Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

PIA
PUOLUSTUS- JA
ILMAILUTEOLLISUUS PIA RY

29.11.2023

Liikenne- ja viestintäministeriö

Lausuntopyynnön diaarinumero: VN/18157/2023

Lausunto: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Teknologiateollisuus ry, Puolustus- ja Ilmailuteollisuus (PIA) ry sekä Kyberala (FISC) ry kiittävät mahdollisuudesta lausua asiasta. Lausunto on edellä mainittujen yhteinen.

Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka tekevät puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Puolustus- ja Ilmailuteollisuus PIA ry edustaa Suomessa toimivaa puolustus-, avaruus-, ilmailu-, ja turvallisuusteollisuutta ja Finnish Information Security Cluster – Kyberala ry edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Molemmat ovat Teknologiateollisuus ry:n toimialayhdistyksiä.

Haluamme kiinnittää huomiota seuraaviin seikkoihin:

Yleistä

1. Kyberturvallisuusdirektiivi 2.0 (NIS2) on yhdessä kyberkestävyyssäädösehdotuksen (CRA) kanssa keskeisimpiä jäsenvaltioiden digitaalisten riskien parempaan hallintaan tähtääviä EU-säädösehdotuksia. NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta asettamalla direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta. Säädöksellä pyritään siis varmistamaan jäsenvaltioiden yhteiskunnan ja huoltovarmuuden kannalta keskeisten toimijoiden yhteinen tietoturvallisuuden vähimmäistaso. On selvää, että yksinomaan vähimmäistason muodollinen täyttäminen tai heikosti suunniteltujen riskienhallintatoimien toteuttaminen ei vielä riitä ko. riskien merkittävään pienentämiseen, mutta säädös tarjoaa silti selvän keinovalikoiman aiemmin omaehtoisesti heikoimmin suoriutuvien organisaatioiden riskitason pienentämiseen.

2. Kiitämme valmisteluvastuussa olevia siitä, että kansallisen toimeenpanon lähtökohdaksi on valittu periaate olla lisäämättä säädöksessä riskienhallintatoimiin liittyen direktiivissä edellytettyä korkeampia vaatimuksia. Tämä on tärkeää suomalaisten yhtiöiden kansainvälisen kilpailukyvyn sekä monikansallisesti toimivien yhtiöiden vaatimuksenmukaisuuden kannalta. Jatkotyössä on keskeistä, että myös valvovien viranomaisten mahdollisesti myöhemmin antamat tarkemmat tekniset määräykset säilyvät säännöksiä tarkentavina eivätkä siten tosiasiallisesti korota vaatimustasoa minimiharmonisoinnin periaatteen mukaisesti. Samalla on tärkeää tukea soveltamisalaan kuuluvia organisaatioita siinä, että riskienhallintatoimet johtavat tosiasiallisesti digitaalisten riskien pienemiseen eli ovat tavoitteeseen nähden vaikuttavia sen sijaan, että toimijoiden kannettavaksi jää vain säädöksestä seuraava hallinnollinen taakka.

3. Koska NIS2-direktiivin kansallinen täytäntöönpano on edellä sen ”rinnakkaista” CER-direktiiviä, tulisi varmistua siitä, että NIS2-lausuntopalautteen myötä esille nousevat seikat välitetään myös CER-direktiivin kansallisen toimeenpanon päävastuussa olevan Sisäministeriön valmistelijoille. Samoin tulisi selvittää, voisiko kansallisen CER-säädöksen valmistelun yhteydessä soveltamisalaan kuuluvien toimijoiden tunnistamiskriteeristöä ja -prosessia hyödyntää soveltuvin osin myös NIS2-soveltamisalaan kuuluvien toimijoiden tunnistamisessa.

4. Liikenne- ja viestintävirastolle esitetään uusien valvontatehtävien lisäksi myös muita viranomaistehtäviä, joista aiheutuu resursointitarpeita. Direktiivin kansallisen toimeenpanon myötä mm. CSIRT-yksikön sekä valvontaviranomaisen tehtävät lisääntyvät ja uudet tehtävät edellyttävät toimintojen sekä tietojärjestelmien kehittämistä. Lisäksi virastolle on osoitettu muiden säädösten perusteella uusia tehtäviä (mm. digipalveluasetus, datanhallinta-asetus). On myös jo nyt tiedossa, että ainakin tuleva kyberkestävyyssäädös, data-asetus sekä tekoälyasetus tulevat edellyttämään lisätehtävien osoittamista virastolle. Siten Liikenne- ja viestintävirasto Traficomin resurssit on turvattava tavalla, jolla varmistetaan säädösten asiallinen toimeenpano, pysyvien viranomaistehtävien hoitaminen tuottavasti sekä mahdollistetaan viranomaisten toiminnan kautta kasvua ja vientiä vauhdittavat liiketoimintamahdollisuudet.

   Edellä mainittuun liittyen soveltamisalaan kuuluvien sekä kyberturvallisuusalan palveluyhtiöiden kannalta ehdotetun 16–17 §:n tehtävien asiallinen hoitaminen edellyttää Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen ympärivuorokautista päivystystä. Kyberturvallisuuskeskuksella on keskeinen tehtävä tiedon välittämisessä toimijoille sekä muille viranomaisille. Esimerkiksi toimijoita torstai-illalla havaittuun ja perjantai-illalla lähetettyyn ensi-ilmoitukseen (velvoite ilmoittaa 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta) reagoitaisiin vasta maanantaina. Tällöin myös ilmoituksen antaja saisi vastauksen aikaisintaan maanantaina, johon mennessä yrityksen olisi pitänyt antaa jo täydentävä poikkeamailmoitus (72 tunnin kuluessa). Mikäli ilmoitus liittyisi muihinkin toimijoihin vaikuttavaan uhkaan, valvova viranomainen ei olisi kyennyt välittämään tietoa muille toimijoille ja viranomaisille direktiivin päämäärien mukaisesti. Tämä tekisi tyhjäksi merkittävän osan direktiivin raportointia koskevista tavoitteista.

