Liikenne- ja viestintäministeriö Perusmuistio EU/199/2025-LVM-10

Hokkanen Emma 20.5.2025

Kyberturvallisuusasetuksen tarkistaminen; ennakkovaikuttaminen

Eduskuntatunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komission työohjelman mukaan komissio antaa vuoden viimeisellä neljänneksellä ehdotuksen ”digitaaliseksi paketiksi”, jonka odotetaan sisältävän myös lainsäädäntöehdotuksen kyberturvallisuusasetuksen ((EU) 2019/881) tarkastelusta.

Komissio on aloittanut julkisen kuulemisen kyberturvallisuusasetuksesta 11.4.2025. Kuulemisen määräaika on 20.6.2025. Komission tietojen mukaan kyberturvallisuusasetuksen tarkistuksessa keskitytään ENISAn toimeksiannon ja eurooppalaisen kyberturvallisuuden sertifiointikehyksen tarkistamiseen sekä tieto- ja viestintätekniikan toimitusketjun turvallisuuteen liittyviin haasteisiin vastaamiseen.

Tällä valtioneuvoston selvityksellä muodostetaan ensimmäisiä ennakkovaikuttamiskantoja koskien kyberturvallisuusasetuksen tarkastelua, jotta Suomi voi vaikuttaa oikea-aikaisesti tulevaan komission esitykseen. Ennakkovaikuttamislinjauksia tullaan tarvittaessa tarkentamaan myöhemmässä vaiheessa. Varsinaiseen ehdotukseen tullaan ottamaan kantaa komission annettua ehdotuksensa.

Suomen kanta

Suomi pitää tärkeänä, että muuttunut toimintaympäristö huomioidaan kattavasti kyberturvallisuusasetusta tarkasteltaessa. Huomiota tulee kiinnittää EU:n varautumisen, kilpailukyvyn sekä teknologisen omavaraisuuden edistämiseen.

Suomi katsoo, että suomalainen kokonaisturvallisuuden toimintamalli soveltuu hyvin EU:n varautumisen ja kriisitoiminnan vahvistamiselle myös kyberturvallisuudessa. Suomi pitää tärkeänä, että yksityisen sektorin toimijat otetaan entistä laajemmin mukaan EU-tason kybervarautumisen vahvistamiseen. Kyberturvallisuus, kyberpuolustus sekä

EU:n ja Naton toimet kyberturvallisuudessa tulee nähdä toisiaan täydentävinä ja toisiaan tukevina.

Suomi pitää tärkeänä, että EU:n digi- ja kyberlainsäädäntö muodostaa selkeän ja eheän kokonaisuuden siten, että velvoitteet ovat selkeitä ja oikeasuhtaisia. Suomi pitää aiheellisena välttää sääntelyä, josta aiheutuu päällekkäisyyksiä, tehottomuutta taikka tarpeetonta hallinnollista- tai sääntelytaakkaa. Suomi pitää tärkeänä, että kyberturvallisuusasetuksen suhdetta muuhun relevanttiin unionin sääntelyyn arvioidaan kattavasti.

Suomi katsoo, että ENISA:n toiminnan tulee olla tehokasta ja läpinäkyvää. Päällekkäisyyksiä kansallisten viranomaisten tehtävien sekä muiden unionin kyberturvallisuuden toimintojen kanssa tulisi välttää. ENISA:n tehtävien tulisi keskittyä toimenpiteisiin, joilla saadaan EU-tasolla erityistä lisäarvoa, kuten kansallisen tilannetietoisuuden täydentäminen, jäsenvaltioiden yhteistyön ja vapaaehtoisen tiedonvaihdon tukeminen sekä lainsäädännön toimenpanossa tukeminen. Suomi pitää tärkeänä, että ENISA:ssa tuotettu ennakointi- ja tilannekuvatieto kyberhäiriöistä hyödyttää jäsenmaita. Suomi katsoo, että kyberpoikkeamiin liittyvän rajat ylittävän tiedonvaihdon tulisi ensisijaisesti perustua vapaaehtoisuuteen. Suomi pitää tärkeänä varmistaa, että ENISA:n ennakointi- ja tilannekuvalla tuotetaan tietoa myös unionin politiikkatoimien suunnittelun tueksi ja EU:n kyberturvallisuuden rahoitusohjelmien käyttöön.

