Finnish Information Security Cluster
Kyberala

15.4.2026

Eduskunta
Suuri valiokunta

Viite: U 17/2026 vp

Lausunto: Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS2-muutosdirektiiviksi

Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa. Yhdistyksen tarkoituksena on edistää digitaalisten teknologioiden riskienhallintaa, toimialan kilpailukykyä ja toimintaedellytyksiä sekä digitaalista turvallisuutta Suomessa ja EU:ssa yhteistyössä julkishallinnon, yritysten ja kansalaisyhteiskunnan kanssa.

Tausta

Komissio on antanut lakiehdotukset koskien kyberturvallisuusasetuksen (CSA2) kokonaisuudistusta sekä siihen liittyvän NIS2-direktiivin muutoksista (NIS2.5). CSA2-ehdotuksen tavoite on luoda vahvempi ja yhtenäisempi EU:n kyberturvallisuusjärjestelmä uudistamalla ENISA:n toimivaltuudet, modernisoimalla ja laajentamalla kyberturvallisuushyödykkeiden sertifiointijärjestelmä ja ottamalla käyttöön EU-tason mekanismi ICT-toimitusketjujen riskien hallintaan. Ns. NIS2.5-ehdotus pyrkii tekemään NIS2-direktiivistä selkeämmän, helpommin noudatettavan ja paremmin yhteen toimivan EU:n kyberturvallisuuslainsäädännön suhteen, vähentäen samalla yritysten hallinnollista taakkaa ja vahvistaen valvontaa.

Tiivistelmä

Yritykset, eritoten vientiyritykset joutuvat toimimaan täysin uudenlaisessa toimintaympäristössä. Siksi tärkein tehtävä on huolehtia yritysten toimintaedellytyksistä ja taloudellisesta turvallisuudesta. Ulkoisia riskejä on vähennettävä turvaamalla EU:n ja Suomen globaali kilpailukyky digitaalisessa siirtymässä sekä vahvistamalla yhteiskunnan resilienssiä. Sääntelyn tulee tuoda selkeyttä ja ennakoitavuutta valvontaan, sertifiointiin ja toimitusketjuriskien hallintaan. Näistä lähtökohdista pidämme kummankin lakiehdotuksen päälinjoja kannatettavina. Jatkovalmistelussa tulisi huomioida ainakin seuraavat seikat:

- ENISA:n oikeusperustaa ei tule yksinomaan laajentaa, vaan täsmentää ja resursseja ohjata operatiiviseen yhteistyöhön sekä eurooppalaiseen tilannekuvan luomiseen jäsenmaiden välille ja sisämarkkinoiden eduksi. Keskeisin keino on valjastaa ENISA:n kyvykkyydet sekä operatiivisista tehtävistä kerätty tieto parantamaan datanhaltijoiden kykyä ehkäistä, havaita ja pysäyttää kyberpoikkeamia.
- EU:n kyberturvallisuussertifiointijärjestelmää tulee uudistaa, jotta sertifiointikehysten kehittäminen nopeutuu, ylläpito selkeytyy ja laajuus kasvaa.
- Yritysten sääntelytaakan keventäminen on perusteltu lisätoimi mahdollistamalla sertifikaattien käyttö muiden säädösten (esim. NIS2, CRA) vaatimusten todentamisessa.
- EU:n ICT-toimitusketjujen turvallisuuden hallinnan mekanismi on tarpeellinen. Sen avulla voidaan tunnistaa kolmansien maiden ja niistä tulevien tuotteiden aiheuttamat ei-tekniset kriittiset ICT-riskit ja mahdollistaa näiden toimittajien rajoittaminen kriittisen infrastruktuurin, julkisten hankintojen ja EU-rahoituksen ulkopuolelle.
- Muita kuin 5G-teknologioita koskevien tulevien rajoituspäätösten tulee sisältää kuhunkin erikseen säädetty siirtymäaika.
- NIS2.5 muutosten avulla on mahdollista keventää tiettyjen toimijoiden hallinnollista taakkaa, täydentää tiettyjen yhteisten vaatimusten toteuttamista sekä yhdenmukaistaa täydentäviä kansallisia vaatimuksia, jotka aiheuttavat ilmeistä haittaa sisämarkkinoiden toiminnalle.

