Tuukka Heikkilä
29.11.2023

dnro VN/18157/2023

Luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Energiateollisuus ry kiittää mahdollisuudesta lausua otsikossa mainitusta esityksestä. Toteamme lausuntonamme seuraavaa:

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Energia-ala on sitoutunut toimimaan vastuullisesti keskeisenä osana yhteiskunnan kriittistä infraa. NIS2-direktiivi kuten myös muut viimeaikaiset kyber- ja fyysisen turvallisuuden lainsäädäntöhankkeet ovat perusteltuja EU:n ja erityisesti Suomen turvallisuusympäristön muututtua merkittävästi.

Olemme tunnistaneet ainakin seitsemän direktiiviä tai asetusta, joita ollaan valmistelemassa tai toimeenpanemassa vuoden 2023 lopussa ja sen jälkeen. On ehdottoman tärkeää, että näiden lainsäädäntöhankkeiden välinen yhteensopivuus varmistetaan niin sisältöjen kuin aikataulujenkin suhteen.

Toinen huomio koskee toimeenpanon jälkeistä käytännön toimintaa. Kuten äskettäin lausunnolla olleessa kyberturvallisuuden verkkosäännön luonnoksessa [Ares(2023)7142081] todetaan, kyberturvallisuuden uudesta sääntelystä johtuvat kustannukset täytyy voida kattaa tulonlähteiltä täysimääräisesti. Muu olemassa oleva sääntely ei saa estää kustannusten kattamista. Esimerkiksi verkkoyhtiöillä täytyy olla mahdollisuus sisällyttää nämä uuden valvontamallin mukaisiin kustannuksiin verkkopalvelujen hinnoittelussa.

Mikäli edellä mainitussa epäonnistutaan, uuden sääntelyn kustannukset haittaisivat suoraan toimijoiden muun toiminnan taloudellisia edellytyksiä. Mukaan lukien ne kyber- ja fyysistä turvallisuutta parantavat toimenpiteet, joita sääntely ei edellytä, vaan jotka ovat toimijoiden oman innovoinnin ja vastuullisuuden tulosta. Tästä löytyy myös näyttöjä, sillä Suomen energia-alalla ei suuria kyberturvapoikkeamia ole tapahtunut. Tämä ei ole siitä kiinni, etteikö yrityksiä olisi ollut.

Soveltamisalaa koskevat huomiot

Lakiluonnoksen perusteella on epäselvää, soveltuvatko velvoitteet sähkön vähittäismyyntiin (b2c ja b2b). Soveltamisalaa tulisi selventää tältä osin. Samalla tulisi arvioida, onko sähkön vähittäismyynti kriittinen alue huomioiden, että mahdollisen poikkeustilanteen vaikutus sähkön fyysiseen toimitukseen on rajattu.

NIS2-velvoitteiden soveltamista yritys- ja konsernirakenteisiin tulisi tarkentaa. Jos yrityksen yksikön tietty toiminto kuuluu NIS2-soveltamisalaan, on epäselvää, mihin toimintoihin NIS2-velvoitteet kohdistuvat; vain kyseisen yksikön soveltamisalaan kuuluvaan toimintaan, koko yksikön toimintoihin vai jopa koko yrityksen/konsernin kaikkiin toimintoihin.

NIS2 mukaisen ”Toimijan” käsite vaikuttaa myös seuraamusjärjestelmään ja sitä tulisi selventää. Ehdotuksessa seuraamusmaksu on sidottu "toimijan" maailmanlaajuiseen liikevaihtoon, mikä voi johtaa merkittävään vaihteluun seuraamusmaksun suuruudessa riippuen siitä, tulkitaanko "toimijaksi" koko konserni vai esimerkiksi yksittäinen tytäryhtiö.

Monikansallisten toimijoiden kohdalla olisi tarpeen selventää, miten näiden toimijoiden ulkomailla sijaitsevat yksiköt otetaan huomioon NIS2-raportointivelvoitteiden osalta Suomen viranomaisten näkökulmasta. On myös otettava huomioon, että monilla soveltamisalan piiriin kuuluvilla yhteisöillä on yksiköitä sekä EU:n alueella että kolmansissa maissa.

Toimijan määrittelyyn liittyen lakiluonnoksessa todetaan, että soveltamisalaan kuuluva toimija voi olla oikeushenkilö tai luonnollinen henkilö, joka harjoittaa liitteissä I tai II määriteltyä toimintaa ja täyttää tai ylittää keskisuuren toimijan määritelmän. Velvoitteiden soveltamisen kokokriteerinä olisi keskisuuret yritykset Komission suosituksen 2003/361/EY perusteella. Suosituksen 2003/361/EY 6 artiklan 2 momentissa määritellään, että yrityksen, jolla on omistusyhteys- tai sidosyrityksiä, tiedot määräytyvät yrityksen tilinpäätös- ja muiden tietojen perusteella tai konsolidoidun tilinpäätöksen perusteella, johon on lisätty yrityksen tiedot.

