TTU Korhonen Marieme(LVM), Lehtilä Olli(LVM)

15.09.2020

JULKINEN

Asia

Suomen EU-ennakkovaikuttaminen – Verkko- ja tietoturvadirektiivin uudelleenarviointi

Kokous

U/E/UTP-tunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

EU:n verkko- ja tietoturvadirektiivillä (NIS-direktiivi) pyritään varmistamaan korkeatasoinen verkko- ja tietojärjestelmien turvallisuus koko unionissa. Direktiivi tuli voimaan 1.8.2016 ja saatettiin kansallisesti voimaan 9.5.2018.

Vuonna 2016 hyväksytyssä verkko- ja tietoturvadirektiivissä komissiolle annettiin velvoite tarkastella määräajoin uudelleen direktiivin toimivuutta ja laatia kertomus Euroopan parlamentille ja neuvostolle. Ensimmäisen kertomuksen määräaika on toukokuussa 2021. Osittain tämän johdosta komissio on päätynyt koko direktiivin uudelleenarviointiin ja uuden ehdotuksen antamiseen loppuvuodesta 2020. Muistiossa esitellään verkko- ja tietoturvadirektiivin uudelleenarviointiin liittyviä huomioita ja näkemyksiä direktiivin kehittämiseksi.

Covid-19-pandemia on osoittanut, että yhteiskunta on yhä riippuvaisempi digitaalisista palveluista ja niiden resilienssistä. Suomessa on kartoitettu liikenne- ja viestintäministeriön johdolla eri hallinnonalojen kokemuksia NIS-direktiivin soveltamisesta kansallisella tasolla. Lisäksi soveltamiseen liittyviä kokemuksia on tarkasteltu myös viranomaistasolla Liikenne- ja viestintäviraston johdolla.

Suomen kanta

Eurooppalainen sääntely turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason. Sääntelyä on edelleen tarpeen kehittää tukemaan parhaalla mahdollisella tavalla luottamuksen kasvattamista digitaalisiin toimintatapoihin ja kasvattamaan yhteiskunnan keskeisten palveluiden turvallisuutta. Kansallisella tasolla on vahva yhteinen näkemys siitä, että tietoturva on yhä merkittävämpi osa koko yhteiskunnan turvallisuutta. Tietoturvaa koskevan sääntelyn tulee seurata yhteiskunnan keskeisten palveluiden digitalisoitumista. Tietoturvaa koskevan sääntelyn ajantasaisuus ja riittävyys on kriittinen edellytys yhteiskunnan keskeisten palveluiden digitalisoitumiselle ja sitä kautta saavutettavan kokonaishyvinvoinnin edistämiselle.

Suomi pitää verkko- ja tietoturvallisuutta koskevan direktiivin uudelleenarviointia tärkeänä. Suomi haluaa parantaa entisestään EU:n yhteistä tietoturvatasoa vahvemmalla sääntelyllä. On tärkeää, että EU:lla on selkeä sääntelykehys tietoturva-asioille, koska useat tietoturvaa koskevat häiriöt ja niiden vaikutukset voivat olla jäsenvaltioiden rajat

ylittäviä. Tämän seurauksena on luontevaa, että yhteiskunnan keskeisiä palveluntarjoajia koskevat tietoturvavaatimukset perustuvat yhteiseen sääntelyinstrumenttiin. Suomi pitää tämän ohella hyvänä, että tietoturvaa koskeva sääntelykehys on yhdenmukainen muun relevantin sääntelyn kanssa, kuten yleisen tietosuoja-asetuksen, telesääntelyn ja EU:n yhteisten 5G-linjausten kanssa.

Suomi pitää kannatettavana, että EU:n yhteisen sääntelyn johdosta jäsenvaltiot toimivat tiiviissä yhteistyössä ja vaihtavat aktiivisesti tietoturvaa koskevia tietoja myös tulevaisuudessa. Direktiivi on mahdollistanut tiiviimmän yhteistyön myös kansallisesti viranomaistahojen välillä. Yhteistyötä on hyvä tiivistää jatkossakin vapaaehtoisuuden pohjalta ja direktiivin velvoitteiden kautta.

Suomi katsoo, että uudelleenarvioinnissa tulisi tarkastella direktiivin soveltamisalaan kuuluvien toimialojen riittävyyttä ja arvioida sääntelyn laajentamisen tarvetta muihin toimialoihin. Lisäksi tulisi arvioida direktiivissä määriteltyjen toimialojen toimijatyyppilistauksen laajentamisen tarvetta kaikkien sektorien osalta, ottaen huomioon toimijan tärkeys huoltovarmuuden kannalta. Direktiivin soveltamisalan uudelleenarvioinnissa tulisi samanaikaisesti pyrkiä välttämään tarpeettoman hallinnollisen taakan lisäämistä.

