Elinkeinoelämän keskusliitto EK

Lausunto

28.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kiitämme lausuntomahdollisuudesta ja toteamme seuraavaa:

NIS2-direktiivi on tärkeä ja yhdessä CER-direktiivin kanssa kyseessä ovat tärkeimmät laajaa elinkeinoelämän kriittisen yritysjoukon riskienhallintaa ja turvallisuutta koskevat lainsäädäntökokonaisuudet lähivuosina. On erittäin tärkeää, että ne implementoidaan Suomeen huomioiden maamme kansalliset erityispiirteet, mm. se, että huoltovarmuusratkaisumme on jo vuosikymmeniä perustunut siihen osallistuvien yritysten kannalta ennen kaikkea osapuolten keskinäiseen luottamukseen sekä omaehtoiseen, sitoutuneeseen ja sopimusperusteiseen kehittämiseen, eikä velvoittavaan regulaatioon. Kun nyt samoja asioita pyritään kehittämään ennen kaikkea regulaatiopohjaisesti, kyseessä on herkkä asia, mikä pitää huomioida tarkoin, jotta vuosikymmenien aikana määrätietoisesti rakennettu luottamus ei kärsi.

Olemme olleet tyytyväisiä siitä, että ministeriö on todennut implementoivansa direktiivin lisäämättä siihen edellytettyyn turvallisuustasoon liittyviä, direktiivissä edellytettyä korkeampia tai tiukempia vaatimuksia. Tämä olisi erittäin tärkeää suomalaisten yritysten kansainvälisen kilpailukyvyn kannalta. Sen vuoksi olisi myös erittäin tärkeää, että myös valvovien viranomaisten mahdollisesti säännösten nojalla myöhemmin antamat tarkemmat tekniset määräykset todella ovat teknisiä, eli kyseistä säännöstä tarkentavia ja täsmentäviä, eivätkä vaatimustasoa faktisesti korottavia. Mikäli tarkempia määräyksiä annettaisiin, olisi myös erittäin tärkeää varmistaa, että ne olisivat tasoltaan ja sävyltään tasapainossa muiden EU-maiden täytäntöönpanolakien ja vastaavien sektoriviranomaisten määräysten kanssa. Soveltamisalaan kuuluvan yrityksen hallinnollista taakkaa lisää aivan olennaisesti se, jos samaan toimintaan liittyvät säännökset eroavat sen eri toimintamaissa ja yrityksen on sovellettava käytännön toiminnassaan hallinnollisesti kovin erilaisia vaatimustasoja. Kun kyseessä on minimiharmonisointidirektiivi, joka määrittää vain jäsenvaltioilta edellytettävän vaatimusten minimitason, näin tullee kuitenkin väistämättä jo kansallisten täytäntöönpanolakien vertailussa käymään, puhumattakaan niiden nojalla mahdollisesti annettavista tarkentavista teknisistä ja toimialakohtaisista määräyksistä.

Valitettavasti toteamus siitä, että Suomessa direktiivi implementoidaan minimitasolla, ei aivan kaikilta osin ehdotuksen perusteella näytä pitävän paikkaansa. Vaikka kokonaan uusia vaatimuksia ei luonnoksessa olisikaan, osa vaatimuksista on yksityiskohtaisempia ja osa valvontaan liittyvistä rajoituksista ja kielloista on kovempia kuin direktiivissä. Lausumme niistä jäljempänä tarkemmin.

Soveltamisalaa koskevat huomiot

Soveltamisalan määritelmä on siihen mahdollisesti kuuluvien yritysten kannalta haasteellinen. Se toimii parhaiten tilanteessa, jossa koko juridisen yhtiön toiminta (esityksessä käytetyt termit toimija / oikeushenkilö) kuuluu soveltamisalaan. Sen sijaan tilanteessa, jossa soveltamisalaan kuuluva toiminta on vain osa juridisen yhtiön toimintaa, määritelmä toimii huonosti, koska lähtökohtaisena edellytyksenä oleva keskisuuren toimijan määritelmä katsottaneen kyseisen juridisen yhtiön kokonaislukujen (liikevaihto, tase ja henkilömäärä) perusteella. Koska direktiivin keskeisenä tavoitteena on kuitenkin varmistaa, että tiettyjen kriittistä toimintaa harjoittavien toimijoiden kyberturvallisuuden taso on riittävä, tulisi määritelmää tarkentaa siten, että toimijan kokokriteerin täyttymistä arvioitaessa käytetään näissä tapauksissa vain kyseisen, soveltamisalaan kuuluvan toiminnan osuutta juridisen yrityksen kokonaisluvuista ja tämä luonnollisesti määrittää myös soveltamisalan yrityksen sisällä, jolloin sisällölliset riskienhallintavaatimukset kohdistuvat vain soveltamisalan toimintaa harjoittavaan organisaation osaan.

Selvää jo ehdotetun 3 §:n sanamuodon mukaan on, että jos konserniin kuuluvista oikeushenkilöistä vain jokin tai jotkut harjoittavat soveltamisalaan kuuluvaa toimintaa, konsernin emoyhtiöltä ja/tai sen tai soveltamisalaan kuuluvaa toimintaa harjoittavan konserniyhtiön tytäryhtiöltä ei voida edellyttää lain velvoitteiden täyttämistä, jos ne eivät harjoita soveltamisalan toimintaa. Tämä rajaus olisi nähdäksemme perusteltua kirjoittaa auki säännöksen yksityiskohtaisiin perusteluihin selvyyden vuoksi.

Haasteellinen on sellainen aika tyypillinen tilanne, jossa konserniin kuuluva tytäryhtiö harjoittaa soveltamisalaan kuuluvaa toimintaa, mutta muut tytäryhtiöt ja emoyhtiö ei. Miten tällöin tulkitaan emoyhtiön osalta tilanne, jos se tuottaa soveltamisalan tytäryhtiönsä ICT-palvelut tai pääosan niistä? Kestävin, joskin melko keinotekoinen tulkinta olisi nähdäksemme se, että soveltamisala ei tästä syystä laajenisi emoyhtiöön, vaan sitä tulisi kohdella soveltamisalan tytäryhtiön välittömänä toimittajana / palveluntarjoajana, jolloin tytäryhtiön tulisi varmistaa sen itselleen tuottamien palveluiden vaatimustenmukaisuus. On vaikea keksiä oikeudenmukaisempaakaan tulkintaa tilanteeseen, koska nähdäksemme vain tällä perusteella ei olisi hyväksyttävää katsoa myös emoyhtiö soveltamisalaan kuuluvaksi.

