FiCom ry | Asko Metsola
1.3.2021

FiComin lausunto NIS 2.0 -direktiivistä

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston kirjelmästä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (COM (2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta (verkko- ja tietoturvadirektiivi). FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Sääntelyn soveltamisalaa on selvennettävä.
- Ehdotuksesta aiheutuvat lisäkustannukset ovat merkittäviä ja epäsuhdassa sen tavoitteisiin nähden.
- Päällekkäistä sääntelyä ja raportointia tulee välttää.
- Riskienhallintatoimenpiteiden tulee olla oikeasuhteisia ja huomioida sektori- ja toimijakohtaiset erityispiirteet.
- Kansallisten ja EU-viranomaisten toimivaltuuksien rajat tulee määritellä tarkemmin.

Komissio on uudelleenarvioituaan vuoden 2020 aikana verkko- ja tietoturvadirektiiviä (NIS-direktiivi) ja sen soveltamiskokemuksia päätynyt ehdottamaan uutta, ns. NIS 2.0 -direktiiviä kyberturvallisuuden korkean tason varmistamiseksi EU:n alueella. Uudessa direktiivissä toimijat jaettaisiin keskeisiin ja tärkeisiin toimijoihin. Ehdotuksen mukaan digitaalisen infrastruktuurin toimijat kuuluisivat keskeisten toimijoiden kategoriaan ja myös datakeskuspalveluntarjoajat, sisällönjakeluverkkojen tarjoajat, luottamuspalveluiden tarjoajat, yleisten sähköisten viestinnän verkkojen ja palvelujen tarjoajat sekä pilvipalveluiden tarjoajat lisättäisiin uusina toimijoina digitaalisen infrastruktuurin toimijoihin. Lisäksi verkon kauppapaikkojen tarjoajat, verkon hakukoneiden tarjoajat sekä verkkoyhteisöalustojen tarjoajat luokiteltaisiin tärkeiksi toimijoiksi. Toimijoiden määritelmät, esimerkiksi pilvipalvelun osalta, ovat kuitenkin epäselvät ja niitä tulee tarkentaa.

Direktiivin velvoitteita ehdotetaan kohdistettavan merkittävään määrään toimijoita tai toimintoja, joille tällaiset vaatimukset ovat täysin uusia. Komissio on arvioinut sääntelystä aiheutuvan 22 % kasvun toimijoiden ICT-kustannuksiin ensimmäisten implementointivuosien aikana, ja niidenkin toimijoiden, jotka kuuluvat jo ensimmäisen NIS-direktiivin soveltamisalaan, kustannukset nousisivat komission arvion mukaan 12 %. Komission mukaan arvioidut lisäkustannukset johtavat sopusuhtaiseen kustannus-hyötysuhteeseen ja vähentävät samalla kyberturvallisuushäiriöitä, mutta arviossa ei ole huomioitu aloja, joissa kyberturvallisuus on jo ennen ehdotetusta direktiivistä tulevia lisävelvoitteita ollut korkealla tasolla. Lisäkustannukset ovat merkittäviä ja epäsuhdassa direktiivin tavoitteisiin nähden.

Pienet- ja mikroyritykset jäisivät lähtökohtaisesti ehdotetun sääntelyn ulkopuolelle. Tästä huolimatta riskien uhkaa ja toisaalta sääntelyn vaikutuksia ei ole ehdotuksessa suhteutettu tarpeeksi toimijoiden kokoon. Suuriin toimijoihin kohdistuu tulevaisuudessa lukuisista muista säädöksistä johtuvia velvoitteita, jolloin kokonaisuudella voi olla jo kilpailullisiakin vaikutuksia. Kuten valtioneuvostokin on kannassaan todennut,

verkko- ja tietoturvaa koskevien uusien velvoitteiden ja vaatimusten tulee olla oikeasuhtaisia ja riskiperusteisia soveltamisalaan kuuluvien toimijoiden kokoon ja toimintaan nähden, sektorikohtaiset erityispiirteet huomioon ottaen. Lisäksi komissio ei ole riittävästi arvioinut sitä, millainen suhde nyt ehdotettavalla sääntelyllä on esimerkiksi eIDAS-sääntelyn, yleisen tietosuoja-asetuksen tai viime vuonna Suomessa täytäntöön pannun telepakettidirektiivin kanssa. Ehdotettu direktiivi ei saa johtaa ylisääntelyyn.

Direktiivin kyberturvallisuusriskien hallintatoimenpiteitä koskevan 18 artiklan 1 kohdan mukaan riskienhallintatoimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen. Todellisuudessa eri toimijoilla on eri ikäisiä laitteita ja rakenteita, joten uusinta tekniikkaa ei voida käyttää kaikissa järjestelmissä. Hallintatoimenpiteet ovat muutenkin säädelty direktiivissä aivan liian yksityiskohtaisesti, sillä ne edustavat nyt ehdotetussa muodossa ideaalitilaa, jota suurimmillakaan toimijoilla ei ole kaikissa tilanteissa mahdollista toteuttaa.

