Suomen Vesilaitosyhdistys ry

Lausunto

29.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Vesilaitosyhdistys pitää perusteltuna, että NIS2-direktiivi toimeenpannaan kansallisesti direktiivin edellyttämän vähimmäistason mukaan. Direktiivin edellyttämä taso tarkentaa merkittävästi lainsäädännön vaatimuksia direktiivin soveltamisalaan kuuluvien vesihuoltolaitosten kyberturvallisuuden riskienhallinnasta ja toteuttaa direktiivin tavoitteen kyberturvallisuuden tason varmistamisesta.

Soveltamisalaa koskevat huomiot

Vesilaitosyhdistys kannattaa NIS2-direktiivin vaatimusten mukaista esitystä lain soveltamisesta toimijoihin. Vesihuollon osalta esitetyn mukaisia keskisuuren toimijan määrittelyn vesihuoltotoiminnan osalta täyttäviä vesihuoltolaitoksia on arviomme mukaan Suomessa noin 22. Tämän lisäksi olemme tunnistaneet 4 vesihuoltolaitosta, jotka ylittävät kokorajan monialayhtiön koko toiminnan osalta. Nämä vesihuoltolaitokset vastaavat noin 60 % Suomen järjestettyjen vesihuoltopalveluiden piirissä olevista asukkaista, eli kattaa suurimman joukon suomalaisista.

Kyberturvallisuuden riskienhallintalain soveltamisalaan kuuluvat lain 3 §:n ja 2 §:n 10) kohdan perusteella kokonsa puolesta vesihuoltolaitokset, jotka täyttävät tai ylittävät komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Viittaus komission suositukseen mahdollistaa joustavuuden kokomäärittelyn pysymiseksi ajan tasalla. Mielestämme lain soveltamisalaan kuuluvien ja mukaan valvottavien toimijoiden kokorajat olisi syytä esittää selvästi konkreettisina lukuina lain perusteluissa tai ainakin lain soveltamisen tueksi annettavissa ohjeissa.

Esitetyn lain kyberturvallisuuden riskienhallinnasta 2 §:n keskisuuren toimijan määrittelevän 10 kohdan perusteluissa todetaan, että mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on lain soveltamisalan mukaista toimintaa, kokorajoitusta arvioidaan toimijan

kokonaistoiminnan perusteella. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Mielestämme tämä linjaus ei ole perusteltu ja asettaa kohtuuttomia ja epätasa-arvoisia vaatimuksia sellaisille toimijoille, jotka eivät muuten kuuluisi lain soveltamisalaan. Tämä linjaus toisi myös hyvin pieniä, osana kuntaorganisaatiota toimivia vesihuoltolaitoksia ja lähes kaikki kunnat lain soveltamisalan piiriin, mikä ei ymmärtääksemme ole ollut lain tavoitteena. Kokorajoitusta tulisi arvioida vain lain soveltamisalan mukaisen toiminnan osalta.

Riskienhallintavelvoitetta koskevat huomiot

Esitetyn lain kyberturvallisuuden riskienhallinnasta pykälissä 7-9 olevat kyberturvallisuuden riskienhallintavelvoite, riskienhallinnan toimintamalli ja riskienhallinnan toimenpiteet vastaavat nähdäksemme hyvin NIS2-direktiivin vaatimuksia. Vaatimukset sisältävät tärkeitä kyberturvallisuuden riskienhallinnan ulottuvuuksia ja toimenpiteitä, joiden toteutus on tehtävä oikeasuhtaisesti suhteessa riskeihin ja toimintaan. Mielestämme 8 § Kyberturvallisuuden riskienhallinnan toimintamallin olisi hyvä noudattaa riskienhallinnan yleistä ja standardoitua konseptia, johon kuuluu vaarojen tunnistus, riskinarviointi ja riskienhallinta. Nyt esitetystä kuvauksesta puuttuu selkeä viittaus riskinarviointiin, mikä on tärkeä vaihe oikeasuhtaisten ja riittävien riskienhallintatoimenpiteiden määrittelemiseksi ja puutteellisesti hallittujen riskien tunnistamiseksi.

8 § perusteluissa todetaan, että toimija voisi luoda kyberturvallisuuden riskienhallinnan toimintamallin itse tai hankkia sen ulkoistetusti ja, että kyberturvallisuuden riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista. Pidämme esitettyä lähestymistapaa tärkeänä, jotta kukin toimija voi täyttää lainsäädännän velvoitteet omaan toimintaansa parhaiten soveltuvalla tavalla ja mahdollisesti jo olemassa olevia käytäntöjä hyödyntäen ja täydentäen.

9 § esitetyissä riskienhallinnan toimenpiteissä edellytetään kyberturvallisuuskoulutuksia ja 10 §:n johdon vastuussa riittävää perehtyneisyyttä. Näiden velvoitteiden täyttämisen tueksi pidämme tärkeänä, että lain soveltamisalaan kuuluville toimijoille järjestetään jatkossa yleistä kyberturvallisuuden riskienhallinnan koulutusta.

