorin kriittisiä toimijoita koskevan valvonnan ja sääntelyehdotusten täsmentämisessä ovat voimassa ja valmisteilla oleva soveltuva sääntely. Jatkovalmistelussa tulisi kiinnittää erityistä huomiota vaikutusten arviointiin oikeasuhtaisten ja toimivien ratkaisuiden saavuttamiseksi.

Väliraportin linjauksia koskevia havaintoja ja muutosesityksiä:

- Ehdotettujen linjausten kohdissa 1-4 tulisi selkiyttää sektoriviranomaisten pääasiallinen valvonta- ja ohjausrooli Kyberturvallisuuskeskuksen tukevasta roolista. Rahoitussektorin valvonta tulisi olla jatkossakin sektorivalvojalla. Rahoitussektorin kriittiseksi luokiteltujen toimijoiden valvonnasta vastaa Suomessa pääasiassa Finanssivalvonta. Finanssivalvonta tekee itsenäisesti valvonnan resursointia ja painopistealueita koskevat päätökset.

- Linjauksen nro 2 osalta (ja osin muidenkin Kyberturvallisuuskeskukselle (KTK) ehdotettujen tehtävien ja resurssien osalta) tarvitaan lisää

perusteluja sille, että KTK:n resursseja pitäisi vahvistaa. KTK:n resursseja on viime vuosina lisätty jo merkittävästi. Liikenne- ja viestintäviraston v. 2019 tilinpäätöksen mukaan viraston henkilötyövuosien kokonaistoteuma v. 2019 oli 919 henkilötyövuotta, josta vuoden 2019 aikana uusia palkattuja työntekijäitä oli 64 henkilöä. Selvityksessä ei ole ilmoitettu KTK:n tämän hetkistä henkilömäärää Liikenne- ja viestintäviraston koko henkilömäärästä.

- Linjaus nro 3 ehdotetaan poistettavaksi, koska julkisen hallinnon tiedonhallinnasta annetussa laissa (tiedonhallintalaki) on jo velvoite johdolle järjestää riittävää koulutusta. Digi- ja väestötietovirasto on tuottanut useita sähköisiä tietoturvallisuuden koulutuskokonaisuuksia viranomaisille ja koko yhteiskunnalle. Linjauksesta ei myöskään käy selkeästi ilmi, että tarkoitetaanko siinä valtion virastojen ja laitosten työnantajavirastoja? Myöskin termin ”sektori” sekä lauseen ”niiden tietoturvaa valvovat viranomaiset” merkitys on epäselvä.

- Linjaukseen nro 7 ehdotetaan lisättäväksi vastuutahoksi tietosuojavaltuutettu, koska tietosuoja-asetuksen mukaisesti organisatoriset ja tekniset suojatoimet ovat tietoturvallisuustoimenpiteitä. Ne olisi tässä otettava huomioon. Tietosuojavaltuutettu toimii valvontaviranomaisena. Lisäksi maininta kansainvälisen lainsäädännön ja sen asettamien rajoitteiden ja vaatimuksien huomioimisesta on kannatettava. Muotoilua tulisi täsmentää niin, että sanamuodossa lähtökohdaksi asetetaan rahoitussektorin kriittisiä toimijoita koskeva voimassa ja valmisteilla oleva soveltuva lainsäädäntö kriteerien määrittelyssä ja soveltamisessa.

- Linjaus 8 tulee poistaa. Viranomaisten asianmukaiseen valmisteluun kuuluu pyytää tarvittaessa lausuntoa toiselta viranomaiselta. Lainsäädännössä ei pitäisi kierrättää lausuntovaatimuksia viranomaisilta toisille. Epäselväksi jää, mille toimialoille velvoite säädettäisiin ja tarkoitetaanko vaatimuksilla lakeja, asetuksia, sitovia määräyksiä vai myös suosituksia ja ohjeita. Lisäksi sanamuodosta ei ole selkeästi havaittavissa sitä, kenellä on velvoite pyytää lausunto Kyberturvallisuuskeskukselta. Sanamuodon tulisi myös olla tarkoituksenmukaisesti rajattu, jotta se ei kattaisi tietoturvan ja tietosuojan ulkopuolelle jäävää operatiivista riskienhallintaa, jolla ei ole liityntää työryhmän toimeksiantoon.

