FiCom ry | ML
14.9.2023

**Liikenne- ja viestintävaliokunnalle**

# FiComin lausunto kybersolidaarisuussäädöstä koskevasta U-kirjelmästä

Liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston kirjelmästä (U 20/2023 vp) eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen). FiCom kiittää mahdollisuudesta lausua ja toteaa seuraavaa:

**FiComin keskeiset viestit**

- **Esityksen tavoite on ymmärrettävä, mutta se on kiireessä laadittu, monimutkainen ja epäselvä, eikä siitä ole tehty vaikutusarviointia.**
- **Valtioneuvoston kanta on kannatettava ja hyvin perusteltu.**
- **Kyberhätätilanteiden mekanismi ja kyberturvallisuusreservi edistävät suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia sisämarkkinoilla, mutta kyberturvallisuusreserviin pääsyn edellytykset tulee olla mahdollisimman selkeitä ja tasapuolisia.**
- **Yrityksille on aina ilmoitettava, jos kotimaiselle viranomaiselle annettuja tietoja luovutetaan ulkomaille tai jos säädöksen tarkoittama ”merkittävä tai laaja-alainen kyberturvallisuuspoikkeama” annetaan ENISA:n arvioitavaksi.**
- **Jos viranomaisille esitetään uusia toimivaltuuksia tai velvoitteita, pitää esitykseen kirjata suhteellisuus- ja välttämättömyysperiaatteet.**

**Esityksen tavoite**

Kybersolidaarisuussäädösehdotuksen yleisenä tavoitteena on vahvistaa EU:n yhteistä kyberhäiriöiden havainnointia, tilannekuvaa sekä kyvykkyyttä vastata kyberhäiriöihin. Sillä halutaan myös vahvistaa solidaarisuutta ja kriittisten toimijoiden toimintavalmiutta merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalle. Tavoitteena on myös edistää Euroopan teknologista riippumattomuutta kyberturvallisuuden alalla. Lisäksi halutaan parantaa kriisinsietokykyä ja edistää tehokasta toimintaa kyberhäiriöiden hallinnassa luomalla jälkikäteinen arviointimekanismi, jonka avulla arvioidaan merkittäviä tai laajamittaisia vaaratilanteita ja niiden hallinnasta saatuja kokemuksia.

Kyberturvallisuusasetukseen ehdotetuilla muutoksilla lisättäisiin tietoturvapalveluntarjoajat kyberturvallisuusasetuksen ja sen velvoitteiden piiriin. Muutoksella luotaisiin tietoturvapalvelutarjoajien sertifiointimekanismi, jolla pyritään lisäämään luottamusta näiden palvelujen laatuun ja siten helpottamaan luotetun eurooppalaisen kyberturvallisuuspalvelualan syntymistä sekä estämään palveluiden pirstaloituminen jäsenmaissa.

**Valtioneuvoston kanta on kannatettava ja hyvin perusteltu**

Esityksen tavoite on lähtökohtaisesti ymmärrettävä, kun otetaan huomioon muuttunut turvallisuustilanne Euroopassa, globaali vastakkainasettelu ja teknologiapolitiikan sekä suurvaltojen väliset jännitteet. Ehdotuksesta paistaa kuitenkin kauttaaltaan, että se on laadittu kiireellä. Ehdotus on monimutkainen ja epäselvä, eikä siitä ole laadittu vaikutusarvioita.

Ehdotetussa kybersolidaarisuussäädöksessä on lukuisia avoimia seikkoja, joita tulee sen jatkovaiheessa vielä merkittävästi tarkentaa ja muokata. Esimerkiksi uusien tilannekuva- ja tiedonvaihtotoimintojen perustaminen johtaa mitä todennäköisimmin päällekkäisyyksiin jo olemassa olevien kanssa, mikä voi aiheuttaa hallinnollisia ja operatiivisia ongelmia. Komissiolla ei aiemmin ole ollut ehdotuksen mukaista roolia kyberturvallisuusasioissa, eikä sille myöskään ole nähty tarvetta, joten komissiolle annettavan toimivallan siirtoa tulee tarkastella erittäin kriittisesti.

FiCom yhtyy valtioneuvoston näkemykseen siitä, että kyberhätätilanteiden mekanismi ja kyberturvallisuusreservi edistävät suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia sisämarkkinoilla sillä **lisäkriteerillä, että kyberturvallisuusreserviin pääsyn edellytykset ovat mahdollisimman selkeitä ja tasapuolisia.**

Valtioneuvoston kannan mukaan tietojen luovutuksesta ja tietojen vaihdosta tarvitaan lisätietoja. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti. FiCom on samaa mieltä, mutta kansallinen turvallisuus tulee ymmärtää laajasti, eikä pelkästään viranomaisnäkökulmasta.

Valtaosa yhteiskunnan kriittisistä toiminnoista – verkot, palvelut, järjestelmät ja ohjelmistot – ovat pääasiassa yksityisten yritysten omistamia ja tarjoamia. Yritykset vastaavat näiden kyberturvallisuudesta, ja toimintojen keskeinen lähtökohta on luottamus. Vahvin kyberturvallisuus rakentuu yritysten ja viranomaisten hyvällä ja luottamuksellisella yhteistyöllä.

Tätä tiedonvaihtoa ja luottamuksellisuutta koskevaa problematiikkaa on avattu hyvin U-kirjelmän sivulla 12. Ehdotus ei täsmennä riittävästi sitä, millaisesta ja minkä tasoisesta tiedonvaihdosta ehdotuksessa tosiasiassa on kyse, miten ja mikä tieto liikkuu eri SOC-verkostojen välillä ja miten sitä on mahdollista luovuttaa esimerkiksi yksityiselle sektorille.

FiCom esittää valtioneuvon kantaan lisättäväksi, että **yrityksille on ilmoitettava, jos kotimaiselle viranomaiselle annettuja tietoja luovutetaan ulkomaille tai jos säädöksen tarkoittama ”merkittävä tai laaja-alainen kyberturvallisuuspoikkeama” annetaan ENISA:n arvioitavaksi**.

Lopuksi FiCom toteaa, että kansallisen viranomaisen resursseista on huolehdittava, jos ja kun sille tulee esityksen myötä uusia tehtäviä, mutta hallinnollista taakkaa ei saa lisätä. Euroopan kyberturvallisuusvirasto ENISA:n tulee toiminnassaan välttää päällekkäisyyksiä kansallisten viranomaisten toimintojen kanssa. ENISA ei saa aiheuttaa yhtään suurempaa hallinnollista taakkaa kansallisille viranomaisille ja sitä kautta yrityksille kuin on aivan välttämätöntä tehtävien hoitamiseksi.

FiCom on valtioneuvoston kanssa samaa mieltä siitä, että kyberturvallisuuden operatiiviset tehtävät unionin tasolla kuuluu säilyttää ensisijaisesti ENISAlla. Ei ole syytä luoda uutta hallinnollista orgaania tai kerrosta esimerkiksi komissiolle. **Ehdotuksen jatkovalmistelussa on tarkoituksenmukaista tavoitella suhteellisuus- ja välttämättömyysperiaatteiden kirjaamista tilanteissa, joissa viranomaisille esitetään uusia toimivaltuuksia ja velvoitteita**.

**Tietoliikenteen- ja tietotekniikan keskusliitto FiCom ry**

Marko Lahtinen
lakiasiat