



Lausunto

03.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Espoon kaupunki kiittää mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi. Vastaajana on kaupungin turvallisuus- ja valmiusyksikkö.

Direktiivin tavoitteena on vahvistaa kansallisen kyberturvallisuuden tasoa kriittisten toimijoiden osalta asettamalla näille uusia velvoitteita mm. riskienhallinnan osalta ja seuraamuksia velvoitteiden laiminlyönnistä.

Yleisenä huomiona esitys on pääosin oikeilla linjoilla tarpeesta valvoa, varautua ja velvoittaa organisaatioita toimiin tietoturvasa kehittämiseksi. Näiden toteutumisen seuranta ja tukeminen voi kuitenkin olla haasteellista mikäli onnistumisen kriteereitä ei ole tarkasti määritelty.

Soveltamisalaa koskevat huomiot

Kunnat eivät ole pääsääntöisesti osa NIS2-direktiiviä, ellei kunnan palveluihin sisälly yhteiskunnalle tai taloudelle kriittisiä palveluita. Näiden tunnistamisen kriteereillä voisi olla positiivinen vaikutus direktiivin noudattamiseen.

Riskienhallintavelvoitetta koskevat huomiot

Kappaleen 2.5 mukaisia riskienhallintavelvoitteita on 10 kappaletta. Näiden tavoitteet ovat ymmärrettäviä, mutta niiden tulkinta voi vaihdella huomattavasti eri toimijoiden kesken.

Raportointivelvoitetta koskevat huomiot

Keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta Kyberturvallisuuskeskukselle 24 tunnin sisällä havaitsemista. Velvoite on liian tiukka mikäli Toiminnolla ei ole ympärivuorokautista toimintaa, koska havaintoon voidaan tavallisesti reagoida vain 8-16 välisenä toimitustyöaikana (8h).

Organisaation Toimintojen ja Toimittajien välillä on tavallisesti myös viivettä, jolloin ko. 8h aikaikkuna voidaan tahattomasti ylittää ellei organisaatio järjestä 24h valvontaa pelkästään velvoitteen täyttämiseksi.

Velvoitteesta ei ilmene millä tavoin KTK:n osallistuminen hyödyttää raportoijaa. Ilman tätä ymmärrystä raportointi voi jäädä pintapuoliseksi ja raportoijan kannalta yksisuuntaiseksi, mutta pakolliseksi muodollisuudeksi.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

Direktiivin 32 artiklan 4 kohdassa velvoitetaan varmistamaan, että valvovalla viranomaisella on toimivaltuudet, kuten valtuus antaa toimijoille varoituksia, sitovia ohjeita tai määrätä toimija lopettamaan direktiivin vastainen toiminta. Valvovalla viranomaisella tulee olla mahdollisuus määrätä tai pyytää tuomioistuimia määräämään hallinnollisia sakkoja.

Kunnat eivät ole seuraamusmaksujen piirissä, mutta seuraamusmaksujen pelotevaikutusta voi rajoittaa organisaation tulojen lähde. Mikäli organisaation tulot ovat pääosin veroista lähtöisin, niin rahojen menetys ei välttämättä rankaise organisaation johtoa, joka yksityisellä puolella olisi yrityksen hallitus ja varat menettävät osakkaat. On todennäköisempää, että julkisella sektorilla rahallisia menetyksiä kompensoitaisiin muualta kuin johdosta, kuten palveluista.

Tämän johdosta olisi tehokkaampaa harkita viranomaisvastuun laajentamista, sekä huomioimaan kenellä on tosiasiallinen päätävävalta tietoturvan toteutumisesta julkisten organisaatioiden hallintosäännöissä ja toimintaohjeissa.

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

-

Säkkinen Harri
Espoon kaupunki