Lakiesityksessä ei ole siirtymäaikaa riskienhallinnan velvoitteiden osalta. Harvalla vesihuoltolaitoksella on tällä hetkellä käytössä systemaattinen toimintamalli kyberturvallisuuden riskienhallintaan eikä tämän toteuttamiseen ole myöskään tarjolla konkreettista työkalua. Tämä tarkoittaa, että kyberturvallisuuden riskienhallinnan toimintamallia täytyy tyypillisesti alkaa rakentaa alusta, vaikka kyberturvallisuuden riskienhallintatoimenpiteitä laitoksilla onkin jo käytössä. Vesihuoltolaitoksilla on kokemusta systemaattisesta talousveden laaturiskien ja viemäröinnin ja jätevedenpuhdistuksen terveys- ja ympäristöriskien hallinnasta verkkopohjaisilla WSP- ja SSP-työkaluilla. Kokemuksen mukaan huolellinen vaarojen tunnistus, riskinarviointi ja riskienhallintatoimien määrittely on laitostasolla kuukausien prosessi valmista työkalua

hyödyntäenkin. Haluammekin tuoda esiin, että esitetyn lain vaatimusten mukaiseen toimintaan pääsemiselle tulee antaa riittävä aika ja tunnistaa myös se, että riskienhallinta on jatkuva ja kehittyvä prosessi, joka ei tule koskaan valmiiksi. On myös syytä tunnistaa kansallisesti ja vesihuoltoalalla olevan kyberturvallisuuden asiantuntijapulan asettamat haasteen toimeenpanolle.

Raportointivelvoitetta koskevat huomiot

Poikkeamailmoitusten tekemisen velvoitteet tarkentuvat nykyisestä sekä ilmoitusten sisällön että niiden kolmiportaisuuden osalta. On tärkeää, että ilmoitusten tekemiseen on käytettävissä sähköinen ja helppo kanava. Ilmoituslomakkeen pitää ohjata toimittamaan kaikki vaadittava tieto ja tarjota myös mahdollisuus pyytää viranomaiselta ohjeita ja neuvoja tilanteen hoitamiseen. Poikkeamailmoitusjärjestelmän tulisi myös muistuttaa ensi-ilmoituksen tehnyttä toimijaa jatko-, väli- ja loppuraporttien toimittamisesta.

Poikkeamailmoituksista Euroopan unionin kyberturvallisuusvirasto ENISA:lle ja muiden jäsenvaltioiden keskitetyille yhteyspisteille luovutettavat tiedot on pidettävä tasolla, joka mahdollistaa tarpeellisten tietojen välityksen, mutta ei sisällä sellaista tietoa, joka voi muodostaa joissain tilanteessa toimijan toiminnalle turvallisuusuhkan.

Valvontaa koskevat huomiot

Vesilaitosyhdistys pitää hyvänä, että vesihuoltolaitosten osalta valvovana viranomaisena on Etelä-Savon ELY-keskus, jolla on vastuu myös vesihuoltolain mukaisesta vesihuoltolaitosten valvonnasta. Pidämme myös hyvänä, että useammalla toimialalla toimivien toimijoiden kohdalla kutakin toimintaa valvoo kyseisen alan asiantuntijaviranomainen. Valvovalla viranomaisella pitää olla riittävä asiantuntemus sekä vesihuollosta että kyberturvallisuuden riskienhallinnasta. Valvoville viranomaisille ja valvonnan apuna mahdollisesti käytettäville asiantuntijoille pitää tehdä turvallisuusselvitykset ja valvontaa suorittavien pitää todistaa valvonnan kohteille henkilöllisyytensä. Valvoville viranomaisille valvonnan yhteydessä kertyvät tiedot valvonnan kohteesta pitää säilyttää tavalla, joka ei vaarannan toimijan toiminnan turvallisuutta.

Seuraamusmaksua koskevat huomiot

NIS2-direktiivi mahdollistaa kansallisen liikkumavaran siten, ettei julkishallinnon toimijoille määrätä direktiivin edellyttämiä hallinnollisia sanktioita. Tämä liikkumavara on nyt käytetty ehdotetun lain 37 §:n 2. momentissa. Pyydämme tarkentamaan laissa ja sen perusteluissa sovelletaanko seuraamusmaksua kuntien taseyksikköinä, liikelaitoksina tai osakeyhtiöinä toimiviin toimijoihin.

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Laki kyberturvallisuuden riskienhallinnasta täsmentää merkittävästi vesihuoltolaitosten velvoitteita kyberturvallisuuden riskienhallintaan ja aiheuttaa siten lisäkustannuksia, vaikka juomaveden toimitus on ollut myös NIS-direktiivin soveltamisalan piirissä. Arvioimme, että vesihuoltolaitoksilla lainsäädännön velvoitteiden täyttämiseen tarvittava henkilötyö ja aiheutuvat kustannukset ovat vähintään samalla tasolla, kuin vaikutustenarvioinnissa esitetyt vaikutukset elintarvikesektorin toimijoilla.

Muut huomiot ja avoin palaute esityksestä

Lain soveltamisalaan kuuluvien toimijoiden pitää ilmoittautua ja ilmoittaa tietonsa valvovalle viranomaiselle toimijaluettelon ylläpitämiseksi 1.1.2025. Tämä edellyttää selkeää ja tehokasta viestintää vesihuoltolaitoksille lain soveltamisalaan kuuluvien toimijoiden kriteereistä, toimialan soveltamisalaan kuulumisesta ja ilmoittamisvelvoitteesta. Lisäksi on pidettävä huoli, että keskisuuren toimijan kokokriteerin jatkossa ylittävät vesihuoltolaitokset ovat tietoisia tulemisestaan lain soveltamisalan piiriin ja siihen liittyvistä velvoitteistaan. Velvollisuus ilmoittaa valvovalle viranomaiselle kahden viikon kuluessa toimijaluettelon tietojen muutoksista tuntuu kohtuuttomalta. Mahdollisuuksien mukaan olisi varmistettava kyseisten tietojen siirtyminen automaattisesti eri järjestelmistä toimijaluetteloon.

Liikanen Riina
Suomen Vesilaitosyhdistys ry