Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry

Lausunto

29.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Liikenne- ja viestintäministeriö on pyytänyt FiComilta lausuntoa luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. 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.
- Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjaista haavoittuvuuskartoitusta koskevaa sääntelyä tulee täsmentää.
- Liikenne- ja viestintäviraston resurssit on turvattava, jotta sekä uudet valvontatehtävät että jo olemassa olevat viraston tehtävät voidaan hoitaa.
- Kyberturvallisuuskeskuksen 24/7-päivystys on säilytettävä.

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

NIS2-direktiivi on luonteva jatko 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.

Esitysluonnoksen 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. 58). Direktiivistä tulee kuitenkin aiheutumaan lisävelvoitteita myös digitaalisen infrastruktuurin toimijoille.

Esimerkiksi kyberturvallisuuden riskienhallinnan toimenpiteitä koskevan 9 §:n 9 kohdan mukaan kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi. Säännöskohtaisten perustelujen mukaan vakaviin ja muihin toimijoihin ulottuviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja kommunikointikanavat muiden toimijoiden varoittamiseksi. 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.

Vastaavasti 9 §:n 11 kohdan mukaan kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään perustason kyberhygieniakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Säännöskohtaisissa perusteluissa on todettu, että perustason kyberhygieniakäytäntöihin voidaan lukea esimerkiksi luottamattomuuden periaate / zero-trust (s. 124). Kyseessä ei kuitenkaan todellisuudessa ole perustason kyberhygieniakäytäntö. Jos toimijalla on esimerkiksi paljon legacy-järjestelmiä, zero-trustin käyttöönotto voi olla kallista ja haastavaa.

Soveltamisalaa koskevat huomiot

-

Riskienhallintavelvoitetta koskevat huomiot

Esitysluonnoksessa todetaan, että NIS2-direktiiviä täytäntöönpanevan sääntelyn yhteismitallisuuden vuoksi suhteessa muihin jäsenvaltioihin esityksen lähtökohdaksi on valikoitunut riskienhallinta- ja raportointivelvoitteiden direktiivin asettama vähimmäistaso (s. 93). Tämä on erittäin kannatettavaa.

Monet yritykset toimivat useammassa EU:n jäsenvaltiossa, ja siksi on tärkeää, että direktiivin vaatimukset ovat samat kaikkialla ja että direktiivi on implementoitu samalla tavoin EU-alueella. Direktiivi on lisäksi varsin yksityiskohtainen ja kattava, joten senkin vuoksi on hyvä, että Suomi ei aseta direktiiviä pidemmälle menevämpiä vaatimuksia.

Kyberturvallisuuden riskienhallintavelvoitetta koskevan 7 §:n 2 momentin mukaan toimijan tulisi toteuttaa ”turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuville riskeille sekä viestintäverkon tai tietojärjestelmän merkitykselle toimijan toiminnan ja palveluntarjonnan kannalta”. Pykälän taustalla on NIS2-direktiivin 21 artikla, jossa ei ole mainittu vaatimusta toimenpiteiden ajantasaisuudesta.

Riskienhallintamenetelmien osalta on kuitenkin huomattava, että ne elävät ajassa, kehittyvät ja ovat myös tekniikka-/teknologiasidonnaisia. Tämän vuoksi on tärkeää, että yrityksille jätetään mahdollisuuksia ja liikkumavaraa siihen, miten ne huolehtivat organisaatioissaan riskienhallinnan käytännön toteutuksesta. Tämä on hyvä huomioida myös säännöskohtaisissa perusteluissa. Niitä ei tule kirjoittaa ehdottomaan muotoon, jotta liikkumavara yksittäisen riskienhallintamenetelmän toimeenpanossa on mahdollista.

Riskienhallintamenetelmien osalta perusteluissa tuleekin tuoda selkeämmin esille, että menetelmät ja käytetty tekniikka ovat keskenään sidoksissa. Esimerkiksi vanhempien verkkoteknologioiden osalta toimenpiteet eivät ole, eivätkä voi olla, yhtä kattavia tai sofistikoituneita verrattuna uudempiin verkkoteknologioihin, koska tekniikka on niissä huomattavasti vanhempaa ja kehittymättömämpää. Tällöin myöskään riskienhallinnan mahdollisuudet (toimenpiteet ja kyvykkyydet) eivät voi olla samalla tasolla kuin mitä ne voivat olla uudemmissa verkkoteknologioissa.

