Metsäteollisuus ry

Lausunto

24.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Metsäteollisuus ry kiittää mahdollisuudesta lausua NIS2-direktiivistä. Hyvien kyberturvallisuuskäytänteiden kehittäminen EU:n laajuisesti nähdään yleisesti hyvänä asiana metsäteollisuudessa. NIS2-direktiivin laajempi soveltamisala lisää uusia toimialoja sääntelyn piiriin ja parantaa kyberturvan tasoa ja kyberturvatietoisuutta pitkällä aikavälillä.

Direktiivin velvoitteiden täyttäminen tuo organisaatioille hyötyä varautumisessa. Organisaatioille on erittäin tärkeää, että NIS2-velvoitteet ovat täytettävissä siten, että niiden toteuttaminen tukee aidosti toiminnan jatkuvuutta ja prosesseja, eikä varsinaiselle toiminnalle koidu kohtuutonta rasitetta.

Toimijoiden tulisi mahdollisimman hyvin pystyä itsenäisesti tunnistamaan, mikäli direktiivin velvoitteet kohdistuvat omaan toimintaan ja missä laajuudessa. GDPR:n tapauksessa suuri määrä organisaatioista ei tiennyt kuinka varautua ja miltä osin. Mikäli lakiin kyberturvallisuuden riskienhallinnasta jää epäselvyyksiä, voi tämä tarkoittaa jälleen toimijoille merkittäviä konsultointikustannuksia, kun selvitetään direktiivin sisältöä ja sen velvoitteiden toteuttamista.

Soveltamisalaa koskevat huomiot

Metsäteollisuuden toimintaa ei ole erikseen mainittu NIS2-direktiivin soveltamisalassa, mutta alan yrityksillä on toimintoja useilla NIS2-direktiivin soveltamisaloilla, joten direktiivin velvoitteet tulevat koskemaan monia metsäteollisuuden yrityksiä. Metsäteollisuuden yrityksillä on toimintaa ainakin seuraavilla NIS2-soveltamisaloilla: energia, jätevesi, kemikaalien valmistus, tuotanto ja jakelu sekä tutkimustoiminta. Metsäteollisuuden yrityksillä on myös joitain liikenteen soveltamisalassa olevia raideliikenteen ja vesiliikenteen toimintoja, jotka voivat aiheuttaa yrityksille NIS2-velvoitteita.

NIS2-velvoitteiden kohdistumista yritys- ja konsernirakenteessa tulisi selventää. Mikäli yrityksen yksikön jokin toiminto kuuluu NIS2-soveltamisalaan, kohdistuvatko NIS2-velvoitteet tällöin vain kyseisen yksikön NIS2-soveltamisalassa olevaan toimintoon, yksikön kaikkiin toimintoihin, vai koko yrityksen kaikkiin toimintoihin? Esimerkiksi: jos yhtiö omistaa yksityisraiteen, mutta varsinainen toiminta ei ole NIS2-soveltamisalassa, tuleeko yhtiölle NIS2-velvoitteet vain raideliikenteen toimintojen osalta vai koko yhtiön osalta?

NIS2-velvoitteiden kohdentumisen periaatteet konsernin sisällä vaativat myös selkiyttämistä. Tuleeko esimerkiksi konsernin emoyrityksen tai muiden konsernin yhtiöiden alkaa toteuttamaan NIS2-käytänteitä, mikäli jokin konsernin yrityksistä on NIS2-direktiivin soveltamisalassa ja siihen kohdistuu valvonta- ja raportointivelvoitteita?

Metsäteollisuus ry:n kantana voidaan todeta, että riippumatta siitä, mikä yhtiö tai osa konsernista on lain mukaan NIS2-velvoitteiden piirissä oleva oikeudellinen henkilö, tulee valvonnan ja raportoinnin kohdistua vain NIS2-soveltamisalassa olevaan toimintaan.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallinnan yksi osa-alue on toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat. Riskienhallintatoimien tulisi olla kohdennettavissa vain niihin toimitusketjun toimijoihin ja osa-alueisiin, jotka liittyvät NIS2-direktiivin soveltamisalassa olevaan toimintaan.