5. Yleisemmin haluamme nostaa esille, että EU:n jäsenvaltioiden harmonisoinnille tulisi osoittaa riittävästi ennakollista huomiota. Kyberturvallisuuden yleisten, tässä tapauksessa eritoten monikansallisten yritysten rajat ylittävien riskienhallintatoimien mahdollisimman kattava yhteensopivuus on tärkeä tavoite. Hyödyntämällä kansainvälisesti tunnustettuja viitekehyksiä, kuten NIST CSF 2.0:aa ja ISO/IEC 27001:stä, voidaan turvallisuuden lisäksi mahdollistaa hallinnollisen taakan vähentämisestä sekä kustannussäästöjen syntymistä. Lisäksi kehysten hyödyntäminen edistää yhteentoimivuutta ja toimijoiden keskinäistä luottamusta. Tiedossamme on, että useammat jäsenvaltiot aikovat nojata kansallisissa vaatimusmalleissaan ko. viitekehyksiä. Mm. kyberturvallisuuden riskienhallintamallin vaatimukset, ml. toimitusketjun riskienhallinta sekä haavoittuvuuksien käsittely ja ilmoittaminen sisältyvät kansainvälisiin standardeihin ja parhaisiin käytäntöihin (mm. ISO 31000, ISO/IEC 27005, ISO/IEC 29147:2018 (CVD) ja NIST CSF 2.0).

Soveltamisalaa koskevat huomiot

6. Suomessa eritoten huoltovarmuusnäkökulma on jo vuosikymmeniä perustunut siihen osallistuvien yhtiöiden sekä viranomaisten keskinäiseen luottamukseen sekä yhtiöiden vapaaehtoisuuteen. Luottamuksen kannalta onkin erittäin tärkeää, että säädös toimeenpannaan kansalliset erityispiirteet huomioiden. Soveltamisala tulisikin kohdentaa yhdenvertaisesti kaikkiin säädöksen tavoitteiden kannalta keskeisiin toimijoihin, joihin kuuluvat myös kansalliseen harkintavallan piiriin kuuluvat turvallisuusviranomaiset sekä muut julkisen hallinnon toimijat. Muussa tapauksessa syntyy vaikutelma, jossa direktiivistä seuraava hallinnollinen taakka sekä kustannukset eivät kohdistu kaikkiin yhteiskunnallisen riskin näkökulmasta tarpeellisiin toimijoihin ja aiheuttaa siten luottamuksen murentumista eritoten elinkeinoelämän ja julkishallinnon välillä.

Eteläranta 10, PL 10, 00131 Helsinki

7. Koska direktiivi edellyttää kussakin jäsenvaltiossa erillistä täytäntöönpanoa käytännössä kansallisen säädöksen/säädösten avulla, vähimmäistasoa koskevat riskienhallintatoimet eri jäsenvaltioissa voivat suurella todennäköisyydellä olla ainakin jokseenkin eriävät. Tämä seikka voi haitata monikansallisten yhtiöiden toimintaa ja aiheuttanee vähimmillään käytännön toimien selvittämisen takia hallinnollista taakkaa. Hallituksen esityksessä tulisikin käsitellä tarkemmin yhtiövaikutuksia suhteessa monikansalliseen yritykseen sekä konsernirakenteessa (emo- ja tytäryhtiö) toimiviin yrityksiin. Lisäksi kansallisella toimeenpanolla on vaikutuksia yritysten toiminta- ja kilpailukenttään ja erityisesti sen tasapuolisuuteen.

8. Lisäksi hallituksen esityksessä tulisi selkeyttää tai tarkentaa riskien arvioinnin ja hallinnan velvoitetta suhteessa organisaatioon, jossa soveltamisalaan kuuluva toiminta on vain osa oikeushenkilön toimintaa. Katsomme, että soveltamisalaan kuulumisen arviointi on perusteltua koskea kutakin rekisteröityä yhtiötä kutakin erikseen koskevana. Kuitenkin riskinarviointi- ja hallintaprosessin kautta (esim. soveltamisalaperusteella eli että liiketoimintayksiköllä ei ole toiminnallista tai vaikutuksellista yhteyttä soveltamisalaan kuuluvan toisen yksikön kanssa) kutakin yhtiötä koskeva oikeus tiettyjen liiketoiminta-alueiden rajaamisesta pakollisten riskienhallintatoimien ulkopuolelle tulisi käsitellä selkeämmin ehdotuksessa.

9. Ehdotuksessa tulisi myös käsitellä nykyistä tarkemmin säädösehdotuksen 3 §:ssä viitattujen liitteessä I tai II tarkoitettujen ns. koosta riippumattomien toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan määrittämistä koskevaa kokonaisuutta. Elinkeinoelämän toimijoiden ennakollinen valmistautuminen edellyttää asian täsmällisempää käsittelyä jo lakisäädöksen valmisteluvaiheessa.