- Linjauksen nro 9 osalta pyydetään kiinnittämään huomiota yleisluontoisen ohjeen tarpeellisuuteen ja tarkoituksenmukaisuuteen ottaen huomioon toimialojen erityispiirteet ja tietotekninen kehitys. Onko tarkoituksena ohjata lainsäädännön ja alemman asteisen säädännön valmistelussa huomioon otettavia tietoturvavaatimuksia? Linjausta nro 9 ehdotetaan täydennettäväksi kursiivilla merkityin osin, huomioiden voimassa olevat säännökset:

    - *Tiedonhallintalautakunta, Tietosuojavaltuutettu* sekä Liikenne- ja viestintäviraston Kyberturvallisuuskeskus laativat ennakollisen ohjeen yleisistä tietoturvavaatimuksissa huomioitavista asioista. Vastuutaho: Liikenne- ja viestintävirasto, *Tiedonhallintalautakunta, Tietosuojavaltuutettu*

- Ehdotettujen linjausten kohdissa 10-12 sanamuotoa tulisi selventää niin, että kriittisiä rahoitussektorin toimijoita koskeva voimassa ja valmisteilla oleva soveltuva lainsäädäntö olisi lähtökohta kriteerien määrittelyssä ja soveltamisessa. Linjausten nro 10 ja 11 pitäisi arvioida, onko tarkoituksenmukaista säätää laissa kriittisten tieto- ja tietoliiken-

neteknisten prosessien ja toimintojen kriittisyyden määrittelyn reunaehdoista. Kyse olisi tällöin jonkinlaisesta riskienarvioinnin toteuttamisesta lainsäädännön tasolla. Mikäli katsotaan, että sääntelyä tarvitaan mainitusta määrittelystä ja määrittelyn reunaehdoista, tulisi ainakin määrittelyn reunaehdoista säätää lakia alemman asteisella sääntelyllä, esimerkiksi viranomaismääräyksillä. Riittävää tältä osin voisi olla toimialaa valvovan viranomaisen lakisääteiseen tehtävään kuuluva toimialan ohjeistaminen määrittelyssä sekä säädännön (määrittelyvelvoitteen) noudattamisen valvonta. Esimerkiksi sähköisen viestinnän palveluista annetun lain 283 §:ssä ei tarkemmin määritellä, mitä tarkoitetaan ”teleyrityksen tarjoaman viestintäpalvelun toimivuuden turvaamiseksi kriittisellä viestintäjärjestelmällä”. Säännökseen ei myöskään sisälly määräyksenantovaltuutta eikä sellaista ole ainakaan selkeästi säädetty lain 244 §:n määräyksenantovaltuuksia koskevassa säännöksessä. Vastikään eduskunnassa käsitellyssä hyväksytyssä lain muutoksessa (EV 189/2020) lain 244 a §:ssä sen sijaan on puolestaan hyvin yleisellä tasolla määritelty viestintäverkon kriittinen osa sekä säädetty, että Liikenne- ja viestintävirasto antaa tarkempia määräyksiä viestintäverkkojen, erityisesti niiden kriittisten osien, teknisestä määrittelystä.

- Ehdotettujen linjausten kohdassa 20 esitetty tavoite vaikuttaa neuvottelutavoitteiden kautta NIS-direktiivin uudelleenarviointityöhön EU:ssa on kannatettava.

- Linjausta nro 23 ehdotetaan muutettavaksi. Kansallisen turvallisuusauditointikriteeristö (Katakri)-auditointien nykyisessä toimintamallissa on valtiovarainministeriössä käynnissä olevassa Haukka-hankkeen selvityksessä ilmennyt puutteita palvelua käyttävien toimijoiden haastatteluissa. Palvelun käyttö on hidasta johtuen Katakri-vaatimusten tulkintaongelmista. Valtiovarainministeriön Haukka-hankkeessa on suunnitteilla Julkri-kriteeristö, joka yhdistää Katakrin ja soveltuvin osin Kyberturvallisuuskeskuksen laatiman pilvipalveluiden turvallisuuden arviointikriteeristön (PiTukri) siten, että yhdistetty kriteeristö on tiivis ja yksikäsitteinen, ja soveltuu täsmällisemmin julkisen hallinnon digitaalisten palvelujen tietoturvallisuuden arviointiin. Julkri-kriteeristö valmistuu vuoden 2021 aikana. Linjauksen nro 23 muutosehdotus on:

    - Arvioidaan Valtorin tietosuojaa ja tietoturvaa koskevia vastuita ja velvoitteita. Vastuiden osalta arvioidaan tarve siirtää virastojen vastuulla olevien tiedonhallinnan tehtäviä Valtorin hoidettavaksi konserniedun varmistamiseksi. Valtiovarainministeriö ohjaa Valtoria soveltamaan Haukka-hankkeessa laadittavaa Julkri-arviointikriteeristöä.

- Linjausta nro 24 ehdotetaan muutettavaksi, koska resursoinnin tulee aina perustua selvitettyyn tarpeeseen. Valtori käyttää tällä hetkellä tietoturva- ja tietosuojatehtäviin 46 henkilötyövuotta. Linjauksen nro 24 ehdotettu uusi muotoilu olisi seuraava:

    - Arvioidaan Valtorin tietoturvan ja tietosuojan vaatimia resursseja ja arvioinnin pohjalta tehdään tarvittavat resursoinnit.

- Linjausta nro 25 ehdotetaan muutettavaksi, koska PiTukri ei ole toimivaltaisen viranomaisen antama sitova arviointikriteeristö. Tiedonhallintalautakunta on antanut 18.12.2020 julkista hallintoa koskevan päivitetyn suosituksen turvallisuusluokitellun tiedon käsittelystä, koskien myös pilvipalveluita. Tiedonhallintalautakunnan suositusta noudattava Julkri-arviointikriteeristö valmistellaan valtiovarainministeriön Haukka-

hankkeessa. Julkri-kriteeristön laadinnassa hyödynnetään myös Kyberturvallisuuskeskuksen laatimaa pilvipalveluiden turvallisuuden arviointikriteeristöä.

- Varmistetaan Tiedonhallintalautakunnan vuoden 2020 suositusten toimeenpano Haukka-hankkeessa vuonna 2021 laadittavan Julkri-kriteeristön avulla, jota julkisen sektorin toimijat hyödyntävät pilvipalveluiden tietoturvallisuusvaatimusten määrittämisessä sekä pilvipalveluntarjoajien ja pilvipalveluihin perustuvien valmistuotteiden tietoturvallisuudentason arvioimisessa hankintoja tehdessään.
- Vastuutaho: VM, Liikenne- ja viestintävirasto, Digi- ja väestötietovirasto

Raportin sivulla 28 on esitetty, että luottokorttitiedot ovat paremmin suojattu kuin ihmisten arkaluonteiset terveystiedot. Valtiovarainministeriö katsoo, että toteamus laajentaa raportin soveltamisalaa tietoturvan ja tietosuojan ulkopuolelle rahoitussektorin osalta. Lisäksi virke luo tarpeetonta vastakkainasettelua terveystietojen ja luottokorttitietojen välille. Valtiovarainministeriö ehdottaa virkkeen poistamista tai muuttamista paremmin työryhmän toimeksiantoa vastaavaksi.

Lopuksi, valtiovarainministeriö kiinnittää huomiota, että resurssien ja kustannusten arviointi on varsin puutteellista eikä kehittämisen resursseja ja kustannuksia ei ole otettu huomioon eikä myöskään jatkuvia kustannuksia ole arvioitu. Osin puutteet kustannusten arvioinnissa liittyvät siihen, että lisäsääntelyn tarve, sisältö ja tarkoitus on kuvattu melko yleisellä tasolla. Selvityksen ehdotukset poliittisiksi linjauksiksi voivat johtaa lisäresurssitarpeisiin, joten selvitykseen tulee lisätä seuraava lause: Ehdotusten mahdolliset resurssitarpeet katetaan valtiontalouden kehyksen puitteissa ja mahdollisia määrärahatarpeita arvioidaan tarvittaessa tarkemmin vuosien 2022-2025 julkisen talouden suunnitelman yhteydessä.

valtiosihteeri kansliapäällikkönä — Juha Majanen

budjettipäällikkö — Sami Yläoutinen

Tiedoksi

LVM, Laura Vilkkonen
VM, Tuija Kuusisto
VM, Jonna Kuparinen