FiCom ry | Asko Metsola
10.9.2024

FiComin lausunto NIS2-direktiivin täytäntöönpanosta

Liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa hallituksen esityksestä kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- On hyvä, että Suomi ei aseta direktiiviä pidemmälle meneviä vaatimuksia. Liian yksityiskohtaisiksi kirjatut vaatimukset kyberturvallisuuden riskienhallinnan toimenpiteille eivät mahdollista riittävää liikkumavaraa yrityksille, joten niitä tulee välttää.
- Raportointivelvoitteet ovat paikoin epäselviä ja laajasti tulkittavia, joten niitä tulee täsmentää.
- Sähköisten viestintäpalvelujen tarjoamisen yhteydessä tapahtuneiden henkilötietojen tietoturvaloukkausten ilmoittaminen ainoastaan Liikenne- ja viestintävirastolle tulee selkeyden vuoksi nostaa myös pykälätekstiin.
- Kun viranomaiset luovuttavat tietoja toisilleen tai eteenpäin EU:n sisällä, niiden tulee ilmoittaa siitä yritykselle, jonka tietoja on luovutettu.
- Liikenne- ja viestintäviraston resurssit on turvattava, jotta sekä uudet valvontatehtävät että jo olemassa olevat viraston tehtävät voidaan hoitaa.
- Kyberturvallisuuskeskuksen 24/7-päivystys on säilytettävä.

NIS2-direktiivin tavoitteista ja tarkoituksesta

NIS2-direktiivi on luontevaa jatkoa EU:n muulle kyberturvallisuutta koskevalle sääntelylle, ja direktiivin tavoite vastata paremmin muuttuneeseen kybertoimintaympäristöön on ehdottoman kannatettava. Kyberturvallisuus on monilla kriittisillä toimialoilla keskeinen tekijä, jotta digitaalinen siirtymä voidaan toteuttaa onnistuneesti ja digitalisaation taloudelliset, sosiaaliset ja kestävyysedut voidaan hyödyntää täysimääräisesti.

Esityksen vaikutuksia riskienhallinta- ja raportointivelvoitteiden soveltamisalaan kuuluville toimijoille koskevan osion mukaan NIS2-direktiivin ei arvioida aiheuttavan digitaalisen infrastruktuurin toimijoille merkittäviä lisävelvoitteita, koska yleisten viestintäverkkojen ja viestintäpalvelujen tarjoajien sekä luottamuspalvelujen tarjoajien osalta toimijoihin on kohdistunut tietoturvavaatimuksia jo aiemmin (s. 72). Direktiivi tulee kuitenkin aiheuttamaan lisävelvoitteita myös digitaalisen infrastruktuurin toimijoille.

Esimerkiksi toimenpiteitä kyberturvallisuutta koskevien riskien hallintaa koskevan 9 §:n 9 kohdan mukaan kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi. Säännöskohtaisten perustelujen mukaan merkittäviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja viestintäkanavat muiden toimijoiden varoittamiseksi (s. 166). Vaikuttaa siltä, että säännöksellä velvoitetaan tunnistamaan muut toimijat ja ilmoittamaan näille merkittävistä poikkeamista. Joitain yhteistyöfoorumeita on toki olemassa

valmiiksi, mutta yleensä ne ovat kansallisen CERT/CSIRT-yksikön tai muun kolmannen osapuolen järjestämiä. Kyseessä on siis työläs lisävelvoite. NIS2-direktiivin soveltamisalaan kuuluvien toimijoiden on itse tunnistettava kuuluvansa direktiivin soveltamisalaan ja nostettava tarvittaessa asia esille omien kumppaneidensa ja alihankkijoidensa kanssa. On huomattava, että vaikka esimerkiksi teleyritykset tuntevat omat asiakkaansa, ei teleyrityksillä välttämättä ole tietoa siitä, onko toimija NIS2-direktiivin soveltamisalaan kuuluva toimija vai ei.