Lakiluonnoksen perusteella voi tulkita, että yritys, joka harjoittaa liitteissä I tai II määriteltyä toimintaa ja toimii konsernissa, jonka konsolidoitu tilinpäätös ylittää keskisuuren toimijan raja-arvot, katsotaan NIS2-lakiluonnoksen mukaiseksi toimijaksi. Tämä lähestymistapa voi olla perusteltu suurten yritysten konserneissa, joissa jokainen harjoittaa ja johtaa tiettyä NIS2-piiriin kuuluvaa toimintaa. Ongelmalliseksi tämä kuitenkin muodostuu tilanteissa, joissa konsernissa on useita tytäryhtiöitä, joiden tarkoitus on rajattu esimerkiksi yrityksen arvoketjun yhden osan tuottamiseen, mutta toiminta kuuluu silti NIS2-soveltamisalan piiriin. Tällaiset rajatun tarkoituksen tytäryhtiöt eivät välttämättä toimi itsenäisesti, ja päätöksentekovaltuudet on keskitetty konsernin ylemmälle tasolle.

NIS2-lakiluonnos voi johtaa tilanteeseen, jossa jokainen konsernin tytäryhtiö katsotaan itsenäiseksi toimijaksi, mikä aiheuttaisi runsaasti ilmoituksia toimijaluetteloon ja mahdollisesti myös poikkeamailmoituksia, jos poikkeama olisi konsernissa laaja-alainen. Lisäksi johdon vastuukysymykset voivat aiheuttaa epäselvyyttä tällaisissa tilanteissa.

→ **Esitämme**, että laki ottaisi tarkemmin kantaa tilanteisiin, joissa konsernin toimintaan kuuluu liitteissä I tai II määriteltyä toimintaa, ja tämä toiminta jakautuu useiden konserniyritysten välille. Tällaisessa tilanteessa olisi selkeintä, jos konsernilla olisi oikeus määrittää toimintaa tosiasiallisesti harjoittava toimija, ilmoittaa tämä toimijaluetteloon ja tehdä mahdolliset poikkeamailmoitukset tämän keskeisen toimijan kautta. Tämä ajatus on jo välillisesti kirjattu johdon vastuuta koskevan 10 §:ään ”…joissa tosiasiallisesti johdetaan sen toimintaa, toimivaa tahoa” jolloin näemme, että konsernia koskeva täsmennys olisi linjassa lain muun tekstin kanssa.

Riskienhallintavelvoitetta koskevat huomiot

<u>Vastuu toimitusketjussa</u>:

Lakiluonnoksen 9 §:n velvoittavien vaatimusten (12 kpl) osalta on ongelmana niiden epätäsmällisyys useassa kohdassa, joka voi johtaa siihen, että asioita tulkitaan ja toteutetaan eri tavoin. Tämä on huomioitava myös kilpailuoikeudellisten näkökohtien kannalta, koska pykälällä saatetaan vääristää kilpailua, kun vaatimuksia toteutetaan eri resursseilla ja kustannustasolla. Vähintäänkin valvova viranomainen tulisi velvoittaa antamaan ennen lain voimaantuloa tarkemmat minimivaatimukset 12 kohdan eri osa-alueille eri toimialoilla. Tilanne kuitenkin muuttuu jatkuvasti, joten ohjeita pitää tarkentaa määrävälein. Ei voi olla pelkästään niin, että oikeusistuin jälkikäteen määrittää, mikä on riittävä taso.

Lakiluonnoksen 9 §:ssä todetaan: ”toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt”

Direktiivin 21 artiklassa todetaan: ” toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat”

Lakiluonnos poikkeaa NIS2 direktiivin esityksestä, jossa vastuu toimittajista rajataan välittömään toimittajaketjuun. Huomioiden, että NIS2 ei sisällä mitään velvoitteita, jotka kohdistuisivat suoraan toimittajiin, on laajempi vaatimus kohtuuton, huomioiden yritysten tosiasialliset toimintamahdollisuudet kaupallisissa neuvotteluissa.

→ **Esitämme**, että lakiluonnos muutetaan direktiivin muotoon, ja lisätään sana ”välitön”.

→ Tämän lisäksi katsomme, että on tarpeen määrittää tarkemmin, mikä on toimijan toiminnan kannalta relevantti toimittaja, jonka toimitukseen NIS2 velvoitteet kohdistuisivat. Esimerkiksi toimijan toimistoympäristöön kohdistuva poikkeama ei välttämättä vaikuta merkittävästi toimijan kykyyn tuottaa liitteiden I ja II alaista toimintaa.

Poikkeamailmoitus:

Lakiluonnoksen 11 §:ssä todetaan seuraavaa ”Toimijan on ilmoitettava viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Ensi-ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta.”

Tietosuoja-asetuksen soveltamiseen perustuvan kokemuksen perusteella ”poikkeaman havaitsemisen” ymmärtäminen voi osoittautua haastavaksi. Ymmärrämme tarpeen saada ilmoitus poikkeamasta mahdollisimman nopeasti, mutta samalla on sekä toimijoiden että vastuullisten viranomaisten etu, jos ilmoituskynnys ei muodostu liian matalaksi.

Esimerkiksi Tietosuojatyöryhmä on suuntaviivoissaan (WP250rev.01, 9/2022) todennut seuraavaa:

> *Rekisterinpitäjän oma tietoisuus: ”Tietosuojatyöryhmä katsoo, että rekisterinpitäjän olisi katsottava tulleen tietoiseksi tietoturvaloukkauksesta silloin, kun sillä on **kohtuullinen varmuus** siitä, että on tapahtunut henkilötietoja vaarantava turvapoikkeama.”*
>
> *Käsittelijän ilmoittama tietoturvaloukkaus: ”Rekisterinpitäjä käyttää henkilötietojen käsittelijää omiin tarkoituksiinsa; tästä syystä rekisterinpitäjän olisi lähtökohtaisesti katsottava saaneen tietoturvaloukkauksen ”tietoonsa”, **kun henkilötietojen käsittelijä on ilmoittanut sille siitä**.”*

→ **Esitämme**, että lakiluonnokseen täsmennetään, milloin toimijan katsotaan tulleen tietoiseksi poikkeamasta:

1. ”Kohtuullinen varmuus” merkittävän poikkeaman tapahtumasta.

2. Toimija tulee tietoiseksi sen toimittajaan kohdistuneesta merkittävästi poikkeamasta lähtökohtaisesti, kun toimittaja tekee ilmoituksen toimijalle, ellei tästä ole muita selkeitä tietoja, joiden perusteella toimittaja voi saada kohtuullisen varmuuden merkittävästi poikkeamasta.

Valvontaa koskevat huomiot

Yleiset huomiot:

Lakiluonnoksessa valvonta on jaettu eri viranomaisille toimialan perusteella, mikä voi aiheuttaa tulkintaepäselvyyksiä, jos useampi viranomainen valvoo samaa toimintaa. Neuvot voivat poiketa toisistaan eri konsernin/yhteisön/yksikön osien välillä. Myös seuraamusjärjestelmän toiminta tilanteessa, jossa useampi viranomainen valvoo yrityksen/konsernin toimintaa, on epäselvä. Tämä liittyy kysymykseen siitä, miten sääntely soveltuu konserneihin ja niiden eri yhteisöihin. Vaikka ehdotuksessa on viranomaisten välistä yhteistyötä koskeva 46 §, se ei suoraan ratkaise mahdollisia tulkintahaasteita.

Johdon toiminnan rajoittaminen:

Lakiluonnoksen 33 § Johdon toiminnan rajoittaminen: ”Valvova viranomainen voi määräajaksi, enintään viideksi vuodeksi, kieltää henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä ja varajäsenenä, hallintoneuvoston jäsenenä ja varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, sekä toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä, jotka ovat keskeisen toimijan ylimpiä johtotehtäviä tai joissa tosiasiallisesti johdetaan sen toimintaa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvoitteita. ”

NIS2 direktiivi 32 artikla 5 kohta:

> *”… Jos pyydettyjä toimia ei toteuteta asetetussa määräajassa, jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet…”*
>
> *”b) **pyytää asiaankuuluvia elimiä tai tuomioistuimia kieltämään väliaikaisesti** kansallisen lainsäädännön mukaisesti ketä tahansa luonnollista henkilöä, joka hoitaa keskeisen toimijan johtotehtäviä toimitusjohtajan tai laillisen edustajan tasolla, hoitamasta kyseisen toimijan johtotehtäviä.”*
>
> *”**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. Tällaisten väliaikaisten keskeyttämisten tai kieltojen määräämiseen on sovellettava asianmukaisia menettelytakeita unionin oikeuden yleisten periaatteiden ja perusoikeuskirjan mukaisesti, mukaan lukien oikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, syyttömyysolettama ja oikeus puolustukseen.”*

Lakiluonnoksen teksti poikkeaa direktiivin tekstistä keskeytyksen tai kiellon määräaikaisuuden osalta, ts. kielto tai keskeytys voi olla voimassa vain siihen asti, että korjaavat toimenpiteet on toteutettu

→ **Esitämme**, että lakiluonnoksen kirjaus muutetaan direktiivin mukaiseen muotoon. Nykyisessä muodossaan kirjaus on kohtuuton ja sisältää tarpeettoman rangaistuselementin, jota ei ole kirjattu direktiivin tekstiin.

Johdon vastuu:

Lakiluonnoksen 10 § käsittelee johdon vastuuta Suomessa. Esitys laajentaa vastuuta toimitusjohtajan alaisiin "johtoryhmiin", mikä poikkeaa Suomen oikeusjärjestelmästä ja direktiivin sanamuodosta. Yhtiöoikeudellisesti vastuu kohdistuu osakeyhtiön toimielimiin, kuten hallitukseen ja toimitusjohtajaan. Johtoryhmille ei ole Suomessa asetettu itsenäistä vastuuta, ja **niiden mainitseminen lakiehdotuksessa tulisi poistaa.**

Lisätietoja asiassa antaa asiantuntija Tuukka Heikkilä, 040 828 1570, tuukka.heikkila@energia.fi