Maa- ja metsätalousministeriö
Jord- och skogsbruksministeriet

Muistio

28.11.2023

VN/18157/2023
VN/18157/2023-MMM-42

Lausunto hallituksen esityksestä kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöön panemiseksi

Liikenne- ja viestintäministeriö on pyytänyt lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöön panemiseksi.

Hallituksen esityksen tausta ja tavoitteet

Luonnoksessa hallituksen esitykseksi ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta, jossa säädettäisiin yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Julkishallinnon osalta velvoitteista säädettäisiin myös julkisen hallinnon tiedonhallinnasta annetussa laissa. Esityksellä kumottaisiin NIS2-direktiiviä edeltävän verkko- ja tietoturvadirektiivin (2016/1148/EU) täytäntöönpanosäädökset useista sektorikohtaisista laeista. Velvoitteiden valvonnan järjestämisessä jatkettaisiin sektorikohtaisesti hajautettua mallia. Esityksellä säädettäisiin myös tietoturvaloukkauksia tutkivasta ja niihin reagoivasta yksiköstä, joka sijaitsisi Liikenne- ja viestintävirastossa. Lisäksi kyberturvallisuuden riskienhallinnasta annettavassa laissa säädettäisiin kansallisen kyberturvallisuusstrategian ja laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelman laatimisesta.

NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen.

Esityksen valmisteluun on johtanut kansallista täytäntöönpanoa edellyttävä EU-säädös 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 (NIS2-direktiivi). NIS2-direktiivi on saatettava kansallisesti voimaan 17.10.2024 mennessä ja kansallisia säännöksiä on sovellettava 18.10.2024 alkaen.

Hallituksen esityksen tavoitteena on NIS2-direktiivin kansallinen täytäntöönpano. NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisten sektoreiden ja toimijoiden osalta.

MMM:n lausunto hallituksen esityksestä

Maa- ja metsätalousministeriö kiittää mahdollisuudesta antaa lausunto hallituksen esityksestä kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöön panemiseksi ja toteaa lausuntopyynnön kohdista seuraavaa:

Postiosoite **Postadress** **Postal Address**	**Käyntiosoite** **Besöksadress** **Office**	**Puhelin** **Telefon** **Telephone**	**Faksi** **Fax** **Fax**	**s-posti, internet** **e-post, internet** **e-mail, internet**
Maa- ja metsätalousministeriö				
PL 30 00023 Valtioneuvosto	Hallituskatu 3 A Helsinki	0295 16001 +358 295 16001		kirjaamo.mmm@gov.fi

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta velvoittamalla jäsenvaltiot asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta. NIS2-direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso Euroopan unionin jäsenvaltioissa.

EU:n yhteinen tavoite vahvistaa kyberturvallisuuttaa kaikissa jäsenmaissa on nykyisessä maailmantilanteessa välttämätön tavoite. Tavoitteen mahdollisimman kustannustehokasta toteuttamista voidaan edistää sillä, että NIS2-direktiivin edellyttämät toimenpiteet pannaan täytäntöön kansallisesti mahdollisimman yhdenmukaisesti eri NIS2-sektoreiden ja -toimijoiden välillä CER-direktiivin tavoitteet huomioon ottaen. Käytännössä yhdenmukainen kansallinen toimeenpano tarkoittaa mm. sitä, että yleislain lisäksi myös toimintaohjeet ja -prosessit valmistellaan ja toteutetaan eri sektorien toimeenpanevien viranomaisten yhteistyönä.

Hallituksen esityksen mukaan NIS2-direktiivin toimeenpanosta yrityksille aiheutuvien kustannusten arvioidaan olevan kokonaisuudessaan vähäisiä suhteessa riskienhallintaan ja riskienhallintatoimenpiteiden toteuttamiseen. Tässä yhteydessä on kuitenkin tärkeää ottaa huomioon, että yrityksille syntyy uuden lainsäädännön soveltamisen myötä lisävelvoitteita, jotka kumuloituessaan lisäävät sekä yritysten hallinnollista taakkaa että kustannuksia. Siksi myös NIS2-toimeenpanon yhteydessä on hallitusohjelman mukaisesti varmistettava, että yrityksiin kohdistuva sääntely on selkeää, ennakoitavaa, oikeasuhtaista, kilpailu- ja teknologianeutraalia ja innovaatiomyönteistä.

