Lausunto
Asianumero: VN/18157/2023
Päivämäärä: 4.9.2024

Hallintovaliokunta

Liikenne- ja viestintäministeriön lausunto hallintovaliokunnalle

Hallintovaliokunta on pyytänyt liikenne- ja viestintäministeriöltä asiantuntijalausuntoa hallituksen esityksestä eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp).

Liikenne- ja viestintäministeriö kiittää lausuntopyynnöstä ja esittää kunnioittavasti lausuntonaan seuraavaa.

Esityksen valmistelu ja tavoite

Esityksen valmisteluun on johtanut EU:n uusi kyberturvallisuusdirektiivi eli Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi). Direktiivi on tullut voimaan 16.1.2023. Direktiivi edellyttää jäsenvaltioita saattamaan sitä täytäntöönpanevat säännökset osaksi kansallista lainsäädäntöä 17.10.2024 mennessä sekä soveltamaan niitä viimeistään 18.10.2024 alkaen.

Liikenne- ja viestintäministeriö asetti tammikuussa 2023 säädöshankkeen valmistelemaan direktiivin kansallisen toimeenpanon edellyttämiä lainsäädäntömuutoksia. Hallituksen esityksessä esitetään lainsäädäntömuutoksia, jotka ovat tämän valmistelutyön tulos.

Esityksen valmistelua on tukenut liikenne- ja viestintäministeriön puheenjohtama työryhmä, jossa olivat edustettuina oikeusministeriö, valtiovarainministeriö, ympäristöministeriö, maa- ja metsätalousministeriö, työ- ja elinkeinoministeriö, sosiaali- ja terveysministeriö, sisäministeriö, puolustusministeriö sekä ulkoministeriö.

Julkishallintoon kohdistuvien velvoitteiden osalta valmistelua on tehty valtiovarainministeriön puheenjohtamassa alatyöryhmässä, jossa olivat edustettuina liikenne- ja viestintäministeriö, oikeusministeriö, työ- ja elinkeinoministeriö, ympäristöministeriö, maa- ja metsätalousministeriö, sosiaali- ja terveysministeriö, sisäministeriö, puolustusministeriö, ulkoministeriö, valtioneuvoston kanslia, opetus- ja kulttuuriministeriö, Verohallinto ja Kuntaliitto.

Esityksessä ehdotetuilla laeilla pantaisiin täytäntöön EU:n kyberturvallisuusdirektiivi. Direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisillä toimialoilla. Esityksellä edistettäisiin tätä tavoitetta. Lisäksi esityksen tavoitteena on vähentää kyberhäiriöiden määrää ja välttää kyberturvallisuuteen liittyvien poikkeamien aiheuttamia keskeytyksiä ja häiriöitä yhteiskunnan toiminnan kannalta keskeisille palveluille ja toiminnoille.

Esityksessä ehdotetaan tehtäväksi direktiivin täytäntöönpano sen vähimmäistason edellyttämällä tavalla sekä soveltamisalan ja velvoitteiden laajuuden osalta. Esityksen valmistelussa on pyritty hyödyntämään direktiivin sallimaa kansallista liikkumavaraa mahdollisimman laajasti.

Esityksen keskeinen sisältö

Esityksessä ehdotetaan säädettäväksi uusi kyberturvallisuuslaki. Laissa säädettäisiin NIS 2 -direktiivin edellyttämistä kyberturvallisuuden riskienhallintaa ja poikkeamaraportointia koskevista vähimmäisvelvoitteista direktiivin soveltamisalaan kuuluville toimijoille. Laissa säädettäisiin myös velvoitteiden valvonnasta sekä muista NIS 2 -direktiivin täytäntöönpanon edellyttämistä viranomaistehtävistä. Yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta ehdotetaan säädettäväksi kuitenkin erikseen julkisen hallinnon tiedonhallinnasta annetussa laissa.

Sähköisen viestinnän palveluista annetussa laissa ehdotetaan säädettäväksi direktiivin verkkotunnusten rekisteröintitietojen tietokantaa koskevan artiklan täytäntöönpanemiseksi tarpeellisista muutoksista. Esityksellä ehdotetaan myös tehtäväksi toimialakohtaisiin lakeihin eräitä kyberturvallisuuslain säätämiseksi tarpeellisia teknisiä muutoksia. Lisäksi toimialakohtaisista laeista ehdotetaan kumottavaksi nykyisin voimassa olevat verkko- ja tietoturvallisuusdirektiivin täytäntöönpanoa koskevat säännökset, koska mainittu direktiivi kumotaan NIS 2 -direktiivillä.

