Liikenne- ja viestintävirasto Traficom

Lausunto

24.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Traficom kiittää mahdollisuudesta lausua ja toteaa, että lakiluonnos on kattavasti valmisteltu ja keskittyy oikeisiin asioihin kyberturvallisuuden edistämisen kannalta. Traficom on päässyt osallistumaan esitysluonnoksen valmisteluun ja Traficomin näkökulmat on hyvin huomioitu. Virasto pitää lakiluonnoksen ja sen taustalla olevan nk. NIS2-direktiivin tavoitteita kannatettavana ja esitettyä sääntelyä Suomen kansallisen kyberturvallisuuden näkökulmasta keskeisenä. Traficom nostaa lausunnossaan esille seikkoja, joita se pitää erityisen tärkeinä ja esittää harkittavaksi eräitä tarkistuksia, jotka eivät ole vielä aiemmassa valmistelussa nousseet esille.

Tiivistelmä ja yleiset huomiot

Yhteiskunnan toimivuuden, turvallisuuden ja luotettavuuden kannalta kriittisten palveluntarjoajien viestintäverkkojen ja tietojärjestelmien kyber- ja tietoturvallisuus sekä näihin liittyvä riskien hallinta ja poikkeamiin puuttuminen on jatkuvasti tärkeämpää. Nämä ovat yhä merkittävämpi osa koko yhteiskunnan turvallisuutta, jota tulee edistää aktiivisesti myös oikeasuhtaisen sääntelyn keinoin. Esitysluonnoksessa säädettäväksi ehdotettava laki kyberturvallisuuden riskienhallinnasta (jäljempänä NIS-yleislakiluonnos) ja sen sisältämät kyberturvallisuuden riskienhallintavelvoitteet olisivat ensimmäiset yhteiset kyberturvallisuusvaatimukset Suomessa ja Traficom katsoo asettavien velvoitteiden olevan perusasioita, jotka kaikkien organisaatioiden tulisi huomioida. Velvoitteiden noudattamisella pystytään nimittäin ehkäisemään kyberhyökkäyksiä ja niiden haitallisia vaikutuksia toimijoihin, niiden asiakkaisiin sekä laajemminkin yhteiskunnassa ja reagoimaan mahdollisiin ongelmiin. Kyberhyökkäyksistä aiheutuvat vahingot, kustannukset ja inhimillinen kärsimys ovat usein moninkertaiset verrattuna kustannuksiin, joita kyberturvallisuuden riskienhallintatoimenpiteistä aiheutuu.

Esitysluonnoksessa säädettävät vaatimukset ja velvoitteet kyberturvallisuuden edistämiseksi ovat välttämättömiä turvallisuuden parantamiseksi digitaalisen yhteiskunnan eri sektoreilla. Traficom katsoo, että esitysluonnoksen taustalla olevassa direktiivissä säädetyt ja nyt kansallisesti täytäntöönpantavat vaatimukset ovat kuitenkin kohtuullisia soveltamisalan kohteena oleville toimijoille. Traficom pitää tärkeänä, että esitysluonnoksen velvoitteet ja vaatimukset mahdollistavat myös riskiperusteisen lähestymistavan, joka perustuu vahvasti soveltamisalaan kuuluvien toimijoiden kokoon ja toimintaan. Koska yhteiskunta on yhä verkottuneempi ja yhä useammat palvelumme nojaavat sähköisiin toimintoihin, palveluihin tai verkkoihin, Traficom pitää tärkeänä, että tulevan kansallisesti täytäntöönpantavan sääntelyn soveltamisalaa on laajennettu ensimmäisen verkko- ja tietoturvadirektiivin jälkeen.

Traficom pitää myös hyvänä, että velvoitteet on luonnosteltu asetettavaksi direktiivin edellyttämän vähimmäistason mukaisesti siten, ettei Suomessa tultaisi sääntelemään toimijoita tiukemmin kuin muissa maissa. Traficom arvioi EU-yhteistyön havaintojensa perusteella, että esitysluonnoksessa olevat vel-voitteet noudattavat yhteiseurooppalaista linjaa, kansainvälisiä standardeja ja yleisiä hyväksyttyjä käytäntöjä sekä teknologianeutraalisuuden periaatetta.

Traficom pitää tärkeänä, että esitysluonnoksesta käy ilmi sääntelyn yleis-luontoisuus, jolloin jo voimassa olevaa sektorikohtaista sääntelyä voidaan tarpeen mukaan soveltaa nyt laadittavan kyberturvallisuutta koskevan yleissääntelyn lisäksi. Edellä mainittu tarve tulee kyseeseen muun muassa tele-sektorin ja ilmailun kohdalla, joissa molemmissa on jo entuudestaan hyvin pitkälle vietyä ja tarkkarajaista sääntelyä myös kyberturvallisuuden ja tietoturvan osalta.

Jotta koko yhteiskunnan kyberturvallisuutta pystytään entisestään paran-tamaan ja kehittämään, se edellyttää resursointia ja resurssien tehokasta kohdentamista niin julkisella kuin yksityisellä sektorilla. Traficomin osalta valvottavien sektoreiden ja toimijoiden määrä kasvaa huomattavasti, mikä tulee ottaa huomioon muun muassa valvonnan järjestämisessä tulevaisuudessa. Lisäksi virastolle tulee kokonaan uudenlaisia tehtäviä, kuten seuraamusmaksulautakuntatehtävä.

Traficom korostaa esitysluonnoksen sisällön mukaisesti, että sektorikohtaisilla viranomaisilla on paras substanssiosaaminen oman toimialansa erityispiirteistä ja muusta toimintaa koskevasta sääntelystä, jolloin kyseisellä valvovalla viranomaisella on paras osaaminen ja ymmärrys toimialansa riskienhallintaan liittyvistä seikoista. Näin ollen Traficom pitää kannatettavana esitysluonnoksen hajautettua lähestymistapaa koskien eri sektoreiden valvontaa. Traficomin Kyberturvallisuuskeskus pyrkii resurssiensa puitteissa tukemaan muita valvontaviranomaisia.

Traficom korostaa, että useissa tapauksissa kyberloukkausten, -häiriöiden tai niiden uhkien selvittäminen edellyttää mahdollisimman nopeita toimia ja tiedonvaihtomahdollisuuksia niin viranomaisten kesken kuin yksityisen sektorin toimijoiden kanssa. Traficom katsoo, että esitysluonnoksessa on onnistuttu valmistelemaan tarvittavia lisäyksiä tiedonkäsittely- ja vaihto-oikeuksiin. Samalla esitysluonnoksessa on kyetty huomioimaan tarvittava tasapaino ja suhteellisuus

tiedon käyttö- ja suojaustarpeiden ja kyberturvallisuusriskien tehokkaan torjunnan ja hallinnan välillä.

Kyberturvallisuutta koskevien häiriöiden torjuminen, niiden havaitseminen ja häiriötilanteista toipuminen sekä muiden kriittisten toimijoiden varoittaminen mahdollisesta häiriöstä tai sellaisen uhkasta edellyttävät, että kyberhäiriötilanteista tai niitä koskevista uhista ilmoitetaan toimialaa valvovalle toimivaltaiselle viranomaiselle. Tämän lisäksi on ensiarvoisen tärkeää, että Traficomin Kyberturvallisuuskeskus saa tiedon häiriöistä ja niitä koskevista uhista. Traficomin Kyberturvallisuuskeskus toimii jo tällä hetkellä esitysluonnoksessa mainittuna kansallisena CSIRT-yksikkönä, jonka toiminnan varaan rakentuu esimerkiksi kyberturvallisuuden kansallisen tilannekuvan koostaminen ja koordinointi. Jotta CSIRT-yksikön työtä voidaan jatkaa tehokkaasti ja tukea voidaan tarjota laajemminkin yhteiskunnan eri sektoreille, Traficom pitää tärkeänä, että esitysluonnoksessa varmistetaan riittävät tiedonsaantia, tiedonvaihtoa ja tiedonkäsittelyä koskevat mahdollisuudet Traficomin Kyberturvallisuuskeskukselle, erityisesti sen CSIRT-yksikölle.

Edellä mainitun ohella Traficom esittää, että oikaisuvaatimusmenettelyn käyttöä tarkennetaan erityisesti valvonta-asioiden osalta. Traficom katsoo, että menettelyn käyttö ei soveltuisi nykyisellä muotoilulla valvonta-asioihin. Lisäksi valvontamenettelyä tulisi tarkastella jatkovalmistelun aikana myös asian-osaisaseman osalta. Jatkovalmistelussa tulisi selkeyttää, että kolmansilla osapuolilla tai esimerkiksi soveltamisalaan kuuluvien toimijoiden asiakkailla ei ole asianosaisasemaa valvontamenettelyssä.

