TTU Vauhkonen Veikko(LVM)

09.05.2022
JULKINEN

Asia
Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa.

Kokous

U/E/UTP-tunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Euroopan komissio julkaisi 22.3.2022 ehdotuksen Euroopan neuvoston ja parlamentin asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 122 final).

Ehdotus perustuu EU:n turvallisuusunionistrategiaan (COM(2020) 605 final) sekä EU:n kyberturvallisuusstrategiaan digitaaliselle vuosikymmenelle (JOIN(2020) 18 final).

Ehdotuksen käsittely Euroopan unionin neuvoston kybertyöryhmässä on alkanut huhtikuussa 2022.

Suomen kanta

Suomi pitää tärkeänä, että EU:n toimielimien, elimien ja virastojen (jatkossa ’instituutiot’) kyberturvallisuuteen kiinnitetään huomiota. Suomi kannattaa tavoitteita niitä koskevan kyberturvallisuustason parantamisesta ja pitää tärkeänä, että EU:n toimielimien, elimien ja virastojen kykyä sietää ja reagoida kyberuhkiin kehitetään. Suomi katsoo, että ehdotettavat toimet tulisi mitoittaa siten, että ne ovat tehokkaita ja oikeasuhtaisia suhteessa ehdotuksen tavoitteisiin.

Suomi tukee ehdotusta yhteisistä sitovista säännöistä kyberturvallisuustason parantamiseksi EU:n instituutioissa ja pitää sitovien sääntöjen asettamista tarpeellisena ehdotuksen tavoitteiden saavuttamiseksi. Suomi tukee ehdotuksia kyberturvallisuuden perustason määrittelystä, kyberturvallisuuden hallinta- ja valvontakehyksen laatimisesta ja kyberturvallisuussuunnitelman laatimisesta EU:n instituutioissa. Suomi suhtautuu avoimesti myös muihin toimenpide- ja sääntelyvaihtoehtoihin, joilla ehdotuksen tavoitteita voidaan edistää.

Suomi katsoo, että EU:n instituutioiden kyberturvallisuutta koskevilla säännöillä tulisi tavoitella vähintään yhteismitallista kyberturvallisuuden vaatimustasoa suhteessa siihen vaatimustasoon jota komission direktiiviehdotuksella EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) päivittämiseksi pyritään saavuttamaan EU:ssa ja jäsenvaltioissa.

Suomi pitää olemassa olevaa CERT-EU:n ja jäsenvaltioiden kansallisten yksiköiden välistä yhteistyötä ja tietojen vaihtamista hyödyllisenä ja tärkeänä. Suomi katsoo, että yhteistyön jatkumisen turvaamiseksi olisi tarpeellista turvata tarvittaessa mahdollisuus luottamukselliseen yhteydenottoon ja tietojen vaihtamiseen CERT-EU:n ja jäsenvaltion turvallisuus- tai tiedustelupalvelun, lainvalvontaviranomaisen tai CERT-toimijan välillä.

Suomi pitää tärkeänä, että perustettava uusi kyberturvallisuuslautakunta IICB ei muodostaisi päällekkäisiä tehtäviä olemassa olevien rakenteiden kanssa. Samoin Suomi pitää tärkeänä, että EU:n kyberturvallisuuskeskus CERT-EU:lle asetettavat uudet tehtävät eivät muodostaisi päällekkäisyyksiä olemassa olevien rakenteiden kanssa. Suomi pitää IICB:lle ja CERT-EU:lle ehdotettuja rooleja ehdotuksien täytäntöönpanon valvomisessa sekä yhteistyön ja koordinoimisen parantamisessa asianmukaisena ja kannattaa niille ehdotettuja tehtäviä.

Suomi pitää ehdotuksen oikeusperustaa ja ehdotettua säädösinstrumenttia asianmukaisena ehdotuksen sisältö ja tavoitteet huomioon ottaen. Asetus, jota sovelletaan sellaisenaan, on asianmukainen oikeudellinen väline EU:n instituutioille asetettavien velvoitteiden määrittelemiseksi ja selkeyttämiseksi.

Pääasiallinen sisältö

Yhteenveto ja tavoitteet

Ehdotuksella säädettäisiin Euroopan unionin instituutioille asetettavista kyberturvallisuusriskien hallinta- ja valvontakehyksen perustamisvelvoitteista sekä kyberturvallisuusriskien hallinta- ja raportointivelvoitteista. Lisäksi ehdotuksella säädettäisiin EU:n kyberturvallisuuskeskukseksi nimettävän CERT-EU:n ja perustettavan kyberturvallisuuslautakunnan (IICB) organisaatioista, toiminnasta ja tehtävistä.

Ehdotuksella tavoitellaan EU:n instituutioiden kyberturvallisuustason parantamista sekä korkean kyberturvallisuustason yhtenäisyyttä ja yhtenäistä saavuttamista. Lisäksi ehdotuksella pyrittäisiin varmistamaan, että EU:n instituutioita koskevat kyberturvallisuussäännöt olisivat yhdenmukaisia EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) päivittämistä koskevan ehdotuksen kanssa.

EU:n instituutioiden velvoitteet korkean kyberturvatason varmistamiseksi

EU:n instituutiot velvoitettaisiin kyberturvatason parantamiseksi laatimaan sisäinen kyberturvallisuusriskien hallinta- ja valvontakehys instituutioon kohdistuvien riskien tunnistamiseksi. Kehyksen tulisi kattaa organisaation koko ICT-ympäristö ja ylin johto velvoitettaisiin valvomaan kyberturvallisuusriskien hallintaan ja valvontaan liittyvien velvoitteiden toteutumista. Lisäksi kuhunkin yksikköön velvoitettaisiin nimettäväksi kyberturvallisuusvastaava.

EU:n instituutiot velvoitettaisiin hallinta- ja valvontakehyksessä tunnistettujen riskien torjumiseksi hyväksymään kyberturvallisuuden perustaso. Kyberturvallisuuden perustasolla tarkoitettaisiin sellaista kyberturvallisuussääntöjen vähimmäisjoukkoa, eli menettelyjä, käytäntöjä ja toimintaan kohdistuvia vaateita, jota tietojärjestelmien ja niiden tarjoajien ja käyttäjien on noudatettava kyberturvallisuusriskien minimoimiseksi. Ehdotuksen liitteissä säädettäisiin osa-alueista ja toimenpiteistä, jotka kyberturvallisuuden perustasossa olisi vähintään otettava huomioon.

Lisäksi EU:n instituutiot velvoitettaisiin suorittamaan vähintään joka kolmas vuosi kyberturvallisuuden kehitystason arviointi, ja hyväksymään arvioinnissa tehtyihin havaintoihin perustuen kyberturvallisuussuunnitelma kyberturvallisuustason parantamiseksi.

IICB

Ehdotuksella perustettaisiin uusi EU:n toimielinten välinen kyberturvallisuuslautakunta (IICB), jonka tehtävänä olisi seurata asetuksen täytäntöönpanoa sekä valvoa CERT-EU:n yleisten painopisteiden ja tavoitteiden täytäntöönpanoa ja antaa CERT-EU:lle strategista ohjausta. IICB koostuisi eräiden EU:n toimielinten, elinten ja virastojen edustajista sekä kolmesta EU:n virastojen verkoston (EUAN) nimittämästä edustajasta. Lisäksi CERT-EU:n johtaja voisi osallistua IICB:n kokouksiin. IICB:n sihteeristötehtävistä huolehtisi komissio.

IICB:n tehtävänä olisi muun ohella hyväksyä CERT-EU:n työohjelma, rahoitussuunnitelma ja vuosikertomus, sekä tarkastella CERT-EU:lta pyydettyjä kertomuksia asetuksen täytäntöönpanon tilasta. IICB seuraisi asetuksen sekä hyväksyttyjen ohjeasiakirjojen, suositusten ja toimintakehotusten täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa. Seuraamuksien osalta IICB voisi antaa EU:n toimielimelle, elimelle tai virastolle varoituksen tai suositella, että asiaankuuluva tarkastusyksikkö tekee tarkastuksen, mikäli IICB katsoisi, että asetusta ei ole sovellettu tai pantu täytäntöön asianmukaisesti.

CERT-EU

Ehdotuksella muutettaisiin CERT-EU:n nimi tietotekniikan kriisiryhmästä unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskukseksi. CERT-EU:n tarkoituksena olisi edistää kyberturvallisuutta EU:ssa muun muassa neuvomalla EU:n instituutioita kyberturvallisuusasioissa, auttamalla niitä havaitsemaan ja reagoimaan kyberturvallisuuspoikkeamiin, sekä toimimalla tietojenvaihdon ja poikkeamiin reagoimisen koordinaatiokeskuksena. CERT-EU tukisi EU:n instituutioita asetuksen täytäntöönpanossa ja valmistelisi IICB:n hyväksyttäväksi toimintakehotuksia, ohjeasiakirjoja ja suosituksia täytäntöönpanoon liittyen.

CERT-EU tekisi yhteistyötä ja vaihtaisi tietoja jäsenvaltioissa vastaavia tehtäviä hoitavien kansallisten elinten kanssa. Tällaisia elimiä olisivat ainakin kansalliset CERT-yksiköt ja kyberturvallisuuskeskukset, CSIRT-yksiköt ja NIS-direktiivin keskitetyt yhteyspisteet. Suomessa keskeistä yhteistyötä CERT-EU:n kanssa tekisi Liikenne- ja viestintävirasto Traficomin Kyberturvallisuus-keskus. CERT-EU jakaisi erityisesti kyberuhista, haavoittuvuuksista, poikkeamista, mahdollisista vastatoimista ja muista seikoista, jotka ovat merkityksellisiä kyberturvallisuuden parantamiseksi. Tietoja, joista käy poikkeaman kohteen identiteetti, voitaisiin vaihtaa ainoastaan kohteen suostumuksella. CERT-EU voisi tehdä yhteistyötä myös muiden kuin jäsenvaltioiden vastaavia tehtäviä hoitavien elinten kanssa harkinnanvaraisesti, jos IICB tämän hyväksyy.

CERT-EU:lla olisi oikeus pyytää EU:n instituutioita toimittamaan kyberturvallisuuteen liittyviä tietoja. EU:n instituutiot velvoitettaisiin ilmoittamaan CERT-EU:lle merkittävistä kyberuhista, haavoittuvuuksista ja poikkeamista ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa niiden havaitsemisesta. Lisäksi ilmoitettava olisi asianmukaisista teknisistä tiedoista. CERT-EU tukisi osapuolia poikkeamiin reagoimisen koordinoinnissa ja yhteistyössä poikkeamien torjumiseksi

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

SEUT 298 artikla. SEUT 298 artiklan nojalla Euroopan unionin toimielimet, elimet ja laitokset tukeutuvat tehtäviään hoitaessaan avoimeen, tehokkaaseen ja riippumattomaan eurooppalaiseen hallintoon. Tätä varten Euroopan parlamentti ja neuvosto antavat tavallista lainsäätämisjärjestystä noudattaen asetuksilla säännökset, joissa kunnioitetaan SEUT 336 artiklan nojalla vahvistettuja henkilöstösääntöjä ja palvelussuhteen ehtoja.

Käsittely Euroopan parlamentissa

Parlamenttikäsittelystä ei ole vielä saatavilla tietoa.

Kansallinen valmistelu

E-kirjelmää on käsitelty seuraavien EU-jaostojen kirjallisessa menettelyssä 9.5.2022 – 11.5.2022:

Viestintäjaosto (EU-19)

Eduskuntakäsittely

Valtioneuvoston E-selvitys E 3/2021 vp: Korkean edustajan ja komission yhteinen tiedonanto: ’EU:n kyberstrategia digitaaliselle vuosikymmenelle’.

Valtioneuvoston E-selvitys E 119/2020 vp: Komission tiedonanto EU:n turvallisuusunionistrategiasta.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Ehdotus ei aiheuta muutoksia kansalliseen lainsäädäntöön eikä vaikuta Ahvenanmaan asemaan.

Ehdotuksella ei arvioida olevan suoria vaikutuksia kansallisiin toimijoihin.

Toimivallanjako EU-asioissa valtakunnan ja Ahvenanmaan välillä määräytyy Ahvenanmaan itse-hallintolain (1144/1994) mukaan.

Taloudelliset vaikutukset

Ehdotus lisäisi CERT-EU:n määrärahatarpeita. CERT-EU tarvitsisi lisävaroja laajennetun tehtävänsä suorittamiseksi. Ehdotuksen mukaan varat uudelleen kohdennettaisiin EU-budjetin sisällä CERT-EU:n palveluja hyödyntävien unionin toimielinten, elinten ja virastojen määrärahoista. Määrärahalisäykset voidaan siis ehdotuksen mukaan hoitaa voimassa olevan monivuotisen rahoituskehyksen puitteissa.

Ehdotuksen vaikutukset kohdistuvat EU:n toimielimiin, elimiin ja virastoihin, eli EU-budjettiin.

Ehdotus ei koske jäsenvaltioita, joten komissio ei ole tehnyt erityistä vaikutustenarviointia. Ehdotuksella ei ole suoria taloudellisia vaikutuksia Suomelle.

Muut asian käsittelyyn vaikuttavat tekijät

Ehdotus on uusi. EU:n velvoittavassa sääntelyssä ole aiemmin käsitelty EU:n instituutioiden kyberturvallisuutta tai puututtu kattavasti kyberuhkaympäristöön ja digitalisaation aiheuttamiin uusiin tietoteknisiin riskeihin.

Ehdotuksen taustalla ovat EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle (JOIN(2020) 18 final) ja EU:n turvallisuusunionistrategia (COM(2020) 605 final).

Asiakirjat

COM(2022) 122 final

Laatijan ja muiden käsittelijöiden yhteystiedot

Veikko Vauhkonen, LVM, +358 295 34 2168, veikko.vauhkonen@gov.fi

EUTORI-tunnus

EU/2022/0349

Liitteet

Viite

Asiasanat
Hoitaa

Tiedoksi