10. Elinkeinoelämän keskusliiton EK:n lausuntoon viitaten toteamme myös, että soveltamisalaan kuuluvien yhtiöiden oikeusturvan kannalta tulisi harkita viranomaisen velvoitetta nimittää tai vähimmillään informoida soveltamisalaan kuuluvia yrityksiä soveltamisalaan mahdollisesta kuulumisesta (vrt. CER-direktiivin nimittämisvelvoite). Asiaa on käsitelty myös yllä kohdassa 3. Hyvän hallinnon periaatteisiin nojaten julkishallinnon tulisi edistää sitä, että kaikki oikeussubjektit voivat tulla tietoisiksi heille kuuluvista velvollisuuksista. Katsomme, että viranomaisten – keskitetysti tai sektorikohtaisesti – tulisi omaksua vähintäänkin varmistava rooli informoida soveltamisalan yrityksiä ja tarjota tietoa tulevista velvoitteista. On syytä huomioida, että osa soveltamisalan yrityksistä voi olla kooltaan pieniä eivätkä välttämättä kuulu esim. elinkeinoelämän toimialajärjestöihin. Viranomaisten aktiivinen toiminta on perusteltua myös siksi, että kaikkien soveltamisalaan kuuluvien yhtiöiden tulee täyttää lain vaatimukset 18.10.2024 lukien ja ilmoittautumismenettelyyn 43 § mukaan niiden tulee ilmoittautua valvovalle viranomaiselle vuoden 2025 alussa. Lain voimaatulon jälkeen jäljelle jäävä aika vaatimusten täyttämiseen on väistämättä varsin lyhyt.

11. Lakiesityksen yksityiskohtaisissa perusteluissa on virheellinen määritelmä keskisuurista toimijoista. Se tulisi korjata vastaamaan komission suositusta 2003/361/EY (eräät suosituksen mukaiset kynnysarvot ovat kumulatiivisia eikä vaihtoehtoisia) soveltamisalaan kuulumiseen liittyviä NIS2-direktiivin liitteisiin viitaten. Direktiivin liitteissä 1 ja 2 on kolme saraketta. Ne on otsikoitu seuraavasti: toimiala, toimialan osa ja toimijatyyppi. Direktiivin 2 artiklan 1. kohdan mukaan direktiivin soveltamisalaan kuuluvat sellaiset keskisuuret ja sitä suuremmat toimijat, jotka ovat direktiivin liitteissä 1 ja 2 määriteltyjä toimijatyyppejä (ja jotka harjoittavat toimintaansa unionissa). Direktiivi ei siis koske mitä tahansa (keskisuurta tai suurempaa) toimijaa, joka harjoittaa toimintaa liitteissä 1 ja 2 määritellyillä toimialoilla. Lakiesityksen 3 § kuitenkin laajentaa soveltamisalaa kattamaan oikeushenkilöä tai

luonnollista henkilöä, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteessä I tai II tarkoitettua toimijatyyppiä ja täyttää tai ylittää keskisuuren toimijan määritelmän. Lakiesityksen soveltamisala on huomattavasti laajempi kuin direktiivin, koska säännöstä on mahdollista tulkita niin, että soveltamisalaan kuuluu määriteltyjen toimijatyyppien lisäksi myös muita toimijoita. Säännöstä tulee muuttaa vastaamaan direktiivin sanamuotoa oikeusvarmuuden säilyttämiseksi.

Riskienhallintavelvoitetta koskevat huomiot

12. Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta 2 § 18 kohdan yksityiskohtaisissa perusteluissa kuvataan kyberriskin hallintaintressiä tarpeettoman tiukasti termein: ”… tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden vaarantava tapahtuma…” Säännöksen perusteluissa voisi selventää, että kyberriskien hallinta on organisaation riskienhallinnan alaista ja lähtee riskin vähentämiseen tähtäävien tulosten määrittämisestä. Siten määritelmää ei tulisi rajata vain luottamuksellisuuteen, saatavuuteen, eheyteen ja aitouteen, sillä organisaatioilla voi nyt tai tulevaisuudessa olla muitakin ns. ”standardimallista” poikkeavia hallintaintressejä. Olisikin perusteltua lisätä ko. virkkeeseen edeltävä termi ”ainakin” (… direktiivin 6 artiklan 9. kohdan määritelmään viitaten ainakin vastaavasti sitä, kuinka todennäköinen viestintäverkossa ja tietojärjestelmässä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden vaarantava tapahtuma olisi…).

13. Ehdotuksen 7 §:n 2 momentin mukaan toimijan tulisi toteuttaa ”turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuville riskeille sekä viestintäverkon tai tietojärjestelmän merkitykselle toimijan toiminnan ja palveluntarjonnan kannalta”. Säännöstä vastaavassa 21 artiklassa ei ole vaatimusta toimenpiteiden ajantasaisuudesta, joskin artiklan ensimmäisestä ja toisesta alakohdasta voidaan päätellä asianmukaisten ja oikeasuhteisten teknisten, operatiivisten ja organisatoristen toimenpiteiden sekä näihin liittyvä viimeisin kehitys huomioon ottaen, edellyttävän myös ajantasaisuutta. Artiklan toisessa momentissa viitataan kuitenkin ”viimeisimpään kehitykseen” turvallisuuden tason ja riskien oikeasuhtaisuuden välillä. Kehotamme ajantasaisuusvaatimuksen tarkastelua sen synnyttävän velvoittavuuden ja osoittamisvelvoitteen kannalta. Säännöksen ei tulisi johtaa tulkintaan, jonka mukaan kaikkien riskienhallintatoimien tulisi aina olla ”uusinta uutta”, vaan että toimet ovat muuttuvien riskien suhteen ajan tasalla.

14. Toimitusketjua koskeva rajaus on syytä lisätä myös kansalliseen säännökseen siten, että vaatimus kattaa vain soveltamisalaan kuuluvan toimijan välittömät palveluntarjoajat. Toimitusketjuvastuiden osalta NIS2-direktiivi viittaa ”välittömiin” palveluntarjoajiin (ellei sopimuksilla ole toisin sovittu), kun taas asiaa koskevassa kansallisessa säännöksessä ei ole tätä rajausta (2 luku 9 § 2 mom. 4) -kohta). Direktiivin 21 artiklan 2. kohdan d) -alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteissä on otettava huomioon toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.