Kyberturvallisuuden riskienhallinnan toimenpiteitä koskevan 9 §:n säännöskohtaisissa perusteluissa on todettu, kuinka ”osa-alueiden yksilöinnin tarkoitus alakohdissa on määritellä vaatimukset toisaalta mahdollisimman tarkasti, jotta ne ovat toimijoille ennakoitavia ja toisaalta teknologianeutraalisti, jotta ne soveltuvat kaikille toimialoille ja jatkuvasti muuttuvaan kyberturvallisuusympäristöön. Vaatimusten määrittely edesauttaa myös sitä, että valvovan viranomaisen perusteet valvontatoimenpiteille ovat selkeät ja ennakoitavat” (s. 119). Kuten esitysluonnoksessakin todetaan, liian tarkasti kirjatut vaatimukset eivät välttämättä mahdollista riittävää liikkumavaraa yrityksille, joten siksi liian yksityiskohtaisia vaatimuksia tulisi välttää.

NIS2-direktiivin 21 artiklan 2 kohdan d alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteissä on otettava huomioon toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat. Alakohta on pantu täytäntöön uuden ehdotetun lain 9 §:n 2 momentin 4 kohdalla, jonka mukaan kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään toimitusketjun

toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Pykälän muotoiluun ei ole lisätty direktiivin rajoitusta välittömistä toimittajista, mikä tulee korjata.

Esitysluonnoksessa 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. 125).

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 esimerkiksi sen, että on huoltovarmuuskriittinen toimija. Jos asiakas ei itse ole tuonut asiaa esille, ei esimerkiksi teleyritys välttämättä voi tätä tietää, vaikka ne lähtökohtaisesti hyvin omat asiakkaansa tuntevatkin. Säännöskohtaisia perusteluja tulee tältä osin tarkentaa.

Raportointivelvoitetta koskevat huomiot

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 ihmisen tekemää 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 kautta ei-vaikutuksellista 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. NIS 1 -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 kyberturvallisuuden riskienhallinnasta annetun lain tietosuojavaltuutetulle tehtävää ilmoitusta koskevan 34 §:n mukaan valvovan viranomaisen on ilmoitettava asiasta tietosuojavaltuutetulle, jos se saa em. laissa tarkoitettujen tehtävien hoitamisen yhteydessä tietoonsa, että lain 2 luvussa säädettyjen velvoitteiden laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta on yleisen tietosuoja-asetuksen 33 artiklan nojalla ilmoitettava yleisen tietosuoja-asetuksen mukaiselle valvontaviranomaiselle. 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. 148).

Esitysluonnoksen 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 34 §:ssä säädetty velvollisuus ei koskisi Liikenne- ja viestintäviraston tietoon tulleita teletoimintaa koskevia henkilötietojen tietoturvaloukkauksia, jotka se käsittelisi sähköisen viestinnän tieto-suojadirektiivin mukaisena toimivaltaisena viranomaisena.

Esitysluonnoksen 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. Johtuen yleisen tietosuoja-asetuksen ankarista seuraamusriskeistä ja tietosuojavaltuutetun toimiston linjanvedosta, palveluntarjoajat joutuvat siis nykyään tekemään vastoin kansainvälistä tulkintaa kaksi erillistä ilmoitusta samasta tietoturvaloukkauksesta. Näin ollen perusteluissa asianmukaisesti ehdotettu tavoitetila tulee oikeustilan selkeyden vuoksi nostaa myös pykälätekstiin, tai vähintäänkin se tulee esittää vielä selkeämmin perusteluissa.

