Xamk

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

Kaakkois-Suomen ammattikorkeakoulu Oy (XAMK) kiittää lausuntomahdollisuudesta hallituksen esitykseen kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. NIS2-direktiivin tarkoituksena on laajentaa kyberturvallisuuden suunnittelun, täytäntöönpanon, valvonnan ja raportoinnin velvoittavuutta EU:ssa ja yhteiskunnassa ja yhtenäistää lainsäädäntöä eri EU-maissa. Johtuen vihamielisen kybertoiminnan (mm. kyberrikollisuus, -vakoilu ja valtiollinen vaikuttaminen) kansainvälisyydestä on tärkeää, että vastatoimetkin ovat kansainvälisiä, vasteet nopeita ja ymmärrys minimivaatimuksista kyberturvallisuudelle samanlainen ympäri EU:n. Tämän mahdollistamiseksi yhtenäinen, kansallisesti velvoittava lainsäädäntö on erittäin tarpeellinen. NIS2-direktiivin tavoittelemat korkean tason asiat eivät ole vain suositeltavia, vaan myös välttämättömiä modernin digitaalisen yhteiskunnan toimivuuden takaamiseksi.

Soveltamisalaa koskevat huomiot

XAMK ei ammattikorkeakouluna lähtökohtaisesti kuulu hallituksen esityksen (HE) mukaisiin sovellettaviin toimialoihin. Lausunnon antamisaikana tehdyn selvityksen perusteella XAMKilla ei myöskään ole muuta sellaista TKI-toimintaa, jonka voitaisiin tämänhetkisen HE:n tekstin perusteella ehdottomasti katsoa kuuluvan direktiivin piiriin. Joitakin nykyisen HE:n muotoilusta johtuvia epävarmuustekijöitä kuitenkin on, mutta niiden lisäksi tässä lausunnossa olevat huomiot koskevat HE:n oletettuja epäsuoria vaikutuksia XAMKin tai ammattikorkeakoulujen toimintaan yleensä.

Terveysalan toimijoita koskeva sääntely laajenee, mutta on vielä epäselvää, mihin kaikkiin toimintoihin tämä tarkkaan ottaen ulottuu. Alkuperäisenä tarkoituksena lienee ollut saattaa kaikki Valviran ja Fimean valvonnan piirissä olevat toiminnot direktiivin alle, mutta näitä ei kuitenkaan ole yksityiskohtaisesti listattu. Tässä erityisesti Valviralle ilmoitettavat koulutuslisenssit (esim. lääkelaskentatentit) ovat toiminto, joka voi vaikuttaa terveysalan kouluttajien velvoitteisiin riippuen siitä, lasketaanko se NIS2:n piirissä oleviin valvottaviin toimintoihin vaiko ei.

Ammattikorkeakoulujen rahoituksessa merkittävää osaa näyttelee kuntasektori. Näin ollen NIS2-direktiivin tuottamat lisäkustannukset kuntasektorille vaikuttavat epäsuorasti myös

ammattikorkeakoulujen rahoitukseen, ja tässä otetaankin kantaa myös sellaisiin määrittelyihin, jotka todennäköisesti vaikuttavat kuntien kyberturvallisuusvelvoitteisiin.

NIS2-direktiivin määritelmät ja laskentatavat eri organisaatioiden kriittisyysluokituksille eivät ole riittävän selkeitä, itsenäisiä ja yhdenmukaisia. Tämä johtuu osaksi muiden valmisteilla olevien direktiivien vaikutuksesta ja osaksi joidenkin määritelmien ”periyttämisestä” muusta sääntelystä. Nykyisellään määritelmistä voi syntyä tilanteita, joissa pienen kunnan eri toimien kriittisyys on paljon korkeammalla tasolla kuin suuren kunnan, riippuen siitä, miten kukin kunta on kriittisten toimialojen palvelunsa organisoinut. Pienelle kunnalle voi siis tulla NIS2-velvoittavuudesta kohtuuttoman suuri kustannustaakka. Onkin tärkeää, että NIS2-direktiivin suomalaisessa toimeenpanossa määritelmät ja niiden tulkinta ovat ristiriidattomia, yhteneviä ja riittävän itsenäisesti tulkittuja ja viitattuja päätekstissä.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintaprosessin alkuvaiheet riskien tunnistamisesta ja arvottamisesta lähtien on lähes kaikissa tieto- ja kyberturvallisuuden standardeissa velvoitettu melkein kokonaan pelkästään toteuttavalle organisaatiolle ilman tarkempaa ohjeistusta. Periaatteena on siis yleisesti, että jokainen organisaatio räätälöi riskienhallintansa omiin prosesseihinsa ja kokoonsa nähden sopivaksi. Tällä periaatteella on hyvänä puolena se, että kaikille organisaatioille on yleensä ylipäätään mahdollista luoda riskienhallintaprosessi. Huonona puolena tällä periaatteella on kuitenkin se, että yhteistä minimiturvallisuustasoa on lähes mahdotonta luoda. NIS2 pyrkii parantamaan tätä tilannetta, mutta HE:ssä on tiettyjä sellaisia asioita, jotka eivät sellaisenaan sovellu kaikkiin organisaatioiden kokoluokkiin, eritoten mikäli hyvin pienetkin yritykset voivat toimialansa puolesta joutua keskeiseksi toimijaksi. Eräs tällainen asia on ZeroTrust, joka tietyillä määritelmillä vaatii pitkän valmistelun ja ison tukiorganisaation.

Riskienhallinnan velvoitteiden toimeenpanolle ei ole annettu määräaikaa. On eri asia antaa uuden direktiivin / lain toimeenpanolle siirtymäaika, kuin jättää lain tarkoitus kokonaan määrittelemättä. Riskienhallinta on olennainen osa NIS2-direktiivin työkalupakkia, ja sitä ei tule vesittää.

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

NIS2-direktiivi tuo kyberturvallisuuden velvoittavaksi yhä useammalle toimialalle ja laajentaa useiden aiempien mukana olleiden toimialojen organisaatioiden velvoitteita. Muutos ei tapahdu ilman riittävää resursointia organisaatioiden nykyisen henkilöstön kyberturvallisuuden osaamiseen ja tulevaisuuden asiantuntijoiden koulutukseen. Tämän vuoksi on hyvin tärkeää, että NIS2-siirtymävaiheen aikana viranomaiset kanavoivat (esim. NIS2-korvamerkittyä) rahoitusta myös erityyppiseen koulutukseen: sekä kyberturvallisuuden perustutkintoihin että jo työelämässä olevien asiantuntijoiden lisäkoulutukseen.

Kiviharju Mikko
Xamk