Suomen Kiertovoima ry

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

Suomen Kiertovoima ry KIVO edustaa kuntien jätelaitoksia, jotka vastaavat jätelaissa kuntien vastuulle säädetyn jätehuollon järjestämisestä. Jäsenlaitoksemme toteuttavat asukkaiden jätehuollon kustannustehokkaasti ja vastuullisesti yhteistyössä yksityisten yritysten ja tuottajayhteisöjen kanssa. Edistämme kiertotaloutta turvallisesti ja terveellisesti.

Soveltamisalaa koskevat huomiot

KIVO pitää hyvänä muutoksena sitä, että NIS2-direktiivissä jätehuolto on lisätty direktiivin soveltamisalaan. KIVO katsoo toimivan jätehuollon olevan sekä kansalaisten että yritystoiminnan kannalta kriittinen ympäristö- ja terveysturvallisuuden mahdollistaja ja ylläpitäjä. Kaikki kriittinen infrastruktuuri tulee olla lain soveltamisalassa tunnistettu, kuin myös toimialojen välillä vallitsevat vahvat sidonnaisuudet (kuten jätevesi ja jätehuolto).

Soveltamisalassa tulisi runkotekstissä määritellä tarkemmin, milloin toimijan liiketoiminta on kynnysarvot ylittävää. Tilanteisiin, joissa toimijan liikevaihto pyörii kynnysarvojen rajamailla, tulisi laissa olla selkeät tulkintasäännöt, jotka mahdollistavat toiminnan suunnittelun pitkäjänteisesti – esim. niin, että kynnysarvo laskettaisiin kolmen edellisen toimintavuoden keskiarvosta. Olisi ongelmallista, mikäli toimijan sisältyminen lain soveltamisalaan vaihtelisi vuosittain.

Liikenne- ja viestintäministeriön tulisi runkotekstiin määritellä laissa tarkoitetut toimijat selkeästi. Liitteisiin ja niihin ohjaaviin viitteisiin perustuva lainsäädäntötekniikka tekee kokonaisuudesta haastavan sen piiriin kuuluville toimijoille ja tekee sen tulkinnasta vaikeampaa. Eri toimijoiden määritelmät (erityinen toimija, tärkeä toimija, kriittinen toimija, keskustason toimija) tulisi selkeästi

määritellä runkotekstissä esimerkiksi kohdassa määritelmät. Nykymuodossaan esityksen luettavuus on toimijan näkökulmasta huono, ja sen keskeisten vaatimusten ymmärtäminen vaatii niin lain, liitteiden ja direktiivin tuntemusta.

KIVO katsoo, että on välttämätöntä että lain toimeenpanossa varmistetaan riittävä ohjeistus ja tiedotus sen piiriin kuuluville toimijoille. KIVO näkee, että monelle toimijalle tulee tulemaan yllätyksenä, että ne jatkossa ovat NIS-sääntelyn piirissä. Kuten esityksen vaikutusarvioinnissakin huomioidaan, soveltamisalaan kuulumisesta muun muuassa seuraa noin 20 % lisäkustannus IT-kuluihin. On kriittistä, että ennen siirtymäajan päättymistä mm. toimijaluetteloon ilmoittautumisen osalta kentän toimijoita tiedotetaan laajasti lakimuutoksesta, etenkin koska velvoitteiden laiminlyönti on säädetty rangaistavaksi.

Jätehuollon valvojana toimii ESA-ELY. KIVO näkee, että on tärkeää kasvattaa ESA-ELY:n asiantuntemusta ja resursseja riittävän koulutuksen järjestämiseksi. Kyberhyökkäykset sekä -rikollisuus kehittyvät koko ajan. Kansallisen koulutuksen on oltava riittävän tasoista ja ajanmukaista. Lisäksi KIVO korostaa, että ehdotus muodostaa toimijoiden näkökulmasta monimutkaisen kokonaisuuden, ja ilman koulutusta sen vaatimusten täyttäminen tulee olemaan niille vaikeaa.

Riskienhallintavelvoitetta koskevat huomiot

KIVO nostaa esiin, että riskienhallintatoimenpiteiden kohdalla vaikuttaa ainakin alkuun, ennen tulkintakäytännön muodostumista, hyvin subjektiiviselta se, mitkä ovat riittäviä riskinhallintatoimenpiteitä (7 §). KIVO toivoo, että täytäntöönpanon aikana varmistetaan riittävä dialogi kentän toimijoiden ja valvovan viranomaisen välillä, jotta toimenpiteistä muodostuisi mahdollisimman tarkoituksenmukaiset ja ymmärrettävät.

