Helsinki
Helsingfors

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

Helsingin kaupunki kiittää mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanosta. Lausunnon antaa kaupunginkanslian strategiaosasto.

Vaikka direktiivi ei lähtökohtaisesti koske kuntatoimijoita, on siinä hyvin otettu huomioon Helsingin kaupungin erityisasema siltä osin kuin Helsingin kaupunki hoitaa laissa hyvinvointialueen järjestämisvastuulle säädettyjä tehtäviä.

Yleisesti todettakoon, että riskienhallinta on perusta kaikelle toiminnalle myös kyberturvallisuuden toteuttamisessa ja siksi sen merkitys kokonaisturvallisuuden toteuttamisessa olisi syytä nostaa vahvasti esiin, vaikka kyseessä on kyberturvallisuusdirektiivi.

Kyberturvallisuusdirektiivin mukaan Suomeen perustetaan kansallinen CSIRT-yksikkö (Computer Security Incide Response Teams), jolle direktiivin soveltamisalaan kuuluvien toimien velvoitteena on raportoida merkittävät tietoturvapoikkeamat. Raportointi tapahtuu kahden määräajan puitteissa eli 24 h, 72 tunnin kuluessa. Lisäksi tulee antaa loppuraportti yhden (1) kuukauden kuluttua. Tämä velvoite voi olla vaikeasti toteutettava laajassa organisaatiossa, jossa tapahtumia on paljon. Viranomaisen tulisi säädöksissään tarkasti määritellä ne kriteerit, joissa raportointivelvoite on (vrt. GDPR, jossa velvoite on kun henkilötiedot ovat vaarantuneet). Lisäksi tulee ottaa huomioon myös erilaiset tilanteet, joissa on epäselvää onko kyseessä merkittävä tietoturvapoikkeama. Viranomaisen on määriteltävä myös milloin tietoturvapoikkeama on merkittävä ja onko syytä raportoida myös epäselvistä tapauksista.

Lisäksi todettakoon, että 24 tunnin raportointivelvoite saattaa edellyttää sitä, että Helsingin kaupungin tulisi järjestää jatkuva valvonta laajasti koko kaupunkikonsernia koskien. Tämä ei ole käytännössä mahdollista.

Tiedonhallintalakiin ehdotetaan lisättäväksi uusi 4 a luku, jossa säädettäisiin yksinomaan NIS2-direktiivin täytäntöönpanon edellyttämistä seikoista. Ehdotettujen säännösten sijoittaminen omaan lukuunsa on perusteltua siksi, että luvun säännökset koskisivat ainoastaan rajattua määrää tiedonhallintayksiköistä ja viranomaisista. Myös 4 a luvussa Liikenne- ja viestintävirastolle ehdotetut NIS2 –direktiivissä tarkoitetun toimivaltaisen viranomaisen eli valvovan viranomaisen tehtävät rajautuisivat ehdotetussa 4 a luvussa säädettyjen velvoitteiden noudattamisen valvontaan. NIS2 -direktiivin täytäntöönpanossa tulisi tarkasti määritellä tiedonhallintalain ja direktiivin väliset yhteentoimivuudet ja eroavaisuudet kuntien velvoitteiden osalta. Näitä kahta lakia tulee tarkastella rinnakkain ja määritellä niiden suhteet niin selvästi, ettei tule tulkinnan varaan siihen noudatetaanko kyberturvallisuuden toimeenpanossa tiedonhallintalakia vai NIS2-direktiiviä jos näissä on velvoitteita, jotka saattavat olla ristiriidassa keskenään.

Esimerkkinä edellisestä on vaikkapa 18b pykälä 1 momentti, jonka mukaan tiedonhallintayksikön olisi tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien tur-vallisuuteen. Momentissa kuvataan myös riskienhallinnan tarkoitus eli viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden henkilöiden suojaaminen kyberuhilta. Tiedonhallintayksikön tulisi riskien tunnistamisen, arvioinnin ja hallinnan keinoin varmistua siitä, että toiminnassa käytettävien verkko- ja tietojärjestelmien turvallisuustaso ja riskienhallintatoimen-piteiden taso on riittävä ja oikeasuhtainen riskeihin nähden. Säännös vastaa pitkälti tiedonhallintalain 13 §:n sääntelyä riskiarviointiin perustuvasta tietoturvallisuustoimenpiteiden mitoittamisesta. Kyberturvallisuus ei käsitteenä täysin vastaa tietoturvallisuuden käsitettä, koska tieto-turvallisuus suojaa tietoa kaikissa muodoissaan – ei pelkästään tietojärjestelmissä. Lisäksi kyberturvallisuuteen määritelmätasolla sisältyy henkilöiden suojaamisen ulottuvuus, joka toki seuraa myös tietoturvallisuuden toteuttamisesta. Tämä kohta sitoo hyvin yhteen tiedonhallintalain velvoitteet ja NIS2-direktiivin velvoitteet, mutta sen voi tulkita merkitsevän sitä, että NIS2 direktiivi koskee kaikki niitä julkisen hallinnon toimijoita, joita myös tiedonhallintalaki koskee.

Soveltamisalaa koskevat huomiot

-

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Inkinen Mikael
Helsingin kaupunki - Kaupunginkanslia, strategiaosasto