Soveltamisalaa koskevat huomiot

Soveltamisalaa koskevat huomiot

Uudet toimialat, toimijat ja määritelmät

Traficom kannattaa NIS-yleislakiluonnoksen mukaisesti sääntelyn soveltamista uu-siin toimialoihin ja toimijoihin, koska esitysluonnoksessa säädettävät vaatimukset ja velvoitteet kyberturvallisuuden edistämiseksi ovat välttämättömiä kyberturvallisuuden parantamiseksi yhteiskunnan eri sektoreilla. Onkin tärkeää, että kyberturvallisuuden riskienhallintavelvoitteet koskevat sekä keskeisiä että tärkeitä toimijoita.

Traficom pitää NIS-yleislakiluonnoksen soveltamisen selkeyden kannalta tärkeänä, että 2 §:n määritelmiin lisättäisiin kuriiritoiminnan määritelmä, koska tätä ei ole lainsäädännössä tai muutoinkaan yleisesti määritelty. Luottamuspalvelun määritel-mään Traficom ehdottaa lisättävän NIS2-direktiiviä vastaavasti viittaus eIDAS-asetuksen 3 artiklan 16 kohtaan, jotta NIS-yleislaissa määriteltäisiin myös luotta-muspalvelu itsessään eikä ainoastaan sen tarjoajaa. Lisäksi Traficom ehdottaa NIS-yleislakiluonnosta myös täydennettäväksi sen osalta, mitkä muut kuin maa-asemalain

mukaiset toiminnanharjoittajat kuuluisivat lain soveltamisalaan, koska kaikki avaruuspohjaisten palvelujen tarjoamista tukevien, maassa sijaitsevan infra-struktuurin ylläpitäjät eivät välttämättä ole maa-asemalain tarkoittamia toiminnanharjoittajia.

NIS-yleislakiluonnoksen 3 §:n mukaan valtioneuvoston asetuksella voitaisiin säätää lain soveltamisesta tiettyyn toimijaan. Traficom ehdottaa yleisesti sovellettavan normin sijaan harkittavaksi valtioneuvoston päätöstä asiasta, jos se on kohdistettu tiettyihin yhtiöihin ja toimijoihin. Lisäksi Traficom ehdottaa harkittavaksi, että voisi olla perusteltua mahdollistaa valtioneuvoston asetuksella tarkempien yleisesti sovellettavien kriteerien säätäminen ilman, että asetuksessa kuitenkaan nimettäisiin tiettyjä yrityksiä.

Lopuksi Traficom kiinnittää huomiota vielä siihen, että 3 §:n 3 momenttia koskevien säännöskohtaisten perusteluiden mukaan 3 momentin mukainen soveltaminen rajautuisi vain sellaisiin liitteissä I tai II tarkoitettua toimintaa harjoittaviin toimijoihin, joihin lakia ei muutoin sovellettaisi, kun ne eivät täyttäisi keskisuuren toimijan määritelmää. Traficom ei pidä tarkoituksenmukaisena rajata 3 momentissa tarkoitettujen kriittisyyskriteereiden soveltamista vain pieniin toimijoihin. Ehdotettu rajaus ei huomioi keskisuurten toimijoiden mahdollista kriittistä roolia ja niihin liittyvää tarvetta määritellä toimija tarvittaessa keskeiseksi toimijaksi. Toisaalta huomi-oon tulisi ottaa myös se mahdollisuus, että 3 momentin mukaisesti keskeiseksi määritetty pieni toimija voi kasvaa keskisuureksi, jonka jälkeen se putoaisi 3 momentin soveltamisalan ulkopuolelle ja voisi muuttua keskeisestä toimijasta muuksi kuin keskeiseksi toimijaksi ja sitä myöten rajatumman valvonnan ja vaatimusten piiriin. Traficom katsoo, että 3 momentin mukaiset perusteet voivat soveltua mihin tahansa toimijaan koosta riippumatta, jolloin mikä tahansa liitteissä I tai II tarkoitettua toimintaa harjoittava toimija tulisi voida määrittää 3 momentin mukaisten kriteerien täyttyessä keskeiseksi toimijaksi. Traficom ei näe tämän tulkinnan olevan ristiriidassa NIS2-direktiivin 3 artiklan kanssa.

Soveltamisalan rajaus

NIS-yleislakiluonnoksen 4.1 §:n mukaan velvoitteita ei sovellettaisi toimintaan tai palveluihin, joita tarjotaan tiettyjen kansalliseen turvallisuuteen liittyvien viranomaistoimien toteuttamiseksi. Traficom kiinnittää huomiota siihen, että säännöksen muotoilu ei vastaa NIS2-direktiivin 2(8) artiklaa, jonka mukaan tietyistä direktiivin velvoitteista voidaan vapauttaa "erityiset toimijat, jotka harjoittavat toimintaa kan-sallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla". NIS-yleislakiluonnoksen direktiivistä eroava muotoilu on ongelmallinen, koska ehdotuksen sanamuodon perusteella vaikuttaisi siltä, että yleisen viestintäpalvelun tarjoaminen esimerkiksi poliisin tai syyttäjälaitoksen käyttöön voisi jäädä viestintäpalvelun tarjoajaa koskevien riskienhallintavelvoitteiden ulkopuolelle, ja vielä selkeämmin näin kävisi siltä osin kuin teleyritysten toiminta liittyy esimerkiksi erikseen laissa säädeltyyn telekuunteluun ja valvontaan. Tällaisissa tilanteissa olisi päinvastoin tärkeää varmistaa, että riskienhallintavelvoitteita sovelletaan toimijoihin täysimääräisesti. Lakiehdotuksen mukainen soveltamisalarajaus tulisi kohdentaa täsmäl-lisemmin niin, ettei se rajoita lain soveltamista tällaisissa tilanteissa.

Suhde CER-direktiiviin

Kuten esitysluonnoksessa todetaan, esityksellä on yhteys kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiivin (nk. CER-direktiivi, (EU) (2022/2557) kansallista täytäntöönpanoa koskevaan säädöshankkeeseen (SM047:00/2022) ja hankkeessa valmisteltavaan hallituksen esitykseen. CER-direktiivin täytäntöönpanosta vastaa sisäministeriö.

Keskeisin liittymäkohta NIS2-ja CER-direktiivien välillä käy ilmi NIS-yleislain 26 §:stä, jonka 2 momentin d-kohdan mukaan keskeisenä toimijana pidetään toimijaa, joka on CER-direktiivin nojalla määritelty kriittiseksi. CER-direktiivi on otettu huomioon myös NIS-yleislakiluonnoksen 2, 3, 17, 27 ja 46 §:ssä sekä tiedonhallintalain 3 §:ssä. Traficom pitää tätä hyvänä ja toteaa, että NIS2- ja CER-hankkeiden säädösten yhteensopivuudesta tulee huolehtia molempien jatkovalmistelussa.

Suhde muuhun Traficomin toimialaan kuuluvaan lainsäädäntöön

Esitysluonnoksessa ehdotetaan mallia, jossa suurin osa NIS2-direktiivin soveltamisalan toimialoista kuuluisi uuden NIS-yleislain piiriin. Lisäksi toimialakohtaisessa erityissääntelyssä voitaisiin säätää tiukemmista tai tarkemmista velvoitteista ja niiden valvonnasta. Traficom kannattaa esitettyä mallia. Traficom arvioi, että toimijoita koskevat vaatimukset ja niiden valvonta eri säädösten perusteella ovat pääsääntöisesti sovitettavissa yhteen. Traficom pitää siten hyvänä ja välttämättömänä NIS-yleislain 5 §:ssä ehdotettua ratkaisua, jonka mukaan muuta sääntelyä sovelletaan yleislain lisäksi. Esimerkiksi yksi Traficomin tehtäviin ennestään kuuluva ja NIS-yleislakiluonnoksessa ehdotettujen toimialojen sääntelyssä olennainen toimialakohtainen laki on sähköisen viestinnän palveluista annettu laki (jäljempänä SVPL), joka koskee teleyrityksiä ja kaikkien toimialojen yhteisöjä yhteisötilaajan ominaisuudessa, kun ne käsittelevät tietoturvasyistä sähköisen viestintää tai viestinnän välitystietoja. NIS-yleislain lakiluonnoksen 5 §:n sanamuoto tukee sitä, että teleyrityksiä koskevaa sääntelyä, kuten SVPL:ää ja sen nojalla Traficomin antamia määräyksiä, voidaan soveltaa täydentävästi suhteessa NIS-yleislakiin siltä osin kuin edellä mainittu sääntely varmistaa korkeamman kyberturvallisuuden tason.