Suomi pitää tärkeänä, että ennen uusien tehtävien osoittamista arvioidaan ENISA:n kyky hoitaa sille osoitetut tehtävät. ENISA:n tehtävien priorisoinnissa tulee huomioida vaikutukset unionin tason kyberturvallisuuteen ja unionin strategisten tavoitteiden saavuttamiseen. Suomi korostaa, että ENISA:n ja Euroopan kyberturvallisuuden osaamiskeskus ECCC:n tehtävissä ja vastuissa tulee välttää päällekkäisyyksiä. Virastojen välisiä synergioita tulee hyödyntää täysimääräisesti resursseja mahdollisimman tehokkaasti hyödyntäen.

Suomi suhtautuu myönteisesti tavoitteeseen sujuvoittaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelua, hyväksymistä ja tarkistamista. Kyberturvallisuuden sertifiointijärjestelmien kehittäminen on tärkeä osa unionin kyberturvallisuuden ja teknologioiden turvallisuuden edistämistä. Suomi pitää tärkeänä varmistaa, että unionilla on kyvykkyys tuottaa yhteisiä kyberturvallisuuden sertifiointijärjestelmiä unionin muiden politiikkatoimien tueksi tehokkaasti, avoimesti ja läpinäkyvästi.

Sertifiointijärjestelmille asetettavien vaatimusten tulisi olla oikeasuhtaisia ja riittävän joustavia ottaen huomioon sertifiointijärjestelmien erilaiset käyttötarkoitukset sekä sääntelyn yksinkertaistamisen tavoitteet. Suomi katsoo, että sertifioinnilla tulisi voida täyttää lainsäädännön kyberturvallisuuden minimivaatimukset. Lisäksi Suomi pitää tärkeänä, että rinnakkain valmisteltavien eurooppalaisten standardien ja sertifiointijärjestelmien suhde on selkeä.

Suomi katsoo, että tieto- ja viestintätekniikan toimitusketjujen turvallisuuden ja resilienssin vahvistaminen ovat keskeinen osa EU:n teknologista omavaraisuutta. Suomi suhtautuu alustavan myönteisesti uusiin ja mahdollisesti velvoittavampiin unionin tason toimenpiteisiin, joilla vahvistetaan tieto- ja viestintätekniikan toimitusketjujen turvallisuutta. Mahdollisten uusien toimenpiteiden tulee tukea nykyisiä toimivia järjestelmiä ja kyvykkyyksiä.

Pääasiallinen sisältö

Vuonna 2019 hyväksytyllä kyberturvallisuusasetuksella säädetään EU:n kyberturvallisuusvirasto ENISA:lle pysyvä mandaatti ja luodaan puitteet tieto- ja viestintäteknologiatuotteiden, palveluiden ja -prosessien kyberturvallisuussertifioinnille EU:ssa. Säädöksen tavoitteena on ollut turvata sisämarkkinoiden toiminta vahvistamalla kyberturvallisuutta, kyberhäiriöiden sietokykyä ja luottamusta EU:ssa.

Komissio on käynnistänyt julkisen kuulemisen koskien kyberturvallisuusasetuksen tarkastelua ja siihen liittyvää vaikutustenarviointia. Kuulemisessa kerätään näkemyksiä erityisesti osa-alueista, joilla ENISAn nykyistä toimeksiantoa sekä eurooppalaisen kyberturvallisuuden sertifiointikehystä olisi tarkistettava, sekä tieto- ja viestintätekniikan toimitusketjun turvallisuuteen liittyvistä haasteista sekä tarpeesta yksinkertaistaa kyberturvallisuustoimenpiteitä ja raportointivelvoitteita.

Kuulemisen yhteydessä annettujen tietojen mukaan komissio harkitsee a) nykytilanteen säilyttämistä, b) muiden kuin lainsäädännöllisten toimien tekemistä tunnistettuihin haasteisiin vastaamiseksi c) kohdennettujen muutosten tekemistä asetukseen tai d) kyberturvallisuusasetuksen kumoamista ja kattavaa uutta sääntelytoimea, jolla vahvistettaisiin ENISAn toimeksiantoa, parannettaisiin sertifiointikehyksen tehokkuutta ja laajennettaisiin sen soveltamisalaa, vastattaisiin tieto- ja viestintätekniikan toimitusketjujen turvallisuushaasteisiin, huomioiden myös muut kuin tekniset riskitekijät. Lisäksi ehdotuksella yksinkertaistettaisiin raportointivelvoitteita ja mahdollisesti myös kyberturvallisuustoimenpiteitä.

Komission vuonna 2024 tekemän arvioinnin mukaan ENISA suoriutui hyvin tehtävistään, mutta sen toimeksiantoa tulisi mukauttaa uuteen lainsäädäntöön sopivaksi. Lisäksi ENISAn tukea ja sidosryhmien osallistamista tulisi parantaa. Eurooppalaisen kyberturvallisuuden sertifiointikehyksen soveltamisalaa ja prosesseja tulisi selkeyttää ja virtaviivaistaa.

ENISA:n tehtävät

Alkuperäisessä kyberturvallisuusasetuksessa ENISA muutettiin Euroopan verkko- ja tietoturvavirastosta Euroopan kyberturvallisuusvirastoksi ja siitä tuli pysyvä EU-virasto. Viraston tehtäviin kuuluu jäsenvaltioiden tukeminen kyberturvallisuuteen liittyvissä asioissa, EU:n kyberturvallisuuspolitiikan kehittämisen tukeminen sekä yhteistyön edistäminen eri sidosryhmien välillä.

ENISA:n tehtäviä tarkennetaan myös muissa EU:n digi- ja kybersäädöksissä. Tehtäviä täydennetään ja tarkennetaan erityisesti kyberkestävyyssäädöksessä ((EU) 2024/2847), kybersolidaarisuussäädöksessä ((EU) 2025/38), NIS2-direktiivissä ((EU) 2022/2555), EU-instituutioiden kyberturvallisuutta koskevassa säädöksessä (2023/2841), Euroopan kyberturvallisuuden osaamiskeskuksen säädöksessä ((EU) 2021/887), uudistetussa eIDAS-asetuksessa ((EU) 2024/1183) sekä asetuksessa finanssialan digitaalisesta häiriönsietokyvystä ((EU) 2022/2554).

ENISA on keskimääräistä pienempi unionin virasto. Viraston tehtävät ovat kuitenkin uuden lainsäädännön myötä laajentuneet merkittävästi. Viraston henkilömäärä ja toimintamenot ovat kasvaneet noin 20 prosentilla vuodesta 2020.

Euroopan unionin neuvosto hyväksyi 6. joulukuuta 2024 päätelmät Euroopan unionin kyberturvallisuusvirastosta (ENISA). Päätelmissä korostetaan kasvavia ja monimutkaistuvia kyberuhkia sekä tarvetta lisätä EU:n ja sen jäsenvaltioiden kyberresilienssiä. Neuvosto kehottaa komissiota arvioimaan kyberturvallisuusasetuksen puitteissa, kuinka ENISA:n mandaattia voitaisiin selkeyttää ja sen roolia operatiivisen yhteistyön tukemisessa vahvistaa. Lisäksi päätelmissä tunnustetaan ENISA:n keskeinen asema kyberturvallisuuspolitiikan kehittämisessä, jäsenvaltioiden tukemisessa ja kyberturvallisuustietoisuuden edistämisessä.

Lisäksi neuvoston keväällä 2024 hyväksymissä päätelmissä kyberturvallisuuden tulevaisuudesta tunnistetaan ENISA:n keskeinen rooli EU:n ja jäsenvaltioiden kyberturvallisuuden parantamisessa. Neuvosto kannustaa ENISA:aa jatkamaan jäsenvaltioiden tukemista unionin lainsäädännön ja politiikan täytäntöönpanossa, kyberuhkien arvioinnissa,

operatiivisen yhteistyön edistämisessä sekä kapasiteetin rakentamisessa. Lisäksi päätelmissä kehotetaan komissiota huomioimaan ENISA:n roolin kehitys kyberturvallisuusasetuksen tarkastelussa ja ENISA:aa asettamaan toiminnalleen selkeät prioriteetit.

Kyberturvallisuussertifioinnit

Kyberturvallisuusasetuksessa luodaan myös puitteet eurooppalaisille kyberturvallisuussertifiointijärjestelmille, jotka koskevat tieto- ja viestintäteknologian tuotteita, palveluja ja prosesseja. Tavoitteena on ollut yhdenmukaistaa sertifiointikäytäntöjä EU:n alueella, lisätä luottamusta digitaalisiin ratkaisuihin, sekä tunnustaa toisissa jäsenmaissa myönnetyt sertifikaatit edistäen sisämarkkinoiden tehokasta toimintaa. Asetuksella (EU) 2025/37 säädöksen soveltamisalaan sertifiointijärjestelmien osalta lisättiin myös tietoturvapalvelut.

ENISA:lla on keskeinen tehtävä tukea eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien (ECCF) valmistelussa yhteistyössä kansallisten kyberturvallisuuden sertifiointiviranomaisten (NCCA) kanssa. Säädöksen voimassaoloaikana on kuitenkin hyväksytty komission täytäntöönpanoasetuksena vasta yksi sertifiointijärjestelmä (yleinen ICT laitteiden ja ohjelmistojen sertifiointijärjestelmä EUCC). Sertifiointijärjestelmät koskien pilvipalveluita, 5G-verkkojen turvallisuutta ja digitaalisia lompakoita ovat keskeneräisiä ja myöhässä ennakoidusta aikataulusta.

Komission varapuheenjohtaja ja komissaari Henna Virkkusen toimeksiantokirjeessä, EU:n sisäisen turvallisuuden strategiassa sekä kyberturvallisuusasetuksen kuulemista koskevassa tausta-asiakirjassa todetaan tarve parantaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien hyväksymisprosessia vastaamaan markkinoiden ja politiikkatoimien tarpeisiin.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Kyberturvallisuusasetuksen ((EU) 2019/881) oikeusperustana on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, joka koskee sisämarkkinoiden toteuttamista ja yhdenmukaistamista jäsenvaltioiden lainsäädännön välillä.

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

Kriisivarautuminen ja hybridiuhat EU-13 jaostokäsittely kirjallisesti 9.-15.5.2025
Viestintä EU-19 jaostokäsittely kirjallisesti 12.-15.5.2025

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Sähköisen viestinnän palveluista annetun lain 304 § 14k mukaan Liikenne- ja viestintävirasto Traficom toimii kyberturvallisuusasetuksen mukaisena kansallisena kyberturvallisuussertifioinnin myöntävänä viranomaisena.

Taloudelliset vaikutukset

ENISA:n budjetista päätetään normaalisti monivuotisten rahoituskehyksien ja EU:n vuotuisten budjettivalmistelun yhteydessä. Tulevaa EU:n monivuotista rahoituskehystä (2028-) koskeviin rahoituskysymyksiin otetaan kantaa osana rahoituskehykseen liittyvää kannanmuodostusta.

Muut asian käsittelyyn vaikuttavat tekijät

Kyberturvallisuuden toimintaympäristö on muuttunut merkittävästi kyberturvallisuusasetuksen voimaan astumisen jälkeen. Lisäksi edellisen komission kaudella valmisteltiin merkittävä määrä uutta kyberturvallisuuden lainsäädäntöä, kuten NIS2-direktiivi, kyberkestävyyssäädös sekä kybersolidaarisuussäädös, joilla on ollut laajoja vaikutuksia ENISA:n tehtäviin, resursointiin sekä kykyyn hoitaa sille osoitetut lakisääteiset tehtävät. Komissio aikoo myös tarkastella mahdollisuuksia keventää viranomaisten ja yritysten hallinnollista taakkaa digisäädösten velvoitteiden osalta. Tällä voi olla vaikutuksia myös ENISA:n tehtäviin sekä yrityksille kohdistettaviin raportointivelvoitteisiin.