Olisi toivottavaa ja tarpeellista, että jatkovalmistelussa säädösesityksen perusteluissa avattaisiin näitä tilanteita nykyistä laajemmin. Näitä tulkintatarpeita tulee varmuudella, eikä ole hyvä, että kukin valvova viranomainen tulkitsee niitä omalla tavallaan ja/tai että kaikki tulkinnat niiden osalta jäävät lain voimaantulon jälkeiseen aikaan. Yritykset tarvitset tulkintatukea jo nyt, valmistautuessaan lain voimaantuloon ja harkitessaan, miltä osin niiden toiminta kuuluu lain soveltamisalaan.

Samat haasteet liittyvät myös seuraamusmaksun määräämisen perusteisiin (ehdotettu 40 §, ks. jäljempänä).

Luonnoksen 3 §:n 1 ja 2 momentissa todetaan: ”Tämän lain soveltamisalaan kuuluvalla toimijalla tarkoitetaan 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. Lisäksi toimijalla tarkoitetaan koosta riippumatta oikeushenkilöä ja luonnollista henkilöä, joka on…” Ehdotamme, että kohtaan selvyyden vuoksi lisätään: ”…tai luonnollista henkilöä, joka omalla nimellään tai toiminimellä harjoittaa…”.

Toivomme lisäksi, että soveltamisessa suhtauduttaisiin hyvin pidättyväisesti soveltamisalan liiketoimintaa omalla nimellään tai toiminimellä harjoittaviin luonnollisiin henkilöihin samoin kuin pieniin osakeyhtiö-, kommandiittiyhtiö- tai avoin yhtiö -muotoisesti toimiviin yrityksiin. Lain velvoitteet ovat hyvin raskaita pienille toimijoille ja on perusteltua olla hyvin pidättyväinen niiden katsomisessa soveltamisalaan kuuluviksi huomioiden myös kytkentä CER-direktiivin kansalliseen täytäntöönpanoon, jonka yksityiskohdat eivät vielä ole tiedossa. CER-kriittisiksi nimettävät tulevat lausuttavana olevan HE-luonnoksen 3 §:n 2 momentin e.-kohdan mukaan suoraan myös lakiesityksen soveltamisalaan keskeisiksi toimijoiksi eli näin myös ennakkovalvonnan piiriin.

Johtuen soveltamisalaa koskevista epävarmuuksista ja tulkinnallisuuksista katsomme myös, että luonnoksen 6 luvun 43 §:n ilmoittautumismekanismi ei ole soveltamisalaan mahdollisesti kuuluvien yritysten oikeusturvan kannalta riittävä. Samalla kun CER-direktiivi asettaa viranomaisille velvollisuuden nimittää soveltamisalan kriittiset yritykset direktiivin määrittelemiltä toimialoilta ja määräajat direktiivin soveltamisalaan kuuluvilta edellytettävien toimien suhteen alkavat kulumaan tästä ilmoituksesta, NIS2-direktiivin täytäntöönpanossa on lähdetty siitä, että yrityksen itsensä on tehtävä tulkinta siitä, sisältyykö se ja miltä osin soveltamisalaan ja tämän perusteella sen on 43 §:n mukaisesti ilmoitettava valvovalle viranomaiselle säännöksen edellyttämät tiedot itsestään ja toiminnastaan. Mielestämme viranomaisilla tulisi olla samanlainen rooli kuin CER-direktiivissä ja vähintäänkin varmistava rooli ja velvollisuus olla etukäteen yhteydessä soveltamisalan yrityksiin ja antaa ohjeet oikein toimimiseksi. On syytä huomioida, että osa soveltamisalan yrityksistä saattaa olla melko pieniä ja niillä on hyvin rajalliset resurssit lainsäädäntöseurantaan ja turvallisuustyöhön.

CER-direktiivi on myös siltä osin yritysten tarpeet paremmin huomioiden kirjoitettu, että siinä selvästi todetaan, milloin tietyt siinä edellytetyt toimet on viimeistään tehtävä siitä lukien, kun yritykselle on ilmoitettu sen kuulumisesta soveltamisalaan. NIS2-direktiivissä tai sen täytäntöönpanolain luonnoksessa ei tällaisia siirtymäaikoja ole. Kun kansallisen lain on oltava voimassa viimeistään 18.10.2024, ilmoittautumismenettelyyn liittyvä 43 § tulisi luonnoksen mukaan voimaan 1.1.2025 ja muita siirtymäaikoja luonnoksessa ei ole. Kaikkien soveltamisalaan kuuluvien yritysten tulisi siis lähtökohtaisesti olla lain edellyttämällä tasolla 18.10.2024 lukien ja niiden tulisi ilmoittautua valvovalle viranomaiselle heti vuoden 2025 alussa. Vaatimus on kohtuuton. Yrityksille tulisi ehdottomasti antaa riittävästi aikaa rakentaa kyberturvallisuutensa edellytetylle tasolle. Riittävää tässä suhteessa ei ole, että viranomaiset tulevat ohjeistamaan yrityksiä ja käyttävät todennäköisesti ja toivottavasti pidättyväisesti lain tiukempia valvontakeinoja soveltamisen alkuvaiheessa. Luonnoksen kiistaton lähtökohta kuitenkin on, että edellytetään täyttä vaatimustenmukaisuutta ensimmäisestä voimassaolopäivästä lähtien, vaikka valvovat viranomaiset olisivatkin valvonnan alkuvaiheessa joustavampia.

On syytä huomioida, että soveltamisalaan tulee myöhemmässä vaiheessa, siis vuonna 2025 ja sen jälkeen myös pieniä yrityksiä, jotka on vasta tuolloin nimetty CER-kriittisiksi. CER-kriittiseksi määrittelemisestä seuraa paitsi CER-direktiivin tarkoittamien vaatimusten täyttämisvelvollisuus määräaikoineen, automaattisesti myös se, että yritys tulee kuulumaan nyt lausuttavana olevan lain keskeisiin toimijoihin eli se tulee myös ennakkovalvonnan piiriin. Tältä osin sen tulisi siis olla lausuttavana olevan lain tavoitetasolla välittömästi saatuaan tiedon määrittelemisestään CER-kriittiseksi, koska myöskään tähän tilanteeseen laissa ei tulisi olemaan mitään erillistä siirtymäaikaa. Jokainen ymmärtää, että tämä asettaa yrityksen täysin mahdottomaan asemaan. Yritys ei kaikissa tapauksissa voi varautua asiaan mitenkään etukäteen, kun CER-kriittiseksi määritteleminen on epävarmaa ja jos se tehdään, myös nyt lausuttavana olevan lain velvoitteet tulevat välittömästi täysimääräisinä voimaan.