Tietoturvallisuuden ylläpidossa ja siihen liittyvässä häiriö- ja uhkatiedon käsittelyssä on huomioitava sähköisen viestinnän luottamuksellisuus, josta säädetään perustuslain 10 §:ssä ja SVPL:ssä. Traficom pitää yleisesti ottaen hyvänä ja välttämättömänä NIS-yleislakiluonnoksessa ehdotettuja säännöksiä tiedonkäsittelyn oikeuksista ja käyttötarkoitusten rajoituksista.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintavelvoitetta koskevat huomiot

Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä huomioitavat osa-alueet on NIS-yleislakiluonnoksessa jaoteltu ja kirjoitettu hieman eri sanoin ja tarkemmin kuin NIS2-direktiivin 21 artiklan 2 kohdassa. Traficom pitää lakiluonnoksen ryhmittelyä hyvänä, vakiintuneiden tietotur-vallisuuskäytäntöjen kannalta ymmärrettävänä ja tarkkuustasoltaan tasapainoisena ja aikaa kestävänä. Lakiluonnoksen perustelut kuvaavat ja konkretisoivat vaatimuksia ja tekevät ne ennakoitaviksi ja selkeiksi toimijoille.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoitetta koskevat huomiot

Poikkeamista ilmoittamisen ja ilmoitusten käsittelyn osalta Traficom pitää ehdotettua kolmiportaista ilmoitusmallia selkeänä. On hyvä, että poikkeamailmoitusten toimittamiselle on määritelty selkeät määräajat ja että myös ilmoitusten sisältö on määritelty tarkasti. Traficom pitää perusteltuna esitettyä mallia, jossa poikkeamailmoitukset toimitetaan ensisijaisesti valvovalle viranomaiselle ja valvova viranomainen huolehtii, että ilmoitukset välitetään myös CSIRT-yksikölle. Käytännössä olisi hyvä, että ilmoitusten tekemiseen tarkoitettu palvelu välittäisi ilmoituksen tiedot suoraan CSIRT-yksikölle ilman että valvovan viranomaisen tarvitsisi ilmoitusta erikseen välittää. Ilmoitusten automaattinen siirtyminen CSIRT-yksikölle tulisi varmistaa erityisesti virka-aikojen ulkopuolella.

Traficom kiinnittää kuitenkin huomiota siihen, että NIS-yleislakiehdotuksen 11 §:ssä merkittävä poikkeama määritellään osin eri tavoin kuin 2 §:n 1 kohdan 16 kohdassa poikkeama. Traficom pitäisi perusteltuna, että poikkeama olisi NIS-yleislakiluonnoksen 2 §:n määritelmän mukainen kautta esitysluonnoksen, koska tämä määritelmä kattaa kaikki tietoturvan osa-alueet. NIS-yleislakiehdotuksen 11 §:ssä olisikin hyvä määritellä lähinnä sitä, mitä tarkoitetaan poikkeamailmoitusvelvollisuuden piiriin kuuluvilla, nimenomaisesti merkittävillä poikkeamilla (muiden, ei niin merkittävien poikkeamien jäädessä sääntelyn ulkopuolelle). Sama selvennystarve koskee myös tiedonhallintalakiin sisällytettävää merkittävän poikkeaman määrittelyä 2.1 §:n 25 kohdassa ja sen perusteluissa.

Selvyyden vuoksi Traficom toteaa, että sen valvomassa, voimassa olevassa muussa säädännössä sekä liikenteen että viestinnän sektoreilla on olemassa poikkeamien ilmoitusvelvollisuuksia, jotka jatkossakin perustuvat eri säädöksiin. Esimerkiksi teletoiminnan häiriöiden osalta on Traficomin näkemyksen jatkossakin mahdollista soveltaa Traficomin antaman teletoiminnan häiriötilanteiden koskevan määräyksen mukaisia ilmoitusmääräaikoja siltä osin kuin ne ovat tiukempia suhteessa ehdotettuun lakiin kyberturvallisuuden riskienhallinnasta. Tämä tulkinta olisi linjassa ehdotuksen 5 §:n 1 momentin kanssa.

Traficom pitääkin ehdotetun lain kannalta hyvänä ja tärkeänä, että 11 §:n 5 momentin mukaan valvovalla viranomaisella on mahdollisuus antaa määräystasolla tarkentavaa sääntelyä poikkeamailmoituksiin liittyen. Traficom kiinnittää kuitenkin huomiota siihen, että 11 §:n 5 momentin 2 kohdan mukaan määräystoimivaltuus poikkeamailmoitusten sisällön osalta rajoittuu vain 13 §:ssä tarkoitettuun poikkeaman loppuraporttiin, eikä 11 §:ssä tarkoitettuihin ensi- ja jatkoilmoituksiin. Traficom katsoo olevan tärkeää, että valvova viranomainen voisi tarvittaessa täsmentää myös ensi-ilmoituksessa ja jatkoilmoituksessa toimitettavia tietoja, mikäli tämä olisi tarkoituksenmukaista kyseisen toimialan valvonnan ja valvonnan priorisoinnin kannalta sekä sen varmistamiseksi, että kyseisissä ilmoituksissa toimitetaan kaikki valvovan viranomaisen kannalta olennaiset tiedot.

Lisäksi lakiehdotuksen 17.3 §:ään ja 34.1 §:ään sisältyy säännöksiä henkilötietojen tietoturvaloukkauksesta ilmoittamisesta tietosuojavaltuutetulle. Säännösten suhde jää epäselväksi ja niissä käytetään osin eroavia sanamuotoja. Traficom esittää, että asiasta säädettäisiin vain 34 §:ssä niin, että säännökset yhdistettäisiin.

Valvontaa koskevat huomiot

Määräystoimivaltuuksia koskevat huomiot

Valvovilla viranomaisilla olisi NIS-yleislakiluonnoksen perustella mahdollisuus tarkentaa lain velvoitteita teknisillä määräyksillä toimialakohtaiset erityispiirteet huomioiden, mitä Traficom pitää erittäin hyvänä, jotta sektorikohtaisia ominaispiirteitä ja alati muuttuvia teknisiä yksityiskohtia koskevia asioita voidaan joustavasti huomioida.

Traficom yhtyy perustuslakiperustelujen arvioon teknisten määräysvaltuuksien luonteesta. Teknologianeutraalius määräystenannossa merkitsee sitä, ettei määräyksillä tule edellyttää jonkin tietyn teknologian käyttöönottoa, jos käytettävissä on erilaisia vastaavan turvallisuuden toteutuksen mahdollistavia ratkaisuja. Määräyksillä tulee kuitenkin voida tarkentaa esimerkiksi tietyn teknologian käyttötapaa tai hallintatoimenpiteitä. Traficom tuo lisäksi esille sen, että määräyksillä voi olla välillistä vaikutusta myös elinkeinovapauden kannalta, sillä teknisillä määräyksillä voidaan edistää sääntelyn ennakoitavuutta toimijoille ja turvata kilpailun tasapuolisuutta, kun mahdollisia investointeja edellyttävä vaatimusten vähimmäistaso on selkeä.

Määräystoimivaltuuksien kattavuuden osalta Traficom kiinnittää huomiota siihen, että NIS-yleislakiluonnoksen 9 §:n 4 momentin mukaiset valvovan viranomaisen määräystoimivaltuudet eivät kata 2 momentin 4 kohdassa tarkoitettua toimitusketjujen turvallisuutta ja 2 momentin 3 kohdassa tarkoitettua hankintojen turvallisuutta. Traficom katsoo, että valvovan viranomaisen määräystoimivaltuuksien tulisi kattaa myös nämä velvoitteet. NIS-yleislakiluonnoksen soveltamisalan piiriin kuuluvien toimijoiden osalta olisi perusteltua, että valvova viranomainen voisi tarvittaessa määräystasolla täsmentää esimerkiksi, miten toimitusketjujen turvallisuuden hallintaan liittyvää

riskinarviointia tulisi tehdä, miten turvallisia hankintoja tulisi tehdä ja millaisia seikkoja toimijoiden tulisi tällaisessa riskinarvioinnissa ottaa huomioon.

Valvontaa koskevat huomiot

Asianosaisasema ja valvontatoiminnan priorisointi

Traficom pitää hyvänä, että NIS-yleislakiluonnoksen 26 §:ssä käsitellään NIS2-direktiivin mukaisesti valvovan viranomaisen oikeutta priorisoida valvontatehtäviään valvontatoiminnan ja -resurssien tarkoituksenmukaiseksi kohdentamiseksi. Traficom pitäisi kuitenkin vielä tarpeellisena selventää NIS-yleislakiluonnoksen perusteluissa, että onko sääntelyn piirissä olevien toimijoiden tarjoamien palveluiden käyttäjiä tai asiakkaita pidettävä valvonta-asiassa asianosaisina, joilla olisi oikeus saada asiansa käsitellyksi valvontaviranomaisessa sekä valituskelpoinen päätös.