Energia-alan osalta Suomi näkee, että direktiivin liitteessä määritettyihin toimijoihin tulisi lisätä sähköntuottajat ja sähköpörssit keskeisiksi palveluntarjoajiksi. Myös maakaasun markkinapaikkojen mukaanotto direktiivin soveltamisalaan olisi perusteltua.

Osa finanssialan toimijoista, kuten korttimaksamisen toimijat (esimerkiksi maksupäätepalvelujen tarjoajat ja korttitapahtumien prosessoijat), ei tällä hetkellä ylety direktiivin soveltamisalaan. Lisäksi soveltamisala ei ylety finanssialalle tärkeisiin ICT-palveluja toimittaviin palveluntarjoajiin (infrastruktuuripalvelut ja järjestelmäintegraattorit). Soveltamisalan ulkopuolelle lukeutuvat myös arvopaperikeskus ja maksulaitokset. Edellä mainittujen toimijoiden sisällyttämistä direktiivin soveltamisalaan tulisi harkita direktiivin uudelleenarvioinnin yhteydessä.

Uudelleenarvioinnissa tulisi harkita direktiivin soveltamisalan ulottamista keskeisiin hallinnon digitaalisia palveluja tarjoaviin organisaatioihin ja näille palveluja tuottaviin yrityksiin. Soveltamisalaa ei kuitenkaan tulisi laajentaa turvallisuusviranomaisten käyttämiin digitaalisiin palveluihin, joista päättäminen on kansallisessa toimivallassa.

Digitalisaation ja automaation myötä tietoturva on entistä tärkeämpää myös liikenteelle. Direktiivin soveltamisalan tulisi kattaa kaikki liikennemuodot. Liikenteen saralla tulisi lisäksi arvioida toimijatyyppilistauksen riittävyyttä ilmailun, merenkulun ja raideliikenteen osalta.

Soveltamisalan mahdollisen laajentamisen rinnalla huomiota tulisi kiinnittää sektorikohtaisiin tietoturvavaatimuksiin, sillä eri sektoreiden digitaaliset palveluympäristöt voivat erota merkittävästi toisistaan. Samoin kehitteillä oleva tai jo olemassa oleva sektorikohtainen tietoturvasääntely tulisi huomioida. Mahdollisimman korkean tietoturvan tason saavuttamiseksi ja varmistamiseksi myös sääntelyssä tulisi kyetä tunnistamaan sektorikohtaisia eroja velvoitteiden asettamisen yhteydessä. Tietoturvan tason kehittämiseksi uudelleenarvioinnissa tulisi kiinnittää huomiota myös tietoturvan tason mittaamiseen. Suomi katsoo, että valvovilla viranomaisilla tulisi olla selkeät mittarit, joilla keskeiset palveluntarjoajat kykenevät osoittamaan tietoturvallisuuden tason. Lisäksi palveluntarjoajille asetettujen tietoturvavaatimusten tulee pohjautua riskiperusteiseen harkintaan.

Suomi pitää hyvänä, että direktiivissä esitettyjä määritelmiä digitaalisista palveluntarjoajista tulisi selkeyttää. Määritelmien selkeyttämisen ei tule itsessään johtaa soveltamisalan laajentamiseen. Samoin direktiivin uudelleenarvioinnissa tulisi tarkastella ja tarvittaessa tarkentaa määritelmiä internetin yhdysliikennepisteen (IXP), verkkotunnuksen (TLD) ja nimipalvelun (DNS) osalta eri maiden soveltamiskokemusten ja käytäntöjen perusteella. Lisäksi digitaalisen palveluntarjoajan pääkonttorin määritelmää tulisi selventää, sillä nyt tulkinta edellyttää Euroopan unionin tuomioistuimen ratkaisukäytännön selvittämistä.

Suomi pitää tarpeellisena, että direktiivin mukaista ilmoituskynnystä tietoturvahäiriöistä tai –poikkeamista tulisi selventää ja madaltaa. Ilmoitusmenettelyä tulisi yksinkertaistaa direktiivin tasolla, jotta helpotettaisiin keskeisten palveluntarjoajien ilmoitusprosessia koko EU:ssa.