Edellä kerrottu pätee soveltuvin osin myös luonnoksen 3 §:n 3 momentin mahdollisuuteen määritellä valtioneuvoston asetuksella lain soveltamisesta tietyt kriteerit täyttävään toimijaan. On välttämätöntä, että kyseiseen asetukseen sisällytetään riittävä siirtymäaika siihen, milloin näin määritellyiltä yrityksiltä edellytetään esimerkiksi lain sisällöllisten riskienhallintavaatimusten täyttämistä.

Koska NIS2-direktiivin kansallisen täytäntöönpanon valmistelu on edennyt CER-direktiivin täytäntöönpanon valmistelua nopeammin,

tulisi varmistua siitä, että NIS2-lausuntopalautteen myötä esille nousevat seikat välitetään myös CER-direktiivin kansallisesta valmistelusta vastaavien tietoon. Samoin tulisi selvittää, voisiko kansallisen CER-säädöksen valmistelun yhteydessä soveltamisalaan kuuluvien toimijoiden tunnistamiskriteeristöä ja - prosessia hyödyntää soveltuvin osin myös NIS2-soveltamisalaan kuuluvien toimijoiden identifioinnissa.

Olisi hyvä jatkovalmistelussa käydä vielä läpi esitysten liitteiden soveltamisalamäärittelyt suhteessa perusteluissa viitattuihin kansallisiin lakeihin. Ainakin kuriiripalvelun ja postipalvelun tarjoajiin liittyy käsittääksemme epäjohdonmukaisuuksia. Vastaavia voi olla muitakin toimialoja koskevissa kirjauksissa.

Esitetyn 2 luvun 4 §:n mukaan lain 2 lukua ei sovelleta toimintaan tai palveluihin, joita tarjotaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen tai turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi. Yksityiset yritykset tarjoavat monia kohdassa tarkoitettuja palveluita, mutta se, mitä kaikkea toimintaa tällä on yksityiskohtaisemmin tarkoitettu ja mikä taho tekee harkinnan ja päätökset tähän liittyen, jää mielestämme esityksessä liian avoimeksi. Säännöstä ja sen yksityiskohtaisia perusteluja tulisi täsmentää.

Riskienhallintavelvoitetta koskevat huomiot

Kyberturvallisuus näyttäytyy hyvin teknisenä asiana ja käsittää suuren määrän erilaisia termejä. Näin on luonnollisesti myös sekä lausuttavassa esityksessä että sen perustana olevassa direktiivissä. Jatkovalmistelussa tulisi kiinnittää erityistä huomiota siihen, että termejä käytetään johdonmukaisesti kaikissa säännöksissä ja niiden perusteluissa.

Esityksen 2 luvun 8 §:ssä asetetaan vaatimus kyberturvallisuuden riskienhallinnan toimintamallin käytölle ja kuvataan siltä vaadittava kattavuus. Säännöksen perusteluissa todetaan, että kyberturvallisuuden riskienhallinnan tulisi ulottua kaikki vaaratekijät huomioiden myös tietojärjestelmien ja niiden avulla harjoitetun toiminnan sekä tarjottavien palveluiden fyysiseen ympäristöön, kuten toimitiloihin. Perustelujen neljännessä kappaleessa ”Kaikki vaaratekijät huomioivan lähestymistavan tulisi kattaa…” mainitaan kuitenkin vain tietoturvallisuusriskit. Selvyyden vuoksi perustelujen tässä kohdassa tulisi mainita myös kyberturvallisuus ja fyysisen toimintaympäristöön liittyvä turvallisuus. 9 §:n kohtia koskevat perustelutekstit olisi tässä suhteessa tarpeen vielä käydä läpi sen varmistamiseksi, että kunkin turvallisuuden osa-alueen kannalta olennaiset asiat ja termit on huomioitu ja niitä käsitellään kaikissa kohdissa yhdenmukaisella tavalla.

Direktiivin 21 artiklan 2.d) -kohdan mukaan kyberturvallisuusriskien hallintatoimenpiteiden hallintamalliin on sisällytettävä myös ”toimitusketjun turvallisuus, mukaan lukien kunkin toimittajan ja sen välittömien toimittajien ja palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.”

Luonnoksen 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.”

Luonnoksen säännöstekstissä ei siis painoteta sitä, 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 vastuun ulottuvuutta koske-van määritelmän jättäminen yksityiskohtaisiin perusteluihin ei ole hyväksyttävää.

Lisäksi asiayhteyden osalta tulisi olla selvää, että välittömien toimittajien ja palveluntarjoajien tulee olla relevantteja nimenomaan soveltamisalaan kuuluvan yrityksen kyberturvallisuuden riskienhallinnan kannalta. Nyt tämä ei selvästi sanamuodosta ilmene, vaan sanamuodon mukainen tulkinta johtaisi siihen, että yrityksen tulisi lähtökohtaisesti varmistua esimerkiksi sellaisen toimittajansa kyberturvallisuuden tasosta, jolla ei ole mitään merkitystä yrityksen oman kyberturvallisuuden kannalta. Esimerkkinä voisi olla toimittaja, joka toimittaa yritykselle vaikkapa sen päivittäin tarvitsemia hygieniatuotteita ilman, että yrityksen ja toimittajan välillä olisi esimerkiksi minkäänlaista ICT-integraatiota tai -yhteyttä. Säännös velvoittaisi varmistumaan lähtökohtaisesti 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 tässä suhteessa riittävää, koska kokonaisuus kuitenkin käytännössä velvoittaisi yritykset lähtökohtaisesti varmistumaan kaikkien toimittajien ja palveluntarjoajien tasosta ja erikseen perustelemaan ja dokumentoimaan, jos ne katsovat, ettei velvollisuus ulotu kyseiseen toimittajaan tai palveluntarjoajaan. Tällaisesta lähestymistavasta seuraa vain tarpeetonta hallinnollista taakkaa. Pykälän kyseistä 2 momentin 4) -kohtaa on myös tältä osin tarkennettava.