KIVO huomauttaa, että poikkeamien tunnistamista koskevat aikamääreet ovat käytännössä haastavia. Esimerkiksi se, onko jokin poikkeama merkittävä, voi olla vaikeaa tunnistaa välittömästi. Toisin sanoen, toimija voi tunnistaa poikkeaman hyvinkin nopeasti, mutta sen vaikutusten arviointi ja täten se, onko toimijalla ilmoitusvelvollisuus poikkeamasta, voi vaatia merkittävästi enemmän aikaa. Tulisikin varmistaa, että toimijat eivät voisi joutua sanktioiden piiriin ”viivyttelyn” vuoksi tämänkaltaisissa tapauksissa. Tämä on tärkeää siitäkin näkökulmasta, että muutoin toimijoilla on intressi ilmoittaa mahdolliset vähäisetkin poikkeamat ”varmuuden vuoksi”, lisäten valvovien viranomaisten hallinnollista taakkaa.

Raportointivelvoitetta koskevat huomiot

KIVO katsoo, että loppuraportin ja ylipäätään raportoinnin osalta tulisi selkeästi tekstiin ilmaista, että raportoinnin sekä poikkeamailmoitukset voi tehdä yrityksen tai toimijan kilpailuttama palveluntuottaja tai palkkaama ulkopuolinen IT-konsultti. Usein vakavissa tietoturva-, tai kyberhyökkäyksissä tutkinnan suorittaa ulkopuolinen taho, jolla on yrityksen tai toimijan henkilöstöä huomattavasti parempi asiantuntemus ja kyky arvioida poikkeamaa sekä sen vaikutuksia lyhyellä ja pitkällä aikavälillä. Käytännössä yrityksiltä tai toimijoilta saattaa puuttua henkilöstö IT-palveluista täysin tai osaaminen alasta on hyvin vähäistä (ulkoistetut palvelut).

Valvontaa koskevat huomiot

Kohdassa: Koordinoitu haavoittuvuuden julkistaminen ja haavoittuvuustietokanta – mahdollisuus ilmoittaa haavoittuvuudesta nimettömästi voi aiheuttaa joissain tilanteissa haasteita. Nimetön ilmianto mahdollistaa myös väärinkäytön.

Lisäksi lain 21 § toimeenpanossa voi olla hyvä pohtia, voisiko CSIRT-yksikölle tehtävien ilmoitusten kanavia yhdistää ilmoittajansuojalainsäädännössä tarkoitettuihin kanaviin.

Seuraamusmaksua koskevat huomiot

KIVO huomauttaa, että ehdotetut seuraamusmaksut ovat Suomen mittakaavassa suuria.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei huomioita.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei huomioita. Verkko- ja tietojärjestelmiä koskevissa kohdissa olisi hyvä mainita erikseen tai sivulauseessa pilvipalvelut.

Verkkotunnusvälittäjiä koskevat huomiot

Ei huomioita. Hyvä kuitenkin ymmärtää, että verkkotunnuksien määrää kasvatettiin hiljattain, ja uusien tunnusten osalta on huomattu väärinkäyttömahdollisuuksia samankaltaisten osoitteiden luomismahdollisuuden myötä.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei huomioita.

Vaikutustenarviointia koskevat huomiot

KIVO tiedustelee, onko NIS2-direktiivissä erikseen todettu, että toimijoilla on velvollisuus tunnistaa, kuuluvatko ne lainsäädännön soveltamisalaan, kuten nyt ehdotuksessa kansallisesta toimeenpanosta Suomessa. Mikäli ei, KIVO katsoo, että ratkaisua tulisi pohtia uudelleen, sillä se siirtää hallinnollisen taakan viranomaisilta kentän toimijoille. Tämä voi muodostua kohtuuttomaksi ottaen huomioon sen, että sääntelyn rikkomuksista on määrätty merkittäviä sanktioita.

Lisäksi KIVO katsoo, että lainsäädäntöuudistus edellyttää myös lisäpanostuksia kyberturvallisuuden koulutukseen, lähtien jo opetussuunnitelmien tasolta. Kyberturvallisuusosaajista on ollut vajetta jo ennen direktiivin toimeenpanoa.

Muut huomiot ja avoin palaute esityksestä

Jätehuollon toimijoiden määrittelyä tulisi tarkentaa. KIVO katsoo, että lain toimeenpanossa ja mieluiten vielä lainsäädäntövaiheessa on selkeytettävä keskeisten, tärkeiden ja kriittisten toimijoiden määritelmää sen osalta, miten ne ovat lainsäädännössä ilmaistu. Esimerkiksi kunnallisten jätelaitosten osalta tulkinnat ja rajanvedot ovat haastavia, johtuen lausunnossamme aiemmin mainitusta liitteisiin ja viittauksiin perustuvasta lainsäädäntötekniikasta. Vähintääkin määritelmien tulkinnasta olisi laadittava selkeyttävä opas.

Lisäksi KIVO nostaa esiin mahdolliset päällekkäisyysvalvontatilanteet sellaisten toimijoiden kohdalla, jotka harjoittavat jätehuollon lisäksi muita lain soveltamisalaan kuuluvia toimintoja. Tästä yksi esimerkki on HSY, joka toimii vesihuollossa, jätehuollossa ja energiantuotannossa saman toimijan sisällä.

Kallus Taina
Suomen Kiertovoima ry