18 artiklan 2 kohta, jonka mukaan toimenpiteisiin tulisi sisällyttää ainakin alakohdissa a-g luetellut toimenpiteet, tulee poistaa. Vaikka lista sisältää aiheellisia ja kannatettavia toimenpiteitä, ei niitä kaikkia kuitenkaan ole mahdollista tai järkevää toteuttaa esimerkiksi koko toimitusketjun kaikkien kumppaneiden kohdalla. Kohdan 2 yksityiskohtainen luettelo on myös ristiriidassa kohdassa 1 edellytettyjen asianmukaisten ja oikeasuhteisten toimenpiteiden kanssa, sillä ”ainakin” toteutettavat toimenpiteet eivät mahdollista toimenpiteiden oikeasuhteisuutta. Kohdan 2 listaan viittaava kohta 4 tulee myös poistaa. Lisäksi artiklan kohta 5, jonka mukaan komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan 2 kohdassa tarkoitettujen osatekijöiden teknisiä ja metodologisia eritelmiä rajaa liikaa toimijoiden mahdollisuuksia asianmukaisten ja oikeasuhteisten toimenpiteiden toteuttamiseen. Kyberturvallisuus on monisyinen ja laaja kokonaisuus, jonka sääntelyssä tulisi keskittyä siihen, että toimijat toteuttavat kunkin tilanteen kannalta oikeasuhteisia ja riittäviä toimenpiteitä sen sijaan, että sääntelyllä asetetaan tiettyjä lueteltuja keinoja, joita voi olla todellisuudessa jopa mahdoton toteuttaa. Lisäksi ehdotus ei ota lainkaan huomioon osaamiseen panostamista.

Ehdotuksen mukaan toimijoiden tulisi raportoida valvovalle viranomaiselle 24 tunnin kuluessa siitä, kun merkittäväksi arvioitu häiriö tai kyberloukkauksen uhka on tullut toimijan tietoon, minkä jälkeen toimijan tulisi toimittaa valvovalle viranomaiselle loppuraportti kuukauden kuluessa häiriöstä. Tiukan ilmoitusvelvollisuuden sijaan tulee tarkemmin arvioida, mitkä häiriöt ja uhat ovat sellaisia, että niistä tarvitsee ylipäätään ilmoittaa valvontaviranomaiselle. Lisäksi ilmoituksissa on huomioitava myös nyt ehdotettavien ilmoitusten kanssa mahdollisesti päällekkäinen, esimerkiksi yleisestä tietosuoja-asetuksesta aiheutuva ilmoitusvelvollisuus toiselle viranomaiselle. Jos ilmoitusvelvollisuus on joissain tilanteissa kahdelle eri viranomaiselle, tulisi se pystyä tekemään samalla kertaa, samojen määräaikojen mukaisesti. Päällekkäistä sääntelyä ja raportointia tulee välttää.

Ehdotus esittäisi keskeisille toimijoille jälkivalvonnan lisäksi myös ennakkovalvontaa. Valvontaviranomaiselle ehdotetaan lukuisia tehtäviä, kuten paikan päällä tehtäviä tarkastuksia ja etävalvontaa sekä toimijoihin kohdistettavia sattumanvaraisia tarkastuksia, säännöllistä auditointia, kohdennettuja turvallisuusauditointeja, turvallisuusskannauksia yms. Näiden osalta Suomessa tulee huolehtia Kyberturvallisuuskeskuksen riittävistä resursseista, mutta lisäksi on varmistettava, että mahdollisen kolmannen osapuolen suorittaman auditoinnin kustannukset toimijoille pysyvät kohtuullisina. Esimerkiksi

tilintarkastus joustaa yritysten koon suhteessa, mutta nyt ehdotettavassa sääntelyssä ei ole mitään takeita siitä, että ulkopuolisen suorittamassa kyberturvallisuusauditoinnissa huomioitaisiin erilaiset ja -kokoiset toimijat.

Komission ehdotuksen mukaan jäsenvaltioiden tulisi määrittää yksi tai useampi valvova viranomainen, joka olisi vastuussa laajamittaisten kyberturvallisuushäiriöiden ja -kriisien operatiivisesta johtamisesta. Olisi selkeämpää, että kukin jäsenvaltio nimeäisi vain yhden operatiivisesta johtamisesta vastaavan viranomaisen. Lisäksi kansallisten ja EU-viranomaisten toimivaltuuksien rajat tulee määritellä tarkemmin.

Kansallisille valvontaviranomaisille ehdotettavien uusien tehtävien lisäksi myös komissiolle ehdotetaan toimivaltaa tehdä arviointeja sekä kontrolleja. Lähtökohtaisesti teleyrityksien toimintaa sääntelee ja niitä koskevia määräyksiä antaa Traficom, joten ehdotus komission kansallisten valvontaviranomaisten kanssa päällekkäisistä toimivaltuuksista luo toimijoille epävarmuutta. Vastaavasti 19 artiklaan ehdotettu yhteistyöryhmän yhteistyössä komission ja ENISAn kanssa tekemä koordinoitu turvallisuusriskinarviointi yksittäisistä kriittisistä tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden toimitusketjuista on käytännön toimijoiden kannalta huolta aiheuttava ehdotus. Riskienhallinta on aina kokonaisvaltaista ja käytetyt keinot vaikuttavat riskiin merkittävästi. Jossain kokonaisuudessa tietty riskienhallintatoimenpide voi muodostaa turvallisen kokonaisuuden ja toisessa taas ei. Myös tältä osin sääntely on aivan liian yksityiskohtainen eikä ota huomioon yrityksissä riskienhallinnasta säännöllisesti käytävää tapauskohtaista arviointia.

Ehdotuksessa esitetään, että velvoitteiden laiminlyönnistä voisi seurata hallinnollinen sanktio, joka olisi enimmillään 10 miljoonaa euroa tai kaksi prosenttia toimijan vuosittaisesta liikevaihdosta. Vaikka sanktion taso määräytyisi ehdotetusti häiriön tai kriisin laajuuden ja aiheutetun vahingon mukaan, kyseessä on silti merkittävä seuraamus.