Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

17.11.2022

Eduskunta
Liikenne- ja viestintävaliokunta

Viite: U 83/2022 vp / Asiantuntijapyyntö

Lausunto: Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (kyberkestävyyssäädös)

Finnish Information Security Cluster – Kyberala ry, joka on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa, kiittää mahdollisuudesta lausua asiasta.

Kyberala pitää U-kirjettä sekä siinä muodostettua Valtioneuvoston kantaa hyvin valmisteltuna ja perusteltuna, sekä **kannattaa ehdotuksen tavoitteita ja soveltamisalaa**, tarkentaen kuitenkin joitain kohtia seuraavasti:

Kyberala katsoo Valtioneuvoston kantaa mukaillen, että neuvottelujen kuluessa asetuksen **soveltamisalasta tulee pyrkiä saamaan mahdollisimman selkeä**, ja että esimerkiksi digitaalisia elementtejä koskevaa määritelmää kuvataan laajemmin asetuksen ”resitaaliosassa”. Sama koskee eri säädösten keskinäisiä suhteita, mm. datasäädös, GDPR, NIS2-, CER-, tuotevastuudirektiivi, tekoälyasetus sekä radiolaitedirektiivin delegoitu säädös.

Ehdotuksella on mahdollisuus horisontaalisena säädöksenä **parantaa kaikkien yhteiskunnan toimijoiden tietoturvaa tosiasiallisesti**. EU:n alueelle sijoittautuneet yritykset ja kuluttajat tarvitsevat tietoturvavastuun aiempaa tasapainoisempaa jakamista heidän itsensä ja digitaalisia elementtejä sisältävien tuotteiden valmistajien välillä.

Pilvipalveluita hyödyntävien tuotteiden osalta tulee varmistua siitä, että ehdotus muodostaa selkeät rajat vastuiden ja velvoitteiden osalta ja on selkeä suhteessa muihin pilvipalveluita koskeviin säädöksiin kuitenkaan heikentämättä ehdotuksen tavoitteita tai **rajaamatta pilviteknologiaa hyödyntäviä tuotteita soveltamisalan ulkopuolelle.** Digitaaliset palvelut sinänsä on jo rajattu ehdotuksen ulkopuolelle. Laitteiden ja ohjelmistojen, jotka hyödyntävät pilvilaskentaa tai -tallennuskapasiteettia tulee olla yhtä turvallisia kuin muidenkin soveltamisalaan kuuluvien laitteiden ja ohjelmistojen.

Säädös on perusteltu, vaikka erityisesti valmistajille (ml. maahantuojat ja jakelijat) tulisi vaatimustenmukaisuuden noudattamisesta uusia kustannuksia, sillä **tähän asti tuotteiden ja ohjelmistojen loppukäyttäjät ovat vastanneet valtaosasta tietoturvallisuuden kustannuksista**. Syntyviä kustannuksia ei välttämättä ole pidettävä kokonaan uusina kustannuksina, vaan kyseessä on pikemminkin **kustannusten jakaminen loppukäyttäjän ja valmistajan (ml. maahantuoja/jakelija) välillä**. Kustannusten jakautumista voidaan verrata esimerkiksi sähkölaitteiden tai ajoneuvojen turvallisuuteen, joiden suhteen valmistaja vastaa osaltaan tuotteiden käyttöturvallisuudesta. Selvää on, että loppukäyttäjille jää kytkettyjen laitteiden ja ohjelmistojen tietoturvallisuuden parantamisen jälkeenkin edelleen merkittävä toiminnallinen vastuu, sekä kustannusvastuu kehittää ja ylläpitää asianmukaista tietoturvaa yhä heikkenevässä digitaalisessa turvallisuusympäristössä.

Eteläranta 10, PL 10, 00131 Helsinki

Aiemmin on voitu suhtautua kriittisesti esim. kansallisiin (pakollisiin) tietoturvamerkkeihin- tai sertifiointeihin eritoten pk-yrityksiin kohdistuvan kustannusrasituksen sekä kehityksen hidastumisen vuoksi. Laajemminkin kansalliset ratkaisut voivat pahimmillaan heikentää kansainvälistä kilpailukykyä, mm. hintakilpailukyvyn tai markkinanoille tuomisen hidastumisen myötä. Koska kyberkestävyyssäädöksen tietoturvaan liittyvät vaatimukset tulevat käytännössä korvaamaan kansalliset ratkaisut, ehdotus on perusteltu myös siksi, että näin **vaatimukset koskevat yhtäläisesti kaikkia sisämarkkinoille asetettuja tuotteita riippumatta ovatko ne valmistettu EU:ssa tai muualla**, jolloin myös kustannusseuraukset kohdistuvat valmistajille tasapuolisesti.

Kyberalan näkemyksen mukaan digitaalisen elementin sisältävistä tuotteista on **välttämätöntä riskiperusteisesti erottaa tietojärjestelmien turvallisuuden kannalta tuotteet, joiden turvallisuusvaatimusten täyttymistä valvottaisiin vahvemmin ulkopuolisen ilmoitetun laitoksen toimesta**. Tätä luokittelua tehtäessä nojattava valmistajan asettamaan tuotteiden pääasialliseen käyttötarkoitukseen. Tähän kytkeytyen kansainvälisen kaupan ja kilpailukyvyn kannalta tuleekin etupainotteisesti panostaa kansallisesti tuotteiden tietoturvallisuuden **arviointilaitosten riittävyyteen ja arviointilaitosten kykyyn** käsitellä kolmannen osapuolten arviota vaativien tuotteiden hyväksynnät.

Edellä mainittuun liittyen jatkovalmistelussa tulee kiinnittää tarkkaa huomiota sääntelyn selkeyteen siinä, millainen muutos (ohjelmistopäivitys) tuotteeseen voi johtaa **vaatimuksenmukaisuuden uudelleen osoittamiseen arviointilaitosmenettelyn piirissä**. Uusien ominaisuuksien tuominen laitteeseen tai ohjelmistoon ei saa johtaa kohtuuttomiin viivästyksiin tai kustannuksiin valmistajille.

Tuotteiden kyberturvallisuuden vaatimustenmukaisuuden tulee käydä tuotteesta selkeästi ilmi. CE-merkinnän osalta tulisikin ilmetä, että kyseessä on nimenomaan kyberturvallisuuteen liittyvä merkintä (verrattuna samassa tuotteessa esiintyviin muihin CE-merkintöihin, jotka tuotteella voi olla, kuten sähköturvallisuus jne.).

Jatkovalmistelussa on tarpeen **arvioida etämyynnin sekä verkkomarkkinapaikkojen asemaa** sekä ehdotuksen suhdetta kolmansissa valtioissa sijaitseviin valmistajiin sen varmistamiseksi, että Unionin sisämarkkinoille ei päädy tuotteita esimerkiksi tuotekuvauksessa vain nimellisesti lähellä sijaitsevan kolmannen maan markkinoille ”tarkoitettuja” tuotteita tai ohjelmistoja.

Komissiolle ehdotetun delegoidun säädösvallan osalta Kyberala pitää tarpeellisena, että neuvottelujen edetessä **arvioidaan delegoidun säädösvallan tarvetta ja laajuutta**.

Lisätiedot:

Toimitusjohtaja Peter Sund
sähköposti: peter.sund@teknlogiateollisuus.fi
puhelin: 050 565 0621