Riskienhallintavelvoitteet

Esityksessä todetaan, että NIS2-direktiiviä täytäntöönpanevan sääntelyn yhteismitallisuuden vuoksi suhteessa muihin jäsenvaltioihin esityksen lähtökohdaksi on valikoitunut riskienhallinta- ja raportointivelvoitteiden direktiivin asettama vähimmäistaso (s. 123). Tämä on erittäin kannatettavaa. Monet yritykset toimivat useassa EU:n jäsenvaltiossa, ja siksi on tärkeää, että direktiivin vaatimukset ovat samat kaikkialla ja että direktiivi on implementoitu samalla tavoin koko EU-alueella. **Direktiivi on varsin yksityiskohtainen ja kattava, joten senkin vuoksi on hyvä, että Suomi ei aseta direktiiviä pidemmälle menevämpiä vaatimuksia**.

Kyberturvallisuuslain riskienhallintaa koskevan 7 §:n 2 momentin mukaan toimijan tulisi toteuttaa ”*riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta*”. Pykälän taustalla on NIS2-direktiivin 21 artikla, jossa ei ole mainittu vaatimusta toimenpiteiden ajantasaisuudesta.

Toimenpiteitä kyberturvallisuutta koskevien riskien hallinnassa koskevan 9 §:n säännöskohtaisissa perusteluissa todetaan toimijalta edellytettyjen toimenpiteiden suhteellisuuden tason osalta, kuinka ”*vaikutuksia tulisi arvioida erityisesti yhteiskunnalle merkityksellisten toimintojen näkökulmasta, ja mitä merkittävämpiä vaikutuksia uhkan toteutumisella voitaisiin arvioida olevan yhteiskunnan tai talouden näkökulmasta, sitä merkittävämpiä hallintatoimenpiteitä olisi tarpeen toteuttaa. Vaikutuksia tulisi siten arvioida toimijan itsensä ohella myös niille, jotka käyttävät tai ovat riippuvaisia toimijan palveluista*” (s. 168–169). Lähtökohtaisesti yritykset pystyvät arvioimaan ja hallitsemaan riskejä suhteessa omaan ja asiakkaidensa toimintaan. Yritykset eivät sen sijaan välttämättä pysty ennustamaan vaikutuksia esim. koko yhteiskunnalle tai taloudelle. Myös omien asiakkaiden riskien arvioinnin edellytys on, että asiakkaat ovat tuoneet esille niiden kannalta kriittiset palvelut tai sen, että ne ovat huoltovarmuuskriittisiä toimijoita tai kuuluvat NIS2-direktiivin soveltamisalaan. Jos asiakas ei itse ole tuonut asiaa esille, eivät teleyritykset välttämättä voi tätä tietää, vaikka ne lähtökohtaisesti tuntevatkin hyvin omat asiakkaansa. **Säännöskohtaisia perusteluja tulee tältä osin tarkentaa**.

Raportointivelvoitteet

Toimijoille tulee nyt täytäntöönpantavan NIS2-direktiivin, jo olemassa olevan yleisen ja sektorikohtaisen sääntelyn sekä tulevan ja paraikaa kansallisesti täytäntöönpantavan muun EU-sääntelyn myötä valtavasti raportointivelvoitteita. Tämän vuoksi poikkeamien raportoinnin täytyy hoitua vain yhden viranomaisen kautta, myös rajat ylittävien poikkeamien osalta. **Raportointikäytännöt ja yksityiskohtaisuuden taso on pidettävä mahdollisimman kevyenä ja maltillisena, jotta raportointi ei vie liiaksi aikaa itse poikkeaman**

tutkimiselta, torjumiselta ja vaurioiden korjaamiselta. Automaation myötä monet poikkeamat hoidetaan ilman manuaalista työtä, joten ei ole tarkoituksenmukaista, että raportointi tulisi kuormittamaan muuten automaation hoitamaa aluetta.