    Uudistamme tässä olennaisilta osin myös EK:n lausunnossa mainitut näkökohdat:

    Säädösehdotuksen 2 luvun 9 § 2 momentin 4) -kohdassa todetaan, että kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on

huomioitava ja ylläpidettävä ajantasaisena mm. ”toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt.”

Säännöstekstissä ei siis rajata, että velvoite kohdistuisi vain välittömiin toimittajiin ja palveluntarjoajiin. Sanamuodon mukainen tulkinta johtaisi siihen, että soveltamisalan yrityksen tulisi hallita kaikkien toimitusketjuissaan olevien riskienhallinta. Se, että vastuu koskee vain välittömien toimittajien ja palveluntarjoajien kyberturvallisuuden varmistamista todetaan kyllä säännöksen yksityiskohtaisissa perusteluissa, mutta koska kyse on merkittävästä vastuun ulottumista koskevasta täsmennyksestä, vaadimme, että tämä todetaan selkeästi jo säännöstekstissä. Tällaisen rajauksen piilottaminen yksityiskohtaisiin perusteluihin ei ole hyväksyttävää.

Lisäksi asiayhteyden osalta tulisi olla selvää, että välittömien toimittajien ja palveluntarjoajien tulee olla syy-seuraussuhteessa nimenomaan soveltamisalaan kuuluvan yrityksen kyberturvallisuuden riskienhallinnan kannalta. Säännökset sanamuodosta asia ei ilmene, vaan johtaisi siihen, että organisaation tulisi lähtökohtaisesti varmistua esimerkiksi sellaisen toimittajansa kyberturvallisuuden tasosta, jolla ei ole merkitystä organisaation oman kyberturvallisuuden kannalta. Esimerkkinä voisi olla toimittaja, joka toimittaa vaikkapa kanttiinituotteita ilman, että yrityksen ja toimittajan välillä olisi tietojärjestelmäyhteyttä tai järjestelmävalvojaoikeuksia. Esimerkkinä voisi olla myös iso teknologiatoimittaja, joka ei liiketoiminnan mitta- ja laajuussuhteiltaan ole vertailukelpoinen yrityksen liiketoiminnan kokoon. Säännös velvoittaisi varmistumaan myös tällaisen toimittajan kyberturvallisuuden riskienhallinnan tasosta, mikä ei ole perusteltua.

Se, että säännöksen 3 momentissa todetaan, että toimenpiteet on suhteutettava esim. poikkeamien vaikutuksiin ei ole riittävää, koska säännös käytännössä johtaisi organisaatiot selvittämään kaikkien toimittajien kyberturvallisuuden tason ja erikseen perustelemaan ja dokumentoimaan, jos se katsoo, ettei velvollisuus ulotu kyseiseen toimittajaan. Tällaisesta lähestymistavasta seuraa vain tarpeetonta hallinnollista taakkaa ja riskien hallinnan tarpeetonta siirtämistä yrityksestä toiseen. Pykälän kyseistä 2 momentin 4) -kohtaa tulee myös tältä osin tarkentaa.

Nostamme lisäksi esille yleisen haasteen liittyen sopimuspohjaiseen (osittaiseen) riskin siirtoon toimitusketjun hallinnassa. Käytännössä monille organisaatioille on haasteellista määritellä sopimukset palveluntarjoajiensa kanssa siten, että vaatimukset tosiasiallisesti täyttyvät, sillä vastuiden ja niiden jakaminen edellyttää yksityiskohtaisuutta. Erityisesti, koska vain yhtiö itse voi arvioida omaan toimintaansa kohdistuvat riskit ja niiden perusteella toimeenpanna riittävät riskienhallintakeinot. Moni ICT-toimitusketjun palveluntarjoaja tarjoaa NIS2-soveltamisalaan kuuluville toimijoille palveluita monikansallisesti eli useamman EU-jäsenvaltion alueelle, jonka seurauksena asiakkailla on maa- ja sektorikohtaisesti useita valvontaviranomaisia ja siten myös kansallisesti täsmennettyjä vaatimuksia. Yrityksillä on suuri intressi pyrkiä sopimukselliseen selkeyteen sopimusriitojen välttämiseksi, koska ne aiheuttavat merkittävää haittaa liiketoiminnalle – puhumattakaan mahdollisen laiminlyönnin seurauksena asiaan kytkeytyvästä hallinnollisesta seuraamusriskistä ja sen selvittämisestä. Ei siis voida olettaa, että sopimusoikeudellisesti olisi riittävää todeta, että ”toimittaja vastaa NIS2-direktiivin velvoitteiden täyttymisestä” tai vaihtoehtoisesti ”asiakas vastaa NIS2-direktiivin velvoitteiden täyttymisestä”

15. Ehdotuksen 8 §:n mukaista riskienhallintamallia tulisi tarkentaa, lakiesityksen riskienhallintavelvoitteiden ymmärtämisen ja toimeenpanon helpottamiseksi. Esimerkiksi EU:n finanssialaa koskevassa asetuksessa digitaalisesta häiriönsietokyvystä (2022/2554) on laajempi riskienhallintajärjestelmää koskeva velvoite (6 artikla 8. kohta), jonka vähimmäisvaatimukset on määritelty lakiesityksen riskienhallinnan toimintamallia tarkemmin. Hyvin vapaamuotoinen velvoite laatia riskienhallintamalli aiheuttaa seurauksen, jossa esim. valvontatoiminnan tai häiriön selvittämisen yhteydessä mallin voi osoittaa vääräksi mutta ei oikeaksi. Myös sen suhde tai mahdollinen päällekkäisyys lakiesityksen 9 §:n 2 momentin 1 kohdan kanssa jää osittain epäselväksi.

16. Lakiesityksen 9 §:n 2 momentin 3 kohta edellyttää myös riskienhallinnan toimintamallin ja -toimenpiteiden osalta haavoittuvuuksien käsittelyn ja julkistamisen käytänteiden huomioimista. Lakiesityksen yksityiskohtaisten perustelujen mukaan velvollisuus koskee toimijaa, joka itse tuottaa viestintäverkko- tai tietojärjestelmäpalvelua. Direktiivin 21 artiklassa ei ole mainintaa vaatimuksen kohdistumisesta vain viestintäverkko- tai tietojärjestelmäpalveluiden tarjoamiseen. Säännöksen perustelut ovat näiltä osin epäselvät. Mikäli kyse olisi merkittävästä velvoitteen rajauksesta, näemme tarpeelliseksi viedä rajaus säännöstekstiin. Mikäli kyseessä on tarkoittamaton epäselvyys, tulee säännöksen perustelut korjata. Onko mahdollisesti ollut tarkoituksena sanoa, että mikäli toimija tarjoaa viestintäverkko- tai tietojärjestelmäpalveluita, olisi toimijan huolehdittava myös näiden turvallisuudesta. Lisäksi näemme tarpeelliseksi täsmentää käsittely- ja ilmoitusvelvollisuutta myöhemmin viranomaisohjeen muodossa.

17. Johdon vastuut ilmenevät selkeästi luonnoksen 10 §:n 1 momentista. Sen sijaan ongelmia sisältyy siihen, kenelle oikeushenkilön henkilökohtainen vastuu kohdentuu. Suomessa yhtiöoikeudellisen vastuun on katsottu koskevan osakeyhtiön hallintoelimiä, eli hallitusta, mahdollista hallintoneuvostoa ja toimitusjohtajaa. Lakiehdotuksessa on mainittu vastuullisina lisäksi myös muita edellisiin rinnastettavassa asemassa olevia (esim. toiminnanjohtaja, asiamies, yhtiömies tai elinkeinonharjoittaja). Säännöksen perusteluissa kuvataan kuitenkin, että ”johdolla tarkoitettaisiin myös toimitusjohtajan välittömään alaisuuteen kuuluvaa tahoa, jos se hoitaa toimijan ylimpiä johtotehtäviä, joissa tosiasiallisesti johdetaan sen toimintaa.” Vastuun laajentaminen saattaa olla perusteltua, mutta säännöksen perusteluista tämä ei kuitenkaan ilmene. Perustuuko vastuun määrittely direktiivin kautta jo voimassa olevaan oikeusperustaan, vai kenties johonkin, jossa kansallisesti olisi harkintavaraa?

    Lisäksi epäselvää on se, soveltuuko vastuu tilanteisiin, jossa toimitusjohtajaa tai siihen rinnastettavaa tahoa ei ole, vai siihen, että vastuu olisi toimitusjohtajan lisäksi esimerkiksi tietohallintojohtajalla tai johtoryhmäjohtokollektiivilla. Toimitusjohtaja tai häneen rinnastettava henkilö vastaa yhtiön juoksevista asioista, joihin kyberturvallisuuden riskienhallinnan toimenpiteetkin kuuluvat, ja järjestää ne yhtiön edun mukaisesti. Hallitusta tai hallintoneuvostoa (joka nimittää myös toimitusjohtajan) alemmille johtokollektiiveille, kuten johtoryhmille ei ole Suomessa asetettu itsenäistä ja erillistä oikeudellista vastuuta. Mikäli direktiivi ei EU-oikeuden sitovuuden kannalta edellytä vastuun laajentamista, tulisi viittaukset toimitusjohtajan alaisiin tahoihin poistaa lakiehdotuksesta. Jatkossa harkittavaksi jää myös, tulisiko kansallista yhtiölainsäädäntöä tarkastella uudelleen vastuukysymysten osalta.

18. Säädösluonnoksessa on todettu direktiivin 21 artiklan edellyttävän, että yhteisön ”--hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen”. Yleisesti on tiedossa, että organisaatioiden hallintoelinten jäsenillä on usein jokseenkin heikot tiedot

kyberturvallisuusriskien hallintakäytännöistä. Koska vaatimus on vähimmäisharmonisoinnin näkökulmasta EU-säädöksessä asetettu ja siten myös kansallista harkintavaltaa rajoittava katsomme, että vaatimus tulee käsittää toimijan velvollisuutena varmistaa hallintoelinten jäsenten aktiivinen altistuminen aiheen kannalta olennaisten tietojen, taitojen tai tapojen omaksumiselle. Direktiivin 20 artiklassa vaatimuksen tavoitteeksi määritetään ”hankkia riittävät tiedot ja taidot kyetäkseen tunnistamaan riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin.” Vaikka toimijoille yksinkertaisin keino todentaa ko. velvoitteen täyttyminen onkin kirjata hallintoelinten jäsenten koulutukseen osallistuminen tai muu oppimista osoittava suorittaminen, tällä keinolla ei voida kuitenkaan varmistaa motivaation, tarkkaavaisuuden ja muistin yhteistoiminnasta johtuvien tietojen ja taitojen laadullista soveltamiskykyä. Siksi ko. tietojen ja taitojen omaaminen tulee voida todentaa ja dokumentoida muutoinkin. Ehdotamme, että säännöksen yksityiskohtaisiin perusteluihin lisätään velvoitetta selkeyttävä kuvaus toimijan harkintavallasta todentaa riittävä perehtyneisyys luotettavalla tavalla. Lisäksi katsomme, että edellytetty ”säännöllisin väliajoin” tapahtuva perehtyneisyyden hankkimista ei ole perusteltu ja tulisikin poistaa. Perehtyneisyys ei ole lineaarisesti tai tasaisesti ”kuluva” ominaisuus, jota täytyy säännöllisesti lisätä, vaikka riskienhallintakäytännöissä tapahtuukin kehittymistä. Perehtyneisyyden tarve voi myös vaihdella toimintaympäristön ja toimijan liiketoiminnassa tapahtuvien muutosten vuoksi.