Traficomin näkemyksen mukaan jää siis epäselväksi, mahdollistaisiko 26 §:ssä tarkoitettu priorisointimahdollisuus kansalaisten tekemien ilmiantojen tai toimenpidepyyntöjen käsittelemättä jättämisen. On epäselvää, pidettäisiinkö esimerkiksi toimijoiden asiakkaina olevia henkilöitä, joihin poikkeama tai väitetysti puutteelliset riskienhallinnan toimenpiteet jollakin tavalla voisivat mahdollisesti vaikuttaa, sellaisina asianosaisina, joilla olisi oikeus saada asiansa käsitellyksi valvontaviranomaisessa ja valituskelpoinen päätös, jossa asia sisällöllisesti tutkitaan ja ratkaistaan. Ehdotuksen 26 §:n mukaan valvova viranomainen voisi jättää asian tutkimatta, jos kyse on ilmeisen perusteettomasta pyynnöstä, mikä näyttää viittaavan siihen, että tällainen vireillepano-oikeus olisi luonnoksessa tarkoitettu olevan olemassa. Traficomin näkemyksen mukaan lakiluonnoksessa tulisi lähteä siitä, että yksittäisille kansalaisille tai muille toimijoiden palveluiden käyttäjille ei synny oikeutta saada sisällöllistä asiaratkaisua mahdollisesti esittämiinsä vaatimuksiin sen johdosta, ettei tällaista tahoa ole pidettävä asianosaisena asiassa, joka koskee toimijan valvontaa ehdotetun lain puitteissa. On perusteltua katsoa, etteivät kyberturvallisuuden riskienhallintavelvoite ja poikkeamia koskeva ilmoitusvelvollisuus taikka niiden väitetty rikkominen koske sillä tavoin suoranaisesti toimijan asiakkaan tai muun sivullisen henkilön oikeutta, etua tai velvollisuutta, että se perustaisi tälle asianosaisaseman ja oikeuden saada asia käsitellyksi sisällöllisesti. Tämä myös osaltaan tukisi valvontatoiminnan priorisointia. Myöskään NIS2-direktiivistä ei voida päätellä, että tällaisen oikeuden antaminen olisi ollut eurooppalaisen lainsäätäjän tarkoitus, toisin kuin esimerkiksi yleisessä tietosuoja-asetuksessa, jonka 79 artiklassa tällainen oikeus nimenomaisesti säädetään. Tämän johdosta Traficom esittää, että vähintään 26 §:n perusteluissa todettaisiin tämä seikka ja tällöin 26 §:n viimeinen momentti voitaisiin poistaa, jottei se anna harhaanjohtavaa käsitystä vireillepano-oikeudesta.

Toimijarekisteri ja sen julkisuus

Traficom toteaa, että toimijoiden velvollisuus ilmoittautua valvovan viranomaisen luetteloon helpottaa olennaisesti viranomaisen toimintaa NIS1-direktiiviin nähden. Toimialan toimijoiden kartoittamistoimien sijaan viranomainen voi käyttää resurssit vaikuttavaan ydintehtäväänsä eli kyberturvallisuuden ohjaukseen ja valvontaan.

NIS-yleislakiluonnoksen 43.4 §:n viittaukset NIS2-direktiiviin nojalla komissiolle, Enisalle ja yhteistyöryhmälle ilmoitettavista tiedoista tuovat Traficomin käsityksen mukaan välillisesti esille sen, että toimijarekisterin ei ole tarkoitus olla julkinen siitä huolimatta, että yritysten toimialatiedot ja tilinpäätöstiedot kaupparekisterissä ovat julkisia ja tiedonhallintalain tarkoittamista tiedonhallintayksiköistä säädetään lailla. Valvovan viranomaisen tulee arvioida tehtävässään saamansa tiedon yleisöjulkisuus tai salassapitotarve julkisuuslain nojalla ja yhteiskunnan kriittisiä yksityisiä ja julkishallinnon toimijoita koskevaa tietomassaa ja sen osittaisjulkisuuttakin tullee arvioida mm. varautumisen valossa. Traficom ehdottaa harkittavaksi sääntelyn tai perustelujen täydentämistä tältä osin, jotta viranomaisten käytännöt muodostuisivat yhdenmukaisiksi. Asiassa voi harkita esimerkiksi toimijaluettelon tietojen automaattista luovutusta CSIRTille 43 §:ssä, sillä tämä tukisi CSIRT-yksikön tehtävien hoitamista ehdotettavan sääntelyn puitteissa.

Traficom arvioi, että julkisuuslain vahinkoedellytyslausekkeiden mahdollistaman harkinnan perusteella toimijarekisterissä olevat tiedot ovat salassapitoperusteen suojaamaa intressiä vaarantamatta luovutettavissa CSIRT-yksikölle ja että esimerkiksi IP-osoitetiedot ovat tarpeellisia CSIRT-yksikön tehtävissä. Luovutusoikeuden voi harkita selkeytettäväksi laissa tai sen perusteluissa -suhteessa yleislain 27 § 2

Tarkastukset ja skannaukset valvovan viranomaisen selvitysmenettelynä

NIS2-direktiivin 32(2) d-kohdan edellyttämä valvovan viranomaisen toimivalta tehdä turvallisuusskannauksia on sisällytetty NIS-yleislakiluonnoksen 29 §:ään ja tiedonhallintalain 18 j §:ään yhtenä tarkastustoimivaltaan sisältyvänä menettelytapana. Tämä ilmenee selkeimmin tiedonhallintalain perusteluissa, missä todetaan, että tarkastus voitaisiin tehdä paikan päällä tai muualla kuin paikan päällä ja tar-kastukseen voisi sisältyä turvallisuusskannauksia. Traficom arvioi, että esitysluonnos mahdollistaa tältä osinkin kyberturvallisuuden valvonnassa ja NIS2-direktiivissä edellytetyt turvallisuusskannaukset tarvittaessa.

Traficom haluaa kuitenkin kiinnittää tarkastustoiminnan osalta huomiota siihen, että vaikka osa turvallisuusskannaukseksi katsottavasta toiminnasta voi tapahtua tarkastusten yhteydessä toimijan sijaintipaikassa, internetin välityksellä tapahtuvaa skannausta ei voitaisi pitää hallintolain 39 §:ssä tarkoitettuna tarkastuksena, mikäli sen tulkitaan tarkoittavan vain paikan päällä tehtävää tarkastusta. Traficom kiinnittää huomiota myös siihen, että hallintolain 39 §:n vaatimuksia esim. asianosaisen läsnäolo-oikeuden osalta on käytännössä hankalaa soveltaa muutoin kuin paikan päällä tehtävään tarkastukseen. Tämän johdosta turvallisuusskannauksista voisi olla syytä säätää erikseen tai vähintään selvemmin erillisellä momentilla. Riippumatta siitä, miten asia ratkaistaan

jatkovalmistelussa, Traficom katsoo tärkeäksi, että NIS-yleislaki ja tiedonhallintalaki perusteluineen yhdenmukaistettaisiin tältä osin.

Arviointilaitosten tai muiden auditoijien käyttäminen

Traficom pitää hyvänä ja tärkeänä selvennyksenä, että tietoturvallisuuden arviointilaitokselta tarvittavan pätevyyden arviointiin otetaan kantaa NIS-yleislakiluonnoksessa, koska asiaan liittyy oikeudellinen kysymys tietoturvallisuuden arviointilaitoksista annetun lain soveltamisesta. Traficom katsoo, että asia olisi tarpeen mainita perustelujen lisäksi myös säännöstasolla esimerkiksi säätämällä, että valvova viranomainen päättää tehtävässä tarvittavasta pätevyydestä ja käytettävistä arviointiperusteista. Arviointilaitoslain nojalla on tällä hetkellä akkreditoitu (FINAS) ja hyväksytty (Traficom) pätevyyksiä ISO27001 mukaiseen sertifiointiin ja Tietoturvallisuuden auditointityökalu viranomaisille Katakrin mukaiseen arviointiin, mutta valvontatehtävissä on usein tarpeen soveltaa esimerkiksi muuta viranomaisen määräystä, ohjetta tai suositusta, komission säädöstä tai toimialalla käytössä olevaa kriteeristöä. Akkreditoidun pätevyyden arvioinnissa toimeksiantoa tehtäessä viranomaisen on olennaista ottaa huomioon esimerkiksi se, onko arviointilaitoksella tosiasiallinen pätevyys tekniseen todentamiseen ja testaamiseen.

Luonnollisesti viranomaisen on varmistettava toimeksisaajan kyvykkyys myös hankittaessa apua muulta kuin tietoturvallisuuden arviointilaitokselta, mutta näihin muihin toimijoihin ei liity erityissääntelyä pätevyyden akkreditoinnista, hyväksynnästä ja itsenäisestä julkisesta hallintotehtävästä, johon avustava tehtävä täytyy sovittaa.

Lisäksi Traficom ehdottaa NIS-yleislakiluonnoksen 29 §:n perusteluissa todettavaksi, että avun hankkimisen tai pyytämisen syynä voi olla erityisosaamisen tarpeen ohella myös resurssien puute.

