Metropolia Ammattikorkeakoulu Oy

Lausunto

24.10.2023 375/00.04.03/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kyberturvallisuusdirektiivin eli NIS2-direktiivin tarkoituksena on vahvistaa lain vaikutuspiiriin kuuluvien organisaatioiden tietoturvan ja kyberturvallisuuden riskienhallintaa. Lain piiriin kuuluvat pääasiassa julkisen sektorin toimijat sekä keskisuuret ja suuret yritykset. Direktiivin voi ymmärtää eräänlaisena kyberturvallisuuden riskienhallintaan velvoittavana lakina, joka asettaa minimivaatimukset organisaatiolle kyberturvallisuuden toimeenpanemiseksi ja raportoimiseksi. Yleisesti on hyvä asia, että kyberturvallisuushallintamallin lainsäädäntöä kehitetään EU-tasoisesti hyvien toimintatapojen levittämiseksi.

Soveltamisalaa koskevat huomiot

Kyberturvallisuusdirektiivin toimeenpaneminen jättää kansallista harkinnanvaraisuutta, jossa toistaiseksi Suomessa opetus- ja koulutusala eivät kuulut direktiivin piiriin. Lisäksi direktiivissä tutkimusorganisaatiolla tarkoitetaan; ”toimijaa, jonka ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin, mutta joka ei ole opetus- ja koulutusalan laitos”. Opetus- ja kulttuuriministeriö ei kuulu myöskään kansallisen toimeenpanon päätyöryhmään, joka vastaa toimisektoreiden erityispiirteiden huomioimisesta. Nykyisellä tulkinnalla Metropolian tutkimus-, kehitys-, innovaatio- ja opetustoiminta (TKIO-toiminta) eivät kuulu direktiivin sääntelyn piiriin.

Terveyssektorin Valviran alaisten toimijoiden on huomioitava NIS2-direktiivin vaatimukset. Lisäksi Valvira on vastuutaho, joka valvoo sääntöjen noudattamista omalla sektorillaan. Esimerkiksi Metropolian sosiaali- ja terveyspalveluita tarjoava HyMy-kylä saattaisi silloin joutua laatimaan itselleen kyberturvallisuusstrategian ja perustamaan tietoturvan/kyberturvallisuuden hallintamallin, jolla se osoittaa hallitsevansa oman toimialueensa kyberturvallisuuden riskit. Olemassa oleva sääntely edellyttää, että terveydenhuollon toimijalla tulee olla tietoturvasuunnitelma (asiakastietolaki 27 §) ja turvallisuussuunnitelma liittyessä Kanta-palveluihin tietoturvapoikkeamien käsittelemiseksi. Lisäksi tietohallintopalvelut myy tietopalveluiden kehitystä, kuten Peppi-tietojärjestelmää ja Vallu-valintakoepalvelua korkeakouluille, niin NIS2-direktiivi astuessa voimaan,

toimijan on harjoitettava kyberturvallisuuden riskienhallintaa liiketoiminnassaan. TVT-palveluntarjoajia (eng. ICT service providers) koskeva sektori on kokonaan uusi toimiala NIS1-direktiivin soveltamisalaan verrattuna. Edellytyksenä on yleisen kokokriteerin täyttyminen, eli kaupallisen toimijan on oltava kooltaan keskisuureen tai suurempaan yritykseen verrattavissa sekä päätoimipaikka NIS2-lainsäädännön vaikutusalueella.

Riskienhallintavelvoitetta koskevat huomiot

Tietohallintopalveluiden on laadittava tietoturvan tai kyberturvallisuuden hallintamalli Peppi-järjestelmälle ja Vallu-valintakoepalveluille, jos sen toiminta on rinnastettavissa TVT-palveluntarjoajaan. Lisäksi HyMy-kylän on toteutettava kyberturvallisuuden riskienhallintaa, joka voi olla haastavaa HyMy-kylän kontekstissa ilman riittävää ohjeistusta valtiotasolta. Vaikka direktiivi ei suoraan nimeä standardia, jonka mukaisesti riskienhallintaa olisi tehtävä, niin asianmukaisen suojauksen saavuttaminen vaatisi organisaatiolta, esimerkiksi ISO 27001:n tai NIST Cybersecurity Framework -kybertuvallisuuden hallintaohjelman omaksumista. Tämä voi olla korkeakoululle haastavaa, jos opetus- ja kulttuuriministeriö ei määrittele yhtenäistä ohjeistusta korkeakouluille hallintamallien toimeenpanemiseksi, mikäli kyberturvallisuusdirektiiviä sovelletaan korkeakoulujen tietyissä toiminnoissa.