Soveltamisala

Esityksessä ehdotetaan, että kyberturvallisuuslain riskienhallinta- ja raportointivelvoitteiden soveltamisalaan kuuluisivat organisaatiot, jotka harjoittavat lain liitteessä I tai II tarkoitettua toimintaa, ja olisivat kooltaan keskisuuria tai suurempia. Keskisuurella tarkoitettaisiin komission suosituksen 2003/361/EY mukaisesti organisaatioita, joiden palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittävät 10 miljoonaa euroa. Eräissä rajatuissa poikkeustapauksissa velvoitteet koskisivat myös tätä pienempiä yrityksiä, jos yritys harjoittaa eräitä keskeisiä toimintoja digitaaliseen infrastruktuuriin liittyen tai häiriöllä olisi muusta ehdotetun kyberturvallisuuslain 3 §:ssä tarkoitetusta syystä johtuva merkittävä haitallinen vaikutus yhteiskunnalle. Soveltamisalaan kuuluvan toimijan olisi ilmoitettava valvovalle viranomaiselle oma-aloitteisesti ehdotetun kyberturvallisuuslain 41 §:ssä tarkoitetut tiedot.

NIS 2 -direktiivin soveltamisala on laajentunut edeltävän verkko- ja tietoturvadirektiivin soveltamisalaan nähden. Soveltamisalaan kuuluvat toimialat ja toimijatyypit määriteltäisiin tyhjentävästi kyberturvallisuuslain liitteissä I ja II sekä julkisen hallinnon tiedonhallinnasta annetun lain soveltamisalaa koskevissa säädöksissä. Pien- ja mikroyritykset jäisivät yllä mainituin poikkeuksin pääsääntöisesti velvoitteiden soveltamisalan ulkopuolelle toimialasta riippumatta. Julkishallinnon osalta NIS 2 -direktiivi pantaisiin täytäntöön sen vähimmäissoveltamisalan mukaisesti, eli tiedonhallintalain uusia velvoitteita sovellettaisiin direktiivin tarkoittamiin keskustason julkishallinnon toimijoihin sekä riskiperusteisesti määrättyihin aluetason toimijoihin, joita olisivat hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä. Direktiivin soveltamisalarajauksen mukaisesti ehdotusta ei sovellettaisi määriteltyihin julkishallinnon toimijoihin, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla.

Esityksessä arvioidaan, että kyberturvallisuuslain soveltamisalaan kuuluisi yhteensä kaikilla toimialoilla noin 2 500–5 000 organisaatiota. Arvioon liittyy merkittäviä epävarmuustekijöitä, joita kuvataan esityksessä. Esityksessä arvioidaan, että kyberturvallisuuslain soveltamisalaan kuuluvista toimijoista noin 10–20 % olisi kuulunut edeltävää verkko- ja tietoturvadirektiiviä täytäntöönpanevien velvoitteiden alaan. Esityksessä arvioidaan, että kyberturvallisuuslain

soveltamisalaan kuuluvista organisaatioista noin 10 % olisi NIS 2 -direktiivissä tarkoitettuja keskeisiä toimijoita, joihin valvontaa ensisijaisesti kohdennettaisiin. Tiedonhallintalain uuden 4 a luvun soveltamisalaan arvioidaan tulevan noin 160 julkishallinnon organisaatiota.

Riskienhallintavelvoite

Esityksessä ehdotetaan, että kyberturvallisuuslain soveltamisalaan kuuluva toimija velvoitettaisiin tunnistamaan, arvioimaan ja hallitsemaan riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Toimija arvioisi itse toimintaan kohdistuvia riskejä sekä määrittäisi ja dokumentoisi arviointinsa perusteella oikeasuhtaisia riskienhallintatoimenpiteitä. Laissa säädettäisiin osa-alueista, jotka arvioinnissa ja riskienhallintaa koskevissa toimenpiteissä olisi vähintään otettava huomioon. Riskienhallinnasta säädettäisiin ehdotetuissa kyberturvallisuuslain 7–10 §:ssä. Julkisen hallinnon osalta vastaavat velvoitteet sisältyisivät tiedonhallintalakiin ehdotettuihin 18 b–18 c §:ään.