Tiedonkäsittely- ja vaihto-oikeuksia koskevat huomiot

Traficom toteaa, että lakiluonnoksessa huomioidaan tarpeellisella tavalla eri tietotyyppien sääntelytausta ja niiden suojaustarpeet; julkisuuslain valossa salassa pidettävät tiedot, turvallisuusluokitteluasetuksen tai kansainvälisen tietoturvallisuus-velvoitteen nojalla turvallisuusluokitellut tai erityissuojattavat tiedot ja kyberturvallisuuden ylläpidon kannalta erityisen merkitykselliset ja välttämättömät perustuslain sähköisen luottamuksellisen viestinnän suojan piiriin kuuluvat tiedot.

Valvovan viranomaisen tiedonsaantioikeuksien ja tietojen luovuttamista koskevien oikeuksien osalta Traficom näkisi tarpeelliseksi yhdenmukaistaa lakiehdotuksen 27 ja 28 §:n sisältöä niin, että valvovalla viranomaisella olisi myös 28 §:ssä tarkoitettujen tietojen osalta oikeus luovuttaa

kyseisessä pykälässä tarkoitetut tiedot toiselle valvovalle viranomaiselle tai CSIRT-yksikölle, jos tietojen luovuttaminen olisi näiden tehtävien hoitamisen kannalta välttämätöntä.

Rajat ylittävät avunpyynnöt

Toisen valtion valvontaviranomaisten avustaminen on huomioitu NIS-yleislakiluonnoksen 6.4 §:ssä, kun Suomelta pyydetään apua. Tämä olisi hyvä huomioida myös NIS-yleislakiluonnoksen 29 §:ssä, jossa todetaan mahdollisuus pyytää apua toiselta viranomaiselta. Toisen valtion viranomaiselle tehdyssä pyynnössä pyynnön kohteeseen ei sovelleta säännöksen perusteluissa mainittua hallintolain 10 §:ää, vaan direktiivin 37 artiklan täytäntöönpanevaa velvoittavaa säännöstä kohdevaltiossa. Lisäksi tulisi olla selvää, että valvova viranomainen voi pyytää toisen jäsenvaltion valvovan viranomaisen apua myös tietojen pyytämisessä valvontamenettelyn kohteena olevalta toimijalta, jolloin avun pyytämistä ja antamista valvontamenettelyssä ei tulisi tarkastella vain 29 §:n mukaisen tarkastuksen kontekstissa.

Oikaisumenettelyn soveltuvuus valvontamenettelyyn

Traficom katsoo, että oikaisuvaatimusmenettely soveltuu huonosti valvontamenettelyssä annettaviin NIS-yleislakiluonnoksen 31-33 §:n mukaisiin päätöksiin. Sama huomio koskee myös tiedonhallintalakiin ehdotettavaa 18 m §:ää. Oikaisuvaatimusmenettelyn käyttäminen olisi ongelmallista erityisesti tapauksissa, joissa sovelletaan NIS-yleislakiluonnoksen lisäksi jotain muuta sääntelyä, kuten esimerkiksi teletoiminnan kohdalla SVPL:ää ja Traficomin määräyksiä. Oikaisuvaatimusmenettelyn soveltaminen vain NIS-yleislakiluonnoksen nojalla tehtäviin päätöksiin johtaisi siihen, että jos samalla valvontapäätöksellä ratkaistaisiin asia myös jonkin toisen lain nojalla - kuten sovellettaessa erityislaissa säädettyjä tietoturvavelvoitteita - johtaisi tämä siihen, että samaankin päätökseen sovellettaisiin yhtä aikaa erilaisia oikaisu- tai muutoksenhakumenettelyitä sen mukaan, mihin lakiin kukin asetettu velvoite tai todettu rikkominen perustuisi. Tämä johtaisi käytännössä erittäin epätarkoituksenmukaisiin ja oikeudellisesti epäselviin tilanteisiin, kun päätöksen kohteen olisi haettava samasta päätöksestä yhtäaikaisesti oikaisua ja valitettava hallinto-oikeuteen erillisillä hakemuksilla, mikä ainoastaan lisäisi hallinnollista taakkaa.

Lisäksi Traficomin näkemys on, että valvontamenettelyssä tehtävät päätökset tulisivat, samoin kuin nykyisten valvontatoimivaltuuksien kohdalla, perustumaan perusteelliseen selvitykseen ja menettelyyn, johon kuuluu myös asianosaisten kuuleminen. Kun valvontapäätös annetaan tällaisen perusteellisen selvittämisen ja kuulemisen jälkeen, ei ole oletettavaa, että päätöstä enää muutettaisiin oikaisuvaatimuksen perusteella, minkä johdosta oikaisuvaatimus muodostuisi muutoksenhakuprosessin osalta turhaksi välivaiheeksi ennen hallinto-oikeuden käsittelyä.

Seuraamusmaksua koskevat huomiot

Seuraamusmaksulautakunta

NIS-yleislain 5 luvussa säädetään seuraamusmaksusta. Seuraamusmaksun määräisi seuraamusmaksulautakunta valvovan viranomaisen esityksestä. Seuraamusmaksulautakunnan puheenjohtajan ja varapuheenjohtajan nimeäisi Liikenne- ja viestintävirasto. Lautakunnan puheenjohtajalla ja varapuheenjohtajalla tulee olla tehtävän edellyttämä riittävä oikeudellinen asiantuntemus. Seuraamusmaksulautakunta olisi uusi elin ja Traficomille täysin uusi tehtäväkokonaisuus. Traficom toteaa, että mm. yhtenäisen seuraamusmaksujen määräämiskäytännön vuoksi seuraamusmaksulautakunta on perusteltu, mutta sen resursointi tulee olemaan haastavaa.

CSIRT-yksikön tehtäviä koskevat huomiot

Toimijarekisteri ja sen julkisuus

Traficom toteaa, että toimijoiden velvollisuus ilmoittautua valvovan viranomaisen luetteloon helpottaa olennaisesti viranomaisen toimintaa NIS1-direktiiviin nähden. Toimialan toimijoiden kartoittamistoimien sijaan viranomainen voi käyttää resurssit vaikuttavaan ydintehtäväänsä eli kyberturvallisuuden ohjaukseen ja valvontaan.

NIS-yleislakiluonnoksen 43.4 §:n viittaukset NIS2-direktiiviin nojalla komissiolle, Enisalle ja yhteistyöryhmälle ilmoitettavista tiedoista tuovat Traficomin käsityksen mukaan välillisesti esille sen, että toimijarekisterin ei ole tarkoitus olla julkinen siitä huolimatta, että yritysten toimialatiedot ja tilinpäätöstiedot kaupparekisterissä ovat julkisia ja tiedonhallintalain tarkoittamista tiedonhallintayksiköistä säädetään lailla. Valvovan viranomaisen tulee arvioida tehtävässään saamansa tiedon yleisöjulkisuus tai salassapitotarve julkisuuslain nojalla ja yhteiskunnan kriittisiä yksityisiä ja julkishallinnon toimijoita koskevaa tietomassaa ja sen osittaisjulkisuuttakin tullee arvioida mm. varautumisen valossa. Traficom ehdottaa harkittavaksi sääntelyn tai perustelujen täydentämistä tältä osin, jotta viranomaisten käytännöt muodostuisi-vat yhdenmukaisiksi. Asiassa voi harkita esimerkiksi toimijaluettelon tietojen automaattista luovutusta CSIRTille 43 §:ssä, sillä tämä tukisi CSIRT-yksikön tehtävien hoitamista ehdotettavan sääntelyn puitteissa.

Traficom arvioi, että julkisuuslain vahinkoedellytyslausekkeiden mahdollistaman harkinnan perusteella toimijarekisterissä olevat tiedot ovat salassapitoperusteen suojaamaa intressiä vaarantamatta luovutettavissa CSIRT-yksikölle ja että esimerkiksi IP-osoitetiedot ovat tarpeellisia CSIRT-yksikön tehtävissä. Luovutusoikeuden voi harkita selkeytettäväksi laissa tai sen perusteluissa - suhteessa yleislain 27 § 2

CSIRT-yksikön tehtäviä koskevat huomiot

Traficom pitää kannatettavana CSIRT-yksikön tehtävistä, toimivaltuuksista ja tiedonkäsittelyoikeuksista säänteleмistä NIS-yleislakiluonnoksessa omassa 3 luvussaan. Erillisessä luvussa säädettävät tehtävät ja tietojenkäsittelyoikeudet selkeyttävät CSIRT-yksikön asemaa kansallisena tietoturvaviranomaisena.

CSIRT-yksikön itsenäinen ja luottamuksellinen asema ovat tärkeitä, jotta CSIRT voi palvella yhteiskuntaa ja NIS-direktiivissä tarkoitettuja toimijoita mahdollisimman kattavasti ja tuloksellisesti. Tästä näkökulmasta Traficom pitää erityisen hyvänä, että CSIRT-yksikölle säädettäisiin kyberturvallisuuden riskienhallinnasta annetun lain 19 §:ssä itsenäinen asema suhteessa valvoviin viranomaisiin. Samasta syystä Traficom kannattaa lain 24 §:ssä säädettyä ns. käyttötarkoituspalomuuria, joka rajaisi CSIRT-yksikölle vapaaehtoisesti tehtyjen tietoturvaloukkausilmoitusten ja niissä CSIRT-yksikölle luovutettujen tietojen käyttämistä tiedon luovuttanutta koskevassa rikostutkinnassa sekä hallinnollisessa päätöksenteossa.