Tiedonvaihto viranomaisten välillä

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjaista haavoittuvuuskartoitusta koskevan ehdotetun uuden lain 20 §:n mukaan CSIRT-yksikkö saa käyttää haavoittuvuuskartoituksessa havaittuja, kartoituksen kohteeseen yhdistettävissä olevia tietoja kyberuhkien tunnistamiseksi, kyberturvallisuuden tilannekuvan ylläpitämiseksi ja haavoittuvuuksista tiedottamiseksi. Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttamista koskevan 24 §:n mukaan CSIRT-yksikkö voi luovuttaa ehdotetun lain nojalla saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 §:n 2 ja 3 momentissa säädetään. Lisäksi valvovan viranomaisen tiedonsaantioikeutta välitystiedosta, sijaintitiedosta ja haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä koskevan 28 §:n mukaan valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden valvomista varten tai

merkittävien poikkeamien selvittämiseksi. Pykälän toisen momentin mukaan sitä, mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa ja 319 §:ssä säädetään Liikenne- ja viestintäviraston viestistä, välitystiedosta, sijaintitiedosta sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta saamien ja hankkimien tietojen salassapidosta, luovuttamisesta ja hävittämisestä, sovelletaan myös valvovan viranomaisen 28 § nojalla saamiin ja hankkimiin tietoihin.

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

Valvontaa koskevat huomiot

Esitysluonnoksen mukaan tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä sekä keskitettynä yhteyspisteenä toimisi jatkossakin Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (s. 49). Uuden ehdotetun lain CSIRT-yksikköä koskevan 19 §:n 2 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 2 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. 133). Yhteistyövelvoite on nostettava myös pykälätasolle.

Edelleen 19 §:n 5 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 tahoille käytettäväksi (palvelukeskus). Pykälän 6 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 27 §:n osalta esitysluonnoksessa on todettu, kuinka valvovalla viranomaisella on tämän lain mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot tässä laissa tarkoitetuilta toimijoilta. 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 tietoja tarvittaessa eteenpäin.

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus sekä kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjaisesta haavoittuvuuskartoituksesta säädetään uuden ehdotetun lain 20 §:ssä. NIS2-direktiivin 11 artiklan 3 kohdassa puhutaan keskeisten ja tärkeiden toimijoiden yleisesti saatavilla olevien verkko- ja tietojärjestelmien ennakoivasta, ei-intrusiivisesta skannauksesta, jonka tarkoituksena on havaita haavoittuvat tai epäturvallisesti konfiguroidut verkko- ja tietojärjestelmät ja ilmoittaa niistä asianomaisille toimijoille. Skannaus ei direktiivin mukaan saa haitata asianomaisten toimijoiden palvelujen toimintaa.

Säädöskohtaisten perustelujen mukaan ”CSIRT-yksiköllä olisi oikeus haavoittamiskartoituksen toteuttamiseksi hankkia tietoja yleiseen viestintäverkkoon kytkettyjen telepäätelaitteiden ja tietojärjestelmien sekä niiden tietoliikennejärjestelyjen yksilöintitiedoista, käytetyistä ohjelmistoista ja niiden toiminnasta, teknisestä toteutuksesta ja niiden avulla tarjotuista palveluista. Haavoittuvuuskartoitus voisi kohdistua myös yleisen viestintäverkon viestintäverkkolaitteisiin, jotka kuuluisivat viestintäverkon käsitteen alaan” (s. 135). Lisäksi myöhemmin perusteluissa todetaan, kuinka ”haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saisi käsitellä tietoja sähköisten viestien sisällöstä. Kohdennetussa haavoittuvuuskartoituksessa CSIRT-yksiköllä olisi kuitenkin oikeus tarkkailla ja käyttää välitystietoja, jos se on tarpeen haavoittuvuuden, kyberuhkan tai turvattoman konfiguroinnin havaitsemiseksi” (s. 136). Henkilötietojen käsittelyperuste haavoittuvuuskartoituksessa olisi säännöskohtaisten perustelujen mukaan yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohta (s. 136).

Lainatut kohdat ovat ristiriidassa sen säännöskohtaisten perusteluiden kohdan kanssa, jonka mukaan ”haavoittuvuuskartoituksella ei olisi sallittua hankkia ja käsitellä luottamuksellisen

viestinnän suojaamia tietoja, kuten välitystietoja tai viestien sisältöä, jossa CSIRT-yksikkö ei ole viestinnän osapuolena” (s. 135). Aiemmin mainittujen lainauksien mukaan CSIRT-yksiköllä olisi oikeus käsitellä välitystietoja ja jälkimmäisen lainauksen mukaan ei. On äärimmäisen tärkeää, että hallituksen esityksessä käytetään selkeää kieltä siitä, puhutaanko esimerkiksi (telepäätelaitteiden) yksilöintitiedoissa välitystiedosta, ja milloin CSIRT-yksiköllä tarkalleen ottaen on oikeus käsitellä välitystietoja ja milloin ei.