Merkittävästä poikkeamasta raportointi

Esityksessä ehdotetaan, että kyberturvallisuuslain soveltamisalaan kuuluva toimija samoin kuin tiedonhallintalain uuden 4 a luvun soveltamisalaan kuuluva tiedonhallintayksikkö velvoitettaisiin ilmoittamaan kyberturvallisuuteen liittyvästä merkittävästä poikkeamasta valvovalle viranomaiselle. Ilmoitusvelvollisuus olisi kolmiportainen siten, että ensi-ilmoitus olisi tehtävä 24 tunnin kuluessa ja jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta. Poikkeaman käsittelyn päätyttyä toimijan olisi tehtävä tapahtumasta ja sen käsittelystä loppuraportti. Viranomaiselle voisi ilmoittaa vapaaehtoisesti myös muista kuin ilmoitusvelvollisuuden alaan kuuluvista poikkeamista, häiriöistä tai kyberuhkista. Toimijan olisi lisäksi ilmoitettava palvelujensa vastaanottajille merkittävästä poikkeamasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista keinoista, jos poikkeama haittaa palvelujen tarjoamista tai aiheuttaa uhkan palvelujen vastaanottajille. Jos poikkeamasta tiedottaminen olisi yleisen edun mukaista, viranomainen voisi velvoittaa toimijan tiedottamaan asiasta tai tiedottaa asiasta itse. Poikkeamasta raportoinnista säädettäisiin ehdotetuissa kyberturvallisuuslain 11–17 §:ssä ja tiedonhallintalain 18 d–18 g §:ssä.

Lausuntokierroksella saadun palautteen johdosta ehdotukseen on lisätty säännös valvovan viranomaisen velvollisuudesta ilmoittaa merkittävästä poikkeamasta poliisille, jos merkittävän poikkeaman epäillään aiheutuvan rikoksesta, josta säädetty enimmäisrangaistus olisi vähintään kolme vuotta vankeutta.

Julkishallinto

Julkisen hallinnon tiedonhallinnasta annettuun lakiin ehdotetaan säädettäväksi uusi 4 a luku, jossa säädettäisiin NIS 2 -direktiivin edellyttämistä velvoitteista direktiivin liitteen I kohdassa 10 tarkoitetuille julkishallinnon toimijoille. Toiminta julkishallinnon toimialalla ei kuuluisi kyberturvallisuuslain liitteisiin I tai II, eivätkä julkishallinnon toimialan toimijat siten sellaisenaan kuuluisi kyberturvallisuuslaissa säädettävien velvoitteiden alaan. Tiedonhallintalain soveltamisalaan kuuluva viranomainen voisi kuitenkin kuulua myös kyberturvallisuuslain soveltamisalaan, mikäli se harjoittaisi toimintaa myös kyberturvallisuuslain liitteessä tarkoitetulla toimialalla. Mikäli julkishallinnon organisaatio kuuluisi samanaikaisesti sekä tiedonhallintalain että kyberturvallisuuslain soveltamisalaan, tulisi sen noudattaa sekä tiedonhallintalain 4 a lukua että kyberturvallisuuslaissa toimijalle asetettavia velvoitteita, jotka ovat keskeiseltä osin vastaavia.

Valvonta ja seuraamukset

Esityksessä ehdotetaan, että kyberturvallisuuslaissa säädettävien velvoitteiden valvonta osoitettaisiin toimialakohtaisille viranomaisille vastaavasti kuin edeltävän verkko- ja tietoturvadirektiivin täytäntöönpanossa on tehty. Valvovia viranomaisia olisivat toimialoittain Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveydenalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus- ja kehittämiskeskus sekä Finanssivalvonta.

Riskienhallinnan asianmukaisuuden valvonta edellyttää asiantuntemusta toimialan erityispiirteistä ja muusta samaan toimintaan kohdistuvasta sääntelystä, johon toimialakohtaisella viranomaisella on paras asiantuntemus. Lisäksi osa viranomaisista valvoo jo ennestään verkko- ja tietoturvadirektiivin tai toimialakohtaisen sääntelyn perusteella asetettuja kyberturvallisuutta koskevia velvoitteita toimialallaan. Valvovasta viranomaisesta ja valvonnasta säädettäisiin ehdotetun kyberturvallisuuslain 4 luvussa ja tiedonhallintalain 4 a luvussa. Liikenne- ja viestintävirasto valvoisi julkishallinnon uusia velvoitteita.