Raportointivelvoitetta koskevat huomiot

19. Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta 4 §:n 5 momentin säännöstekstin mukaan ”Tässä laissa ei velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua”. Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan myös yhteiskunnan perustoimintoja uhkaavaa toimintaa. On oletettavaa, että ainakin jotkin toimijoiden raportointivelvollisuuden piiriin liittyvät asiat kuuluvat rajoituksen piiriin. Säännöksen yksityiskohtaisissa perusteluissa tulisi käsitellä myös esimerkkitilannetta, jossa yhtiömuotoinen toimija katsoisi 11, 14–15 tai 27 §:iin liittyvän (merkittävän) poikkeama- tai uhkatiedon kuuluvan kansallisen turvallisuuden vaarantumisriskin piiriin. Tulisiko tieto antaa valvovalle viranomaiselle tai palvelun vastaanottajille tästä huolimatta vai olisiko säännös tiedon luovuttamisen rajoitusperuste? Lisäksi myös kansallinen turvallisuus olisi tarpeen määritellä ehdotuksen 2 §:ssä. Liikesalaisuuksien suojan vaarantavien ilmoitusten käsittelyyn liittyvät suojatoimet tulee myös käsitellä.

20. Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta 14 § 2 momentin toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa. Säännöksen yksityiskohtaisten perustelujen mukaan kyberuhkalla tarkoitettaisiin potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä viestintäverkkoja tai tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti (määritelmä 2 § 1 mom. 12) -kohta). Vaikuttaa siltä, että säädösehdotuksen 2 §:stä puuttuu määritelmä merkittävästä kyberuhasta, vaikka 14 §:ssä asetetaan velvoitteita juuri merkittävän, ei ”perusmuotoisen” kyberuhkan varalle. Määritelmän (tarvittaessa) lisääminen on välttämätöntä säännöksen soveltamisen kannalta.

21. Yleisimmin, ja mahdollisten tarkempien viranomaisohjeiden suhteen kriteerien tulisi välttää liian laajoja tai alhaisia ”kynnysarvoja”, jotka aiheuttavat liiallisen raportoinnin kautta hallinnollista työtä vieden huomiota pois itse tapahtumien torjuntatyöstä. Kriteerien tulisi myös tunnistaa säännellyn toimintakentän toiminnallisuudet ja siten kriteeristöjä muodostettaessa tulisi tehdä tiivistä yhteistyötä ko. sektoreiden kanssa. Esimerkiksi nykyisessä NIS1 -täytäntöönpanoasetuksessa digitaalisten palveluntarjoajien raportointikriteereinä käytetty “käyttäjätunti”-mittari ei vastaa johdonmukaisesti tilapäistä pilvipalvelun tason laskua tai lisääntynyttä latenssia, joko siksi, että yksittäisten käyttäjien tietoja ei ole saatavilla tai siksi, että ei tiedetä, onko palvelu saatavilla tietylle käyttäjälle (tai käyttäjille) 60 minuutin ajan. Siten tulisi mieluummin selventää, että termi “käyttäjä” tai vastaava sisältää yritysasiakkaat tai tilaajat ja että säännellyt toimijat arvioivat tapahtuman merkittävyyttä vaikutusten perusteella yritystilien tai tilaajien lukumäärään, jos yksittäisten käyttäjien tietoja ei ole saatavilla.

    Saatavuus -kriteerin osalta merkittävyyden tulisi riippua tapahtuman kestosta, laajuudesta (leviämisestä) ja syvyydestä (vaikutuksen kohteena olevien käyttäjien tai tilien lukumäärä organisaatiossa). Suosittelemme käyttämään palvelun tason alenemisen ja vaikutuksen kohteena olevien asiakkaiden prosenttiosuutta vaihtoehtoisina kriteereinä käyttäjätunti kriteerille. Esimerkiksi kattava palvelu katsotaan saatavuudeltaan merkittäväksi, kun kyseisen palvelun suorituskyky laskee alle 65 % kahden tunnin ajan joko (a) 5 000 000 yksittäiselle käyttäjälle unionissa tai (b) 10 %:lle tilaajalle (tenant), joista vähintään 35 %:lla yksittäisistä käyttäjistä tai tileistä kussakin tilauksessa (tenant) on tällainen lasku.

    Luottamuksellisuutta, eheyttä tai aitoutta koskevien tapahtumien osalta suosittelemme käyttämään NIS1 -kriteeriä ja prosenttiosuutta, eli 100 000 tai 5 % unionin palvelun käyttäjien lukumäärästä. Arviointi ja siihen liittyvä raportointivelvollisuus tulisi perustua luotettavaan tietoon, ei spekulaatioon.

22. Koska säädösehdotuksen tavoitteena on aiempaa vaikuttavampi kyberuhkien ja poikkeamien torjuntatyö, joka korostuu erityisesti vakavissa poikkeamatilanteissa, toimijoiden ja myös viranomaisten on toimittava nopeasti yhteisymmärryksessä poikkeamasta johtuvien vaikutusten poistamiseksi ja vahinkojen minimoimiseksi. Tavoitteen saavuttamisen varmistamiseksi tulisi tarvittaessa täydentää tai antaa tarvittavat säännökset ja huolehtia tarpeellisten resurssien varaamisesta Traficomin tietoturvaloukkausten ilmoituspalvelun tai muun vastaavan järjestelmän kehittämiseksi siten, että lakiehdotuksen 11 §:ssä asetettujen velvoitteiden sekä 18 §:n mainitun toiminnan tarkoituksenmukaisen järjestämisen suhteen toimijan on mahdollista toimittaa ilmoitus toimivaltaisille valvoville viranomaisille sekä antaa suostumuksensa/pyytää tietojen välittämistä myös esitutkintaviranomaiselle (esim. poliisi) sekä tietosuojavaltuutetulle keskitetysti. Tätä korostaa myös se tosiasia, että useat yhtiöt toimivat useilla aloilla ja näin saattavat tulla valvonnan kohteeksi usean viranomaisen toimesta. On ilmeistä, että eritoten pakollisten/vapaaehtoisten ilmoitusten sekä muualla laissa olevien raportointivelvoitteiden (GDPR, CER, DORA) kannalta direktiivin tavoitteiden sekä toimijoiden hallinnollisen taakan kohtuullistaminen edellyttävät keskitettyä, nopeaa ja tehokasta verkkopalvelua sekä samojen tai toisiinsa liittyvien ilmoitusten välittämistä kerralla useammalle viranomaiselle. On erittäin tärkeätä, että lain täytäntöönpanossa huomioidaan myös vielä ehdotusvaiheessa olevien lakiehdotusten, kuten kyberkestävyyssäädöksen vaikutus toimijoiden raportointivelvoitteisiin.

23. Vaikka säädösehdotuksen 19 §:n CSIRT-toiminnon tehtävät on lueteltu asianmukaisesti, ehdotuksen perusteluissa tulisi korostaa erityisesti raportointivelvoitteiden soveltamisalaan

kuuluvien toimijoiden suuntaan annettavien ennakkovaroitusten, hälytysten, ilmoitusten ja tietojen merkitystä vahvasti sitovana periaatteena. Tämä on tarpeellista ei vain kyberturvallisuuden operatiivisen toteuttamisen kannalta, vaan myös säädöksen taustalla olevan luottamuksen säilyttämisen ja kehittämisen kannalta eritoten elinkeinoelämän ja julkishallinnon välillä. Datan ja digitalisaation kehitys edellyttää yhä selvemmin sen syvällistä sisäistämistä, että kyberturvallisuuden kehittäminen ei ole mahdollista kummankaan osapuolen yksipuolisin toimin. Huoltovarmuuskriittisten yritysten välistä säännöllistä tietoturvaloukkausten tapahtumatietojen säännöllistä jakamista ja raportoimista tulee jatkaa ja vahvistaa (HAVARO-työ), jotta osallistuvilla yrityksillä on motiivi myös osallistua tilannekuvayhteistyön vahvistamiseen.

19 §:n 2 momentin 9 kohdan mukaan CSIRT-yksikön tehtävänä on antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta. Säännökseen ei kuitenkaan ole sisällytetty direktiivin 11 artiklan 4-kohtaan sisältyvää CSIRT-yksiköille asetettua velvoitetta luoda yhteistyösuhteet asiaankuuluviin yksityisen sektorin sidosryhmiin. Ei ole pidettävä riittävänä, että asia todetaan vain säännöksen perusteluissa. Yhteistyövelvoite tulee sisällyttää itse säännökseen direktiivin edellytysten mukaisesti.

24. 20 §:ssä tarkoitetun viestintäverkkojen ja tietojärjestelmien verkkopohjaisen haavoittuvuuskartoituksen osalta ehdotuksessa ei ole käsitelty sitä, kuinka eri jäsenvaltioiden CSIRT-yksiköiden tekemiä haavoittuvuuskartoituksia koordinoidaan. Lienee sanomattakin selvää, mutta ehdotuksessa mainitsematta jäänyttä, että ko. haavoittuvuuskartoituksissa ilmenneet potentiaaliset löydökset toimijan ympäristöstä tulee käsitellä luottamuksellisena viranomaisen ja toimijan välillä, koska tällaisen tiedon vuotaminen aiheuttaa kasvavan riskin toimijalle. Puutteelliseksi ovat jääneet kysymykset mm. monikansallisten yhtiöiden laajojen IP-osoitealueista tai palveluntarjoajien sellaisista IP-osoitteista, joiden palveluita hallinnoivat asiakkaat itse. Samoin puutteelliseksi on jäänyt myös monikansallisten teknologiajättien haavoittuvuustietojen hallinnointi ja tarvittavien muutosten toimeenpano kansallisvaltioissa.

25. Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry:n huomioihin viitaten pidämme erittäin tärkeänä, että säädösehdotuksen 34 §:n liittyen korjataan kansallinen oikeustila, jossa sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen soveltamiskäytännöstä on seurannut, että ainakin teletoimintaa harjoittavat palveluntarjoajat joutuvat tekemään kaksi erillistä ilmoitusta samasta henkilötietojen tietoturvaloukkauksesta. Toimijoiden edun sekä prosessiekonomian ja -laadun kannalta on perusteltua, että valvovan viranomaisen ilmoitusvelvollisuus tietosuojavaltuutetulle on kattava, kun se saa tietoonsa, että lain 2 luvussa säädettyjen velvoitteiden laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta olisi yleisen tietosuoja-asetuksen 33 artiklan nojalla ilmoitettava yleisen tietosuoja-asetuksen mukaiselle valvontaviranomaiselle.