Eteläranta 10, PL 10, 00131 Helsinki

ENISA:n oikeusperusta

ENISA:n oikeusperustaa on arvioitava kriittisesti ja keskityttävä tehtäviin, joissa se voi tuottaa eniten eurooppalaista lisäarvoa – sellaista, jota jäsenvaltiot eivät voi saavuttaa yksin. ENISA:lla on tällä hetkellä liian paljon tehtäviä (määräksi on arvioitu noin 170), ja niitä on tarpeen karsia huomattavasti. Monet ENISA:n nykyisistä tehtävistä ovat osin päällekkäisiä muiden virastojen tai jäsenvaltioiden toimintojen kanssa, mikä heikentää viraston kykyä saavuttaa tavoitteitaan ja tuottaa riittäviä tuloksia. ENISA:n rooli EU:n kansainvälisessä yhteistyössä vaatii myös arviointia, sillä sen vaikutus jää epäselväksi. Katsomme, että mm. seuraavia tehtäviä tulisi harkita hyvin kriittisesti ja edellyttää tehtävien voimakasta karsintaa:

- Teollisuudelle (yrityksille) tarjottava tuki, kuten parhaiden käytäntöjen ja teknisten ohjeiden laatiminen, tulisi poistaa kokonaan, tai asettaa matalammalle prioriteettitasolle. Euroopassa toimiva kyberturvallisuusala on jo keskeinen toimija torjuntatekniikoiden, -toimintamallien sekä -teknologioiden kehittämisessä sekä ratkaisujen kaupallistamisessa. Tämän lisäksi kansalliset viranomaiset tekevät vastaavaa työtä, eikä ENISA ole siten parhaassa asemassa ohjaamaan toimintaa.
- ENISA:n tarjoamaa kyvykkyyksien kehittämisen tukea tulee vähentää, sillä se kuuluu jäsenvaltioiden vastuulle. Tämä koskee myös erityisiä aloitteita, kuten kiristyshaittaohjelmien torjuntaa, toimialakohtaista tukea sekä ENISA:n järjestämiä harjoituksia ja kilpailuja.
- EU:n komission tulisi koordinoida ICT-toimitusketjujen ei-teknisiä riskejä ja ENISA:n tarjota tukea soveltuvin osin, sillä tehtävä edellyttää ICT-teknologian osaamisen lisäksi vahvaa ymmärrystä yritysten toimitusketjuihin liittyvistä riskeistä sekä kattavaa osaamista kolmasien valtioiden yritystaloudesta, oikeusjärjestelmistä sekä turvallisuus- ja muista poliittisista olosuhteista.
- ENISA:n koulutus-, osaamis- ja tietoisuustoimintoja tulee vähentää, sillä nämä tehtävät kuuluvat jäsenvaltioille sekä markkinoille, jotka ovat kyvykkäämpiä hoitamaan niitä.
- EU:n kyberturvallisuusosaamiseen liittyvät rahoitustoimet tulisi siirtää Euroopan kyberturvallisuusosaamiskeskukselle (ECCC), jotta varat voidaan ohjata jäsenvaltioiden kyberturvallisuuden kehittämiseen.
- ENISA:n ei tule harjoittaa TKI-toimintaa, koska se kuuluu ECCC:n tehtäviin.
- ENISA:n ei tule kehittää, ohjata tai osallistua kyberturvallisuuden harjoitustoimintaan, ellei kyse ole välttämättömästä tuesta EU:n toimielimille ja virastoille.
- ENISA:n tulee pidättäytyä kokonaan eurooppalaisten harmonisoituihin ICT- ja kyberturvallisuusstandardointiin osallistumisesta tai ainakin päällekkäisestä toiminnasta. Standardoinnin tulee säilyä eurooppalaisten standardointijärjestöjen (ESO) tehtävänä.
- ENISA:n nykyiset asiantuntijarakenteita sekä toimintaperiaatteita tulee uudistaa, jotta teollisuuden osallistuminen olisi riittävää ja vaikuttavaa. Viraston rooli tulee ymmärtää teollisuuden tarpeita palvelevaksi – ei yksityisen sektorin kyberturvallisuuden "koordinoijaksi".