Suurin osa telepäätelaitteen yksilöivistä tiedoista on välitystietoa - Liikenne- ja viestintävirasto Traficomin mukaan jopa päätelaitteen mallitieto eli TAC-koodi - joten säännöskohtaisiin perusteluihin on saatava selkeyttä erityisesti mainittujen tietojen välitystietoluonteeseen. Nyt ehdotetussa muodossa vaarana on, ettei pykälää pystytä soveltamaan käytännössä sen ristiriitaisuuden vuoksi. Lisäksi hallituksen esitykseen on lisättävä erikseen selventävä mainita, ettei tällä kavenneta teleyrityksen sähköisen viestinnän palveluista annetun lain 138 § ja 272 § mukaisia käsittelyperusteita.

Kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä koskevan ehdotetun uuden lain 22 §:n 4 momentti, tietoturvaloukkausten havainnointipalveluun liittyvää tiedonkäsittelyä koskeva 23 § ja kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttamista koskeva 24 § ovat erityissääntelyä suhteessa sähköisen viestinnän palveluista annettuun lakiin koskien sähköisen viestinnän tietojen luovuttamista. Esitysluonnoksesta jää epäselväksi, voiko 22 §:ssä tarkoitettuihin vapaaehtoisiin jakamisjärjestelyihin osallistuva olla yksityinen taho, esimerkiksi teleyritys, vai ainoastaan viranomainen. Jos vapaaehtoisiin jakamisjärjestelyihin osallistuva taho voi olla ns. kuka tahansa, 22 §:n 4 momentin säännöksillä siitä, kuinka sen lisäksi, mitä sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetään tietojen luovuttamisesta, CSIRT-yksikkö voi luovuttaa jakamisjärjestelyyn osallistuvalle taholle ehdotetun uuden lain mukaisia tehtäviä suorittaessaan saamansa tiedon kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, laajentaa huomattavasti sitä piiriä, jolle viranomainen voi SVPL 319 § 3 momentin nojalla luovuttaa näitä tietoja. On perusteltua kysyä, onko tällainen laajennus tarkoituksenmukainen? Lisäksi säännöksen perusteluissa tulee selventää, mikä jakamisjärjestelyihin osallistuvan tahon käsittelyperuste on SVPL:n nojalla.

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-yksiköllе 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 esitysluonnoksessakin todetaan, kyberturvallisuusosaajista on Suomessa pulaa. Tämä saattaa aiheuttaa rekrytointihaasteita sekä viranomaisille että sääntelyn kohteena oleville toimijoille (s. 84). Lähivuosina EU:sta on tulossa myös 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

Esitysluonnoksen mukaan uuden ehdotetun kyberturvallisuuden riskienhallinnasta annetun lain 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. 130). Vastaavasti julkisen hallinnon tiedonhallinnasta annettuun lakiin ehdotetaan uutta poikkeamailmoituksen vastaanottamista koskevaa 18 d §:ää, jonka mukaan Liikenne- ja viestintäviraston on ilman aiheetonta viivytystä 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. 166).

Mainitussa tiedonhallintalain uudessa 18 d §:n 1 momentissa asetetaan viranomaisille velvoite toimittaa ilman aiheetonta viivytystä, viimeistään 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta, 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. 166). Esitysluonnoksessa on ehdotettu lisäksi käytettävän NIS2-direktiivin 34

artiklan 7 kohdan mukaista kansallista liikkumavaraa siitä, ettei julkishallinnon toimijoille määrätä direktiivin edellyttämiä hallinnollisia sanktioita.

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 seuraavalla viikolla arjen koitettua. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen 24/7-päivystys on säilytettävä.

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

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. 177). Esitysluonnoksessa 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 lakiin kyberturvallisuuden riskienhallinnasta, ja sektorikohtaisesta lakitasoisesta sääntelystä luovuttaisiin kokonaan?

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

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Metsola Asko
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry