Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Asiantuntijapyyntö Liikenne- ja viestintävaliokunta perjantai 18.11.2022 klo 11.15 / U 83/2022 vp /

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen lausunto kyberkestävyyssäädöksestä

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselta lausuntoa koskien U-kirjettä U 83/2022 vp Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (kyberkestävyyssäädös).

Kyberturvallisuuskeskus kiittää mahdollisuudesta lausua asiasta ja kannattaa esitystä.

Yleistä

Internetiin suoraan tai välillisesti liitettävien digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuus on tärkeää yksilön yksityisyyden ja fyysisen sekä taloudellisen turvallisuuden takaamiseksi. Tuotteiden määrän lisääntyessä jatkuvasti niiden kyberturvallisuudella on keskeinen merkitys myös yhteiskunnan digitaalisten ratkaisujen ja palveluiden turvaamisessa sekä tietoverkkojen toimintavarmuuden varmistamisessa.

Traficomin Kyberturvallisuuskeskus valvoo, että Suomessa on toimivat ja turvalliset tietoverkot. Kyberturvallisuuskeskus tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. Lausunto on laadittu tehtävien hoitamisen näkökulmasta.

Säädöksen soveltamisala, vastuut ja suhde muuhun sääntelyyn

Säädöksen soveltamisalaan kuuluvat tuotteet toimivat lähtökohtaisesti osana laajaa digitaalista ekosysteemiä, johon kohdistuu monenlaista sääntelyä ja jonka toimintaan osallistuu monia eri tahoja.

Kyberturvallisuuskeskus kannattaa vastuun kohdentamista aiempaa voimakkaammin kuluttajalta valmistajalle. Vastuiden kohdentamisen ja rajaamisen näkökulmasta on tärkeää, että valmistajat, jälleenmyyjät ja maahantuojat pystyvät tunnistamaan selkeästi vastuunsa. Kaikkien toimijoiden tulisi pystyä muodostamaan selkeä kokonaiskuva säädösten välisistä suhteista sekä eri säädösten soveltamisalasta. Kyberturvallisuuskeskus katsoo, että on tärkeää välttää päällekkäistä sääntelyä.

Kyberturvallisuusvaatimukset, suhteellisuusperiaate ja säädöksen siirtymäaika

Kyberturvallisuuskeskuksen kokemuksen perusteella asetuksen soveltamisalaan kuuluvien tuotteiden nykyinen kyberturvallisuustaso on suurelta osin puutteellinen. Tuotteiden kyberturvallisuustason nostaminen vaatii aikaa, työtä ja osaamista,

jonka lisääminen vie aikaa ja sekä taloudellisia että henkilöresursseja. Nykyisistä osaajista on suurempi kysyntä kuin tarjonta, ja säädös voimaan astuessaan tullee lisäämään kysyntää ja koulutustarvetta voimakkaasti. Kyberturvallisuuskeskus pitää tärkeänä, että säädöksestä seuraava kasvava koulutustarve tunnistetaan ja siihen reagoidaan kansallisella tasolla.

Kyberturvallisuuskeskus katsoo, että edellä mainitut seikat olisi hyvä huomioida myös säädöksen jatkovalmistelussa, kun tarkastellaan tarvittavaa siirtymäaikaa sekä tavoitteita liittyen säädöksessä asetettuun kyberturvallisuustasoon ja vaatimusten kattavuuteen. Kyberturvallisuuskeskus kannattaa kattavaa ja riittävän kyberturvallisuustason takaavaa sääntelyä painottaen, että tuotteille asetettavien vaatimusten ja niiden todentamiskäytäntöjen tulee olla huolellisesti mitoitettuja ja suhteessa tuotteeseen kohdistuviin riskeihin.

Markkinavalvonta, ilmoitetut laitokset ja viranomaisvaikutukset

Säädöksen soveltamisalaan kuuluviin tuotteisiin ei tähän saakka ole kohdistunut pakottavia kyberturvallisuusvaatimuksia eikä siten myöskään markkinavalvontaa. Tuotteille ei myöskään ole olemassa vakiintuneita ja yleisesti hyväksyttyjä kyberturvallisuusvaatimuksia testauskäytäntöineen. Tämän vuoksi säädöksen toimeenpano edellyttää vaatimusten ja niiden vaatimustenmukaisuuden valvontakäytäntöjen luomista. Lisäksi tulee määrittää riittävät kyvykkyydet ja osaaminen vaatimuksenmukaisuutta arvioiville yksityisen sektorin ilmoitetuille laitoksille.

Tavat, joilla kyberturvallisuusvaatimuksia tällä hetkellä testataan, eivät kaikilta osin sovi yhteen muilla toimialoilla vakiintuneiden markkinavalvonnan käytäntöjen kanssa. Vaatimustenmukaisuuden tarkastamisessa pyritään asettamaan vaatimukset, joiden täyttyminen todetaan yksiselitteisesti (kyllä/ei). Kyberturvallisuusvaatimukset ja niiden testauskäytännöt eivät monilta osin tue tällaista lähestymistapaa, minkä vuoksi säädöksessä asetettujen vaatimusten tulkinta teknisellä tasolla ja testauksessa tulee vaatimaan erityistä huolellisuutta. Kyberturvallisuuskeskus pitää tärkeänä, että työssä huomioidaan erityisesti asetettujen vaatimusten kustannusvaikutukset ja saavutettavien hyötyjen oikeasuhtaisuus.

Säädöksen edellyttämät vaatimukset testaus- ja valvontakäytäntöineen joudutaan luomaan suurelta osin alusta pitäen. Tuotteiden tämänhetkinen vaatimaton kyberturvallisuustaso edellyttää riittävää markkinavalvontaa säädöksen vaikuttavuuden varmistamiseksi. Kyberturvallisuuskeskus pitääkin erityisen tärkeänä sitä, että säädöksen toimeenpanossa otetaan huomioon kyberturvallisuustoimialan nuoruudesta seuraava poikkeuksellinen tarve luoda uusia määrityksiä, vaatimuksia ja käytäntöjä. Tämä edellyttää tiivistä yhteistyötä eri viranomaisten ja yksityisen sektorin välillä sekä riittävän resursoinnin varmistamista vastuuviranomaisissa.