Itsenäisestä asemasta seuraava luottamus CSIRT-toiminnan riippumattomuuteen ja esitysluonnokseen laadittu palomuurisäännös mahdollistavat sen, että CSIRT-yksikkö saa jatkossakin vapaaehtoisuuteen perustuvia ilmoituksia laajasti eri toimi-joilta suomalaisessa yhteiskunnassa. Tämä on edellytys kyberturvallisuuden kansallisen tilannekuvan muodostamiselle, joka taas mahdollistaa sen, että CSIRT-yksikkö voi luovuttaa relevantteja kyberturvallisuuteen liittyviä uhkatietoja suomalaisille organisaatioille ehdotetun 22 §:n mukaisten kyberturvallisuustietojen vapaaehtoisten jakamisjärjestelyjen puitteissa. Traficomin näkemyksen mukaan ehdotetut säännökset CSIRT-yksikön luottamuksellisesta asemasta parantaisivat kyberturval-lisuuteen liittyvien uhkatietojen jakamista esimerkiksi suomalaisille huoltovarmuuskriittisille organisaatioille, jotta nämä voisivat parhaalla mahdollisella tavalla suojautua kyberuhkilta ja poikkeamilta.

Traficomin toteaa, että NIS-yleislakiluonnoksen 43 §:n mukaisen toimijaluettelon tiedot, etenkin sen 1 momentin a-c kohtien mukaiset toimijoiden nimet, yhteystiedot ja IP-osoitealueet olisivat hyödyllisiä CSIRT-yksikön 19 §:ssä säädettyjen tehtävien tehokkaan hoitamisen kannalta. Näin ollen Traficom ehdottaa 43 §:n täydentämistä esimerkiksi 17.1 §:n kanssa vastaavalla tavalla, eli velvoittamalla valvovat viranomaiset automaattisesti toimittamaan toimijaluettelon tiedot CSIRT-yksikölle. Traficom ehdottaa vastaavaa lisäystä ehdotetun tiedonhallintalain 4 a luvun 18 a §:ään.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Suhde CER-direktiiviin

Kuten esitysluonnoksessa todetaan, esityksellä on yhteys kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiivin (nk. CER-direktiivi, (EU) (2022/2557) kansallista täytäntöönpanoa koskevaan säädöshankkeeseen (SM047:00/2022) ja hankkeessa valmisteltavaan hallituksen esitykseen. CER-direktiivin täytäntöönpanosta vastaa sisäministeriö.

Keskeisin liittymäkohta NIS2-ja CER-direktiivien välillä käy ilmi NIS-yleislain 26 §:stä, jonka 2 momentin d-kohdan mukaan keskeisenä toimijana pidetään toimi-jaa, joka on CER-direktiivin nojalla määritelty kriittiseksi. CER-direktiivi on otettu huomioon myös NIS-yleislakiluonnoksen 2, 3, 17, 27 ja 46 §:ssä sekä tiedonhallintalain 3 §:ssä. Traficom pitää tätä hyvänä ja toteaa, että NIS2- ja CER-hankkeiden säädösten yhteensopivuudesta tulee huolehtia molempien jatkovalmistelussa.

Raportointivelvoitetta koskevat huomiot

Traficom kiinnittää kuitenkin huomiota siihen, että NIS-yleislakiehdotuksen 11 §:ssä merkittävä poikkeama määritellään osin eri tavoin kuin 2 §:n 1 kohdan 16 kohdassa poikkeama. Traficom pitäisi perusteltuna, että poikkeama olisi NIS-yleislakiluonnoksen 2 §:n määritelmän mukainen kautta esitysluonnoksen, koska tämä määritelmä kattaa kaikki tietoturvan osa-alueet. NIS-yleislakiehdotuksen 11 §:ssä olisikin hyvä määritellä lähinnä sitä, mitä tarkoitetaan poikkeamailmoitusvelvollisuuden piiriin kuuluvilla, nimenomaisesti merkittävillä poikkeamilla (muiden, ei niin merkittävien poikkeamien jäädessä sääntelyn ulkopuolelle). Sama selvennystarve koskee myös tiedonhallintalakiin sisällytettävää merkittävän poikkeaman määrittelyä 2.1 §:n 25 kohdassa ja sen perusteluissa.

Toimijarekisteri ja sen julkisuus

Traficom toteaa, että toimijoiden velvollisuus ilmoittautua valvovan viranomaisen luetteloon helpottaa olennaisesti viranomaisen toimintaa NIS1-direktiiviin nähden. Toimialan toimijoiden kartoittamistoimien sijaan viranomainen voi käyttää resurssit vaikuttavaan ydintehtäväänsä eli kyberturvallisuuden ohjaukseen ja valvontaan.

NIS-yleislakiluonnoksen 43.4 §:n viittaukset NIS2-direktiiviin nojalla komissiolle, Enisalle ja yhteistyöryhmälle ilmoitettavista tiedoista tuovat Traficomin käsityksen mukaan välillisesti esille sen, että toimijarekisterin ei ole tarkoitus olla julkinen siitä huolimatta, että yritysten toimialatiedot ja tilinpäätöstiedot kaupparekisterissä ovat julkisia ja tiedonhallintalain tarkoittamista tiedonhallintayksiköistä säädetään lailla. Valvovan viranomaisen tulee arvioida tehtävässään saamansa tiedon yleisöjulkisuus tai salassapitotarve julkisuuslain nojalla ja yhteiskunnan kriittisiä yksityisiä ja julkishallinnon toimijoita koskevaa tietomassaa ja sen osittaisjulkisuuttakin tullee arvioida mm. varautumisen valossa. Traficom ehdottaa harkittavaksi sääntelyn tai perustelujen täydentämistä tältä osin, jotta viranomaisten käytännöt muodostuisivat yhdenmukaisiksi. Asiassa voi harkita esimerkiksi toimijaluettelon tietojen automaattista luovutusta CSIRTille 43 §:ssä, sillä tämä tukisi CSIRT-yksikön tehtävien hoitamista ehdotettavan sääntelyn puitteissa.

Traficom arvioi, että julkisuuslain vahinkoedellytyslausekkeiden mahdollistaman harkinnan perusteella toimijarekisterissä olevat tiedot ovat salassapitoperusteen suojaamaa intressiä vaarantamatta luovutettavissa CSIRT-yksikölle ja että esimerkiksi IP-osoitetiedot ovat tarpeellisia CSIRT-yksikön tehtävissä. Luovutusoikeuden voi harkita selkeytettäväksi laissa tai sen perusteluissa - suhteessa yleislain 27 § 2

Tarkastukset ja skannaukset valvovan viranomaisen selvitysmenettelynä

NIS2-direktiivin 32(2) d-kohdan edellyttämä valvovan viranomaisen toimivalta tehdä turvallisuusskannauksia on sisällytetty NIS-yleislakiluonnoksen 29 §:ään ja tiedonhallintalain 18 j §:ään yhtenä tarkastustoimivaltaan sisältyvänä menettelytapana. Tämä ilmenee selkeimmin tiedonhallintalain perusteluissa, missä todetaan, että tarkastus voitaisiin tehdä paikan päällä tai muualla kuin paikan päällä ja tarkastukseen voisi sisältyä turvallisuusskannauksia. Traficom arvioi, että esitysluonnos mahdollistaa tältä osinkin kyberturvallisuuden valvonnassa ja NIS2-direktiivissä edellytetyt turvallisuusskannaukset tarvittaessa.

Traficom haluaa kuitenkin kiinnittää tarkastustoiminnan osalta huomiota siihen, että vaikka osa turvallisuusskannaukseksi katsottavasta toiminnasta voi tapahtua tarkastusten yhteydessä toimijan sijaintipaikassa, internetin välityksellä tapahtuvaa skannausta ei voitaisi pitää hallintolain 39 §:ssä tarkoitettuna tarkastuksena, mikäli sen tulkitaan tarkoittavan vain paikan päällä tehtävää tarkastusta. Traficom kiinnittää huomiota myös siihen, että hallintolain 39 §:n vaatimuksia esim. asianosaisen läsnäolo-oikeuden osalta on käytännössä hankalaa soveltaa muutoin kuin paikan päällä tehtävään tarkastukseen. Tämän johdosta turvallisuusskannauksista voisi olla syytä säätää erikseen tai vähintään selvemmin erillisellä momentilla. Riippumatta siitä, miten asia ratkaistaan jatkovalmistelussa, Traficom katsoo tärkeäksi, että NIS-yleislaki ja tiedonhallintalaki perusteluineen yhdenmukaistettaisiin tältä osin.

Oikaisumenettelyn soveltuvuus valvontamenettelyyn

Traficom katsoo, että oikaisuvaatimusmenettely soveltuu huonosti valvontamenettelyssä annettaviin NIS-yleislakiluonnoksen 31-33 §:n mukaisiin päätöksiin. Sama huomio koskee myös tiedonhallintalakiin ehdotettavaa 18 m §:ää. Oikaisuvaatimusmenettelyn käyttäminen olisi ongelmallista erityisesti tapauksissa, joissa sovelletaan NIS-yleislakiluonnoksen lisäksi jotain muuta sääntelyä, kuten esimerkiksi teletoiminnan kohdalla SVPL:ää ja Traficomin määräyksiä. Oikaisuvaatimusmenettelyn soveltaminen vain NIS-yleislakiluonnoksen nojalla tehtäviin päätöksiin johtaisi siihen, että jos samalla valvontapäätöksellä ratkaistaisiin asia myös jonkin toisen lain nojalla - kuten sovellettaessa erityislaissa säädettyjä tietoturvavelvoitteita - johtaisi tämä siihen, että samaankin päätökseen sovellettaisiin yhtä aikaa erilaisia oikaisu- tai muutoksenhakumenettelyitä sen mukaan, mihin lakiin kukin asetettu velvoite tai todettu rikkominen perustuisi. Tämä johtaisi käytännössä erittäin epätarkoituksenmukaisiin ja oikeudellisesti epäselviin tilanteisiin, kun

päätöksen kohteen olisi haettava samasta päätöksestä yhtäaikaisesti oikaisua ja valitettava hallinto-oikeuteen erillisillä hakemuksilla, mikä ainoastaan lisäisi hallinnollista taakkaa.

Lisäksi Traficomin näkemys on, että valvontamenettelyssä tehtävät päätökset tulisivat, samoin kuin nykyisten valvontatoimivaltuuksien kohdalla, perustumaan perusteelliseen selvitykseen ja menettelyyn, johon kuuluu myös asianosaisten kuuleminen. Kun valvontapäätös annetaan tällaisen perusteellisen selvittämisen ja kuulemisen jälkeen, ei ole oletettavaa, että päätöstä enää muutettaisiin oikaisuvaatimuksen perusteella, minkä johdosta oikaisuvaatimus muodostuisi muutoksenhakuprosessin osalta turhaksi välivaiheeksi ennen hallinto-oikeuden käsittelyä.

CSIRT-yksikön tehtäviä koskevat huomiot

Traficomin toteaa, että NIS-yleislakiluonnoksen 43 §:n mukaisen toimijaluettelon tiedot, etenkin sen 1 momentin a-c kohtien mukaiset toimijoiden nimet, yhteystiedot ja IP-osoitealueet olisivat hyödyllisiä CSIRT-yksikön 19 §:ssä säädettyjen tehtävien tehokkaan hoitamisen kannalta. Näin ollen Traficom ehdottaa 43 §:n täydentämistä esimerkiksi 17.1 §:n kanssa vastaavalla tavalla, eli velvoittamalla valvovat viranomaiset automaattisesti toimittamaan toimijaluettelon tiedot CSIRT-yksikölle. Traficom ehdottaa vastaavaa lisäystä ehdotetun tiedonhallintalain 4 a luvun 18 a §:ään.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

NIS-yleislain ja tiedonhallintalain suhde

Traficom toteaa, että tiedonhallintalain muutosluonnoksessa on tunnistettu hyvin se, että tiedonhallintalain yleiset tietoturvallisuusvelvoitteet ja ehdotetut kyberturvallisuusriskien hallintavelvoitteista syntyvät tietoturvallisuusvaatimukset ovat osittain päällekkäisiä. Osittainen päällekkäisyys koskee myös tiedonhallintayksikön dokumentointivelvoitteiden ja tiedonhallintalautakunnan edistämistehtävän sekä Traficomille ehdotetun valvontatehtävän alaa.

Traficom arvioi, että tiedonhallintalain muutosluonnoksen mukainen sääntely mahdollistaa tiedonhallintayksiköiden ja niiden kyberturvallisuuden kannalta tarkoituksenmukaisen toteutusmallin, jossa lain 4 luvun edellyttämiä tiedonhallintamalliin sisällytettäviä yleisiä tietoturvallisuustoimenpiteitä voidaan täydentää ehdotetun 4 a luvun edellyttämillä riskinhallintatoimenpiteillä ja tiedonhallintayksikkö voi itse harkita kokonaisuuden suunnittelu- ja dokumentointirakenteen. Traficom yhtyy tiedonhallintalain muutosluonnoksen perusteluiden toteamukseen Tiedonhallintalautakunnan ja Traficomin yhteistyön tarpeesta, joka koskee erityisesti lautakunnan suosituksia 4 luvusta ja Traficomin toimivaltaisena viranomaisena laatimaa ennakoivaa ohjeistusta tai suosituksia 4 a luvusta.

Traficomin vakiintuneena ja johdonmukaisena toimintaa ohjaavana periaatteena on aina pyrkiä valvontatarpeen odottamisen sijaan antamaan ennakoivaa ohjausta ja neuvontaa ja organisoida yhteistyötä. Valvontatehtävien ja toimivaltuuksien selkeyden kannalta Traficom kiinnittää kuitenkin huomiota siihen, että Traficomin valvontatoimivallasta eivät voi rajautua ulos perustason toimenpiteet, joiden voidaan katsoa sisältyvän sekä 4 luvun tietoturvatoimenpiteisiin että 4 a luvun riskinhallintatoimenpiteisiin, sillä tämä vesittäisi käytännössä valvontatoimivallan olennaisen aineellisen alan ja aiheuttaisi myös tarpeettomia tulkinta- ja rajanvetokysymyksiä.

Tiedonhallintalaki CSIRT-yksikön näkökulmasta

Traficom ehdottaa CSIRT-yksikön ja valvovan viranomaisen erottamista säännöstasolla tiedonhallintalain muutosluonnoksen 4 a luvussa. Traficomin näkemyksen mukaan uuden 4 a luvun sääntelytapa, jossa viitataan pelkästään Liikenne- ja viestintävirastoon, eikä sen rooliin CSIRT-yksikkönä tai valvovana viranomaisena, tekee CSIRT-yksikön aseman tiedonhallintalain kokonaisuudessa monitulkintaiseksi ja vaikeasti hahmotettavaksi. Sääntelytapa ei myöskään vastaa NIS-yleislakiluonnoksen sääntelyä, jossa valvovat viranomaiset ja CSIRT-yksikkö nimenomaisesti erotetaan toisistaan säännöstasolla. Esimerkiksi tiedonhallintalain ehdotetun 18 f §:n mukaiset vapaaehtoiset ilmoitukset tehtäisiin yleisesti Liikenne- ja viestintävirastolle, jolla pykälän perustelujen mukaan tarkoitettaisiin Traficomia sen molemmissa edellä mainituissa rooleissa. CSIRT-yksikön ja valvovan viranomaisen tehtävät sekoittuvat ehdotetuissa säännöksissä ongelmallisella tavalla myös ainakin 18 a §:n 2 momentissa, 18 d §:ssä, 18 e §:ssä, 18 g §:n 3 momentissa, 18 i §:ssä ja 18 j §:ssä.

Liikenne- ja viestintävirasto korostaa lisäksi, että NIS2-direktiivin mukaista valvontatoimintaa ei tulisi sitoa nykyiseen SVPL:n mukaiseen valvontatoimintaan. Traficomin näkemyksen mukaan 18 i §:n mukaisista valvovan viranomaisen tiedonsaanti- ja tiedonkäsittelyoikeuksista tulisi säännellä NIS-yleislaissa ja tiedonhallintalain 4 a luvussa ja siten välttää viittauksia SVPL:ään. Tästä johtuen Traficom ehdottaa joko poistamaan 18 i §:n 2 momentin viittaukset SVPL:n säännöksiin tai korvaamaan ne viittauksilla NIS-yleislakiluonnoksen relevantteihin säännöksiin.

Tiedonhallintalain 18 §:n turvallisuusluokitteluvelvollisuuden laajentaminen

Tiedonhallintalain muutosluonnoksessa 18 §:n mukaista velvollisuutta tiedon turvallisuusluokitteluun laajennetaan Suomen Erillisverkot Oy:öön, kun se hoitaa turvallisuusverkkolain mukaisia julkisia hallintotehtäviä.

Traficom on tulkinnut nykyisen tiedonhallintalain 18 §:n koskevan myös Suomen Erillisverkot Oy:tä ja hyväksyttyjä tietoturvallisuuden arviointilaitoksia niiden laissa säädetyissä julkisissa

hallintotehtävissä. Traficom toteaa muuotsluonnoksessa todetun tiedonhallintalain 18.1 §:n tyhjentävän soveltamisalan vuoksi, että Suomen Erillisverkot Oy:n velvoitteiden osalta tulisi huomioida lisäksi SVPL:n 271 b:n mukaiset tehtävät PRS-palveluntarjoajana. Edelleen Traficom katsoo, että turvallisuusluokitteluvelvoite tulisi ulottaa myös hyväksyttyihin tietoturvallisuuden arviointilaitoksiin julkisissa hallintotehtävissä, joita niillä on tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaisessa arviointitoiminnassa, jossa niiden tulee lain 13 §:n mukaan noudattaa hallintolakia, julkisuuslakia ja kielilakia.

Julkishallinnon valvontatehtävä

Tiedonhallintalain muutosluonnoksessa julkishallinnon valvontatehtävä on osoitettu Traficomille. Traficom katsoo, että valvontatehtävä sopii luontevasti Traficomin hoidettavaksi, mutta kiinnittää huomiota resurssivaikutusten vuoksi valvonnan tarkoituksenmukaiseen kohdentamiseen.

Traficom katsoo, että NIS2-direktiivissä tarkoitetut kyberturvallisuuden riskienhallintatoimenpiteitä koskevat vaatimukset ja esitetty tiedonhallintalain 4 a luku tulisi koskea julkishallinnon toimijoita mahdollisimman laajasti. Sen sijaan julkishallinnon valvontatoimenpiteet tulisi kohdistaa NIS2-direktiivin tavoitteiden valossa vain niihin toimijoihin, joiden osalta valvontatoimien vaikuttavuus on yhteiskunnan kriittisten toimintojen kannalta NIS2-direktiivin tavoitteiden mukainen.

NIS2-direktiivin englanninkielisessä kieliversiossa ennakollisen valvonnan piiriin kuuluvista julkishallinnon toimijoista käytetään termiä "central government". Direktiivin suomenkielisessä kieliversiossa termi on käännetty keskustason julkishallinnon toimijaksi. Tämä on käsitteenä viraston käsityksen mukaan laajempi kuin englanninkielisen termin käännös valtion keskushallinto. Keskustason julkishallinnon toimijoiksi on tiedonhallintalain soveltamisalalta poimittu 1) ministeriöt, virastot ja laitokset 4) valtion liikelaitokset ja 7) muut julkisoikeudelliset laitokset. Traficomin näkemyksen mukaan näistä liikelaitokset ja muut välilliseen julkishallintoon kuuluvat julkisoikeudelliset laitokset eivät kuulu direktiivin määritelmään. Esim. tiedonhallintalain perusteluissa on todettu, että "itsenäiset julkisoikeudelliset laitokset, kuten Kansaneläkelaitos, Suomen Pankki, Työterveyslaitos, Keva, Kuntien takauskeskus, Suomen Riistakeskus ja Suomen Metsäkeskus, ovat valtionhallinnosta erillisiä organisaatioita, joiden toiminnasta ja tehtävistä säädetään erikseen laissa." Näin ollen Traficom toivoo vielä jatkovalmistelussa arvioitavan, voivatko valtionhallinnosta erilliset organisaatiot olla osa valtion keskushallintoa tai kuulua direktiivin määritelmään.

Traficom katsoo, että valvottavien julkishallinnon toimijoiden joukkoa tulisi tarkastella suhteessa NIS2-direktiivin tavoitteisiin ja huolehtia, että valvontaresurssit tulisi kohdennettua direktiivin tavoitteiden kannalta mahdollisimman tarkoituksenmukaisesti. Mikäli kansallista liikkumavaraa käyttäen julkishallinnon toimijoista sisällytetään ennakollisen valvonnan piiriin laajempi joukko toimijoita kuin NIS2-direktiivi edellyttää, siihen tulee osoittaa tarvittavat resurssit.

Verkkotunnusvälittäjiä koskevat huomiot

Automaattinen päätöksenteko

Traficom toteaa, että esitysluonnoksessa SVPL:n 167 §:n 2 momentilla pyritään käytännössä automaattiseen ratkaisumenettelyyn (ARM) riskiarvion perusteella tunnistettujen verkkotunnusten rekisteröinnin estämisen nopeuttamiseksi (väärät käyttäjätiedot). Tältä osin Traficom ehdottaa SVPL 43 lukuun lisättäväksi hallinnollisen oikaisuvaatimusmenettelyn, joka on välttämätön ARM:ssa.

Traficom katsoo, että sekä esitysluonnoksen mukaisessa SVPL 167 § 2 momentissa että voimassa olevassa SVPL 169 § 1 momentissa tarkoitetussa poistamisessa on kyse hallintoasioiden ratkaisuista. Traficom pitää tarkoituksenmukaisena, että virheellisiin tai puutteellisiin käyttäjätietoihin perustuvia asioita voitaisiin käsitellä ja ratkaista automaattisesti. Kyseisiä asioita ei voimassa olevan lain perusteella voitaisi kuitenkaan ratkaista automaattisesti, koska kyseisiin ratkaisuihin ei saa vaatia oikaisua hallintolain 53 f §:n edellyttämällä tavalla. Jotta Traficom voisi ratkaista kyseiset asiat automaattisesti, Traficom katsoo, että sähköisen viestinnän palveluista annetun lain 43 lukua tulisi muuttaa siten, että verkkotunnuksen rekisteröijä saisi vaatia oikaisua 167 § 2 momentissa ehdotettuun estämisratkaisuun ja 169 § 1 momentissa tarkoitettuun poistamispäätökseen.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Hallituksen esitysluonnos sisältää esityksen NIS1-täytäntöönpanosäännösten kumoamisesta, minkä seurauksena useisiin esimerkiksi liikenteen säädöksiin esitetään muutoksia. Traficom pitää hyvänä, että näiltä osin kansallinen sääntely keskitetään yleislakiin.

Traficom kiinnittää kuitenkin huomion hallituksen esityksen 7.4 kohtaan, jossa perustellaan ilmailulain pykälien kumoamista (s. 177). Ehdotetun tekstin mukaan säännökset kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettavaan lakiin sisältyisi lennonvarmistuspalvelun tarjoajia ja lentoaseman pitäjiä koskevat vastaavat velvollisuudet. Traficom toteaa, että NIS1-täytäntöönpanossa on lennonvarmistussektorilla ollut kansallisesti laajennettu soveltamisala, kun velvoitteet on kohdistettu kaikkiin lennonvarmistuspalveluntarjoajiin, sen sijaan että ne olisi kohdistettu vain lennonjohtopalvelun tarjoajiin, kuten sekä NIS1 että NIS2 edellyttävät. Nyt tarkasteltavana olevassa hallituksen esitys-luonnoksessa tämä laajennus on poistettu ja soveltamisalan piiriin tulevat vain lennonjohtopalvelun tarjoajat. EU:n ilmailun erityistä kyberturvallisuussääntelyä on kuvattu hallituksen esityksessä hyvin, ja erityisesti nämä erityissäännökset huomioon ottaen aiemman kaltaiselle kansalliselle laajennukselle ei ole perusteita.

Vaikutustenarviointia koskevat huomiot

Resurssivaikutukset

Traficom kiinnittää huomiota siihen, että kyberturvallisuuden kansallinen vahvistaminen ja NIS2-direktiivin toimeenpano edellyttävät niin työtä kuin järjestelmäkehitystä eli lisäresursointia niin toimijoiden kuin viranomaistenkin osalta. NIS-yleislakiesityksessä viranomaisille esitetään kokonaan uusia tehtäviä. Uusien tehtävien hoitamiseksi esitysluonnoksessa Traficomille on esitetty 8,5 htv:n lisäystä ja 0,5 htv:n lisäystä nimenomaisesti verkkotunnusvälittäjien valvontaan. Tällä lisäresursoinnilla virasto suoriutuisi NIS2-direktiivin toimeenpanon edellyttämistä keskeisimmistä tehtävistä vain vähimmäistasolla hyödyntäen mahdollisuuksia tehostaa nykyisiä toimintoja, kohdentaa olemassa olevia resursseja uudelleen viraston sisällä ja priorisoida tehtäviään.

Esitetyillä resursseilla virasto pystyisi hoitamaan vain vähimmäistasolla valvontatehtävät, ilmoitusten käsittelyn ja niihin vastaamisen, ilmoitusjärjestelmän kehittämisen, skannauskyvykkyyden kehittämisen, haavoittuvuuskoordinaation ja seuraamusmaksulautakunnan tehtävät.

Esitetyillä resursseilla ei olisi mahdollista parantaa Traficomin nykyistä valvontatehtävien hoitoa eikä edistää uusia tehtäviä seuraavista Traficomille osoitetuista tehtäväkokonaisuuksista: verkkotunnusten rekisteröintipalvelut, viranomaisten analyysi- ja forensiikkakyvykkyys, kriittisten toimialojen tukeminen, kansainvälinen yhteistyö, sertifiointi ja standardisointi, ICT-kyvykkyyksien ja automaation kehittäminen.

Muut huomiot ja avoin palaute esityksestä

-

Varjola Kalle
Liikenne- ja viestintävirasto Traficom