21.12.2020
Mika Linna

LIIKENNE- JA VIESTINTÄMINISTERIÖLLE

FINANSSIALA RY:N LAUSUNTO LIIKENNE- JA VIESTINTÄMINISTERIÖN TIETOTURVAN JA TIETOSUOJAN PARANTAMISTA YHTEISKUNNAN KRIITTISILLÄ TOIMIALOILLA SELVITTÄVÄN TYÖRYHMÄN VÄLIRAPORTTIIN (DIAARINUMERO: VN/24348/2020)

Liikenne- ja viestintäministeriö on 15.12.2020 pyytänyt Finanssiala ry:n lausuntoa väliraportista tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (diaarinumero VN/24348/2020).

A. Ehdotukset poliittisiksi linjauksiksi

Yleisiä huomioita

1. Finanssiala ry (FA) pitää hyvänä, että liikenne- ja viestintäministeriö (LVM) on käynnistänyt selvityshankkeen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan eri sektoreilla. Finanssitoimialalla on pitkä kokemus ja hyviä tuloksia tietoturvan ja tietosuojan systemaattisesta ja pitkäjänteisestä kehittämisestä ja se on valmis osallistumaan selvitysten toteuttamiseen, mikäli se arvioidaan hyödylliseksi. Ottaen huomioon, että merkittävä osa väliraportin ehdotuksista joko suoraan tai välillisesti kohdistuu yksityisen sektorin toimijoihin, FA pitää tarpeellisena, että selvitystä jatkettaessa myös elinkeinoelämä otettaisiin mukaan työryhmän toimintaan.

2. Kuten väliraportista ilmenee, finanssisektori on varautunut hyvin tietoturva- ja tietosuojauhkiin. Huoltovarmuuskeskuksen tuoreen selvityksen ”Kyberturvallisuuden nykytila eri toimialoilla” perusteella kyberturvallisuuden tila finanssisektorilla (4.20/5.00) oli selvästi paras ja esimerkiksi teleliikennealaa (3.96), ICT- ja ohjelmistoalaa (3.86), energia-alaa (3.73) ja terveydenhoitoalaa (3.69) selvästi parempi. Väliraportissa todetaan edelleen, että viranomaisvalvonnassa saatujen havaintojen perusteella myös tietosuojan osalta vahvasti säännellyt alat kuten finanssisektori, ovat valveutuneimpia ja paremmin resursoituja, mikä näkyy mm. tietoturvailmoituksissa ja tietoisuudessa sääntelyn vaatimuksista ja niiden noudattamisesta. Tietoturvan ja tietosuojan tason parantaminen näyttäisikin olevan selkeästi suurempi ongelma muilla sektoreilla. Selvityksen tavoitteen kannalta vaikuttaakin selvältä, ettei parannusta tietoturvan ja -suojan yleiseen tasoon saavuteta finanssisektoriin kohdistuvilla lisävaatimuksilla tai sääntelyllä, vaan mahdollisten uusien toimenpiteiden painopisteen tulee olla niillä sektoreilla ja julkisen sektorin yksiköissä, joissa on havaittu puutteita ja kehittämistarpeet ovat suurimmat.

3. FA haluaa kiinnittää LVM:n huomiota siihen, että termi ”yhteiskunnan kriittiset toimialat” on luonteeltaan kuvaileva eikä sitä ole määritelty lainsäädännössä. Jos termiä halutaan käyttää sääntelytarkoituksissa, sen sisältöä ei FA:n näkemyksen mukaan tule jättää asiayhteydestä pääteltäväksi, vaan termi tulee määritellä yksiselitteisesti. Sekaannusten välttämiseksi määritelmän tulisi myös olla yhteensopiva huoltovarmuuden turvaamista ja kansallista turvallisuutta koskevien sääntelyjen kanssa. Poliittisissa linjauksissa näyttäisi olevan epäjohdonmukaisuutta myös termien ”hallinnonala”, ”toimiala” ja ”sektori” käytössä, mikä vaikeuttaa linjausten kohteen, sisällön ja vaikutusten hahmottamista. FA pitää tärkeänä, että terminologia on yksiselitteistä ja linjauksista käy selvästi ilmi, miltä osin kyse on elinkeinoelämään ja miltä osin viranomaisiin kohdistuvista vaatimuksista.

Tietoturvallisuutta ja tietosuojaa koskeva sääntely ja ohjeistus finanssitoimialalla

4. Finanssitoimialaan osalta väliraportin liitteenä olevassa tietoturvavaatimuksia koskevassa sääntelykatsauksessa näyttäisi olevan puutteita ja epätäsmällisyyksiä, jotka FA:n näkemyksen mukaan tulee huomioida työryhmän jatkotyössä ja toimenpidesuosituksissa. Katsauksessa ei mainita lainkaan FA:n henkilötietojen käsittelyä finanssialalla koskevia käytännesääntöjä, jotka määrittävät henkilötietojen käsittelyn periaatteet, edistävät hyvää henkilötietojen käsittelytapaa ja pyrkivät lisäämään asiakkaiden luottamusta finanssitoimialaan ja -palveluihin. Katsauksessa ei myöskään huomioida vireillä olevia EU:n lainsäädäntöhankkeita verkko- ja tietoturvadirektiivin (NISD) päivittämiseksi ja rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskevaksi asetukseksi (DORA).

5. DORA-ehdotuksessaan komissio toteaa, että digitaalisen toiminnan häiriönsietokykyä koskevien yksityiskohtaisten ja kattavien sääntöjen puuttuminen EU:n tasolla on johtanut kansallisten sääntelyaloitteiden lisääntymiseen ja ilman riittävää koordinointia ne aiheuttavat finanssialan toimijoille päällekkäisiä ja epäjohdonmukaisia vaatimuksia sekä merkittäviä hallinnollisia kustannuksia. Tämän lisäksi FA haluaa muistuttaa, että finanssialan toiminnalle välttämättömien maksu- ja selvitysjärjestelmien häiriöttömän toiminnan turvaaminen ja niihin liittyvät kysymykset kuuluvat Euroopan unionin toiminnasta tehdyn sopimuksen 127 artiklan 2 kohdan ja Euroopan keskuspankkijärjestelmän ja Euroopan keskuspankin perussäännön 22 artiklan nojalla Euroopan keskuspankin johdolla toimivan Euroopan keskuspankkijärjestelmän yksinomaiseen toimivaltaan. Ottaen edelleen huomioon Euroopan finanssivalvontaviranomaisten laajat toimivaltuudet ja Euroopan keskuspankin roolin rahoitusjärjestelmän kannalta merkittävimpien luottolaitosten (Suomen osalta mm. Nordea ja OP ryhmä) välittömänä valvojana, FA pitää johdonmukaisena ja välttämättömänä, että rahoitusmarkkinoiden digitaalisen toiminnan häiriönsietokykyä ja tietoturvallisuusvaatimuksia koskeva sääntely toteutetaan EU:n tasolla eikä kansallisella tasolla ryhdytä sääntelytoimiin, jotka ovat ristiriidassa eurooppalaisen sääntelyn kanssa tai vaarantavat tasapuolisen kilpailun edellytyksiä eurooppalaisilla yhteismarkkinoilla.

6. NISD- ja DORA-hankkeiden osalta FA haluaa myös kiinnittää LVM:n huomiota EU-oikeudelliseen vilpittömän yhteistyön periaatteeseen, joka velvoittaa jäsenvaltioita toteuttamaan kaikki toimenpiteet, joilla varmistetaan unionin perussopimuksista ja säädöksistä johtuvien velvoitteiden täyttäminen. FA:n tulkinnan mukaan tämä tarkoittaa myös velvollisuutta pidättyä kansallisista sääntelytoimenpiteistä, jotka voivat olla ristiriidassa EU:ssa vireillä olevien lainsäädäntöhankkeiden kanssa.

7. Sääntelykatsauksessa on esitetty, että Finanssivalvonnan (FIVA), Euroopan pankkiviranomaisen (EBA) ja Kansainvälisen arvopaperimarkkinavalvojien yhteisön (IOSCO) antamat ohjeet ja suositukset olisivat ei-sitovia, mikä ei vastaa niiden tosiasiallista luonnetta. FIVA katsoo, että ohjeet edustavat heidän näkemyksiään siitä, miten lakia tulee eri tilanteissa tulkita tai soveltaa, ja varaa oikeuden puuttua toimintaan lain rikkomisen takia, jos finanssimarkkinoilla toimiva toimii näiden tulkintojen vastaisesti. Euroopan valvontaviranomaisia (mm. EBA) koskevien EU-asetusten 16 artiklan mukaan sekä kansallisten valvontaviranomaisten että finanssimarkkinoilla toimivien on kaikin tavoin pyrittävä noudattamaan niiden antamia ohjeita ja suosituksia. Vastaavalla tavalla myös IOSCO:n antamat ohjeet ja suositukset ohjaavat vahvasti niiden soveltamisalan piirissä olevien toimijoiden toimintaa. FA katsookin, että väliraportin liitteen sääntelykatsauksessa mainitut FIVA:n, EBA:n ja IOSCO:n ohjeet siirretään nykyisestä sarakkeestaan otsikon ”Asetukset / määräykset” alle.

Finanssiala ry:n kommentit ehdotettuihin poliittisiin linjauksiin

8. Linjauksessa 1 ehdotetaan, että viranomaisten väliselle yhteistyölle tietoturvaloukkaustilanteissa luodaan yhtenäinen säädöspohja. Kokemukset finanssialalta osoittavat, että tietoturva- ja tietosuojaloukkausten ehkäisemisen, havaitsemisen ja selvittämisen kannalta alan toimijoiden ja palveluntuottajien välinen tietojenvaihto on vähintään yhtä tärkeää kuin viranomaisten välinen tietojenvaihto. Tehokas, kattava ja käytännössä reaaliaikainen tietojenvaihto on välttämätön osa toimialan varautumista ja reagointia jatkuvasti kehittyviin ja muuttuviin uhkiin. Onkin ensiarvoisen tärkeää, että viranomaisten välistä yhteistyötä koskevaa sääntelyä tarkennettaessa myös elinkeinoelämän toimijoiden strategista, taktista ja operatiivista tietojenvaihtoa koskevat säännöt selkeytetään ja tietoturva- ja tietosuojauhkien torjunnan edellyttämälle tietojenvaihdolle luodaan tukeva säädöspohja.

9. Linjauksessa 2 esitetään, että Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen (KTK) resursseja vahvistetaan, jotta se pystyy antamaan riittävästi apua ja toimialakohtaista neuvontaa muille hallinnonaloille. Ehdotusta on sinänsä hyvä, mutta vastuuvirkamiesten toimialakohtaista neuvontaa rajata ei pidä rajata vain sektoriviranomaisille, vaan se tulee ulottua myös asianomaisen toimialan yrityksiin. On myös välttämätöntä, että KTK:n resurssien riittävyys varmistetaan niin, etteivät mahdolliset uudet tehtävät vaaranna nykyistä hyvin sujuvaa yhteistyötä mm. finanssialan toimijoiden kanssa.

10. Linjaus 3 on tarpeellinen, mutta on huomattava, että tietoturvallisuuden ja tietosuojan toimintaympäristöt ja uhkakuvat muuttuvat jatkuvasti, joten koulutuksen tarve on jatkuva, mikä tulee edellyttämään merkittäviä panostuksia KTK:n kouluttajaresursseihin. Koulutuksen tarve ei myöskään rajoitu vain tietoturvavalvonnan parissa työskenteleviin, vaan sen tulee riittävässä laajuudessa kattaa koko henkilöstö. Vaihtoehtona voisi olla virastokohtaisten tietoturvapäälliköiden nimeäminen, joiden vastuulla on huolehtia mm. virastonsa henkilöstön tietoturvakoulutuksesta.

11. Linjaus 4 on hyvä, mutta edellyttänee myös panostuksia esim. kartoituspalvelun käyttäjien tukeen. Pelkkä tieto mahdollisesta ulkoverkon haavoittuvuudesta ei riitä, vaan käyttäjät saatavat myös tarvita ohjausta siitä, mihin toimenpiteisiin heidän tulisi ryhtyä tilanteen korjaamiseksi.

12. Linjauksessa 5 esitettyjen yhdenmukaisten, kattavien, luotettavien ja turvallisten teknisten tiedonsiirtoratkaisujen tarve on ilmeinen ja ne tulisi toteuttaa mahdollisimman nopealla aikataululla. Hallinnonalojen sisäisten ja välisten siirtojen ohella ratkaisujen tulisi mahdollistaa myös hallinnonalojen ja yritysten väliset tietojen siirrot.

13. Linjauksessa 6 esitetty Havaro-palvelun käyttäjäpiirin laajennus on kannatettavaa.

14. Linjauksen 7 mukaisesti elinkeinoelämän toimijoita velvoittavien tietoturvavaatimusten tulee olla selkeitä, oikeasuhtaisia, lakiin perustuvia sekä Suomea koskevien EU- ja kansainvälisoikeudellisten velvoitteiden mukaisia. Linjauksessa esitetty tietoturvaa koskevien sitovien määräysten antovaltuuksien delegointi asetustakin alemmalle tasolle vaikuttaa ylimitoitetulta ja hyvän periaatteiden vastaiselta. Muutokset tietoturvan ja tietosuojan kannalta merkittävissä teknisissä tai toiminnallisissa järjestelyissä saattavat edellyttää toimijoilta merkittäviä taloudellisia panostuksia, minkä vuoksi tällaisista velvoitteista tulisi ehdottomasti säätää lain tasolla.

15. Linjaus 8 edellyttää, että toimialojen olisi pyydettävä KTK:n lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvittaessa myös vaatimusten toimeenpanosta. Mikäli toimialoilla tässä yhteydessä viitataan yrityksiin tai muihin elinkeinoelämän toimijoihin, kyse näyttäisi oleva merkittävästä puuttumisesta mm. elinkeinonvapauteen, mitä tuskin voidaan pitää perusteltuna, tarpeellisena tai edes mahdollisena. Jos taas kyse on hallinnonaloille asetettavasta velvoitteesta, linjauksen sanamuotoa on tarkennettava.

16. Linjaus 9 on perusteltu eikä siihen ole huomautettavaa.

17. Linjauksissa 10, 11, 12 ja 13 esitetään tarkemmin määrittelemättömälle joukolle kriittisten toimialojen toimijoita erittäin pitkälle meneviä kansallisia velvoitteita määritellä, dokumentoida, luokitella, auditoida ja sertifioida tieto- ja tietoliikenneteknisiä prosessejaan ja toimintojaan. Tältäkin osin vaatimukset näyttäisivät merkittävällä tavalla puuttuvan ainakin elinkeinonvapauteen, mitä tuskin voidaan pitää perusteltuna, tarpeellisena tai edes mahdollisena. Toteutuessaan näin raskaat velvoitteet todennäköisimmin johtaisivat vain siihen, että asianomaisten palvelujen tarjonta siirtyisi kansallisen lisäsääntelyn ulottumattomiin Suomen rajojen ulkopuolelle. Mikäli linjauksissa ehdotettuja vaatimuksia halutaan edistää, niistä saatavat hyödyt on kyettävä osoittamaan. Lisäksi on varmistettava, että velvoitteet ovat oikeasuhtaisia eikä niistä aiheudu toimijoille kohtuutonta taloudellista, hallinnollista tai toiminnallista rasitusta.

18. Linjauksiin 14, 15 ja 16 ei ole huomautettavaa.

19. Linjauksen 17 osalta on tärkeää, että mahdollisissa lainsäädäntömuutoksissa varmistetaan, että Liikenne- ja viestintävirastolla on eri liikennemuotojen tietoturvaa koskevia määräyksiä antaessaan velvoite tehdä yhteistyötä liikenne- ja ajoneuvovakuutuksia myöntävien vakuutuslaitosten kanssa.

