

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Listayhtiöiden neuvottelukunta ("LYNK") katsoo, että luonnoksessa hallituksen esitykseksi NIS2-direktiivin implementoimiseksi on huomattavan paljon täydennettävää, ennen kuin lakiluonnos voisi toimia käytännössä yhtiöiden kannalta.

Nostamme tässä lausunnossamme eräitä keskeisimpiä seikkoja esiin, joihin jatkovalmistelussa tulisi kiinnittää huomiota.

Soveltamisalaa koskevat huomiot

Säätelyn soveltamisala laajentuu kattamaan huomattavaa osaa suomalaisista yhtiöstä. NIS2-velvoitteiden kohdistumista yritys- ja konsernirakenteessa tulisi selkeyttää.

Epäselvää on esimerkiksi se, jos yrityksen yksikön jokin toiminto kuuluu NIS2-soveltamisalaan, kohdistuvatko NIS2-velvoitteet vain kyseisen yksikön NIS2-soveltamisalassa olevaan toimintoon, yksikön kaikkiin toimintoihin vai koko yrityksen kaikkiin toimintoihin.

Myös NIS2-velvoitteiden kohdentumisen periaatteet konsernin sisällä vaativat selkeyttämistä. Epäselvää on esimerkiksi se, tuleeko konsernin emoyhtiön ja/tai kaikkien konsernin tytäryhteisöjen toteuttaa NIS2:n mukaisia velvoitteita, mikäli jokin konserniin kuuluva tytäryhtiö (tai osa siitä) harjoittaa soveltamisalan piiriin kuuluvaa toimintaa.

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.

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta (KyberturvallisuusL) valvonta on jaettu eri viranomaisille sen mukaan, mistä toimialasta on kyse. Useat yritykset ja/tai konsernit harjoittavat toimintaa, joka saattaa tulla valvonnan kohteeksi usean viranomaisen toimesta. Tällöin vaarana on valvonnan päällekkäisyydestä aiheutuvat tulkintaepäselvyydet, jos useampi viranomainen valvoo toimintaa.

- Epäselvyyttä voi aiheuttaa esimerkiksi tilanne, jossa viranomaisten antamat neuvot eroavat saman konsernin/yhteisön/yksikön eri osille.
- Seuraamusjärjestelmän osalta on myös epäselvää, miten seuraamuksia määrätään tilanteessa, jossa yrityksen/konsernin toimintaa valvoo useampi viranomainen.
- Tämä epäselvyys liittyy läheisesti edellä esiin nostettuun epäselvyyteen siitä, miten sääntelyn katsotaan soveltuvan konserneihin ja niissä oleviin eri toimintaa harjoittaviin yhteisöihin. Toki ehdotuksessa on mukana 46§ koskien viranomaisten välistä yhteistyötä, mutta se ei suoraa tuota ratkaisua yllä mainittuihin mahdollisiin tulkintahaasteisiin.

Seuraamusmaksua koskevat huomiot

Edellä käsitelty tulkintaepäselvyys siitä, koskeeko ”toimijan” käsite toimintaa harjoittavaa yhteisöä vai yhteisön koko konsernia vaikuttaa myös seuraamusjärjestelmään. Ehdotuksessa seuraamusmaksu on sidottu ”toimijan” maailmanlaajuiseen liikevaihtoon, jolloin seuraamusmaksun suuruus voi yhtiörakenteesta riippuen vaihdella merkittävästi, mikäli ”toimijaksi” tulkitaan koko konserni tai toisaalta esimerkiksi yksittäinen tytäryhtiö.

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. Ehdotusta tulisi selventää siltä osin, miten menetellään sellaisessa tilanteessa, jossa yhteisöä valvoo useita toimivaltaisi viranomaisia yhteisön monialaisen toimialan seurauksena.

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ehdotetun KyberturvallisuusL:n 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.

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

Lisäksi 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.

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 kieltä 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 keskeyttämisistä 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 kieltä on näin tarkoitettu alun perin painostuskeinoksi, ei rangaistukseksi. Jostain 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.

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Suominen Santeri
Elinkeinoelämän keskusliitto EK - Listayhtiöiden neuvottelukunta