Raportointivelvoitetta koskevat huomiot

Kyberturvallisuusdirektiivi perustaa Suomeen kansallisen CSIRT-yksikön (Computer Security Incident Response Teams), jolle direktiivin soveltamisalaan kuuluvat toimijat raportoivat merkittävät tietoturvapoikkeamat kolmiportaisesti, kuten ensi-ilmoitus 24 h kuluessa, jatkoilmoitus 72 h kuluessa ja loppuraportti 1 kk kuluessa poikkeamasta. Tämä voi osoittautua haastavaksi organisaatiolle, jos se ei ole aikaisemmin soveltanut tietoturvan tai kyberturvallisuuden hallintamallia toiminnassaan. Lisäksi viranomaiselle tulisi raportoida kyberturvallisuusuhista ja läheltä piti -tilanteista, jotka ovat vaikeasti määritettävissä ja alttiita subjektiivisille tulkinnoille tietoturva- ja kyberturva-alalla. Lainsäätäjän on määritettävä tarkat kriteerit, mitkä mahdolliset kyberturvallisuuteen liittyvät poikkeamat tulisi raportoida viranomaiselle suhteessa niiden todennäköisyyteen ja vaikuttavuuteen, esimerkiksi tulisiko toimijan raportoida ylivoimaiseen esteeseen (force majeure) verrattavat tapahtumat viranomaisille?

Valvontaa koskevat huomiot

Korkeakoulujen, kuten Metropolian toiminta läpi leikkaa useiden eri yhteiskunnan sektoreiden toimia-aloja. Esimerkiksi HyMy-kylän toiminnassa valvontaviranomainen olisi Valvira, kun taas tietohallinnon tarjoamat Peppi-järjestelmä ja Vallu-valintakoepalvelu kuuluvat Liikenne- ja viestintäviraston valvonnan alaisuuteen. Toisin sanoen Metropoliassa jouduttaisiin implementoimaan erillisiä kyberturvallisuuden hallintaohjelmia, jotka kattavat tarkasti rajatun määritellyn sektorin, esimerkiksi HyMy-kylän toiminnan. Lisäksi vaarana on, että valvontaviranomaiset antavat erilaisia suosituksia toimeenpanna kyberturvallisuuden hallintamallia, joka on otettava huomioon Metropolian omassa laajemmassa tietoturvan hallintamallissa.

Seuraamusmaksua koskevat huomiot

Seuraamussanktiot ovat oikein mitoitettuja. Jos Metropolian tiettyihin toimintoihin sovelletaan kyberturvallisuusdirektiiviä, niin maksun määräytyminen herättää kysymysmerkkejä sen suhteen,

miten ne määritettäisiin? Esimerkiksi tulisiko sanktiomaksu tietohallinnon liikevaihdon perusteella, jos sen tarjoamat palvelut kuuluvat NIS2:n piiriin?

CSIRT-yksikön tehtäviä koskevat huomiot

Ei huomioita.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei huomiota.

Verkkotunnusvälittäjiä koskevat huomiot

Ei huomioita.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei huomioita.

Vaikutustenarviointia koskevat huomiot

Komission mielestä NIS-direktiivin uudistaminen on perusteltua, koska sillä toivotaan parannettavan toimijoiden resilienssiä eli kriisikestävyyttä. Sidosryhmäyhteistyön näkökulmasta edellisellä on positiivisia vaikutuksia, kun toimija A voi luottaa toimijan B:n kyberturvallisuuden hallintamallin olevan minivaatimustasolla. Lisäksi lainsäädäntö kannustaa toimijoita omaksumaan kyberturvallisuus- ja tietoturva-alojen parhaat käytännöt. Arviot IT-kustannuksien 12–22 % kasvusta, riippuen organisaation kyberturvallisuuden hallintamallin lähtötasosta voi tuoda yllättäviä lisäkustannuksia, joihin ei ole varauduttu pidemmällä aika välillä, kun kyberturvallisuusdirektiivi astuu voimaan 18.10.2024.

Muut huomiot ja avoin palaute esityksestä

Kyberturvallisuusdirektiivi ei tuo korkeakouluille uusia velvoitteita tietoturva- ja kyberturva-asioissa. Toisaalta tietyt erityispiirteet korkeakoulukentällä, kuten Metropoliassa HyMy-kylän toiminta ja tietohallintopalveluiden kaupallinen TVT-palvelumyynti voidaan katsoa kuuluvan direktiivin soveltamisalaan, riippuen tulkinnasta. Komission arvion mukaan NIS2-direktiivin mukaisilla velvoitteilla arvioidaan olevan ensimmäisten toimeenpanovuosien aikana soveltamisalaan kuuluvan toimijan nykyisiä kyberturvallisuuteen liittyviä IT-kustannuksia keskimäärin 12–22 % korottava vaikutus riippuen siitä, onko velvoitteiden kohteena oleva toimija kuulunut NIS1-direktiivin soveltamisalaan. Tietoturvan ja kyberturvallisuuden lisääntyneet vaatimukset tuovat lisärasitteita Metropolian IT-kuluille, jos korkeakoulun tietyissä toiminnoissa sovelletaan direktiiviä, esimerkiksi toimeenpanemalla kyberturvallisuuden hallintamallia kyberturvallisuusriskien hallitsemiseksi.

Rannikko Roope
Metropolia Ammattikorkeakoulu Oy - Roope Rannikko, tietoturva-asiantuntija & tietohallintopalvelut; Kimmo Nikkanen, tietohallintojohtaja & tietohallintopalvelut