ENISA:n uusien tehtävien osalta keskeistä on operatiivisen yhteistyön ja tilannekuvaan liittyvien tehtävien priorisoiminen ja huolellinen muotoilu. Tärkeintä on kehittää ENISA:n valmiuksia hyödyntää kyvykkyyksiään sekä keräämäänsä tietoa kyberuhkien ehkäisyn, havaitsemisen ja datanhaltioiden torjuntatoimien tukemiseen liittyviä tehtäviä varten. Samalla tulee huomioida, että vaikka jäsenvaltioiden välinen tiedonvaihto on tarpeen tietoturvaloukkauksien ehkäisemisessä, selvittämisessä ja mahdollisesti jossain määrin myös torjumisessa, keskeisin työ tehdään datanhaltijoiden (ml. tieto- ja viestintäjärjestelmien haltijat) toimesta. Kyse on siis digitaaliseen tietoon ja -järjestelmiin liittyvästä toimintariskien hallintakyvystä ja ENISA voi parhaimmillaankin vain tukea ko. kyvykkyyksien ylläpitoa.

Eteläranta 10, PL 10, 00131 Helsinki

ENISA:n tulee vahvistaa EU:n yhteistä tilannekuvaa tarjoamalla relevanttia teknistä tietoa, kuten NIS2-direktiivi ja kyberkestävyyssäädös (CRA) edellyttävät. Yhteistyö muiden EU:n toimielinten kanssa on tarpeellista, mutta tilannekuvajärjestelmän tulee nimenomaan tukea jäsenvaltioiden kansallisia kyvykkyyksiä, ei päällekkäisiä toimintoja. On välttämätöntä huomioida, että jäsenvaltioiden – eritoten Suomen – kansallinen kyberturvallisuusviranomainen tuottaa jo keskeistä tukea kansallisesti datanhaltijoiden eduksi eikä ENISA:n tehtävien tule heikentää kansallisen toiminnan myönteisiä vaikutuksia. Jäsenvaltioiden kyberturvallisuuden hallintaan liittyvien virastojen tulisi kartoittaa tehtävät, joissa toimivallan siirto ENISA:lle tuottaisi suurempaa lisäarvoa tai merkittäviä säästöjä jäsenvaltioissa.

Vastaavasti ENISA:n toimintamäärärahojen ja henkilöstöresurssien kasvattaminen tulee harkita huolellisesti viraston oikeusperustan ja tehtävien mukaisesti. ENISA:n oikeusperustan muuttamisen ei tule johtaa jäsenvaltioiden kyberturvallisuusvirastojen kustannusten lisääntymiseen, vaan pikemminkin kustannussäästöihin.

EU:n kyberturvallisuussertifiointijärjestelmä

Sertifiointijärjestelmän uudistus on tervetullut ja tärkeä askel kohti selkeämpää, ketterämpää ja vaikuttavampaa eurooppalaista kyberturvallisuuden varmistamista. Ehdotus vahvistaa ENISA:n roolia sertifiointijärjestelmien laadinnassa, teknisessä ylläpidossa ja kehittämisessä, mikä parantaa järjestelmien ajantasaisuutta sekä varmistaa, että ne vastaavat nopeasti muuttuvaan uhkaympäristöön ja teknologiseen kehitykseen. Järjestelmä tuleekin uudistaa ehdotuksen mukaisesti. Sertifiointijärjestelmän uudistamisessa tulisi huolehtia yleisesti, että kehykset:

- Parantavat tuotteiden ja palveluiden turvallisuutta,
- Varmistavat sääntelyn noudattamisen,
- Helpottavat pääsyä sisämarkkinoille,
- Vähentävät oikeudellisia ja taloudellisia riskejä (vaatimuksenmukaisuus),
- Vahvistavat asiakkaiden luottamusta,
- Pienentävät hallinnollista taakkaa, ja
- Ovat hankittavissa kustannustehokkaasti myös PK-yrityksille.

Erityisen tärkeää on, että sertifioinnin hankkimisen kustannukset säilyvät työn ja kustannusten osalta houkuttelevalla tasolla. Tällöin sertifioinnista muodostuu entistä hyödyllisempi väline yrityksille, jotka voivat sen avulla osoittaa vaatimustenmukaisuutensa useiden EU-säädösten alla yhdenmukaisesti ja pienemmällä hallinnollisella taakalla. Tämä selkeyttää sisämarkkinoiden toimintaa, helpottaa tuotteiden ja palvelujen turvallista markkinoillepääsyä sekä vahvistaa eurooppalaista kilpailukykyä. Lisäksi uudistus voi vahvistaa EU:n strategista autonomiaa ja varmistaa, että sertifiointi tukee myös tulevaisuuden teknologioita, kuten moderneja salausratkaisuja, sekä eurooppalaisten toimijoiden pitkäjänteistä turvallisuus- ja innovaatiokykyä.