Soveltamisalaa koskevat huomiot

NIS2-direktiivin yleinen soveltamisala määritellään sen 2 artiklassa. NIS2-direktiivin raportointi- ja riskienhallintavelvoitteet kohdistuvat sen 3 artiklassa määriteltäviin keskeisiin ja tärkeisiin toimijoihin.

NIS2-direktiivin 2 artiklan nojalla direktiiviä sovelletaan sen liitteissä I ja II tarkoitettua toimijatyyppiä oleviin julkisiin ja yksityisiin toimijoihin, jotka tarjoavat palvelujaan tai harjoittavat toimintaansa Euroopan unionissa. Lisäksi edellytyksenä on, että toimija täyttää komission suosituksessa 2003/361/EY olevat keskisuuria yrityksiä koskevat edellytykset tai ylittää keskisuurten yritysten määrittelyssä käytettävät kynnysarvot. Liitteissä I ja II on listattu tarkemmin direktiivin soveltamisalaan kuuluvat toimijatyypit.

Lakiehdotuksen 26 §:ssä määritellään keskeinen toimija, mutta tärkeää toimijaa ei lakiehdotuksessa ole määritelty. Sen sijaan esityksen perusteluista (s. 141) tärkeän toimijan määritelmä löytyy: ”Keskeisiin toimijoihin olisi sovellettava ennakoivaa valvontaa ja *tärkeisiin toimijoihin, eli muihin kuin keskeisiin toimijoihin*, olisi sovellettava lähtökohtaisesti vain jälkikäteistä valvontaa silloin, jos on näyttöä, viitteitä tai tietoja, joiden mukaan tärkeä toimija ei noudata NIS2-direktiivin ja sitä täytäntöönpanevan sääntelyn velvoitteita.” Lakiehdotuksessa tärkeä toimija on korvattu termillä muu kuin keskeinen toimija, mikä voi aiheuttaa huomattavaa epäselvyyttä esim. ohjeistuksen antamisen yhteydessä. Näin ollen tärkeä toimija tulisi määritellä suoraan eikä epäsuorasti muun kuin keskeisen toimijan kautta.

Esityksestä ei käy selvästi ilmi se, miten soveltamisalaan kuuluvat keskeiset ja keskeistä pienemmät vesihuoltolaitokset tunnistetaan niissä tapauksissa, joissa vesihuoltolaitos on osa kunnan organisaatiota, esim. liikelaitos tai taseyksikkö. Henkilöstön ja liikevaihdon tarkastelu ylittyvät pienelläkin kunnalla, vaikka vesihuoltolaitoksen koko olisi huomattavan pieni eikä omaa henkilöstöä olisi lainkaan. Koska soveltamisalaa ei ole tarkoituksenmukaista laajentaa mainitun kaltaisiin pieniin toimijoihin tai niissä tapauksissa koko emokuntaan, MMM ehdottaa, että lakiin kirjataan poikkeussäännös tai tarkennus niiltä osin, kun toimiala on osa kunnan omaa palveluntuotantoa. Vesihuoltolain mukaan kunnan tulee kirjanpidossaan eriyttää vesihuolto muista toiminnoista, joten on mahdollista tunnistaa keskeiset ja keskeistä pienemmät vesihuoltotoimijat suoraan.

Riskienhallintavelvoitetta koskevat huomiot

NIS2-direktiivin riskienhallintavelvoitteet ovat vähimmäistason velvoitteita ja ne on pyritty muotoilemaan mahdollisimman teknologianeutraalisti, jotta ne kestäisivät aikaa ja soveltuisivat laajalle

joukolle erilaisia toimijoita. Toimijat voisivat halutessaan ottaa käyttöön pidemmälle meneviä riskienhallintatoimia ja kansallisesti olisi jatkossankin mahdollista säätää tiukemmista riskienhallintavelvoitteista. Riskienhallintavelvoitteista on säädetty direktiivin 20 ja 21 artikloissa.

Lakiehdotuksen 9 §:n 4 momentin mukaan valvova viranomainen voi antaa toimialallaan tarkempia teknisiä määräyksiä:

1) kyberturvallisuuden riskienhallinnan toimintamallissa huomioitavista osa-alueista ja riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyistä;

2) kehittämisen ja ylläpidon sekä haavoittuvuuksien käsittelyn menettelyistä;

3) omaisuudenhallinnasta ja toimintojen tärkeysluokittelun perusteista;

4) henkilöstöturvallisuuden, kyberturvallisuuskoulutuksen, poikkeamien havainnoinnin ja

hallinnan sekä jatkuvuuden hallinnasta;

5) pääsynhallinnan, todentamisen ja salauksen menetelmistä;

6) perustason kyberhygieniakäytännöistä, joilla varmistetaan viestintäverkko- ja tietojärjestelmäturvallisuuden perusluonteiset hallintatoimenpiteet;

7) viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön, tilaturvallisuuden ja välttämättömien resurssien hallintatoimenpiteistä.

Direktiivin toimeenpanon valmistelussa tulisi jatkossa luoda kaikille toimialoille yhteisiä ohjeita, joilla varmistetaan riskienhallinnan vähimmäistason velvoitteiden yhdenmukainen toteutus kansallisesti eri toimialaoilla. Näiden ohjeiden pohjalta myös valvovilla viranomaisilla on paremmat edellytykset antaa tarkempia teknisiä määräyksiä omalle toimialalleen.

Raportointivelvoitetta koskevat huomiot

Keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle. Toimijat voivat myös vapaaehtoisesti ilmoittaa muista kuin merkittävistä poikkeamista, kyberuhkista ja läheltä piti -tilanteista valvovalle viranomaiselle. Valvovan viranomaisen puolestaan on toimitettava em. ilmoitukset ja raportit CSIRT-yksikölle.

Toimijoiden sekä valvovien viranomaisten työn helpottamiseksi olisi luotava yhteinen ilmoitusprosessi ja -sovellus, jonka kautta eri toimialojen toimijat voisivat lähettää raportteja ja ilmoituksia ja jonka kautta raportit ja ilmoitukset menisivät yhtäaikaisesti sekä valvovalle viranomaiselle että CSIRT-yksikölle.

Valvontaa koskevat huomiot

NIS2-direktiivissä säädetään vähimmäisvaatimukset valvontatoimenpiteille ja -keinoille, joita valvovien viranomaisten on voitava kohdistaa keskeisiin ja tärkeisiin toimijoihin. Keskeisiin toimijoihin olisi sovellettava kattavaa valvontajärjestelmää, johon kuuluu etukäteis- ja jälkikäteisvalvonta, ja tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää, johon kuuluu vain jälkikäteisvalvonta.

Lakiehdotuksessa ei ole määritelty tärkeitä toimijoita koskevaa jälkikäteisvalvontaa direktiivin artiklaa 33.2.a vastaavasti. Lakiehdotuksen 26 §:n 3 momentissa todetaan, että valvova viranomainen voi kohdistaa valvontaa ja 29–31 §:ssä tarkoitettuja toimia muuhun toimijaan kuin keskeiseen toimijaan vain, jos on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säädöksiä. Virkkeellä viitattaneen tärkeitä toimijoita koskevaan jälkikäteisvalvontaan, mutta kumpaistakaan ei suoraan mainita. Tästä voi aiheutua huomattavaa epäselvyyttä esim. ohjeistuksen antamisen sekä valvonnan suorittamisen yhteydessä.

Seuraamusmaksua koskevat huomiot

ei huomioita

CSIRT-yksikön tehtäviä koskevat huomiot

Hallituksen esityksen mukaan NIS2-direktiivin 10 artikla velvoittaa jokaisen jäsenvaltion nimeämään yhden tai useamman CSIRT-yksikön, jonka tehtävänä on reagoida tietoturvaloukkauksiin ja tutkia niitä. CSIRT-yksikön tehtäviä on täsmennetty 11 artiklassa, jonka mukaan CSIRT-yksikön tulee muun muassa seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia, antaa näitä koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja, avustaa direktiivin soveltamisalaan kuuluvia toimijoita, reagoida poikkeamatilanteisiin, kerätä ja analysoida poikkeamatietoja, ylläpitää kyberturvallisuuden tilannekuvaa ja osallistua CSIRT-verkoston toimintaan. Tarkempi luettelo CSIRT-yksiköiden tehtävistä löytyy direktiivin 11 artiklan 3 kohdasta. CSIRT-yksiköille kohdistetut vaatimukset on sijoitettu direktiivin 11 artiklan 1 kohtaan. Lisäksi CSIRT-yksiköillä tulee olla tekniset valmiudet suorittaa niille annetut tehtävät.

Esityksessä CSIRT-yksikön tehtäväksi on tunnistettu tietoturvaloukkauksiin reagointi. Sen sijaan direktiivin 10.1 artiklan mukaan CSIRT-yksikön tehtävä on vastata poikkeamien käsittelystä tarkasti määrättyä prosessia noudattaen. CSIRT-yksikön tehtäviä tulisikin ehdotuksessa tarkentaa direktiivin sanamuotoa vastaavaksi.

Lakiehdotuksen 2 §:n 17 kohdan mukaan poikkeaman käsittelyllä tarkoitetaan mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä. Määritelmä on NIS2-direktiivin 6 artiklan 8 alakohdan mukainen. Lakiehdotuksesta ei kuitenkaan löydy kohtaa, jossa tarkemmin säädettäisiin poikkeaman käsittelystä; sen sijaan 17 §:ssä ehdotetaan säädettävän *poikkeamailmoitusten* käsittelystä.

Koska poikkeaman käsittelyn ja poikkeamailmoitusten käsittelyn määrittely ja keskinäinen suhde on nykymuotoisenaan esityksessä epäselvä, ehdotetaan, että poikkeamailmoitusten käsittely määriteltäisiin 2 §:ssä, jotta ilmoituskäytännöstä tulisi mahdollisimman yhdenmukainen eri toimialoilla.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Tiedonhallinnan muutosvaikutusten arvioinnin mukaan tiedonhallintayksiköiden tulisi huolehtia kyberturvallisuuden riskienhallinnasta. Riskienhallinnan velvoitteet aiheuttavat jonkin verran muutoksia tiedonhallintaan. Tiedonhallintayksikön olisi laadittava kyberturvallisuuden riskienhallinnan toimintamalli ja käytävä läpi tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi säädetyt riskienhallinta-toimenpiteet ja toteutettava ne riskienhallinnan perusteella omassa toiminnassaan. Lisäksi nämä toimenpiteet tulee dokumentoida riskienhallinnan toimintamalliin. Toimintamallin muodostavista asiakirjoista ja muista tiedoista muodostuu tiedonhallintayksikölle uusi hallittava tietoaineisto ja velvollisuus ylläpitää tietoaineistoa.

Todennäköistä on, että julkisen hallinnon toimijoiden kyberriskienhallinnan kypsyystaso on varsin heterogeenista. Näin ollen on myös todennäköistä, että NIS2-velvoitteiden täyttäminen edellyttää monelta toimijalta varsin huomattavaa taloudellista ja työmäärällistä panostusta. Julkisen sektorin toimijoille lisärahoitusta tuskin on paljonkaan saatavilla, joten direktiivin toimeenpanemiseksi olemassa olevien resurssien käyttö on suunniteltava ja priorisointeja tehtävä. Prosessien ja menettelyjen tarkentamisessa on lisäksi huomioitava, miten mm. tiedonhallintalain soveltamiseen tuotetut nykykäytännöt, prosessit ja työkalut tukevat NIS2:n mukaisten toimenpiteiden toteuttamista.

Tiedonhallintavaikutusten kuvauksessa toivotaan tuotavan selvästi esiin se, että julkisen sektorin toimijoiden riskienhallintakyvykkyys on varsin vaihtelevaa ja siltä osin NIS2-toimeenpanosta voi aiheutua merkittäviäkin lisäkustannuksia joillekin julkisen sektorin toimijoille.

Verkkotunnusvälittäjiä koskevat huomiot

ei huomioita

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

ei huomioita

Vaikutustenarviointia koskevat huomiot

Hallituksen esityksellä katsotaan olevan taloudellisia vaikutuksia soveltamisalaan kuuluville yrityksille erityisesti riskienhallinta- ja raportointivelvoitteiden sekä toimijaluetteloon ilmoittautumisen kautta. Esitys lisää soveltamisalan toimijoiden kustannuksia ja hallinnollista taakkaa, mutta kyberturvallisuuden parantumisella nähdään olevan myös positiivisia vaikutuksia sekä yritysten liiketoimintaedellytyksille, että kansantaloudelle ja yhteiskunnan kriisinkestävyydelle. Kyberturvallisuuden riskienhallintaan investoiminen parantaa soveltamisalaan kuuluvien yritysten toimintavarmuutta ja edistää liiketoimintaa digitalisoituvassa yhteiskunnassa. Kyberturvallisuushäiriöiden vähentyminen säästäisi toimijoita häiriöiden haitallisista vaikutuksista aiheutuvilta kustannuksilta.

Esityksellä katsotaan olevan kustannusvaikutuksia yrityksille erityisesti riskienhallintaa koskevan velvoitteen kautta. Riskienhallintavelvoitteista aiheutuvien kustannuksien lisäksi toimijoille aiheuttavat vähäisiä kustannuksia raportointivelvoite merkittävistä poikkeamista ja ilmoittautumisvelvoite valvovan viranomaisen ylläpitämään toimijaluetteloon. Näistä aiheutuvat kustannukset arvioidaan kokonaisuudessaan vähäiseksi suhteessa riskienhallintaan ja riskienhallintatoimenpiteiden toteuttamiseen. Kustannuksia yrityksille voi aiheutua myös valvovan viranomaisen yritykseen kohdistamista valvontatoimenpiteistä.

Esityksen mukaan yrityksille aiheutuvien kustannusten arvioidaan olevan kokonaisuudessaan vähäisiä suhteessa riskienhallintaan ja riskienhallintatoimenpiteiden toteuttamiseen. Tässä yhteydessä on tärkeää ottaa huomioon, että yrityksille syntyy jonkinlaisia lisäkustannuksia jokaisen uuden lainsäädännön noudattamisen vuoksi. Kun nämä kumuloituvat ajan mittaan, niin kustannuksia ei voida luonnehtia vähäisiksi vaan olisi tarkasteleva laajemmin sitä hallinnollisen taakan kokonaisuutta, joka tietyn toimialan yrityksille kumuloituu.

Luvussa 9. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta (s. 75) todetaan, että omaisuudenhallinnan tulisi kattaa sekä fyysinen että aineeton omaisuus, ja myöhemmin tekstissä (s. 121) omaisuudenhallinnan määritellään tarkoittavan ”niitä menettelyjä ja toimenpiteitä, joilla toimija hallinnoi toiminnan kannalta olennaista laite-, ohjelmisto- ja tieto-omaisuuttaan”. Esityksen mukaan omaisuudenhallinta on kyberturvallisuusriskien hallinnassa keskeinen keino, jonka huolellinen hoitaminen ennalta ehkäisee riskien toteutumista ja auttaa riskienhallinnassa. Toimijalla olisi oltava säännölliset ja dokumentoidut omaisuudenhallinnan menettelyt ja ohjeet, jotka pitävät sisällään toimintojen, prosessien ja tietojen tunnistamisen. Omaisuudella tarkoitetaan esimerkiksi tiloja, laitteita, ohjelmistoja, palveluita, henkilöitä, aineetonta omaisuutta ja resursseja kuten immateriaalioikeuksia tai IP-osoitteita. Omaisuudenhallinnan määritelmää tulisi yhdenmukaistaa sekä tarkentaa, miltä osin se kattaa toimijoiden fyysisen omaisuuden, esimerkiksi vesihuoltolaitosten putkistot.

Muut huomiot ja avoin palaute esityksestä

Valmistussektori on NIS2-direktiivin II -liitteessä jaettu lääkinnällisten laitteiden, tietokoneiden sekä elektronisten ja optisten tuotteiden, sähkölaitteiden, muiden koneiden ja laitteiden, moottoriajoneuvojen, perävaunujen ja puoliperävaunujen sekä muiden kulkuneuvojen valmistuksen osa-alueisiin. kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet. Listaus sisältää myös metsäkoneiden valmistajat, jotka olisivat kooltaan komission pk-yrityksiä koskevan kokomääritelmän mukaisesti keskisuuria tai suurempia (vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa). Tällaisia metsäkonevalmistajia voisivat olla mm. Ponsse, John Deere, Logset ja Komatsu Forest.

Lopuksi todetaan vielä, että lausuntokierroksella ollut hallituksen esitys sisältää vielä useita, myöhemmin täydennettäviä kohtia (mm. kohta 11.2 Suhde talousarvioesitykseen). Nämä kohdat tulee käsitellä ja niistä tulee tiedottaa koordinoidusti hallituksen esityksen jatkovalmistelun yhteydessä.

Kansliapäällikön sijaisena osastopäällikkö Tuula Packalen

Ylijohtaja Pentti Lähteenoja

Liitteet

Jakelu

Tiedoksi

VN/18157/2023-MMM-42

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Lähteenoja Pentti 91214229F	Packalen Tuula 91228524L
2023-11-28	2023-11-29