Nostamme lisäksi esille yleisen haasteen liittyen sopimuspohjaiseen (osittaiseen) riskinsiirtoon 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 alueella, 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”. Viittaamme tältä osin jäsenyhdistystemme Teknologiateollisuus ry:n, Puolustus- ja ilmailuteollisuus (PIA) ry:n ja Kyberala (FISC) ry:n yhteiseen lausuntoon.

Riskienhallintamenetelmien osalta, erityisesti kun puhutaan teknologisten ympäristöjen riskienhallinnasta, on huomattava, että ne elävät ajassa, kehittyvät ja ovat myös tekniikka-/teknologiasidonnaisia. Tämän vuoksi on tärkeää, että yrityksille jätetään mahdollisuuksia ja liikkumavaraa siihen, miten ne huolehtivat organisaatioissaan riskienhallinnan käytännön toteutuksesta. Tämä on hyvä huomioida myös säännöskohtaisissa perusteluissa, mahdollistaen liikkumavara yksittäisen riskienhallintamenetelmän toimeenpanossa, eikä kirjoittaa perusteluita ehdottomaan muotoon.

Riskienhallintamenetelmien osalta perusteluissa tuleekin tuoda selkeämmin esille se, että menetelmät ovat sidonnaisia käytettyyn tekniikkaan. Esimerkiksi vanhempien verkkoteknologioiden osalta toimenpiteet eivät ole, eivätkä voi olla yhtä kattavia tai sofistikoituneita verrattuna uudempiin verkkoteknologioihin, koska tekniikka on niissä huomattavasti vanhempaa ja kehittymättömämpää. Tällöin myöskään riskienhallinnan mahdollisuudet (toimenpiteet ja kyvykkyydet) eivät voi olla samalla tasolla kuin mitä ne voivat olla uudemmissa verkkoteknologioissa. Viittaamme tältä osin myös Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry:n lausuntoon.

Luonnoksen 2 luvun 9 §:n kohtia koskevat yksityiskohtaiset perustelut ovatkin paikoitellen liian yksityiskohtaisia. Turvallisuuslainsäädännön, erityisesti teknologiaan liittyvän turvallisuuslainsäädännön lähtökohtana tulisi olla, että siinä määritellään tavoiteltu turvallisuuden taso, mutta jätetään keinot toimijan itsensä päätettäviksi, koska samaan turvallisuuden tasotavoitteeseen voidaan usein päästä vaihtoehtoisilla keinoilla. Nyt perusteluissa mennään jo paikoitellen liian yksityiskohtaiselle tasolle huomioiden myös sen, että säännöksen 4 momentissa annetaan valvoville viranomaisille lisäksi oikeus antaa toimialallaan tarkempia teknisiä määräyksiä useiden eri turvallisuuden osa-alueiden menettelyistä, menetelmistä ja toimenpiteistä. Nämä ovat juuri niitä keinoja, joiden valinnan tulisi olla toimijan itsensä päätettävissä. Vain se tuntee oman toimintansa riskit ja voi arvioida, mikä menetelmä soveltuu tai ei sovellu omaan toimintaansa sekä harkita, millainen menetelmien ja hallintakeinojen kokonaisuus on kulloinkin kustannustehokkain. Toivomme, että tämä huomioidaan jatkovalmistelussa ja säännösten ja perusteluiden sanamuodot kirjoitetaan sellaiseen muotoon, että kysymys on näiltä osin esimerkinomaisista kuvauksista, miten asia voidaan hoitaa, mutta niissä ei myöskään suljeta pois tai niistä ei voi saada käsitystä, ettei toisenlainenkin tapa hoitaa asia voisi tulla kyseeseen.

Johdon vastuuta koskeva luonnoksen 10 §:n 1 momentti on nähdäksemme hyvin kirjoitettu. Siitä ilmenee selvästi, mistä johto vastaa.

Sen sijaan se, mille toimijoille oikeushenkilön sisällä henkilökohtainen vastuu kohdentuu, on erittäin ongelmallinen. Suomessa lainsäädännöllisesti on lähdetty siitä, että yhtiöoikeudellinen vastuu koskee osakeyhtiön toimielimiä, eli hallitusta, mahdollista hallintoneuvostoa ja toimitusjohtajaa. Vastuun ulottaminen toimitusjohtajan välittömässä alaisuudessa kuuluviin tehtäviin (”johtoryhmiin”) on Suomen oikeudelle vieras, eikä vastaa direktiivin sanamuotoja (”lailliset edustajat”). Myös hallituksen esityksen perusteluissa viitataan ”hallintoelimeen”, jollainen johtoryhmä ei ole. Yhtiöoikeudellisesti hallitus (tai hallintoneuvosto) nimittää toimitusjohtajan ja valvoo hänen toimintaansa. Toimitusjohtaja taas vastaa yhtiön operatiivisesta johtamisesta ja järjestää sen parhaaksi katsomallaan tavalla. Johtoryhmille ei ole Suomessa asetettu itsenäistä vastuuta ja viittaukset toimitusjohtajan alaisiin (”johtoryhmiin”) tulisi poistaa lakiehdotuksesta.

HE-luonnoksen sivulla 12 on todettu direktiivin 21 artiklan edellyttä-vän, että yhteisön ”-- hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen”. Ajatus osakeyhtiön hallintoelinten pakollisista koulu-tusvelvoitteista on Suomen oikeudelle vieras, eikä ole tavanomaista, että esimerkiksi yhtiön hallitustyölle asetetaan operatiivisia koulutus-velvoitteita. Yleisen huolellisuusvelvoitteen perusteella yhteisöt arvioi-vat itsenäisesti miten paljon mahdollista koulutusta yhteisön toimieli-met mahdollisesti tarvitsevat erilaisten lakisääteisten velvoitteiden to-teuttamiseksi. Sääntelyn osalta pitääkin siis pitää selkeästi erillään hallituksen valvontarooli ja toimivan johdon (toimitusjohtajan) rooli. Tässä suhteessa ehdotettu 10 § on nähdäksemme toimitusjohtajaan sovellettavin osin hyvin kirjoitettu (”Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.”). Sanamuoto jättää harkinnan aivan oikein oikeushenkilön sisällä tehtäväksi, kuten pitääkin. Tämän tulisi riittää.