NIS 2 -direktiivissä edellytetään, että jäsenvaltiot voivat määrätä hallinnollisia seuraamusmaksuja velvoitteiden vastaisesta toiminnasta. Esityksessä ehdotetaan, että hallinnollisten sanktioiden enimmäismäärät olisivat tasolla, joka on alin direktiivin sallima enimmäismäärä. Hallinnolliset sanktiot määräisi seuraamusmaksulautakunta valvovan viranomaisen esityksestä. Seuraamusmaksulautakunta olisi uusi Liikenne- ja viestintäviraston yhteydessä toimiva sivutoiminen elin, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä. Hallinnollisen seuraamusmaksun määräämisestä säädettäisiin ehdotetun kyberturvallisuuslain 5 luvussa. Ehdotuksessa käytettäisiin kansallista liikkumavaraa siten, että tiedonhallintalaissa ei säädettäisi seuraamusmaksusta eikä seuraamusmaksua voitaisi määrätä julkishallinnon organisaatiolle silloinkaan, kun se kuuluisi harjoittamansa toiminnan johdosta samanaikaisesti kyberturvallisuuslain soveltamisalaan.

Tietoturvaloukkauksiin reagoiva ja niitä tutkiva CSIRT-yksikkö

Esityksessä ehdotetaan, että tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä sekä kansallisena keskitettynä yhteyspisteenä toimisi jatkossakin Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. CSIRT-yksikön tehtävät vastaisivat Kyberturvallisuuskeskuksen nykyisiä tehtäviä keskeisiltä osin esimerkiksi kyberuhkien, haavoittuvuuksien ja poikkeamien seurannan ja analysoinnin osalta sekä tietoturvallisuuden seurannan osalta. CSIRT-yksikön toiminta olisi järjestettävä Liikenne- ja viestintävirastossa toteutettavasta valvonnasta erilliseksi. CSIRT-yksikön tehtävistä säädettäisiin ehdotetun kyberturvallisuuslain 3 luvussa.

Kyberturvallisuusstrategia sekä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma

NIS 2 -direktiivissä edellytetään, että jäsenvaltiot hyväksyvät kyberturvallisuusstrategiat sekä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelmat.

Esityksessä ehdotetaan, että kyberturvallisuusstrategian hyväksyisi valtioneuvosto. Esityksessä ehdotetaan, että Liikenne- ja viestintävirasto vastaisi NIS 2 -direktiivin edellyttämän laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelman laatimisesta yhteistyössä valvovien viranomaisten sekä poliisin, suojelupoliisin, Puolustusvoimien ja Huoltovarmuuskeskuksen kanssa.

Ehdotetun kyberturvallisuuslain 42 ja 43 §:ssä säädettäisiin kyberturvallisuusstrategian ja hallintasuunnitelman laatimisesta. Esityksellä ei ehdoteta muutettavaksi turvallisuusviranomaisten nykyisiä toimivaltuuksia tai tehtävänjakoa laajamittaisen kyberturvallisuuspoikkeaman ja -kriisin hallitsemisessa.

Valtioneuvoston kanslia asetti 8.3.2024 hankkeen valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämiseksi. Osana hanketta asetettiin alatyöryhmä valmistelemaan Suomen kyberturvallisuusstrategian uudistamista. Uudistetun kyberturvallisuusstrategian luonnoksesta on järjestetty lausuntokierros.

Sähköisen viestinnän palveluista annettu laki

Sähköisen viestinnän palveluista annettuun lakiin ehdotetaan tehtäväksi muutoksia, joilla pantaisiin täytäntöön verkkotunnusten rekisteröintitietojen tietokantaa koskevat NIS 2 -direktiivin 27 ja 28 artikloiden edellyttämät seikat aluetunnusrekisteriä ja verkkotunnusvälittäjiä koskien. Esityksessä ehdotetaan muutettavaksi säännöksiä, jotka koskevat verkkotunnusvälittäjän viranomaiselle ilmoittamien tietojen sisältöä, verkkotunnusrekisteriin merkittäviä tietoja sekä pääsyä verkkotunnusrekisterin tietoihin.