20. Linjausten 18, 19 ja 20 osalta on tärkeää varmistaa, että poliisi- ja valvontaviranomaisten resurssit ovat on määrältään ja laadultaan riittävät. Samassa yhteydessä tulisi myös kriittisesti arvioida identiteettivarkauden ja muiden tietoverkkorikosten rangaistusasteikkojen riittävyyttä sekä mahdollistaa näihin liittyvien rikosepäilyjen edellyttämät tutkintakeinot ja esimerkiksi esitutkinnan rajaaminen nykyistä laajemmin. Epäiltyjen tietoturva- ja tietosuojaloukkausten raportointikynnyksen alentamiseksi on ensiarvoisen tärkeää laajentaa ja nopeuttaa näiden selvittelyä ja esitutkintaa sekä mitoittaa niihin liittyvät rangaistusasteikot sellaisiksi, että tekijä joutuu aidosti punnitsemaan tekonsa seuraamuksia ennen sen toteuttamista. Nykytilanteessa merkittävä osa ilmoitetuistakin tietoverkkorikoksista jäänee tutkimatta, jolloin uhrin kannalta rikosepäilyn ilmoittaminen merkitsee vain tarpeetonta lisätyötä.

21. Linjauksessa 21 mainitun NIS-direktiivin soveltamisalan osalta olisi arvioitava, ovatko ehdotetut uudet toimijat energia- ja rahoitusalalta aidosti direktiivin alkuperäisen tarkoituksen mukaisia yhteiskunnan toiminnalle keskeisten palvelujen tarjoajia tai digitaalisen palvelun tarjoajia, vai tarkoittaisiko niiden sisällyttäminen direktiivin soveltamisalan tarpeetonta laajentamista. Direktiivin soveltamisalaa tai sisältöä uudelleen arvioitaessa on varmistettava, etteivät muutokset ole päällekkäisiä tai ristiriidassa toimialakohtaisten säädösvaatimusten kanssa.

22. Linjausten 22, 23, 24, 25, 26 ja 27 osalta on tärkeää, että tietoturvallisuus- ja tietosuojavaatimukset otetaan vakavasti myös julkisella sektorilla. Julkisuudessa kuvatun kaltaiset potilastietojen vuodot, poliisin tietojärjestelmien luvattomat hyödyntämiset yksityisiin tarkoituksiin,

Lahden, Porin ja Kokemäen tietojärjestelmien lamaantumiset, kyvyttömyys suojautua viranomaisten palveluja lamauttaneilta palvelunestohyökkäyksiltä, ulkoministeriöön kohdistunut tietomurto, jne. osoittavat, etteivät haasteet rajoitu vain yksityisen sektorin toimijoihin. Tietoturvallisuuden osalta on selvää, ettei kyse ole Valtorille tai muulle palveluntuottajalle ulkoistettavissa olevasta teknisestä ongelmasta, vaan finanssisektorin tapaan viimesijaisen vastuun tulee aina olla ulkoistavalla taholla. Tietosuojan osalta Suomessa on valittu linja, jonka mukaan tietosuoja-asetuksen sanktioita ei kohdisteta julkiseen sektoriin. Tämä näyttäisi johtavan käytännössä siihen, että tietosuojan tasoon ei ole ollut tarpeen kiinnittää niin suurta huomioita julkisella sektorilla eikä siihen ole varattu tarpeeksi resursseja. Mikäli sanktiot koskisivat kaikkia toimijoita, saattaisi tilanne olla parempi tietosuojan tason suhteen ja asiaa tulisikin arvioida tässä yhteydessä uudelleen.