Lisäksi huomautamme, että koulutusvelvollisuudesta on rajattu pois myös julkisyhteisön hallintoelimet (s. 45, kohta 3.16.4). Samaa lähestymistapaa tulisi edellä kerrotuin perustein soveltaa myös yksityisiin yhteisöihin. Viittaamme edellä johdon vastuuseen ja koulutusvelvollisuuteen liittyen myös Listayhtiöiden neuvottelukunnan (LYNK) lausuntoon.

Raportointivelvoitetta koskevat huomiot

Raportointi perustuu hyvin tiukkoihin määräaikoihin ja se, että valvonta ja sen myötä raportointi tulee monialayhtiöissä hajautumaan useille eri viranomaisille ja toiminnan ollessa kansainvälistä myös useiden eri maiden viranomaisille.

Monikansallisten toimijoiden osalta tulisi selkiyttää sitä, miten toimijoiden ulkomailla olevat yksiköt huomioidaan NIS2-raportointivelvoitteiden osalta Suomen viranomaisen näkökulmasta. Tähän liittyen on myös huomioitava se, että useilla soveltamisalan piiriin tulevilla yhteisöillä on yksiköitä EU:n alueella sekä kolmansissa maissa.

Luonnoksen 4 luvun 34 §:n mukaan valvovan viranomaisen on tietyissä tilanteissa raportoitava havainnoistaan tietosuojavaltuutetulle. Säännösesityksen perusteluissa sivun 148 ensimmäisessä kappaleessa on käsitelty sitä, miten tietoturvaloukkauksista tulee nykylain mukaan raportoida, mikäli ilmoittaja harjoittaa sähköisen viestinnän palveluista annetussa laissa tarkoitettua teletoimintaa. Todetun mukaan tällöin riittäisi, että myös sellaisista tietoturvaloukkauksista riittäisi teleoperaattorin ilmoitus Liikenne- ja viestintävirastolle, joissa on kyse henkilötietojen loukkauksesta. Käsityksemme kuitenkin on, että tietosuojavaltuutettu edellyttää ilmoitusta erikseen myös tietosuojavaltuutetun toimistolle. Asiaa tulisi selkeyttää. Viittaamme tältä osin Tietoliiken-teen ja tietotekniikan keskusliitto FiCom ry:n lausuntoon, jossa asiaa on tarkasteltu yksityiskohtaisemmin.

Kannatamme edellä kerrotussa tilanteessa, mutta yleisesti kaikilla muillakin toimialoilla sitä, että yrityksellä tulisi olla velvollisuus tehdä samasta poikkeamatilanteesta vain yksi ilmoitus ja vastaanottavan viranomaisen tulisi huolehtia viestimisestä muille tarvitseville viranomaisille. Tulevaisuudessa sama tietoturvaloukkaus laukaisee usein raportointivelvollisuuden sekä nyt lausuttavana olevan lain että yleisen tietosuoja-asetus GDPR:n nojalla, mikäli henkilötietoja on vaarantunut. Mikäli kysymys on laajemmasta tietoturvaloukkauksesta ilmoittajan toiminnassa, raportointivelvollisuus molemmille tahoille laukeaa lisäksi niissä kaikissa EU:hun kuuluvissa toimintamaissa, joita loukkaus tai sen vaikutukset koskevat. On yrityksen kannalta täysin kohtuutonta, että tilanteessa, jossa sen tulisi keskittää resurssit syntyneen vakavan ongelmatilanteen hoitamiseen, paljon työaikaa tulee menemään moninkertaiseen (24 h / 72 h) raportointiin usealle viranomaiselle useassa toimintamaassa. On ehdottomasti pyrittävä ”yhden luukun periaatteeseen” ensin kotimaassa ja toivottavasti pidemmällä aikavälillä koko EU:ssa.

Olemme myös erittäin huolissamme viranomaisten resurssoinnista ja viranomaisvastetta koskevista vaatimuksista. Liikenne- ja viestintävirastolle esitetään uusien valvontatehtävien lisäksi myös muita viranomaistehtäviä, joista aiheutuu resursointitarpeita. Direktiivin kansallisen toimeenpanon myötä mm. CSIRT-yksikön sekä toimialakohtaisten valvontaviranomaisten 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 viestintäviraston resurssit on turvattava tavalla, jolla varmistetaan sekä säädösten asiallinen toimeenpano, nykyisten ja uusien viranomaistehtävien hoitaminen tuottavasti sekä mahdollistaen sen, että viranomaistoiminta tukee yritysten kasvua ja vientiä vauhdittavia liiketoimintamahdollisuuksia.

Vaikka valvovilla viranomaisilla olisi velvollisuus vastata poikkeaman raportoineelle yritykselle ja tukea sitä ongelman selvittämisessä, luonnoksen mukaan niillä ei olisi velvollisuutta 24/7/365 päivystyksen järjestämiseen ja niiden tulisi vastata poikkeamailmoituksen tehneelle taholle ”viivytyksettä ja mahdollisuuksien mukaan 24 tunnin kuluessa, mutta kuitenkin virka-aikojen puitteissa” (s. 130). Samalla kuitenkin soveltamisalan yrityksiltä edellytettäisiin käytännössä välitöntä raportointikyvykkyyttä riippumatta poikkeaman havaintohetkestä. Tämä ei ole kohtuullista. Jos lainsäädännöllä luodaan vaatimuksia sekä yrityksille että niitä valvoville viranomaisille, on huolehdittava siitä, että viranomaiset myös kykenevät vasteen antamaan silloin, kun sitä tarvitaan. Jos tämä ei käytännössä toteudu, se johtaa helposti siihen, että lainsäädäntö koetaan yrityksissä ennen kaikkea hallinnollisena taakkana. Tällaisessa lainsäädännössä sen yhteiskunnallisiin tavoitteisiin päästään vain, jos vastuut ovat myös käytännössä tasapainossa keskenään. Liikenne- ja viestintäviraston nykyinen valtionhallinnolle ja huoltovarmuuskriittisille toimijoille tarkoitettu 24/7-päivystys tulee ehdottomasti säilyttää ja myös toimialakohtaisilla valvovilla viranomaisilla tulisi olla velvollisuus päivystyksen järjestämiseen.

Viittaamme edellä viranomaisten resurssoinnista lausutun osalta myös jäsenyhdistystemme Teknologiateollisuus ry:n, Puolustus- ja ilmailuteollisuus (PIA) ry:n ja Kyberala (FISC) ry:n yhteiseen lausuntoon.

Valvontaa koskevat huomiot

Edellä raportoinnin yhteydessä toimme esiin huolemme viranomaisten resurssoinnin riittävyydestä. Luonnollisesti sama huoli liittyy myös valvontaan. Riittävän resurssoinnin lisäksi on välttämätöntä huolehtia siitä, että valvovien viranomaisten osaaminen on riittävää. Esityksen 2 luvun 9 §:n toimenpiteet edellyttävät jo yksinään laajapohjaista ja varsin syvää asiantuntemusta. On tarpeen miettiä, miten tämä varmistetaan kustannustehokkaasti. Onko valvovien viranomaisten mahdollisuus käyttää resursseja ristiin keskenään tai onko tietyn osaamisen osalta tarpeet järkevää hoitaa resurssipoolijärjestelyiden avulla?

Ehdotuksessa valvonta on jaettu eri viranomaisille sen mukaan, mistä toimialasta on kyse. Useat yritykset ja/tai konsernit toimivat useilla aloilla ja näin saattavat tulla valvonnan kohteeksi usean viranomaisen toimesta. Tällöin vaarana ovat valvonnan päällekkäisyydestä aiheutuvat tulkintaepäselvyydet, jos useampi viranomainen valvoo toimintaa. Epäselvyyttä voi aiheuttaa esimerkiksi tilanne, jossa viranomaisten saman konsernin/yhteisön/yksikön eri osille antamat neuvot ja ohjeet eroavat toisistaan.

Ehdotetun 33 §:n tarkoittamien toimintakieltojen soveltamisala on hyvin laaja ja aiheuttaa tulkintaepäselvyyttä siitä huolimatta, että soveltaminen on rajoitettu keskeisin toimijoihin. Kuten edellä olemme ehdotetun 10 §:n osalta todenneet, siitä ja myös 33 §:stä tulisi poistaa viittaukset toimitusjohtajan alaisuudessa toimiviin henkilöihin (”johtoryhmään”) edellä kerrotuin perustein. Myös edellä todettu viranomaisvalvonnan jakautuminen useille valvoville viranomaisille voi aiheuttaa epävarmuutta seuraamusjärjestelmän ennakoitavuudesta osakeyhtiön johdossa toimiville.

Johdon toiminnan rajoittamista koskeva 33 §:n luonnos on erittäin ongelmallinen muutoinkin, eikä vastaa direktiivissä edellytettyä:

Kyseessä on ensinnäkin asiallisesti ottaen Suomen rikoslainsäädännön liiketoimintakieltoa vastaava rajoitus, tosin rajoitettuna vain kyseisiin tehtäviin. Henkilön toimintaa nykyisessä tehtävässään nykyisen työnantajansa palveluksessa voitaisiin rajoittaa ilman, että sen kohteeksi joutuva henkilö on todettu lainvoimaisesti syyllistyneen rikokseen. Enimmillään viiden vuoden määräaika kiellon voimassaololle on myös poikkeuksellisen ankara. Tällainen seuraamus on hyvin poikkeuksellinen, perustuslain elinkeinovapauden kannalta hyvin ongelmallinen ja mielestämme luonnoksessa esitetyn mukaisena mahdoton hyväksyä.

Säännösluonnos on epäselvä sen suhteen, minkä toimijan piirissä olevia tehtäviä se koskee. On varmasti tarkoitettu mahdollistaa kiellon määrääminen koskien toimintaa samassa tehtävässä, johon laiminlyönnit liittyvät. Käytettyä sanamuotoa, ”kieltää henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä…” voi kuitenkin tulkita niinkin, että kielto koskisi vastaavia tehtäviä myös muissa lain tarkoittamien keskeisten toimijoiden piirissä. Tätä ei varmaankaan ole tarkoitettu, mutta sanamuotoa on ilmeisen tarpeellista tarkentaa tältä osin, jotta väärinkäsityksiltä vältytään. Direktiivissäkin tämä kohdentuminen on todettu selvästi: ”…kieltämään väliaikaisesti...hoitamasta kyseisen toimijan johtotehtäviä.”

Direktiivin rajoituksia ja kieltoja koskevassa 32 artiklassa todetaan: ”Tämän kohdan nojalla 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.” Tästä on pääteltävissä, että kielto on näin tarkoitettu alun perin painostuskeinoksi, ei rangaistukseksi. Jostain kummallisesta syystä lausuttavana olevassa luonnoksessa ei tällaista rajoituksesta vapautumista ole mainittu ollenkaan, ei myöskään säännösehdotuksen yksityiskohtaisissa perusteluissa, mikä muuttaa sen puhtaasti rangaistukseksi. Tämä ei ole hyväksyttävää. Vaadimme, että säännöksen sanamuotoon on kirjoitettava edellä kerrottuun direktiivin artiklaan kirjattu mahdollisuus vapautua kiellosta korjaamalla rajoituksen määräämiseen johtaneet puutteet.

Esityksen 4 luvun 27 §:ssä annetaan valvoville viranomaisille oikeus saada laissa tarkoitetuilta toimijoilta valvonnan kannalta tarpeelliset tiedot salassapitovelvollisuuden estämättä. Säännöksen yksityiskohtaisissa perusteluissa (s. 143, toinen kappale) todetaan: ”Jos valvonnan kohteena oleva toimija olisi ulkoistanut osan tai kaikki kyberturvallisuusprosesseistaan ja valvova viranomainen esittäisi toimijalle tietopyynnön, toimija olisi velvollinen toimittamaan tiedon riippumatta siitä, onko tieto toimijan vai ulkoistetun tahon hallussa. Toimija olisi tarvittaessa velvollinen hankkimaan pyydetyt tiedot toimittajaltaan ja toimittamaan ne valvovalle viranomaiselle.” Tämä on liian suoraviivaisesti todettu. On syytä huomioida, että näiden osapuolten välillä on tyypillisesti sopimussuhde, ja sopimuksessa on voitu sopia siitä, mistä asioista toimittaja tai palveluntarjoaja on velvollinen antamaan tietoja. Osa valvovan viranomaisen pyytämistä tiedoista voi myös olla sellaisia esimerkiksi tuotteeseen tai palveluun liittyviä tietoja, jotka toimittaja tai palveluntarjoaja katsoo omaan liike- tai ammattisalaisuuteensa kuuluviksi, eikä siksi suostu toimittamaan niistä pyydettyä tietoa. Toivomme, että tämä huomioidaan perustelutekstissä ja velvoitetaan toimija pyytämään tietoa, mutta ellei se siitä edellä kerrotusta tai muusta perustellusta syystä saa, sille ei tästä saa aiheutua mitään negatiivista seurausta. On myös hyvä huomioida, että osa B-to-B-sopimussuhteista, esimerkiksi tilojen vuokrasuhteet, voivat olla hyvin pitkiä, eikä niiden ehdoista välttämättä ole mahdollista kesken sopimuskauden sopia aiemmasta poiketen.

Saman säännösehdotuksen 1 momentissa todetaan: "Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta." Kohtaan 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. Viittaamme tältä osin jäsenyhdistystemme Teknologiateollisuus ry:n, Puolustus- ja ilmailu-teollisuus (PIA) ry:n ja Kyberala (FISC) ry:n yhteiseen lausuntoon.

Seuraamusmaksua koskevat huomiot

Olemme edellä kuvanneet haasteita liittyen velvoitteiden kohdentumiseen saman juridisen oikeushenkilön sisällä ja konserneissa (Soveltamisalaa koskevat huomiot). Samat haasteet liittyvät myös mahdollisten hallinnollisten seuraamusmaksujen määräämiseen. Ehdotetun 40 §:n sanamuodon mukaan tulisi olla selvää, että siinä toimijalla viitataan laajimmillaankin siihen välittömään juridiseen oikeushenkilöön, jonka soveltamisalaan kuuluvasta toiminnasta on kyse. Jos kyse on konserniyhtiöstä, tällöin ei huomioida koko konsernin kokonaisliikevaihtoa Suomessa tai globaalisti tai muiden mahdollisten konserniyritysten liikevaihtoa. Selvyyden vuoksi rajaus olisi hyvä kirjoittaa selvästi säännöksen yksityiskohtaisiin perusteluihin.

Sanamuodon mukainen tulkintakaan ei kuitenkaan johda oikeudenmukaiseen lopputulokseen tilanteessa, jossa seuraamusmaksun määräämisen perusteena olevat säännösten rikkomiset tai väärinkäytökset liittyvät vain osaan kyseisen oikeushenkilön harjoittamasta toiminnasta. Voi esimerkiksi hyvin olla tilanne, jossa soveltamisalaan kuuluva toiminta kattaa vain 10 % kyseisen oikeushenkilön kokonaisliikevaihdosta. Seuraamusmaksun suuruus määritettäisiin ilmeisesti tästä huolimatta sen kokonaisliikevaihdon perusteella. Seuraamusmaksun määräytymiseen tulisi vaikuttaa vain sen liikevaihdon, joka on esityksen tavoitteiden kannalta keskeinen eli sen oikeushenkilön tai sen toiminnan liikevaihto, jonka kyberturvallisuuden riittävän tason varmistaminen on tavoitteena. Muuta ei tulisi huomioida. Toissijaisesti katsomme, että vähintäänkin säännökseen tulisi kirjoittaa velvoite kohtuullistaa seuraamusmaksua soveltamisalaan kuuluvan ja po. virheiden tai puutteiden kannalta relevantin toiminnan laajuus huomioiden.

Seuraamusjärjestelmän osalta on myös epäselvää, miten seuraamuksia määrätään tilanteessa, jossa yrityksen/konsernin toimintaa valvoo useampi viranomainen. Tämä liittyy läheisesti edellä esiin nostettuun epäselvyyteen siitä, miten sääntelyn katsotaan soveltuvan konserneihin ja niissä oleviin eri toimintaa harjoittaviin yhteisöihin. Toki viranomaisten välistä yhteistyötä koskeva ehdotuksen 46 § pyrkii selventämään yhteistyön tarkoitettua sisältöä ja toimintatapoja, mutta se ei suoraan tuo ratkaisua yllä mainittuihin mahdollisiin tulkintahaasteisiin.

Esityksen 5 luvun 38 §:ssä säädettäisiin seuraamusmaksulautakunnasta, johon liittyen haluamme kiinnittää huomiota seuraavaan:

Säännöksen yksityiskohtaisissa perusteluissa (s. 148–149) todetaan, että seuraamusmaksulautakunta ei olisi päätoiminen, vaan se kokoontuisi tarvittaessa seuraamusmaksun määräämistä koskevan asian käsittelemiseksi. Lautakuntaan kuuluisivat Liikenne- ja viestintäviraston nimeämät puheenjohtaja ja varapuheenjohtaja, sekä kunkin valvovan viranomaisen nimeämät jäsen ja varajäsen. Lautakunnan tehtävä olisi jäsenelle ja varajäsenelle sivutoiminen. Mikäli tällä on tarkoitettu, että puheenjohtajan ja varapuheenjohtajan tehtävät olisivat päätoimisia, vastustamme ehdotusta. Kun lautakunta kokoontuu vain tarvittaessa, päätoimisuudelle ei ole perusteita, eikä tällainen olisi järkevää julkisten varojen käyttöä. Mikäli puolestaan on tarkoitettu, kuten pidämme todennäköisenä, että myös puheenjohtajan ja varapuheenjohtajan tehtävät olisivat sivutoimisia, tämä olisi syytä nimenomaisesti todeta väärinkäsitysten välttämiseksi, koska nyt heitä ja muita jäseniä ja varajäseniä käsitellään tekstissä erikseen.

Koska seuraamusmaksulautakunnan tehtävänä on objektiivisesti harkita soveltamisalaan kuuluvan toimijan toimintaa tapahtumissa, joihin liittyvät usein myös valvovien viranomaisten ja Liikenne- ja viestintäviraston CSIRT-yksikön toimet, olisi nähdäksemme perus-teltua, että päätöksentekoon eivät voi osallistua sellaiset virkamie-het, jotka ovat osallistuneet harkittavana olevaan tapahtumaket-juun liittyviin valvontatoimiin tai kyseisen valvottavan valvontaan yleisesti. Seuraamusmaksulautakuntaan liittyvissä säännösehdo-tuksissa tai niiden perusteluissa ei ole kuitenkaan kiinnitetty näi-hin kysymyksiin huomiota, eikä jääviyskysymyksiä ole huomioitu edes viittaussäännöksin. Nähdäksemme tämä olisi tarpeen.

CSIRT-yksikön tehtäviä koskevat huomiot

Vaikka säädösehdotuksen 3 luvun 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.

Säädösehdotuksen 3 luvun 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. Yhteistyövelvoite tulee sisällyttää itse säännökseen direktiivin edellytysten mukaisesti. Ei ole riittävää, että asia todetaan yksinomaan säännöksen perusteluissa.

Saman luvun 20 §:ssä tarkoitetun viestintäverkkojen ja tietojärjestel-mien verkkopohjainen haavoittuvuuskartoituksen osalta ehdotukses-sa ei ole käsitelty sitä, kuinka eri jäsenvaltioiden CSIRT-yksiköiden te-kemiä haavoittuvuuskartoituksia koordinoidaan. Puutteelliseksi ovat jääneet kysymykset mm. monikansallisten yhtiöiden laajoista IP-osoitealueista tai palveluntarjoajien sellaisista IP-osoitteista, joiden palveluita hallinnoivat asiakkaat itse.

Viittaamme näiltä osin myös jäsenyhdistystemme Teknologiateollisuus ry:n, Puolustus- ja ilmailuteollisuus (PIA) ry:n ja Kyberala (FISC) ry:n yhteiseen lausuntoon.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Mielestämme on selvää, että kriittisten julkisten, soveltamisalaan kuu-luvien palvelutoimijoiden on yksityisten yritysten tavoin järjestettävä valmius reagoida poikkeamiin myös virka-ajan ulkopuolella. Sää-dösehdotuksen perusteluosion sivulla 165 on todettu, että niiden ”päi-vystyksen tarve, kohde ja laajuus arvioidaan viranomaisen (tiedonhal-lintalain) 18 b ja c §:ien mukaisesti toteutetussa riskienhallinnassa”. Liikenne- ja viestintäviraston valtionhallinnon puheena olevan lain noudattamista valvovana viranomaisena tulee huolehtia, että kriittisis-sä julkisissa palveluissa myös päivystys poikkeamien varalta on riittä-vän kattavaa ja toimivaa. Tämä on monilta osin myös palveluita käyttä-vien ja tarvitsevien yritysten ja kansalaisten etu.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Säädösluonnoksen yksityiskohtaisempi taloudellisten yritysvaikutusten arviointi on tehty perustuen erityisesti Liikenne- ja viestintäministeriön säädöksen valmisteluvaiheessa Insta Advance Oy:ltä tilaaman selvityksen tuloksiin direktiivin 21 artiklan mukaisen riskienhallintavelvoitteen kustannuksista suomalaisille yrityksille. Selvityksessä kustannuksia arvioitiin yksinomaan elintarvike- ja valmistussektoreilla, koska näillä toimialoilla yritykset eivät olleet kuuluneet NIS1-direktiivin soveltamisalaan ja toimialoilla huomattava määrä yrityksiä tulee nyt kuulumaan NIS2-direktiivin soveltamisalaan.

On hyvä, että tällainen selvitys osana valmistelua on toteutettu ja se on tehty yrityksiä osallistaen. Mielestämme säädösesityksen yritysvaikutusten arvioinnin tulisi kuitenkin olla vielä yksityiskohtaisempaa ja sitä tulisi laajentaa myös muille toimialoille. Soveltamisalan toimialat poikkeavat monella tapaa toisistaan ja yhtä alaa koskevista havainnoista ei voida yksiselitteisesti johtaa päätelmiä kaikkia toimialoja koskien. Jää lisäksi epäselväksi, onko selvityksessä huomioitu direktiivin 21 artiklan edellyttämät toimenpiteet kokonaisuudessaan, koska niiden kokonaisuus ei kaikilta osin avaudu itse artiklasta, tai nyt lausuttavana olevan esityksen 2 luvun 7–9 §:stä, vaan kokonaisuuden ymmärtääkseen pitää käydä yksityiskohtaisesti läpi lausuttavan säännöksen yksityiskohtaisissa perusteluissa lueteltuja toimia ja niiden vaikutuksia. Osa teknisistä toimenpiteistä voi olla hyvin kalliita. Kiinnitämme huomiota siihen, että antaessaan esityksen direktiivin sisällöksi Euroopan komissio arvioi, että NIS1-soveltamisalaan kuuluvien yritysten ICT-kustannukset nousevat NIS2:n myötä keskimäärin 12 % ja NIS1-soveltamisalaan kuulumattomien yritysten kustannukset peräti 25 %. Tämä komission arvio on todettu myös luonnoksessa. Tällaiset kustannusnousut ovat vähänkin isommissa yrityksissä helposti useita miljoonia euroja. Lisäksi on hyvä huomioida, että esitetyn 2 luvun 9 §:n 4 momentin mukaan valvovat viranomaiset voivat sektorikohtaisesti antaa tarkempia teknisiä määräyksiä useista sellaisista asioista, joiden toteuttaminen voi olla hyvin kallista.

Muut huomiot ja avoin palaute esityksestä

Luonnoksessa on kohtalaisen kattavasti avattu, mikä siinä käytetyillä termeillä tarkoitetaan tässä yhteydessä. Joitakin puutteita määritelmissä vielä on. Niissä olisi hyvä kattaa myös ainakin 22 §:n 2 momentin 5) -kohdassa todettu vaarantumisindikaattori, joka ei mielestämme avaudu riittävästi ao. kohdasta.

Luonnoksen 4 §:n 5 momentin säännöstekstin mukaan ”Tässä laissa ei velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaaran-taisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua”. Säännösesityksen yksityiskohtaisissa perusteluissa on käytetty esimerkkinä kansallisen yhteyspisteen mahdollisuutta tällä perusteella kieltäytyä luovuttamasta tietoa direktiivin täytäntöönpanoon liittyville kansainvälisille toimijoille. Säännös on kuitenkin erittäin olennainen myös soveltamisalan yritysten näkökulmasta; myös niillä tulee olla mahdollisuus vedota säännökseen ja tästä syystä sen tulkinnan tulee olla selkeä. Tämän vuoksi ainakin kansallinen turvallisuus olisi tarpeen määritellä myös 2 §:ssä.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Lainsäädäntö ja hallinto

Tommi Toivola

Johtaja

Rajamäki Markku
Elinkeinoelämän keskusliitto EK - Yrityslainsäädäntö ja hallinto