Teknologiateollisuus

Eduskunta
Liikenne ja viestintävaliokunta
LIV@eduskunta.fi

1.3.2021

Asiantuntijapyyntönne 25.2.2021

Valtioneuvoston kirjelmä 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)

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Kyberala ry kiittää mahdollisuudesta antaa asiantuntijalausuntonsa otsikossa mainitussa asiassa.

Kyberala katsoo, että uudistettavan verkko- ja tietoturvadirektiivin (NIS) tavoitteet ovat monin paikoin tarpeellisia. On tärkeää, että merkittävien toimialojen ja niiden toimitusketjujen kyberturvallisuuteen kiinnitetään kasvavasti huomiota yhteiskuntien digitaalisen sieto- ja toimintakyvyn turvaamiseksi.

Soveltamisalan laajentuminen edellyttää lisää selkeyttä

Kyseessä on merkittävä aiemman NIS-direktiivin soveltamisalan laajennus kokonaan uusille aloille. Direktiivi vaikuttaa näiltä osin paikoin vaikeatulkintaiselta. Monet käsitteet, rajanvedot ja velvoitteet kaipaavat siksi edelleen selkeyttämistä. Vaikeatulkintaisuudesta johtuen on todennäköistä, että myös jäsenvaltioiden viranomaisilla tulee olemaan tulkintahaasteita kansallisella ja EU-tasolla. Jo pelkästään kilpailukyky- ja tasapuolisuuskysymyksistä johtuen on erittäin tärkeää, että sääntelyä selkeytetään ja harmonisoidaan sekä varmistetaan yhdenmukaiset tulkinnat eri jäsenvaltioissa. Lisäksi on varmistettava, että ehdotus on sopusoinnussa muun olemassa olevan tai valmisteltavan EU-sääntelyn kanssa.

Hallinnollisen kuorman sijaan tarvitaan toimivia ja tehokkaita investointeja

Direktiivin kyberturvallisuuden kehittämistoimien painopiste vaikuttaa olevan erityisesti yritysten raportointivelvoitteiden kasvattamisessa. Se tarkoittaa pahimmillaan hallinnollisen kuormituksen kasvamista varsinaisen tietoturvallisuuden kustannuksella. Samoin laajenevat velvoitteet tarkoittavat kasvavaa riskiä päällekkäisestä ja moninkertaisesta raportoinnista eri viranomaisille. Kyberalan näkökulmasta yrityksille tulisi tuottaa kannusteita laadukkaaseen riskienhallintaprosessiin perustuviin ja tehokkaisiin investointeihin, joilla kyberturvallisuuden tasoa olisi mahdollista aidosti parantaa. Se voitaisiin toteuttaa esimerkiksi toimialoille suunnattujen kohdennettujen rahoitusvälineiden ja -ohjelmien avulla.

Tiedonvaihdon ja -kulun parantamisen tulisi edistää yhteistyötä

Parhaimmillaan tiedon jakaminen on silloin kun molemmat osapuolet hyötyvät siitä. Tehostuva jäsenvaltioiden välinen viranomaisyhteistyö ja parempi tiedonvaihto ovat tärkeitä tavoitteita, mutta

Teknologiateollisuus ry
Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

tiedonvaihdon tulisi hyödyttää myös yksityisen sektorin toimijoita. Tietoja lakisääteisten velvoitteiden perusteella luovuttavien toimijoiden tulisi siksi saada viranomaisilta palautetta ja analysoitua hyödynnettävissä olevaa tietoa käyttöönsä. Kaikkiaan direktiivistä puuttuu tällä hetkellä tietoturvallisuuden parantamiseen kannustava julkisen ja yksityisen sektorin välinen yhteistyö, painopisteen jäädessä taloudellisten sanktioiden uhalla velvoitettuihin toimiin.

Riskiperusteisuus on onnistumisen edellytys muuttuvassa ympäristössä

Kyberala pitää hyvänä, että direktiivissä korostetaan kattavan ja laadukkaan riskienhallinnan merkitystä. Vain siten on mahdollista turvata onnistuneet ja oikein kohdennetut panostukset. On kuitenkin huomioitava, että ehdotuksessa tehokas riskienhallinta liudentuu monin osin, koska mainitusta riskiperusteisuudesta huolimatta yrityksille asetetaan runsaasti pakollisia kontrollikeinoja, joiden skaalautuvuus eri toimialoille, yritysten kokoluokkiin sekä kyberturvallisuuden tasoon on väistämättä haastavaa. Siksi tulisi etukäteen määriteltyjen kontrollikeinojen sijaan määritellä toimenpiteiden päämäärät ja tavoitteet. Tällöin myös nopeasti muuttuvassa uhkaympäristössä ja teknologioiden kehittyessä erilaisiin uhkiin voitaisiin vastata joustavasti ja tehokkaasti.

Sertifiointi

Direktiivissä ehdotetaan pakollista sertifiointia tietyille toimijoille. Kyberala kiinnittää huomiota siihen, että EU:n kyberturvallisuusasetuksessa sertifiointi on määritelty vapaaehtoiseksi. Sertifiointia voidaan luonnollisesti suositella ja hyödyntää kyberturvallisuuden parantamisessa ja luottamuksen kasvattamisessa, mutta pakollisuudella voi olla arvaamattomia seurauksia sekä eri kokoisille yrityksille että markkinoiden toiminnalle. Lähtökohtaisesti olisi perusteltua hyödyntää jo olemassa olevia, tunnustettuja ja yhdessä teollisuuden kanssa kehitettyjä kansainvälisiä kehyksiä vapaaehtoisuuden pohjalta. Uusien tiukkojen ja lakisääteisten sertifiointivaatimusten seurauksena voisi olla eurooppalaisen kasvun ja innovointihalukkuuden heikentyminen.

Viranomaistehtävien kasvattamisen sijaan on panostettava yhteistyöhön

Direktiivin perusteella valvontaviranomaisille olisi tulossa uusia tarkastustehtäviä, jotka tarkoittavat esimerkiksi erilaista ennakkovalvontaa, auditointeja ja skannauksia. Kyberala muistuttaa, että viranomaisresurssien ja -tehtävien voimakas kasvattaminen jo tällä hetkellä työvoimapulasta kärsivällä alalla on teollisuudelle merkittävä haaste.

Kyberala katsoo, että esitettyjä tarkastuksia ja auditointeja ei tule asettaa yksinomaan viranomaistehtäväksi, vaan niissä tulisi voida hyödyntää alan yrityksissä olevaa osaamista ja voimavaroja. Tätä mallia voitaisiin verrata yrityksiin kohdistuvaan tilintarkastustoimintaan ja se toisi järjestelmään joustavuutta sekä samalla tukisi eurooppalaisen kyberturvallisuusteollisuuden kehittymistä ja kasvua.