Raportointivelvoitteita täsmennettävä

Raportointivelvoitteet ovat paikoin epäselviä ja laajasti tulkittavia. Esimerkiksi uuden ehdotettavan lain 14 §:ssä säädetään poikkeamasta ja kyberuhkasta ilmoittamisesta muulle kuin viranomaiselle. Pykälän toisen momentin mukaan toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Kyberuhka on kuitenkin varsin laaja käsite, joten pykälästä ei selvästi käy ilmi, mistä pitäisi ilmoittaa ja mistä ei. Olisiko kalastelusähköposti kenties ilmoitettava kyberuhka? Entä kyberrikolliset, kuten NoName 057(16)-palvelunestohyökkäysryhmä tai APT29-/Cozy Bear-hakkeriryhmä? Molempien toiminta voi kuitenkin vahingoittaa viestintäverkkoa.

Jos kyberuhkan sijaan puhuttaisiin esimerkiksi haavoittuvuudesta, velvoite olisi selkeämpi. Esimerkiksi päätelaitehaavoittuvuuksista ilmoitetaan asiakkaille jo nyt verkkosivujen kautta. Vaihtoehtoisesti velvoitetta tulisi avata esimerkiksi toteamalla, että palvelujen vastaanottajille tulisi ilmoittaa niistä ajankohtaisista kyberuhista, joihin he voivat omalla toiminnallaan varautua tai suojautua.

Kun ilmoitettavia kyberuhkia arvioidaan, tulee välttää liian laajoja tai alhaisia kynnysarvoja, jotka aiheuttavat liiallisen raportoinnin myötä tarpeetonta työtä tai vievät huomiota pois itse tapahtumien torjuntatyöstä. Säännellyn toimintakentän toiminnallisuudet tulee tunnistaa, ja kriteeristöjä muodostettaessa tulee tehdä tiivistä yhteistyötä säänneltyjen sektoreiden kanssa. Esimerkiksi voimassa olevan ns. NIS1 -direktiivin täytäntöönpanon osalta digitaalisten palveluntarjoajien raportointikriteereinä käytetty “käyttäjätunti”-mittari ei vastaa johdonmukaisesti tilapäistä pilvipalvelun tason laskua tai lisääntynyttä latenssia. Näin siksi, että yksittäisten käyttäjien tietoja ei ole saatavilla tai siksi, että ei tiedetä, onko palvelu saatavilla tietylle käyttäjälle (tai käyttäjille) 60 minuutin ajan. Pikemminkin tulisi selventää, että silloin, kun arvioidaan kyberuhkien vaikutuksia käyttäjiin, otetaan huomioon myös yritysasiakkaat tai tilaajat. Säännellyt toimijat arvioisivat tapahtuman merkittävyyttä yritystilien tai tilaajien lukumäärän vaikutusten perusteella, jos yksittäisten käyttäjien tietoja ei ole saatavilla. Palvelun tason alenemisen ja vaikutuksen kohteena olevien asiakkaiden prosenttiosuus olisi suositeltava vaihtoehtoinen kriteeri käyttäjätuntien rinnalle. Tällöin merkittävyys riippuisi tapahtuman kestosta, laajuudesta (leviämisestä) ja syvyydestä (vaikutuksen kohteena olevien käyttäjien tai tilien lukumäärä organisaatiossa). Arvioinnin ja siihen liittyvän raportointivelvollisuuden tulisi perustua luotettavaan tietoon, ei spekulaatioon.

Läheltä piti -tilanteen määritelmä vastaa sinänsä NIS2-direktiivin määritelmää, mutta sen osalta olisi syytä harkita määritelmän tarkentamista kansallisella tasolla. Nykyinen muotoilu on hyvin laaja ja epäselvä.

Sähköisten viestintäpalvelujen erityislainsäädäntö henkilötietojen tietoturvaloukkausten ilmoittamisesta huomioitava pykälätasolla

Ehdotetun kyberturvallisuuslain tietosuojavaltuutetulle tehtävää ilmoitusta koskevan 33 §:n mukaan valvovan viranomaisen olisi ilmoitettava tietosuojavaltuutetulle, jos se valvonnan tai täytäntöönpanon yhteydessä havaitsee sellaisen laiminlyönnin, joka voisi johtaa tai on jo johtanut sellaiseen henkilötietojen tietoturvaloukkaukseen, josta on ilmoitettava tietosuojavaltuutetulle yleisen tietosuoja-asetuksen nojalla. Säännöskohtaisten perustelujen mukaan yleisen tietosuoja-asetuksen 33 artiklan mukaista ilmoitusvelvollisuutta ei sovelleta yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamisen yhteydessä tapahtuneisiin henkilötietojen tietoturvaloukkauksiin, koska sen sijasta sovelletaan erityislainsäädäntöä (Tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, k. 44) (s. 200).