23. Linjaukset 28, 29, 30, 31 ja 32 ovat lähtökohtaisesti kannatettavia. Tietosuojan tason nosto lähtee pitkälle yrityksen toimintakulttuurista sekä oletusarvoisen ja sisäänrakennettujen tietosuojavaatimusten huomioimisesta uusia järjestelmiä ja prosesseja käyttöönotettaessa. Ehdotus tietosuojan vaatimusten huomioimisesta jo hankintojen yhteydessä on sen vuoksi erittäin kannatettava. Riittävää tietosuojan tasoa voi olla vaikea toteuttaa jälkeenpäin ohjelmistoihin ja järjestelmiin, jos sitä ei ole otettu huomioon alusta alkaen suunnittelu- ja toteutusvaiheesta lähtien. Toimenpide-ehdotuksissa otetaan myös kantaa tietosuojasertifiointimekanismeihin ja erityisesti niiden puutteeseen. Suomessakin olisi pikaisesti saatava käyttöön ulkopuolisten tahojen myöntämät sertifioinnit, joilla rekisterinpitäjät voisivat osoittaa vaatimusten noudattamisen. Vaikka sertifioinnit ovat kalliita, niiden tuomat hyödyt ja kustannukset tulisi suhteuttaa tietosuojaa koskevien vaatimusten noudattamisesta koituviin ja usein huomattaviksi nouseviin kokonaiskustannuksiin.

24. Linjaukset 33 ja 34 ovat myös kannatettavia. Tietosuojavaltuutetun toimiston resurssit on turvattava määrällisesti ja laadullisesti ja mahdollisia uusia tehtäviä asetettaessa on varmistettava, etteivät ne vaaranna nykyisten tehtävien asianmukaista hoitamista.

25. Linjauksessa 35 ehdotettua mobiilipäätelaitteeseen asennettavaa sovellusta kehitettäessä olisi selvitettävä mahdollisuudet tehdä ilmoitus tietoturvaloukkauksesta samalla kertaa usealle viranomaiselle. Esimerkiksi sähköiseen tunnistamiseen kohdistuvasta tietoturvaloukkauksesta tulee pankkien nykyisin tehdä ilmoitus Tietosuojavaltuutetulle, Finanssivalvonnalle ja Kyberturvallisuuskeskukselle. Sen sijaan, että toimija joutuu tekemään useita eri ilmoituksia, viranomaisten menettelytavat ja raportointialustat tulisi yhdenmukaistaa niin, että yksi ilmoitus riittäisi ja toimija voisi keskittyä ongelman pikaiseen ratkaisemiseen sen sijaan, että rajallisia resursseja käytetään ilmoitusten laatimiseen. Samalla olisi luontevaa sallia ilmoituksen tekeminen myös englanniksi, mikä helpottaisi ja nopeuttaisi erityisesti monikansallisten toimijoiden raportointia.

Muita näkökohtia

26. Mahdollisten standardointi- ja niihin liittyvien auditointivelvoitteiden osalta FA pitää tärkeänä, että lainsäädännössä yksilöidään, mikä taho ja mitä menettelyä noudattaen määrittelee kyseeseen tulevat standardit. Standardit on määriteltävä yksiselitteisesti, jotta toimijoilla on mahdollisuus huomioida vaatimukset omissa toimintaprosesseissaan ja ICT-sopimuksissaan. FA:n näkemyksen mukaan standardit eivät myöskään voi olla puhtaasti kansallisia (esim. Suomen kansalliset KATAKRI-, PITUKRI- tai VAHTI-ohjeet ja standardit), vaan samojen sääntöjen tulee soveltua läpi palvelu- ja hankintaketjujen siitä riippumatta, missä päin yhteismarkkinoita toimintaa harjoitetaan, asiakkaat sijaitsevat, palveluja tarjotaan tai alihankkijat toimivat.

27. Edellä todetun mukaisesti FA haluaa lopuksi kiinnittää huomiota siihen, että väliraportissa kuvatut säädös- ja toimenpide-ehdotukset edellyttäisivät huomattavia panostuksia sekä elinkeinoelämän että viranomaisten puolella. Tämän vuoksi FA pitää välttämättömänä, että niiden taloudelliset ja hallinnolliset kustannukset arvioidaan mahdollisimman luotettavasti hankkeen jatkokäsittelyn yhteydessä.

Väliraportin muut osat, kommentit:

Kommentit sisältyvät poliittisia linjauksia koskeviin ehdotuksiin annettuihin kommentteihin.

FINANSSIALA RY
Taina Ahvenjärvi