FiCom ry | ML
17.11.2022

Liikenne- ja viestintävaliokunnalle

FiComin lausunto kyberkestävyyssäädöksestä U 83/2022 vp

Liikenne- ja viestintävaliokunta on pyytänyt FiCom ry:ltä lausuntoa valtioneuvoston kirjelmästä U 83/2022 vp eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (kyberkestävyyssäädös). FiCom kiittää mahdollisuudesta lausua asiasta ja toteaa seuraavaa:

FiComin keskeiset viestit:

- **Valtioneuvoston kanta on kaikin puolin hyvin laadittu ja perusteltu. Kanta luo hyvän, tarpeellisen ja tässä vaiheessa riittävän kattavan ja seikkaperäisen mandaattipohjan tulevia trilogineuvotteluja varten.**
- **FiCom puoltaa valtioneuvoston kantaa ehdotuksen tarpeellisuudesta.**
- **On tärkeää, että sääntely on selkeää, eikä se ole päällekkäistä jo olemassa/vireillä olevan alemman tasoisen sääntelyn kanssa. Säädösten keskinäisten suhteiden on oltava selviä. Erityistä huomiota tulee kiinnittää siihen, että kyberkestävyyssäädös ei muiden säädösten kanssa luo päällekkäisiä velvoitteita tai päällekkäistä hallinnollista taakkaa sen kohteena oleville toimijoille.**
- **FiCom pitää valtioneuvoston kannan tavoin tärkeänä, että kyberkestävyyssäädöksen vaatimukset ja arviointimenettely ovat riskiperusteisia ja että ulkopuolisen ilmoitetun laitoksen suorittamaa arviointia edellytetään vain kaikkein kriittisimmiltä verkkolaitteilta. Muiden tuotteiden osalta riittäisi lähtökohtaisesti valmistajan itsearviointi.**
- **Vaatimustenmukaisuusarvioinnit eivät saa muodostaa pullonkaulaa ja aiheuttaa viiveitä uuden teknologian käyttöönottoon ja siten heikentää EU-alueen kilpailukykyä. Ehdotuksen vaatimukset eivät saa hidastaa esimerkiksi kansallisesti tärkeiden 5G- ja 6G-verkkojen kehittämistä ja rakentamista.**
- **Säädöksessä komissiolle esitetään annettavaksi delegoitua lainsäädäntövaltaa. Tämän toimivallan on oltava selkeää, tarkkarajaista, oikeasuhtaista, tarkoituksenmukaista ja hyvin perusteltua, jotta sääntelystä ja velvoitteiden laajuudesta ei muodostu ennustamatonta.**

Kyberkestävyyssäädöksen tavoite ja soveltamisala

Euroopan komissio antoi 15.9.2022 ehdotuksen kyberkestävyyssäädökseksi (Cyber Resilience Act, CRA). Sen tavoitteena on saada markkinoille turvallisempia tuotteita ja tehdä turvallisuusseikoista kuluttajille ja muille käyttäjille läpinäkyvämpiä ja samalla kasvattaa EU:n kyberpuolustuskykyä. Tavoitteena on tälläkin tavoin suojella kuluttajia, muita käyttäjiä ja markkinaa kyberturvallisuusloukkauksilta. Tarkoitus on varmistaa, että laitteissa ja ohjelmistoissa on vähemmän haavoittuvuuksia, ja valmistajat ottavat turvallisuusnäkökohdat vakavasti tuotteen koko elinkaaren ajan.

Sääntelyn soveltamisala kattaisi tuotteet, joissa on digitaalinen elementti ja jotka ovat tai joiden katsotaan olevan liitettävissä toiseen laitteeseen tai verkkoon joko suoraan tai epäsuorasti. Sääntely kattaisi myös ohjelmistot. Soveltamisalan ulkopuolelle jäisivät erikseen säädetyt kohteet, kuten siviili-ilmailu ja yksinomaan kansallisen turvallisuuden tai maanpuolustuksen käyttöön tehdyn laitteet ja ohjelmistot.

Sensitivity: Confidential

Markkinoille saisi jatkossa tuoda vain tuotteita ja ohjelmistoja, jotka täyttävät asetuksen vaatimukset. Vaatimusten täyttymisestä voidaan poiketa muun muassa näyttely- ja demonstraatiotarkoituksissa tai keskeneräisen ohjelmiston rajoitetussa testauksessa, kunhan käy selvästi ilmi, että se ei täytä asetuksen vaatimuksia. Vaatimuksenmukaisuus ilmaistaisiin CE-merkinnällä.

Ehdotus sisältää velvoitteet valmistajalle, maahantuojalle ja jakelijalle. Lisäksi ehdotus sisältää säännökset vaatimustenmukaisuuden arvioinnista, vaatimustenmukaisuuden arviointilaitoksista, markkinavalvonnasta ja täytäntöönpanosta sekä seuraamusmaksuista.