Pääasiallinen sisältö

Kyseessä on ensimmäinen koko EU:n laajuinen yleinen tietoturvasäädös, jossa usealle kriittisen infrastruktuurin toimialojen keskeisille palveluntarjoajille asetettiin velvoite raportoida tietoturvapoikkeamista ja –uhkista. Näitä toimialoja ovat energia, liikenne, finanssiala, terveydenhuolto, juomaveden toimittaminen ja jakelu, digitaalinen infrastruktuuri sekä eräät muut digitaaliset palvelut.

Kansallisella tasolla tietoturvallisuuteen liittyviä velvoitteita valvovat sektorikohtaiset valvontaviranomaiset. Tämä tarkoittaa kansallisella tasolla Liikenne- ja viestintävirastoa, Energiavirastoa, Finanssivalvontaa, Sosiaali- ja terveysalan lupa- ja valvontavirastoa (Valvira) sekä elinkeino-, liikenne- ja ympäristökeskusta. Liikenne- ja viestintäviraston sähköisen viestinnän palveluista annetun lain mukaiset tehtävät olivat jo ennen NIS-direktiiviä kattavat tietoturvaloukkauksiin reagoimiseksi ja loukkauksien tutkimiseksi. Tämän johdosta Liikenne- ja viestintävirasto katsottiin sopivaksi yhteyspisteeksi EU-yhteistyössä muiden jäsenvaltioiden viranomaisten kanssa. NIS-direktiivin myötä Liikenne- ja viestintäviraston roolissa on korostunut entisestään kansalaisten ja yritysten tukeminen ja auttaminen tietoturvasta huolehtimisessa.

Verkko- ja tietoturvadirektiivin mukaisella sääntelyllä on mahdollistettu viranomaisten tiiviimpi yhteistyö ja tiedonvaihto tietoturvaloukkauksista. Tiedonvaihtoa on tehostettu verkko- ja tietoturvadirektiivin perusteella myös EU:n tasolla NIS-yhteistyöryhmän ja CSIRT-verkoston (Computer Security Incident Response Teams) parissa.

Voimassa olevan lainsäädännön mukaan keskeisen palvelun tarjoajan on ilmoitettava valvovalle viranomaiselle merkittävistä tietoturvaloukkauksista tai niiden uhkista. Tällaisia tietoja ovat esimerkiksi tiedot haittaohjelmista (ns. tietokonevirus), ohjelmistohaavoittuvuuksista (ts. ohjelmiston väärinkäytön mahdollistava ohjelmointivirhe) tai vaikkapa tiedot tapahtuneesta tietomurrosta.

Ilmoitusvelvollisuus koskee nykyään vain sellaisia häiriöitä tai poikkeamia, joilla on merkittävä vaikutus keskeisten palvelujen jatkuvuuteen. Valvova viranomainen voi antaa tarkempia määräyksiä siitä, milloin tietoturvaloukkausta olisi pidettävä merkittävänä. Merkittävyyden arvioinnissa olisi huomioitava palvelun käyttäjien lukumäärä, häiriön kesto sekä maantieteellinen levinneisyys. Merkittävyyden kynnys on osaltaan vaikuttanut siihen, että direktiivin perusteella annettuja ilmoituksia on ollut kohtuullisen vähän. On kuitenkin huomioitava, että valvovat viranomaiset voivat saada ilmoituksia tietoturvahäiriöistä myös elinkeinoharjoittajien vapaaehtoisesti tekemien ilmoituksien

välityksellä. Esimerkiksi Liikenne- ja viestintävirasto saa merkittävän osan tietoturvaloukkaus- ja haavoittuvuustiedoista juuri elinkeinoharjoittajien vapaaehtoisesti tekemien ilmoituksien kautta.

Direktiivin implementoinnin yhteydessä tehtiin muutoksia ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin. Lisäksi muutoksia tehtiin liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin sekä vesihuoltolakiin. Mainittuihin lakeihin lisättiin säännökset yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajien velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa tietoturvallisuuteen liittyvistä merkittävistä poikkeamista valvovalle viranomaiselle sekä tietyissä tapauksissa yleisölle. Laeissa ei ole määritelty tarkemmin miten riskienhallinnasta olisi huolehdittava, vaan tältä osin toimijalla olisi mahdollisuus valita liiketoimintaansa, järjestelmiinsä ja muuhun riskienhallintaansa parhaiten sopivat menetelmät tietoturvariskien hallitsemiseksi.

