Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TRAFICOM/238926/03.03.01/2022
31.5.2022

Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kirjallinen asiantuntijalausunto: Valtioneuvoston selvitys (E 63/2022 vp): Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kiittää liikenne- ja viestintävaliokuntaa mahdollisuudesta lausua valtioneuvoston selvityksestä koskien asetusehdotusta toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa.

Kyberturvallisuuskeskus pitää merkittävänä, että kyberturvallisuus on nostettu vahvemmin esille EU:n sääntelyhankkeissa. Kyberturvallisuuskeskus pitää tärkeänä, että myös EU:n toimielimien ja virastojen kyberturvallisuuteen, sisäiseen turvallisuuteen ja turvallisuuskäytäntöihin luottamuksellisen tiedon käsittelyssä kiinnitetään tehokkaammin huomiota. EU:n toimielimet ja virastot käsittelevät kaikkien jäsenvaltioiden kannalta merkittäviä asiakokonaisuuksia, jonka vuoksi mainittujen instituutioiden kykyä sietää ja reagoida kyberuhkiin, -häiriöihin ja -hyökkäyksiin tulee kehittää. Tämän osalta tulee huomioida, että EU:n toimielimet, elimet ja laitokset ovat todennäköisesti houkutteleva kohde kyberrikollisille.

Käsillä oleva asetusehdotus laatii yhteisen kyberturvallisuustason EU:n instituutioille. Kyberturvallisuuskeskus pitää kannatettavana, että asetusehdotuksessa mainittua kyberturvallisuustasoa, vaatimuksia ja velvoitteita pyritään yhdenmukaistamaan uudistettavan EU:n verkko- ja tietoturvadirektiivin sisällön kanssa. Esimerkiksi EU:n yhteisen kyberturvallisuutta koskevan tilannekuvan ylläpitäminen ja avunannon mahdollinen koordinointi vaativat yhä laajempaa luottamuksellisen tiedon käsittelyä. Esitetyt vaatimukset ja velvoitteet kehittävät osaltaan luottamuksellisten tietojen käsittelyä myös EU:n toimielimissä ja virastoissa.

Kyberturvallisuuskeskus haluaa korostaa, että kyberturvallisuuden varmistaminen koostuu useista eri tasoilla toteutettavista toimenpiteistä. Kyberturvallisuuskeskuksen näkökulmasta sitovien sääntöjen ja sääntelyn asettaminen on tarpeellista kyberturvallisuuden kehittämiseksi ja varmistamiseksi myös EU-instituutioiden toiminnassa. Kyberturvallisuuskeskus haluaa kuitenkin muistuttaa, että asetusehdotuksen velvoitteita tulisi täydentää teknisimmillä ohjeilla ja toimintatapaa koskevalla ohjauksella. Tässä ohjauksessa erityisesti CERT-EU:lla on merkittävä rooli. Lisäksi tulee kiinnittää huomiota asetettujen velvoitteiden ja vaatimusten valvontaan sekä toimintojen ja järjestelmien arviointiin kyberturvallisuuden tason osoittamiseksi.

Kyberturvallisuuskeskus pitää tärkeänä, että CERT-EU:n ja jäsenvaltioiden kansallisten kyberturvallisuustoimijoiden yhteistyö pysyy tiiviinä myös tulevaisuudessa. Uusi sääntely korostaa CERT-EU:n koordinoivaa roolia EU-instituutioita koskevien kyberuhkien, -häiriöiden ja haavoittuvuuksien osalta. Samalla CERT-EU:lla on keskeinen rooli EU-instituutioita koskevan kybertilannekuvan muodostamiseksi. Kyberturvallisuuskeskus pitää tärkeänä, että CERT-EU:n muodostama tilannekuva olisi myös jäsenvaltioiden kansallisista

asiantuntijoista koostuvan CSIRT-verkoston käytettävissä. Kyberturvallisuuskeskus pitää tärkeänä, että CERT-EU:lle vahvistettavat tehtävät tai uuden toimielinten välisen kyberturvallisuuslautakunnan tehtävät eivät muodosta päällekkäisiä tehtäviä jo olemassa olevien kyberturvallisuustoimijoiden, kuten EU:n kyberturvallisuusviraston (ENISA) kanssa.

Kyberturvallisuuskeskus haluaa korostaa, että luottamukseen perustuva yhteistyö on yksi tärkeimmistä kulmakivistä kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Esimerkiksi tiedonvaihto viranomaisten kesken ja erityisesti tiedonvaihto viranomaisten ja yksityisen sektorin välillä ei toimisi ilman luottamukseen perustuvaa yhteistyötä. Kyberturvallisuuskeskuksen toiminnan kannalta on keskeistä, että uusi sääntely mahdollistaa luottamuksellisen yhteydenoton ja tietojen vaihtamisen CERT-EU:n ja Kyberturvallisuuskeskuksen välillä. Kyberturvallisuuskeskus katsoo, että CERT-EU:n kanssa tulee voida ottaa yhteyttä siten, että yhteydenottoa ei ilman suostumusta anneta tiedoksi muille toimijoille, joihin esimerkiksi käsillä olevassa asetusehdotuksessa viitataan. Kyberturvallisuuskeskus katsookin, että tiedonjakovelvoitteiden tulisi tarvittaessa nojata nimenomaisen kiellon sijasta suostumukseen, kun pohditaan tietojen edelleen luovuttamista EU-instituutioiden ja CERT-EU:n kesken.

Kyberturvallisuuskeskus pitää sääntelyn ohella hyödyllisenä, että EU:n instituutiot ja jäsenvaltiot järjestävät säännöllisesti kyberturvallisuutta koskevia harjoituksia. Aktiivinen harjoittelu on keskeinen työväline jäsenvaltioiden ja EU-instituutioiden yhteistyön kehittämiseksi erilaisissa häiriötilanteissa. Kyberturvallisuutta koskevat harjoitukset tarjoavat myös mahdollisuuden kehittää kyberturvallisuutta koskevaa EU-yhteistyötä ja tilannekuvan muodostamista eri viranomaisten kesken. Kyberturvallisuuskeskus katsoo, että harjoittelun merkitys korostuu, kun kyberturvallisuuden parissa toimivien tahojen mandaattia muutetaan tai vahvistetaan taikka silloin, kun perustetaan kokonaan uusia toimijoita.

Kyberturvallisuuskeskus haluaa lopuksi korostaa, että EU:n kilpailukyvyn ja kyberturvallisuutta koskevan omavaraisuuden vahvistaminen edellyttävät, että Euroopassa panostetaan kyberturvallisuuteen yhä vahvemmin. Kyberturvallisuuden kehittäminen edellyttää luonnollisesti lisäresursseja niin EU:n tasolla kuin kansallisesti.

Olli Lehtilä
Johtava asiantuntija
Kyberturvallisuuskeskus
Liikenne- ja viestintävirasto