LIIKENNE- JA VIESTINTÄMINISTERIÖ
KOMMUNIKATIONSMINISTERIET

Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2) täytäntöönpanoa koskevaksi lainsäädännöksi

5.9.2024
Hallintovaliokunta
Erityisasiantuntija Marko Priiki

Esityksen tavoite ja tausta

- Tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisillä toimialoilla.
- Tavoitteena on vähentää kyberhäiriöiden määrää ja välttää kyberturvallisuuteen liittyvien poikkeamien aiheuttamia keskeytyksiä ja häiriöitä yhteiskunnan toiminnan kannalta keskeisille palveluille ja toiminnoille.
- Esityksen valmisteluun on johtanut EU:n uusi kyberturvallisuusdirektiivi (NIS 2), joka edellyttää jäsenvaltioita saattamaan sen täytäntöönpanemiseksi tarpeelliset säännökset osaksi kansallista lainsäädäntöä 17.10.2024 mennessä ja soveltamaan niitä viimeistään 18.10.2024 alkaen.
- Kyberturvallisuusdirektiivi kumoaa verkko- ja tietoturvadirektiivin, jossa vastaavista velvoitteista säädettiin aiemmin. Keskeisinä erona kyberturvallisuutta koskevien velvoitteiden soveltamisala laajenee ja velvoitteista säädetään tarkkarajaisemmin.

Esityksen valmistelu

- 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.
- Lausuntokierros 8 viikkoa loka-joulukuussa 2023. Valmistelun aikana järjestettiin kolme avointa kuulemistilaisuutta sekä kuultiin keskeisiä etujärjestöjä päätyöryhmässä.
- Lainsäädännön arviointineuvoston lausunto helmikuussa 2024.

Keskeiset ehdotukset

- Uusi kyberturvallisuuslaki, jossa säädettäisiin NIS 2 -direktiivin edellyttämistä kyberturvallisuutta koskevista riskienhallinta- ja raportointivelvoitteista sekä viranomaistehtävistä.
- Julkishallintoon kohdistuvista velvoitteista säädettäisiin julkisen hallinnon tiedonhallinnasta annetussa laissa, uudessa 4 a luvussa.
- Lähtökohtana direktiivin vähimmäistason edellytykset; ei kansallisia lisäyksiä soveltamisalaan tai velvoitteiden tasoon.
- Valvontamalli: velvoitteiden valvonta toimialakohtaisille viranomaisille verkko- ja tietoturvadirektiivin valvontaa jatkaen.
    - Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Valvira ja Fimea. Liikenne- ja viestintävirastolla koordinoiva ja keskitetyn yhteyspisteen rooli.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus vastaisi tietoturvaloukkauksia tutkivan ja niihin reagoivan CSIRT-yksikön tehtävistä.
- Hallinnollisen seuraamusmaksun määräisi seuraamusmaksulautakunta, joka koostuisi sivutoimisista valvovien viranomaisten nimeämistä jäsenistä. Hallinnollisen seuraamusmaksun enimmäismäärä olisi direktiivin alin sallima enimmäismäärä. Seuraamusmaksua ei voitaisi määrätä julkishallinnon toimijalle.
- Sähköisen viestinnän palveluista annetussa laissa pantaisiin täytäntöön verkkotunnusrekisteriä koskeva artikla. Toimialakohtaisista laeista ehdotetaan kumottavaksi vanhan verkko- ja tietoturvadirektiivin täytäntöönpanosäännöksiä sekä tehtäväksi eräitä kyberturvallisuuslain johdosta tarpeellisia lainsäädäntöteknisiä muutoksia.

Esityksen yhteyksiä Petteri Orpon hallitusohjelmaan – Vahva ja välittävä Suomi

8 Uuden aikakauden ulko- ja turvallisuuspolitiikka

- Kyberturvallisuutta vahvistetaan tiiviissä yhteistyössä yritysten, elinkeinoelämän ja kolmannen sektorin kanssa huomioiden, että iso osa kriittisestä infrastruktuurista on yksityisessä omistuksessa (8.5).
- Hallitus uudistaa kansallisen kyberturvallisuusstrategian vastaamaan muuttunutta toimintaympäristöä (8.5).

6 Kasvun kaava

- Hallitus parantaa tietoturvaa kriittisillä toimialoilla sekä toteuttaa kyberturvallisuuden kehittämisohjelman (6.4).
- EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä (6.1).

3 Kunnat, kaupungit ja valtion aluehallinto

- Kuntien toiminnan ja tehtävien mitoitusta ja toteutustapojen yksityiskohtaista sääntelyä karsitaan (3.1).

Kyberturvallisuuslaki

1 luku – Soveltamisala ja yleiset säännökset

2 luku – Velvoitteet riskienhallinnasta ja poikkeamista ilmoittamisesta

3 luku – CSIRT-yksikkö ja sen tehtävät

4 luku – Velvoitteiden valvonta

5 luku – Hallinnollinen seuraamusmaksu

6 luku – Muut säännökset

- Mm. kyberturvallisuusstrategian ja laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelman laatiminen.

Liitteet I ja II: Soveltamisalaan kuuluvien toimialojen ja toimijatyyppien määrittäminen

Arvioidut vaikutukset

- Esityksellä parannetaan yhteiskunnan toiminnan kannalta keskeisten toimialojen ja palveluiden kykyä sietää, vastustaa ja palautua kyberhäiriöistä, kyberhyökkäyksistä ja muista tietojärjestelmiin ja viestintäverkkoihin haitallisesti vaikuttavista häiriöistä.
- Kyberturvallisuuslain soveltamisalassa olevalle yritykselle arvioidaan aiheutuvan kustannuksia kyberturvallisuutta koskevasta riskienhallinnasta lain edellyttämällä vähimmäistasolla vaihteluvälillä noin 0,2–0,8 % vuotuisesta liikevaihdosta. Yleisesti IT-kustannukset vaihtelevat koosta, kybermaturiteetista ja toimialasta riippuen vaihteluvälillä 1,5–5 %.
- Esityksessä arvioidaan, että noin 10–20 % organisaatioista, joita uudet velvoitteet koskevat, on kuulunut myös edeltävän verkko- ja tietoturvadirektiivin soveltamisalaan.
- Arvioihin organisaatioiden kokonaismäärästä ja yritykselle aiheutuvista kustannuksista liittyy esityksessä kuvattuja epävarmuustekijöitä. Yrityskohtaiset erot IT- ja kyberturvallisuuskustannuksissa ovat merkittäviä ja olennaisessa suhteessa yrityksen toimintaan. Toimialojen nykyinen maturiteettitaso kyberturvallisuudessa on vaihteleva.

Arvioidut vaikutukset viranomaistoimintaan

- Uusien yksityiskohtaisempien riskienhallintavelvoitteiden noudattamisesta ei pääsääntöisesti arvioida aiheutuvan merkittäviä lisäkustannuksia viranomaisille. Voimassa oleva tiedonhallintalain sääntely kattaa osin jo nykyisellään direktiivin mukaiset velvoitteet.
- Esityksellä arvioidaan olevan uusien valvonta- ja muiden tehtävien hoitamisesta aiheutuvia taloudellisia vaikutuksia Liikenne- ja viestintävirastolle, valvoville viranomaisille ja tietosuojavaltuutetulle. Lisäksi esityksellä on vähäisiä vaikutuksia Finanssivalvonnalle ja Oikeusrekisterikeskukselle. Hallituksen esityksessä esitetään arvio kunkin viranomaisen osalta esityksen mukaisten tehtävien aiheuttamasta resurssitarpeesta ja työmäärästä.