Esityksen mukaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat ilmoittavat palveluun kohdistuvista tietoturvaloukkauksista Liikenne- ja viestintävirastolle sähköisen viestinnän palveluista annetun lain 275 §:n ja henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY mukaisten henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä annetun komission asetuksen 611/2013 mukaisesti. Näin ollen 33 §:ssä säädetty velvollisuus ei koskisi Liikenne- ja viestintäviraston tietoon tulleita teletoimintaa koskevia henkilötietojen tietoturvaloukkauksia, jotka se käsittelisi sähköisen viestinnän tietosuojadirektiivin mukaisena toimivaltaisena viranomaisena.

Esityksen perusteluissa esitetty tila vastaa Euroopan tietosuojaneuvoston tulkintaa sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta, ja on siten erittäin kannatettava. Tämä ei kuitenkaan valitettavasti vastaa Suomessa tällä hetkellä noudatettua viranomaisen tulkintakäytäntöä. **Riippumatta tietosuojaneuvoston lausunnosta, tietosuojavaltuutetun toimisto edellyttää myös yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajilta Liikenne- ja viestintävirastolle tehdyn ilmoituksen lisäksi erillistä ilmoitusta henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle.** Yleisen tietosuoja-asetuksen ankarien seuraamusriskien ja tietosuojavaltuutetun toimiston linjanvedon vuoksi palveluntarjoajat joutuvat siis nykyään tekemään kaksi erillistä ilmoitusta samasta tietoturvaloukkauksesta, mikä on vastoin kansainvälistä tulkintaa. **Näin ollen perusteluissa asianmukaisesti ehdotettu tavoitetila tulee oikeustilan selkeyden vuoksi nostaa myös pykälätekstiin, tai vähintäänkin se tulee esittää vielä selkeämmin perusteluissa.**

Tiedonvaihto viranomaisten välillä

CSIRT-yksikköä koskevan 19 §:n perusteluiden mukaan CSIRT-yksikkö luovuttaa kyberturvallisuuslain nojalla saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 §:n 2 ja 3 momentissa säädetään (s. 177).

Luovutettaessa tietoja viranomaisten kesken kansallisesti tai EU:n sisällä, tulee näiden ilmoittaa luovutuksesta yritykselle, jonka tietoja on luovutettu. Teleyrityksen toiminta perustuu luottamukseen. Tämän vuoksi teleyrityksen hallinnoimat luottamukselliset tiedot ovat hyvin kriittistä omaisuusdataa, jota hallinnoidaan erittäin huolellisesti. Luovuttavalla teleyrityksellä on selkein kokonaisymmärrys luovutetusta datasta. Luovuttava teleyritys on asianosainen, ja sillä on intressi tietää, mihin sen luottamuksellinen tieto

päätyy. Tästä syystä yritykselle on keskeistä tiedostaa ja ymmärtää, millä viranomaisilla on käytössään sen dataa.

Jos annetaan oikeuksia, syntyy samalla myös vastuita ja velvollisuuksia. FiComin mielestä viranomaisen ilmoitusvelvollisuus luo luottamusta läpinäkyvyydellään. Se antaa mahdollisuuden valvoa, että datan edelleenluovutukset ovat perusteltuja ja lainmukaisia. Jos mukana on esimerkiksi välitystietoja, on teleoperaattoreilla myös rekisterinpitäjän roolissa suotavaa olla tieto edelleenluovutuksista jo läpinäkyvyyden vuoksi.

