Burger-In Oy

Lausunto

10.11.2023

Asia: VN/18157/2023

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

## Lausunnonantajan lausunto

### Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

EU:n uuden Kyberturvallisuusdirektiivin (NIS2-direktiivi) tavoite EU:n yhteisen sekä jäsenvaltioiden kansallisen kyberturvallisuuden tason vahvistamiseksi kriittisten sektoreiden ja toimijoiden osalta on yhteiskunnan toimivuuden kannalta erittäin tärkeä. On elintärkeää varmistaa yhteiskunnalle kriittisten sektorien toimintavarmuus ja jatkuvuus myös mahdollisen kyberhyökkäyksen sattuessa.

### Soveltamisalaa koskevat huomiot

NIS2-direktiivissä soveltamisala on laajempi kuin NIS1:ssä, ja soveltamisalaan kuuluviin toimijoihin on lisätty kriittisten toimijoiden lisäksi tärkeät toimijat, ja uusina sektoreina jälkimmäisiin liittyen mm. elintarvikkeiden tuotanto, jalostus ja jakelu. Soveltamisalaan kuuluu määritellyillä sektoreilla toimivat, kokoluokaltaan keskisuuret ja suuret yritykset. On huomattava, että keskisuuren yrityksen raja-arvot – 50 työntekijää ja liikevaihto yli 10 miljoonaa euroa – ylittyvät hyvin laajassa joukossa erilaisia Suomeen sijoittautuneita elintarvikesektorin yrityksiä.

Esitämme kohteliaimmin kantanamme, että kansallisen liikkumavaran salliessa, NIS2-direktiivin soveltamisalaan uutena toimialana lisätty elintarvikkeiden tuotanto, jalostus ja jakelu määriteltäisiin kansallisessa laissa tarkkarajaisemmin. Direktiivin soveltamisala liitteen II kohdan 4 mukaisen määritelmän*) mukaisena laajentaisi direktiivin velvoitteineen koskemaan hyvin isoa joukkoa keskisuuria ja isoja elintarvikkeiden tuotantoa, jalostusta tai jakelua harjoittavia yrityksiä:

*) Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 178/2000 3 artiklan alakohdassa määritellään elintarvikeyritykset, jotka harjoittavat tukkukappaa sekä teollista tuotantoa ja jalostusta hyvin laajasti:

Food business means any undertaking, whether for profit or not and whether public or private, carrying out any of the activities related to any stage of production, processing and distribution of food.

Direktiivin tavoitteet huomioon ottaen, lain soveltamisalasta tulisi rajata pois sellaiset keskisuuret tai isot yritykset, joiden mahdollisesti kohtaamien kyberturvallisuusriskien yhteiskunnalliset vaikutukset jäävät marginaalisiksi. Tällaisia yrityksiä ovat esim. toimijat, joiden osalta teollinen elintarviketuotanto ja tukkukauppa kohdistuu lähinnä oman liiketoiminnan piiriin kuuluviin yrityksiin. Esimerkiksi Hes-Pro Finland Oy:n, joka kokoluokaltaan kuuluu direktiivin soveltamisalaan, tuotanto ja tukkukauppa palvelee vain Hesburger-ketjun toimipaikkoja. Elintarvikkeita jakelevien yritysten osalta soveltamisalaan tulisi kuulua vain sellaiset, joiden toiminta kattaa esimerkiksi yli 0,5 % kansallisesta ruuantuotannosta. Ts. lain soveltamisalan piiriin tulisi lukea vain sellaiset yritykset, joihin kohdistuva kyberhyökkäys muodostaisi kriittisen uhan kansalliselle elintarviketuotannolle.

NIS2-direktiivin 3 artikla velvoittaa jäsenvaltiot laatimaan luettelon keskeisistä ja tärkeistä (sekä verkkotunnusten rekisteröintipalveluja tarjoavista) toimijoista. Tämän kansallisen velvoitteen myötä kansallisella lainsäätäjällä lienee liikkumavaraa myös tärkeiden toimijoiden määrittelyssä laissa.

**Riskienhallintavelvoitetta koskevat huomiot**

Kyberturvallisuuden riskienhallinnasta annetun lain mukaisia velvoitteita sovellettaisiin direktiivin tämänhetkisen soveltamisalan mukaisesti myös elintarvikesektorilla. Liikenne- ja viestintäministeriö tilasi keväällä 2023 Insta Groupilta vaikutustenarvioinnin, jonka tavoitteena oli arvioida elintarvike- ja valmistussektorille aiheutuvia kuluja NIS2-direktiivin 21 artiklassa olevien hallintatoimenpiteisiin liittyvien velvoitteiden täyttämiseksi. Selvityksen perusteella riskienhallintavelvoitteet yrityksen koko toimitusketjun turvallisuutta koskevine velvoitteine tulisivat aiheuttamaan merkittäviä kustannuksia elintarvike- ja valmistussektorin yrityksille, sekä kertaluontoisesti että vuosittain jatkuvaluonteisesti.

Yritysten tulee luonnollisesti pyrkiä noudattamaan NIS2-direktiivin listaamia, sinänsä aiheellisia tietoturvavaatimuksia ilman velvoittavaa lakiakin, mutta sanktiouhkaisia vaatimuksia ei tulisi kohdistaa toimijoihin, jotka eivät ole tosiasiallisesti kriittisiä esim. elintarviketuotannon kannalta.

**Raportointivelvoitetta koskevat huomiot**

NIS2-direktiivin mukaan sekä keskeisten että tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle. Poikkeama katsotaan merkittäväksi, jos se on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita tai jos poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai

aineetonta vahinkoa. Erityisesti pelkästään asianomaiselle toimijalle aiheutuneiden taloudellisten tappioiden johdosta tehtävä raportointi on omiaan aiheuttamaan tulkintaepäselvyyksiä.

**Valvontaa koskevat huomiot**

Riippumatta soveltamisalaa koskevista huomioista, on hyvä, että direktiivissä tärkeiden toimijoiden osalta sovelletaan kevyempää valvontajärjestelmää, johon kuuluu vain jälkikäteisvalvonta. Tämä osaltaan keventää soveltamisalaan jäävien tärkeiden toimijoiden byrokraattista hallintotaakkaa.

**Seuraamusmaksua koskevat huomiot**

Seuraamusmaksut ovat hyvin korkeita, ja sanktiouhkaisia vaatimuksia ei tulisi kohdistaa toimijoihin, jotka eivät ole tosiasiallisesti kriittisiä esim. elintarviketuotannon tai -jakelun kannalta.

**CSIRT-yksikön tehtäviä koskevat huomiot**

ei kommentteja

**Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot**

ei kommentteja

**Verkkotunnusvälittäjiä koskevat huomiot**

ei kommentteja

**Kumottavaksi ehdotettuja säännöksiä koskevat huomiot**

ei kommentteja

**Vaikutustenarviointia koskevat huomiot**

ei kommentteja

**Muut huomiot ja avoin palaute esityksestä**

Pidämme lakiuudistusta tarpeellisena ja tärkeänä. Kyberturvallisuustason parantaminen ja varmistaminen on yrityksille välttämätöntä ja sillä on myös positiivisia liiketaloudellisia vaikutuksia. Huolto- tai kybervarmuuteen liittyvän sääntelyn ja valvontamenettelyn pitäisi kuitenkin kohdistua vain yhteiskunnallisesti merkityksellisiin yrityksiin, kuten olemme lausunnossamme tuoneet esiin.

Lummevuo Anne-Mari
Burger-In Oy - ja Hes-Pro Finland Oy