EU:n ICT-toimitusketjujen turvallisuuden hallinnan mekanismi

EU:n ICT-toimitusketjujen turvallisuuden hallinnan mekanismi on tarpeellinen. ICT-toimitusketjujen turvallisuuden hallintamekanismi rakentuisi EU-tasoiselle, riskiperusteiselle ja teknologianeutraalille kehykselle, jonka tavoitteena on tunnistaa kriittiset ICT-komponentit (komponentti, järjestelmä, laite, palvelu tai alusta, joka on välttämätön tai herkkä osa kriittistä infrastruktuuria, keskeinen toimitusketjun toimivuudelle ja sen väärinkäyttö voi aiheuttaa merkittävää haittaa) ja niihin liittyvät toimittajariippuvuudet sekä arvioida näihin liittyvät ei-tekniset kyberriskit kuten kolmansien maiden lainsäädännöllinen tai geopoliittinen vaikutusvalta. Mekanismi antaisi komissiolle mahdollisuuden nimetä maita ja toimittajia, jotka muodostavat rakenteellisen kyberturvallisuusriskin EU:n kriittisille sektoreille (NIS2-sektorit), ja tämän perusteella rajoittaa näiden toimittajien osallistumista keskeisiin ICT-komponentteihin ja

julkisiin hankintoihin koko unionin alueella. Mekanismin avulla vältettäisiin jäsenvaltioiden toisistaan poikkeavat lähestymistavat, jotka haittaisivat sisämarkkinoiden toimintaa ja johtaisivat epätasaiseen turvallisuustasoon.

Toimitusketjujen kautta toteutettavat tietoturvaloukkaukset ja ei-tekniset riskit ovat kasvaneet merkittävästi ja vaikuttavat laajasti EU:n taloudelliseen sekä yhteiskunnalliseen turvallisuuteen. Koska kriittiset infrastruktuurit ovat yhä tiiviimmin kytkeytyneitä toisiinsa, yhden toimittajan kyberturvallisuuden vaarantuminen aiheuttaa ulkoisvaikutuksia muualla yritysekosysteemissä ja yhteiskunnassa. Näitä riskejä ei voida torjua pelkästään teknisin vaatimuksin, sillä niiden juuret voivat olla toimittajamaiden lainsäädännössä, poliittisissa rakenteissa tai tahallisessa vahingollisessa vaikuttamisessa. Tämän vuoksi unionitason mekanismi on välttämätön, jotta riskit voidaan arvioida yhdenmukaisesti ja jotta jäsenvaltiot voivat toteuttaa koordinoituja ja oikeasuhtaisia suojatoimia koko sisämarkkinan turvaamiseksi.

Käytännössä mekanismi täyttää aukon, jota EU:n NIS2-direktiivi ja kyberkestävyyssäädös (CRA) eivät voi kattaa. Muiden säädösten edellyttämä tekninen vaatimustenmukaisuus ei riitä, mikäli eurooppalaisten toimijoiden data kulkee epäluotettavan infrastruktuurin kautta.

EU-tason sitova sääntely on tarpeen, koska ns. 5G-työkalupakin pirstaleinen toimeenpano jäsenmaissa on johtanut vaihteleviin riskienhallinnan tasoihin. Televerkkojen resilienssi ja toimintavarmuus ovat liiketoiminnan kannalta kriittisiä, sillä ne tukevat palveluiden jatkuvuutta, tuotantoketjuja ja digitaalisia riippuvuuksia eri toimialoilla. Toimet turvallisuuden, toimintavarmuuden ja häiriönsietokyvyn vahvistamiseksi ovat kannatettavia elinkeinoelämän digitalisaatiolle sekä Euroopan kilpailukyvylle. Mikäli Suomen tavoitteena on tulevaisuudessa entistä integroituneempi EU:n telemarkkina sekä toimintavarmat ja luotettavat verkot, jäsenvaltioiden toisistaan poikkeavat käytänteet korkean riskin toimittajiin ovat haitallisia sekä sisämarkkinoiden toiminnalle, että Euroopan turvallisuudelle ja digitaaliselle suvereniteetille. Mobiiliverkkojen osalta noin 190 000 tukiasemaa EU:ssa toimii yhä korkean riskin toimittajien varassa (noin 32 % kaikista tukiasemista).