Ilmailulain velvoitteet koskevat lennonvarmistuspalvelun tarjoajaa sekä yhteiskunnan toiminnan kannalta keskeisen lentoaseman pitäjää. Rautatielain velvoitteet koskevat valtion rataverkon haltijaa sekä liikenteenohjauspalveluita tarjoavaa yhtiötä. Alusliikennepalvelulain velvoitteet koskevat alusliikennepalvelun tarjoajaa. Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain velvoitteet koskevat yhteiskunnan toiminnan kannalta keskeisen sataman pitäjää. Liikenteen palveluista annetun lain mukaiset velvoitteet koskevat älykkään liikennejärjestelmän ylläpitäjää. Sähkömarkkinalain velvoitteet koskevat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskevat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä vähintään 5000 kuutiometriä vuorokaudessa. Vesihuoltolain sääntelyä täydennettiin samalla siten, että mainittujen laitosten olisi ilmoitettava viranomaiselle myös muista kuin tietoturvallisuuteen liittyvistä merkittävistä vesihuollon häiriötilanteista.

Sähköisen viestinnän palveluista annettuun lakiin otettiin vastaavat velvoitteet koskien eräitä digitaalisten palveluiden tarjoajia. Velvoitteet koskevat verkossa toimivan markkinapaikan tarjoajaa, hakukonepalvelun tarjoajaa sekä pilvipalvelun tarjoajaa.

Lisäksi säädettiin valvovien viranomaisten oikeudesta tehdä tietoturvallisuuteen liittyvien velvoitteiden valvonnassa tarvittavaa yhteistyötä ja vaihtaa tarvittaessa salassa pidettäviä tietoja. Valvoville viranomaisille säädettiin myös velvoite ilmoittaa tarvittaessa tietoturvallisuuteen liittyvistä häiriöistä toisille EU:n jäsenvaltioille, mikäli häiriöllä on merkittävä vaikutus keskeisten palvelujen tarjoamiseen kyseisessä jäsenvaltiossa. Liikenne- ja viestintävirastolle on säädetty velvollisuus tehdä tarvittaessa yhteistyötä muiden jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä EU:n verkko- ja tietoturvadirektiivin 10 artiklan mukaisen yhteistyöryhmän kanssa.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

-

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

EU-ministerivaliokunta 18.9.2020

Viestintäjaoston (EU19) kirjallinen menettely 2.9.2020-4.9.2020
Liikennejaoston (EU22) kirjallinen menettely 2.9.2020-4.9.2020
Oikeus- ja sisäasioiden jaoston (EU7) kirjallinen menettely 2.9.2020-4.9.2020
Kilpailukykyjaosto (EU8) kirjallinen menettely 2.9.2020-4.9.2020
Rahoituspalvelut ja pääomaliikkeet -jaosto (EU10) kirjallinen menettely 2.9.2020-4.9.2020
Energia ja Euratom –jaoston (EU21) kirjallinen menettely 2.9.2020-4.9.2020
Terveysjaosto (EU33) kirjallinen menettely 2.9.2020-4.9.2020

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

-

Taloudelliset vaikutukset

Suomen kannassa todetaan, että direktiivin nykyistä soveltamisalaa tulisi laajentaa. Soveltamisalan laajentaminen synnyttäisi uusia tehtäviä ja velvoitteita toimialoille, jotka eivät ole tällä hetkellä verkko- ja tietoturvadirektiiviä koskevan sääntelyn piirissä.

Verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanoprosessin ja siihen liittyvän esityksen (HE 192/2017) yhteydessä arvioitujen taloudellisten vaikutusten mukaan ei ole tunnistettu merkittäviä taloudellisia vaikutuksia esityksessä tarkoitetuille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille taikka digitaalisten palveluiden tarjoajille.

Muut asian käsittelyyn vaikuttavat tekijät

-

Asiakirjat

Komission julkisen kuulemisen kysely: Consultation on the revision of the NIS Directive

Laatijan ja muiden käsittelijöiden yhteystiedot

Neuvotteleva virkamies Olli Lehtilä, puh. 0295 342 106
Erityisasiantuntija Marième Korhonen, puh. 0295 342 134

EUTORI-tunnus

Liitteet Komission julkisen kuulemisen kysely: Consultation on the revision of the NIS Directive

Viite

Asiasanat	kyber, tietoturva, tietoyhteiskunta
Hoitaa	**LVM, OM, SM, TEM, UM, VNK**
Tiedoksi	EUE, MMM, OKM, PLM, RUOKA, STM, TULLI, VM, VTV