Sisäisen turvallisuuden strategiassa todetaan, että kilpailukykykompassin mukaisesti EU:n kyberturvallisuuslainsäädäntökehikkoa tulee yksinkertaistaa osana kyberturvallisuusasetuksen tarkastelua. Lisäksi on mahdollista, että asetukseen ehdotetaan täydennyksiä koskien sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuuden toimintasuunnitelman toimeenpanoa ja kiristyshaittaohjelmien lunnaiden maksua.

Kyberlainsäädännön lisäksi nopea teknologinen kehitys, uudet kyberuhat, taloudellisen turvallisuuden ja teknologisen omavaraisuuden kysymykset, siviili-sotilasyhteistyön kehittäminen, ENISA:n rooli operatiivisissa tehtävissä sekä varautumisunionin sekä sisäisen turvallisuuden strategian toimenpiteiden toteuttaminen ovat teemoja, jotka myös vaikuttavat kyberturvallisuusasetuksen tarkasteluun.

Huomionarvoista on myös, että vuonna 2021 (EU) 2021/887 asetuksella perustetun Euroopan kyberturvallisuuden osaamiskeskuksen (ECCC) tehtävät ovat osittain päällekkäisiä ENISA:n tehtävien kanssa. ENISA ja ECCC tekevät yhteistyötä muun muassa hallinnollisissa asioissa, mutta vastuiden selkeyttämiselle erityisesti kyberturvallisuusosaamiseen ja taitoihin sekä teknologioiden ennakointiin liittyen on korostunutta tarvetta. Tämän vuoksi säädöksessä voidaan tarkastella myös ENISA:n ja ECCC:n välistä tehtävänjakoa.

Vuonna 2019 EU:ssa laadittiin yhteinen riskiarviointi ja 5G-keinovalikoimaksi (5G toolbox) kutsutut suositukset, joilla vahvistetaan 5G-verkkojen turvallisuutta EU:ssa teknisillä ja strategisilla toimenpiteillä. Kesällä 2023 julkaistun seurantaraportin mukaan suurin osa jäsenvaltioista on toimeenpannut suositukset, mutta jäsenmaiden välillä on eroja toimeenpanotavoissa. Komissio on viime vuosina pyrkinyt edelleen edistämään EU:n 5G-keinovalikoiman toimeenpanoa jäsenvaltioissa. Komissio on erityisesti kiinnittänyt huomiota strategiseen suositukseen korkean riskin laitetoimittajien rajoituksiin liittyen. Lisäksi parhaillaan valmistellaan erillistä keinovalikoimaa ICT-toimitusketjujen turvallisuuden vahvistamiseksi.

Komission 1.4.2025 julkaisemassa tiedonannossa EU:n sisäisen turvallisuuden strategiaksi tuodaan esille, että komissio aikoo tarkastella laajemmin ICT-toimitusketjujen ja infrastruktuurin turvallisuutta ja resilienssiä osana kyberturvallisuusasetuksen päivittämistä. On mahdollista, että kyberturvallisuusasetuksen tarkastelun yhteydessä asetukseen ehdotetaan sisällytettäväksi velvoittavia säännöksiä koskien teknologista omavaraisuutta kyberturvallisuudessa, esimerkiksi turvallisten viestintäverkkojen tai ICT-toimitusketjujen osalta. Komission odotetaan myös vuoden 2025 aikana ehdottavan Digital Networks Act-lainsäädäntökokonaisuutta, joka saattaa myös sisältää viestintäverkkojen turvallisuutta vahvistavia toimia.

Asiakirjat

-

Laatijan ja muiden käsittelijöiden yhteystiedot

Erityisasiantuntija Emma Hokkanen, LVM, emma.hokkanen@gov.fi p. +358 050 4306366
Neuvotteleva virkamies Marième Korhonen-Cara, LVM, marieme.korhonen-cara@gov.fi p. 0295 342 134
Hallitussihteeri Veikko Vauhkonen, LVM, veikko.vauhkonen@gov.fi, p. +358 50 340 0578
EU-erityisasiantuntija Maija Rönkä, VNK, maija.ronka@gov.fi, p. +358 50 525 4966

VAHVA-tunnus

EU/199/2025

Liitteet

Viite