Teleyritykset luovuttavat todella suuria datamassoja valvoville viranomaisille myös muuta kuin nyt ehdotettavaan lakiin perustuvaa tarkoitusta varten. Jos viranomaisen ei tarvitse ilmoittaa yritykselle tietojen edelleenluovutuksesta, miten yritys voisi varmistua siitä, että viranomaiskentässä ei tarpeettomasti välitetä yrityksen jotain tiettyä tarkoitusta varten keräämää tietoa? Jos vastaanottavalla viranomaisella on toimivalta käsitellä luovutettuja tietoja, voisi viranomainen pyytää ne suoraan yritykseltä. Erityisesti sijainti- ja välitystietojen kohdalla on tarpeen varmistaa, että viranomaisella on varmasti ymmärrys siitä, miten teleoperaattoritietoja voi lukea ja tulkita, ettei niiden pohjalta tehdä virheellisiä päätelmiä. Tulkintaohjeistusta ja -tukea on vaikea tarjota, elleivät teleoperaattorit tiedä, kenelle viranomaisille tietoa on jaettu. Yrityksellä on paras tietämys luovutettavasta datasta ja sen alkuperäisestä asiayhteydestä

Valvonta

Esityksen mukaan tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä sekä keskitettynä yhteyspisteenä toimisi jatkossakin Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (s. 60). Uuden ehdotetun lain CSIRT-yksikön tehtäviä koskevan 20 §:n 1 momentin 9 kohdan mukaan CSIRT-yksikön tehtävänä on antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta. Pykälään ei kuitenkaan ole lisätty NIS2-direktiivin 11 artiklaan sisältyvää CSIRT-yksiköille asetettua velvoitetta luoda yhteistyösuhteet asiaankuuluviin yksityisen sektorin sidosryhmiin. Tämä on sisällytetty pykälän perusteluihin, joiden mukaan pykälän 1 momentin 9 kohdan mukaan CSIRT-yksikkö voisi edistää yhteistyötä yksityisen sektorin sidosryhmien kanssa antamalla ohjeita ja suosituksia esimerkiksi yhteisten tai standardoitujen käytäntöjen, luokitusjärjestelmien ja taksonomioiden hyväksymiseksi ja käyttämiseksi (s. 180). **Yhteistyövelvoite on nostettava myös pykälätasolle**.

Edelleen 20 §:n 4 momentissa on säädetty siitä, kuinka CSIRT-yksikkö voi tarjota tietoturvaloukkausten havainnointipalvelua suoraan sitä pyytäville toimijoille tai muille tahoille sekä sellaisille tietoturvapalvelun-tarjoajille, jotka tarjoavat tietoturvaloukkausten havainnointipalvelua toimijoille tai muille yhteisöille käytettäväksi (*palvelukeskus*). Pykälän 5 momentin mukaan toimijan tai muun tahon pyynnöstä tarjotusta palvelusta voidaan periä maksu. Vastaavaa maksullista havainnointipalvelua ei sisälly NIS2-direktiiviin.

Valvovan viranomaisen tiedonsaantioikeutta koskevan uuden ehdotettavan lain 28 §:n osalta esityksessä on todettu, kuinka valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta

koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Lisäksi valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten.

Epäselväksi jää, mikä käytännössä muuttuu, ja onko esimerkiksi teleyrityksillä tiedonluovutusvelvollisuuksia teletiedosta myös muille viranomaisille kuin oman alansa valvovalle viranomaiselle Liikenne- ja viestintävirasto Traficomille. Nykyisin teleyritykset luovuttavat tietoja Traficomille, joka luovuttaa tiedot tarvittaessa eteenpäin.

Liikenne- ja viestintäviraston resurssit on turvattava

Liikenne- ja viestintävirastolle esitetään uusien valvontatehtävien lisäksi myös muita viranomaistehtäviä, joista aiheutuu lisäresursointitarpeita. NIS2-direktiivin myötä CSIRT-yksikön tehtävät lisääntyvät merkittävästi, ja uudet tehtävät edellyttävät uudenlaisten toimintojen perustamista sekä olemassa olevien toimintojen sekä tietojärjestelmien kehittämistä.

CSIRT-yksikölle ehdotettujen uusien tehtävien sekä Liikenne- ja viestintävirastolle osoitettavien valvontatehtävien on arvioitu edellyttävän lisäresursseja yhteensä 8–17 henkilötyövuotta. Näiden pelkästään NIS2-direktiivin täytäntöönpanosta johtuvien lisäresurssien lisäksi on arvioitu, että virasto tarvitsee lähivuosina digipalveluasetuksen valvonnan takia 6,5 henkilötyövuoden lisäresurssin (HE 70/2023 vp, s. 44) ja datanhallinta-asetuksen myötä 1,5 henkilötyövuoden lisäresurssin (HE 50/2023 vp, s. 22). Digipalveluasetusta koskevan hallituksen esityksen mukaan Liikenne- ja viestintävirastolle on osoitettu viime vuosien aikana useita uusia tehtäviä, joihin ei ole esityksistä huolimatta saatu rahoitusta (HE 70/2023 vp, s. 45). Lisäksi virasto on jo ottanut haltuun monia tehtäviä viraston olemassa olevalla rahoituksella ja tehtäviä järjestelemällä.

Kuten hallituksen esityksessä todetaan, kyberturvallisuusosaajista on Suomessa pulaa. Tämä saattaa aiheuttaa rekrytointihaasteita sekä viranomaisille että sääntelyn kohteena oleville toimijoille (s. 107). EU:sta on tulossa kansallisesti täytäntöön pantavaksi myös mm. data-asetus ja tekoälyasetus, joiden valvontavastuut ja niistä mahdollisesti aiheutuva lisäresurssien tarve on vielä päättämättä.

Liikenne- ja viestintäviraston resurssit on turvattava, jotta sekä uudet valvontatehtävät että jo olemassa olevat viraston tehtävät voidaan hoitaa. Lisäresurssien rahoitus tulee toteuttaa muulla tavalla kuin korottamalla viestintämarkkinamaksua, koska valvonta kohdistuu muihin tahoihin kuin teleyrityksiin. Huomioitavaa on, että Liikenne- ja viestintäviraston valvonta täytyy uusien virastolle tulevien tehtävien myötä eriyttää sen tehtävistä ilmoituksia vastaanottavana viranomaisia. Myös tämä edellyttää lisäresursseja.

Kyberturvallisuuskeskuksen 24/7-päivystys tulee säilyttää

Esityksen mukaan uuden ehdotetun kyberturvallisuuslain poikkeamailmoituksen vastaanottamista koskevan 16 §:n mukaan valvovan viranomaisen olisi vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä.

Säännöskohtaisten perustelujen mukaan vastaus tulisi antaa viivytyksettä ja mahdollisuuksien mukaan 24 tunnin kuluessa, mutta kuitenkin virka-aikojen puitteissa. Valvovalta viranomaiselta ei siten edellytettäisi esimerkiksi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä (s. 175). Vastaavasti julkisen hallinnon tiedonhallinnasta annettuun lakiin ehdotetaan uutta poikkeamailmoituksen vastaanottamista koskevaa 18 e §:ää, jonka mukaan valvovan viranomaisen eli Liikenne- ja viestintäviraston olisi pykälän 1 momentin mukaan viipymättä ja mahdollisuuksien mukaan 24 tunnin kuluessa 18 d §:n 1 momentissa tarkoitetun ensi-ilmoituksen vastaanottamisesta annettava viranomaiselle vastaus. Säännöskohtaisten perustelujen mukaan tämä ei kuitenkaan edellyttäisi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä (s. 223).

Tiedonhallintalain uuden 18 d §:n 1 momentissa asetetaan viranomaisille velvoite toimittaa ilman aiheetonta viivytystä, viimeistään 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta, julkishallinnon valvovalle viranomaiselle, Liikenne ja viestintävirastolle poikkeamaa koskeva ensi-ilmoitus. Säännöskohtaisten perustelujen mukaan tietoiseksi tuleminen voi riippua siitä, tapahtuuko poikkeama virka-aikaan vai yöllä tai viikonloppuna. Säännöksellä ei perustelujen mukaan velvoiteta viranomaista järjestämään ympärivuorokautista päivystystä ensiraportin toimittamista varten, vaan päivystyksen tarve, kohde ja laajuus arvioidaan viranomaisen 18 b ja c §:n mukaisesti toteutetussa riskienhallinnassa (s. 222). Esityksessä on ehdotettu lisäksi käytettävän NIS2-direktiivin 34 artiklan 7 kohdan mukaista kansallista liikkumavaraa siitä, ettei julkishallinnon toimijoille määrätä direktiivin edellyttämiä hallinnollisia sanktioita (s. 201).

Tällä hetkellä Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ylläpitää valtionhallinnolle ja huoltovarmuuskriittisille toimijoille tarkoitettua 24/7-päivystystä. Jatkossa Kyberturvallisuuskeskuksen ympärivuorokautiselle päivystykselle ei siis viranomaisten tietoiseksi tulemista koskevaan säännöksen ehdotetun poikkeuksen mukaisesti välttämättä olisi tarvetta, eikä virastolta toisaalta edellytettäisi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä poikkeamailmoituksiin vastaamista varten.

FiComin jäsenten näkökulmasta ehdotetun sääntelyn mahdollistama valvovan viranomaisen ympärivuorokautisesta päivystyksestä luopuminen olisi huomattava heikennys nykytilanteeseen - varsinkin, kun yrityksillä olisi joka tapauksessa velvoite lähettää ennakkovaroitus merkittävästä poikkeamasta 24 tunnin kuluessa sen havaitsemisesta. Kyberturvallisuuskeskuksen CERT-toiminnolla on keskeinen rooli informaation ja uhkatilanteen tiedottamisessa kansallisille kriittisen infran toimijoille sekä muille viranomaisille. Esimerkiksi torstai-iltana tapahtuneesta merkittävästä poikkeamasta perjantai-iltana lähetettyyn ensi-ilmoitukseen saataisiin vastaus aikaisintaan maanantaina, jolloin yrityksen olisi pitänyt antaa jo varsinainenkin poikkeamailmoitus, mikä pitää tehdä 72 tunnin kuluessa poikkeaman havaitsemisesta. Jos ilmoitus liittyy uhkaan, joka voi vaikuttaa muidenkin toimijoiden riski- ja uhkatilanteeseen, valvova viranomainen ei olisi pystynyt informoimaan muita viranomaisia ja toimijoita kuin vasta seuraavana arkipäivänä viikonlopun jälkeen. **Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen 24/7-päivystys on säilytettävä**.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Muutettavan sähköisen viestinnän palveluista annetun lain Liikenne- ja viestintävirastolle tehtäviä häiriöilmoituksia koskevan 275 §:n perusteluissa on todettu, kuinka voimassa olevan 275 §:n 4 momentin nojalla annettuja määräyksiä koskisi siirtymäsäännös (s. 236). Esityksessä ei kuitenkaan ole kuvattu

tarkemmin, mitä tämä tarkoittaa. Miten käy esimerkiksi Liikenne- ja viestintäviraston määräykselle 66A teletoiminnan häiriötilanteista?

Ylipäätään voisi harkita, onko tarpeen, että 275 §:ssä on edelleen mukana teleoperaattoreiden erillisvelvoite raportoida tietoturvauhista Traficomille. Olisiko selkeämpää, että raportointivelvoitteet olisi selkeästi koottu vain kyberturvallisuuslakiin ja sektorikohtaisesta lakitasoisesta sääntelystä luovuttaisiin kokonaan?

Toivottavaa olisi, ettei samoista asioista ole muuta sääntelyä, vaikka esityksessä sellainen mahdollisuus annetaan. Direktiivi on kuitenkin yksityiskohtainen ja kattava, joten myös teletoiminnan osalta olisi selkeämpää, että uuden lain kanssa päällekkäisestä sääntelystä luovuttaisiin.