On myös olennaista huomioida, että ehdotettu 36 kuukauden siirtymäaika koskee tällä hetkellä ainoastaan mobiiliverkkoja ja perustuu jo pitkään voimassa olleeseen 5G-työkalupakin (5G Security Toolbox) suositukseen ja on ollut teleoperaattorialan tiedossa jo entuudestaan. Käytännössä muutostoimet on toteutettava 2030-luvun alkuun mennessä sekä turvallisen viestinnän, että myös tulevan sukupolven verkkojen vuoksi. Suomen osalta mahdollisesti poistettavaksi määrättävän teknologian korvattavuuteen julkisista varoista tulisi huomioida laitteistojen elinkaari, lopullinen siirtymäaika sekä liiketoimintaperusteiset päätökset korkean riskin teknologian hankinnasta suositusten vastaisesti. 6G-verkkojen käyttöönotto alkaa jo tämän vuosikymmenen lopulla ja koska se rakentuu 5G-verkon päälle, korkean riskin komponentit tulisi joka tapauksessa poistaa ensin. Rahoituksen osalta: NATON 1,5 % puolustusmenotavoitteen osuudesta tulisi joka tapauksessa käyttää kriittisen infrastruktuurin, ml. verkkojen suojaukseen.

Muita teknologioita koskevien tulevien rajoituspäätösten tulee sisältää kuhunkin erikseen säädetty siirtymäaika, sillä näiden sektoreiden toimitusketjut voivat olla monimutkaisempia, riskinarvioinnit vaativat aikaa ja myös hallintatoimet voivat koostua asteittaisista keinoista.

NIS2.5:n muutokset

Muutosdirektiivi on tervetullut kehitysaskel päätavoitteenaan vähentää sääntelyn monimutkaisuutta, keventää toimijoiden hallinnollista taakkaa ja varmistaa, että NIS2-direktiiviä voidaan soveltaa johdonmukaisesti koko unionissa. Ehdotetut keinot ovat pääosin perusteltuja,

eritoten oikeusvarmuuden, että sisämarkkinan toiminnan kannalta. Kannatamme eritoten seuraavia muutoksia:

1. Uuden *small mid-cap* -yritysluokan lisäys ja näiden toimijoiden määrittäminen jatkossa "*important entities*" -kategoriaan kevyemmällä valvonnalla yritysten ja valvovien viranomaisten hallinnollisen taakan tasapainottamiseksi.
2. Soveltamisalan täsmennys erityisesti terveydenhuollon, sähköntuotannon, vedyn tuotannon ja kemikaalisektorin osalta kansallisen tason epäselvyyksien vähentämiseksi.
3. European Digital Identity Wallet ja European Business Wallet -palveluiden sisällyttäminen NIS2:n soveltamisalaan koosta riippumatta, “essential entity” -luokassa.
4. Toimijoiden, jotka omistavat tai operoivat merikaapeleita tai niihin liittyvää infrastruktuuria (kuten landing station -rakenteet), sisällyttäminen soveltamisalaan.
5. Jäsenvaltioiden velvoite sisällyttää PQC-siirtymäpolitiikat kansallisiin kyberturvallisuusstrategioihin 2030/2035 aikataulujen mukaisesti.
6. Komission velvoite laatia yhtenäiset ohjeet toimitusketjuvaatimusten soveltamisesta, jotta yrityksille ei aseteta perusteettomia tai päällekkäisiä due diligence -velvoitteita.
7. Ransomware-raportoinnin yhdenmukaistaminen ottamalla käyttöön harmonisoitu tietomalli, sekä ilmoitusvelvoite lunnaiden maksamisesta.
8. Jäsenvaltioiden oikeus edellyttää yrityksiltä eurooppalaista CSA2:n mukaista Cyber Posture Certification -sertifikaattia kattaen NIS2-direktiivin vaatimukset, jolloin viranomaiset eivät voi määrätä päällekkäisiä lisävelvoitteita.

Lisätiedot:

Peter Sund
Toimitusjohtaja
Kyberala ry
050 565 0621
peter.sund@teknlogiateollisuus.fi