FiCom puoltaa valtioneuvoston kantaa

Valtioneuvoston kanta on kaikin puolin hyvin laadittu ja perusteltu. Se luo hyvän, tarpeellisen ja tässä vaiheessa riittävän kattavan ja seikkaperäisen mandaattipohjan tulevia trilogineuvotteluja varten.

FiCom puoltaa valtioneuvoston kantaa ehdotuksen tarpeellisuudesta. On syytä huomioida se, että ehdotus ei koske ainoastaan kuluttajatuotteita, vaan myös tukku- ja yritystuotteita sekä esimerkiksi suljettuja verkkoja ja niiden tuotteita eli niin sanottuja privaattiverkkoja.

Kyberkestävyyssäädös on tärkeä osa säädösketjua, jossa kriittisen infrastruktuurin direktiivi (Critical Entities Resilience Directive, CER) turvaa huoltovarmuuskriittisten toimijoiden ja palveluiden resilienssiä ja verkko- ja tietoturvadirektiivi (NIS 2) puolestaan verkko- ja pilvipalvelutoimijoiden resilienssiä.

Ehdotus lisää verkkoturvallisuutta niillä alueilla, joihin tietoturvallisuutta koskeva sääntely ei ole vielä kohdistunut. Muiden säädösten kanssa tulee kuitenkin olla hyvin tarkkana. FiCom näkemyksen mukaan keskeistä on sääntelyn selkeys. Se ei saa olla päällekkäistä jo olemassa/vireillä olevan alemman tasoisen sääntelyn kanssa, ja säädösten keskinäisten suhteiden on oltava selviä. Erityistä huomiota tulee kiinnittää siihen, että kyberkestävyyssäädös ei muiden säädösten kanssa luo päällekkäisiä velvoitteita tai päällekkäistä hallinnollista taakkaa sen kohteena oleville toimijoille. Esimerkiksi tietoturvaloukkauksiin liittyvän ilmoitusvelvollisuuden tulee olla selkeä niin, että samasta tapahtumasta raportoidaan vain yhdelle viranomaiselle, eikä eri säädöksistä tule rinnakkaisia ilmoitusvelvollisuuksia eri viranomaisille.

Sääntely ei saa heikentää kilpailukykyä eikä 5G ja 6G -verkkojen kehitystä ja rakentamista

FiCom katsoo valtioneuvoston tavoin, että vaatimustenmukaisuuden täyttymisen arvioinnissa on tarpeen hyödyntää mahdollisimman pitkälle hyväksi havaittuja, jo olemassa olevia menettelyjä. Uusia yhteisiä vaatimuksia tulee asettaa vain silloin, kun niitä ei ole olemassa. Vaatimuksenmukaisuusarviointia koskevien kriteerien ja arviointiprosessin tulee olla läpinäkyviä ja ennustettavia ja perustua mm. kansainvälisiin standardeihin, jotta asetusta sovelletaan yhdenmukaisesti koko EU-alueella.

Vaatimustenmukaisuusarvioinnit eivät saa muodostaa pullonkaulaa ja aiheuttaa viiveitä uuden teknologian käyttöönottoon ja siten heikentää EU-alueen kilpailukykyä. Esimerkiksi mobiiliverkkoteknologioissa tehdään jatkuvaa ja laajamittaista kansainvälistä standardointityötä, jossa yhtenä keskeisenä ominaisuutena on verkkoturvallisuus. Tämä tulisi huomioida vaatimuksissa. Ehdotuksen vaatimukset eivät saa hidastaa esimerkiksi kansallisesti tärkeiden 5G- ja 6G-verkkojen rakentamista siitä syystä, että verkkolaitteet eivät saa ehdotuksessa edellytettyjä hyväksyntöjä, prosessi kestää liian pitkään tai arviointilaitoksissa on ruuhkaa.

FiCom pitää valtioneuvoston kannan tavoin tärkeänä, että kyberkestävyyssäädöksen vaatimukset ja arviointimenettely ovat riskiperusteisia, ja ulkopuolisen ilmoitetun laitoksen suorittamaa arviointia edellytetään vain kaikkein kriittisimmiltä verkkolaitteilta. Muiden tuotteiden osalta riittäisi lähtökohtaisesti valmistajan itsearviointi. Riskiperusteinen lähestymistapa velvoitteisiin on keskeistä, jotta

velvoitteet ovat oikeassa suhteessa riskiin nähden. Liian raskaita velvoitteita ei tule asettaa silloin, kun niille ei ole perusteltua tarvetta.

Ehdotuksessa komissiolle esitetään annettavaksi delegoitua lainsäädäntövaltaa. Tämän toimivallan on oltava selkeää, tarkkarajaista, oikeasuhtaista, tarkoituksenmukaista ja hyvin perusteltua, jotta sääntelystä ja velvoitteiden laajuudesta ei muodostu ennustamatonta.

Tietoliikenteen- ja tietotekniikan keskusliitto FiCom ry

Marko Lahtinen
lakiasiat

Sensitivity: Confidential