On hyvä asia, että hallituksen esityksessä ei edellytetä minkään standardin hankkimista NIS2-direktiivin vaatimuksien todentamiseksi. Riskienhallinnan viitekehyksen määrittämisen kannalta toimijoiden määrittelytyötä voisi kuitenkin helpottaa, jos voitaisiin todeta esimerkiksi ISO 27001-standardin mukaisten toimien kattavan NIS2-vaatimukset ilman, että toimijalta edellytetään ko. standardoinnin hankkimista.

Ehdotetun Kyberturvallisuuslain 10§:ssä on käsitelty johdon vastuuta. 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. 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.

Hallituksen esityksen sivulla 12 on todettu artiklan 21 edellyttävän, että yhteisön ”--hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen”. Ajatus osakeyhtiön hallintoelinten pakollisista

koulutusvelvoitteista on Suomen oikeudelle vieras, eikä ole tavanomaista, että esimerkiksi yhtiön hallitustyölle asetetaan operatiivisia koulutusvelvoitteita. Yleisen huolellisuusvelvoitteen perusteella yhteisöt arvioivat itsenäisesti, miten paljon mahdollista koulutusta yhteisön toimielimet mahdollisesti tarvitsevat erilaisten lakisääteisten velvoitteiden toteuttamiseksi. Sääntelyn osalta pitäisi siis pitää selkeästi erillään hallituksen valvontarooli ja toimivan johdon (toimitusjohtajan) rooli. Koulutusvelvollisuudesta on rajattu pois myös julkisyhteisön hallintoelimet (s. 45, kohta 3.16.4). Samaa lähestymistapaa tulisi soveltaa myös yhteisöihin.

Raportointivelvoitetta koskevat huomiot

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 metsäteollisuusyrityksillä on yksiköitä EU:n alueella sekä kolmansissa maissa.

Valvontaa koskevat huomiot

Ehdotuksen 33§:ssä olevien toimintakieltojen soveltamisala on hyvin laaja ja aiheuttaa tulkintaepäselvyyttä siitä huolimatta, että soveltaminen on rajoitettu ”keskeisin toimijoihin”. Pykälästä tulisi poistaa viittaukset toimitusjohtajan alaisuudessa toimiviin henkilöihin (”johtoryhmään”) edellä mainituin perustein. Lisäksi viranomaisvalvonnan jakautuminen useille valvoville viranomaisille voi aiheuttaa epävarmuutta seuraamusjärjestelmän ennakoitavuudesta osakeyhtiön johdossa toimiville.

Seuraamusmaksua koskevat huomiot

Seuraamusmaksun suuruutta määriteltäessä tulisi pystyä huomioimaan se, miltä osin toimijan toiminta kuuluu NIS2-direktiivin soveltamisalaan. Seuraamusmaksua tulisi voida kohtuullistaa NIS2-soveltamisalassa olevan toiminnan laajuus huomioiden.

Yleisesti voidaan todeta, että GDPR:ssä ja NIS2-direktiivissä seuraamusmaksujen enimmäismäärän suuruus vaikuttaa ylimitoitetulta ja epärealistiselta. Seuraamusmaksujen tavoite on toki selvä: luodaan iso riskikuva, mikä pakottaa toimimaan direktiivin mukaisesti. Seuraamusmaksuja määrittäessä tulee kuitenkin kysyä, voidaanko pahimmillaan jopa vaarantaa kriittisen organisaation tulevaisuus ylisuurilla sanktioilla.

CSIRT-yksikön tehtäviä koskevat huomiot

ei lausuttavaa

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

ei lausuttavaa

Verkkotunnusvälittäjiä koskevat huomiot

ei lausuttavaa

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

ei lausuttavaa

Vaikutustenarviointia koskevat huomiot

Metsäteollisuus ry:n kantana voidaan todeta, että olisi toivottavaa kohdentaa NIS2-velvoitteet lähtökohtaisesti vain niihin yksiköihin ja toimintoihin, joissa on direktiivin soveltamisalaan kuuluvaa toimintaa. Toimija voisi edelleen huomioida halutessaan kaikki yksiköt ja toiminnot NIS2-direktiivin riskienhallinta- ja raportointivelvoitteiden mukaisesti, mutta yritykselle jäisi enemmän mahdollisuuksia linjata siitä, mitkä toiminnot ovat olennaisia NIS2-direktiivin soveltamisalaan kuuluvan toiminnan osalta.

Muut huomiot ja avoin palaute esityksestä

ei lausuttavaa

Anttonen Olli
Metsäteollisuus ry