Valvontaa koskevat huomiot

26. Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta 26 §:ssä säädetty viranomaisvalvonnan jakautuminen useille valvoville viranomaisille voi aiheuttaa epävarmuutta jäljempänä 31–33 sekä 35 §:n seuraamusjärjestelmän ennakoitavuudesta ja johdonmukaisuudesta. Ehdotuksen perusteluissa ja tarvittaessa säännöstasolla tulisi täsmentää keinoja, joilla valvovien viranomaisten yhdenmukaista toimintaa edistetään ja toimijoiden oikeus yhdenvertaiseen kohteluun varmistetaan.

27. Ehdotuksen 27 § 1 momentin kohtaan "Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta." tulee lisätä maksuttomuuden kohtuullisuusrajoite. Mikäli välttämättömien tietojen luovuttaminen aiheuttaa merkittävää takkaa toimijalle, tulee viranomaisen korvata työstä aiheutuneet kustannukset (esimerkiksi tietomassan erottelu tai konvertointi). Kohtuuttomasta taakasta on voitava painavien perusteiden läsnä ollessa kieltäytyä. Rajoitusedellytys on välttämätön myös siksi, että ehdotuksen 36 §:n mukaan tiedon luovutuksesta ei voi vaatia oikaisua. Lisäksi säännöstä koskevissa tarkemmissa perusteluissa tulisi selventää valvontatehtävän suorittamiseksi luovutettujen tietojen käsittelystä, eritoten säilyttämisajoista ja tiedon poistamisesta.

28. Ehdotuksen 29 §:n mukaan ”tarkastus voitaisiin tehdä toimijan tiloissa tai tietojärjestelmässä. Tietojärjestelmässä tehtävä tarkastus voisi olla esimerkiksi teknisten riskienhallintakeinojen havainnointia taikka tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista.” Näin toteutettuna tarkastusoikeus antaisi viranomaiselle tai kolmannelle osapuolelle oikeudet yrityksen tietojärjestelmiin ja tietoihin. Kyseiset tietojärjestelmät tai -varannot voivat sisältää hyvin luottamuksellista tietoa yrityksen asiakkaiden riskeistä – mukaan lukien viranomaisasiakkaiden omista riskeistä. Toimivaltuutta koskeva direktiivin artiklat 32 ja 33 sisältävät velvoitteen toteuttaa ainoastaan ”2. kohdan f) -alakohdan mukaisesti ”pyynnöt saada pääsy dataan, asiakirjoihin ja tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi” ei voi tulkita niin, että toimivaltuus tarkoittaisi toimijan tietojärjestelmiin kohdistuvaa käyttöoikeutta, saatikka ylläpitäjätason sellaista. Pykälän toimivaltuutta kuvaava viranomaisen oikeus tarkoittaa toimijan velvollisuutta suostua ja edesauttaa tarkastusoikeuden toteuttamista viranomaisen valitsemin keinoin. Direktiivissä on kuitenkin selkeästi todettu, että viranomaisella on oikeus ainoastaan esittää pyyntö pääsystä dataan ja tietoihin. Olisi lain tarkoitusperien vastaista velvoittaa toimijaa luovuttamaan kolmannelle osapuolelle oikeudet tietojärjestelmiin ja tietoihin. Näin ollen säännöstä tulee tarkentaa niin, että dataan, tietoon ja tietojärjestelmiin oikeuttavan pääsyn ja muiden käytänteiden, mukaan lukien viranomaisen lukuun toimivan tahon roolin on perustuttava myös toimijan suostumukseen. On myös muistettava, että ulkopuolinen tarkastukseen osallistuva voi olla tietoturvapalveluiden osalta toimijan kilpailija.

29. Lisäksi ehdotetun 33 §:n tarkoittamien toimintakieltojen soveltamisala on laaja ja aiheuttaa epäselvyyttä siitä huolimatta, että soveltaminen on rajoitettu keskeisin toimijoihin. Säännös on epäselvä sen suhteen, minkä toimijan piirissä olevia tehtäviä se koskee. Direktiivin asiaa koskevan 32 artiklan mukaan ”…määrättyjä väliaikaisia keskeyttämisiä tai kieltoja on sovellettava ainoastaan siihen asti, kun asianomainen toimija toteuttaa tarvittavat toimet korjatakseen ne puutteet tai noudattaakseen niitä toimivaltaisen viranomaisen vaatimuksia, joiden johdosta seuraamukset määrättiin.” EK:n lausuntoon viitaten tästä on pääteltävissä, että kielto on tarkoitettu ensisijaisesti 35 §:n mukaisten uhkasakon, teettämis- ja keskeyttämisuhkan tehostamiseksi tai vaihtoehdoksi, ei rangaistukseksi. Näin ollen säännöstä tulee tarkentaa rajoituksesta vapautumiseen liittyvän kohdan osalta (…sekä varattava kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi ja toimintarajoitteen purkamiseksi).

Seuraamusmaksua koskevat huomiot

30. Erityisesti konsernirakenteisten yhtiöiden haasteet liittyvät myös mahdollisten hallinnollisten seuraamusmaksujen määräämiseen. Ehdotetun 40 §:n sekä 2 §:n mukaan on pääteltävissä, että toimijalla tarkoitetaan seuraamusmaksun kohteena olevaa oikeushenkilöä. Säännöskohtaisissa perusteluissa olisi kuitenkin syytä selkeyttää myös se, että

konserniyhtiöiden tilanteessa ei huomioida konsernin kokonaisliikevaihtoa tai muiden konserniyritysten liikevaihtoa.

Teknologiateollisuus ry	Kyberala ry	PIA ry
Matti Mannonen Johtaja, Uudistuva teollisuus	Peter Sund Toimitusjohtaja	Tuija Karanko Pääsihteeri

Lisätiedot:

Peter Sund, 050 565 0621
peter.sund@teknlogiateollisuus.fi

Risto Rajala, 040 5156187
risto.rajala@teknologiateollisuus.fi