Emma Hokkanen
Tieto- ja turvallisuusosasto, Turvallisuusyksikkö
Liikenne- ja viestintäministeriö

Asiantuntijalausunto
Eduskunnan puolustusvaliokunta

19.10.2023

Puolustusvaliokunnan asiantuntijapyyntö, 21.9.2023

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen) (U 20/2023 vp): Liikenne- ja viestintäministeriön asiantuntijalausunto

Liikenne- ja viestintäministeriö kiittää mahdollisuudesta antaa lausunto valtioneuvoston kirjelmästä U 20/2023 vp. Liikenne- ja viestintäministeriö lausuu kunnioittavasti seuraavan:

Ehdotuksen taustaa ja pääasiallinen sisältö

Euroopan komissio antoi 18.4.2023 ehdotuksen (COM(2023) 209 final) Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten (**kybersolidaarisuussäädös**). Uuden sääntelyn lisäksi asetuksella muutettaisiin asetusta (EU) 2021/694 (**Digitaalinen Eurooppa -ohjelma**). Komissio antoi 18.4.2023 myös ehdotuksen (COM(2023) 208 final) Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) 2019/881) muuttamisesta tietoturvapalvelujen osalta (**kyberturvallisuusasetuksen muuttaminen**). Tämä ehdotus täydentää kybersolidaarisuussäädösehdotusta siten, että tietoturvapalveluntarjoajat tulisivat kyberturvallisuusasetuksen soveltamisalaan.

Kybersolidaarisuussäädös

Kybersolidaarisuussäädösehdotuksen tavoitteena on vahvistaa EU:n yhteistä kyberhäiriöiden havainnointia, tilannekuvaa sekä kyvykkyyttä vastata kyberhäiriöihin. Lisäksi tavoitteena on vahvistaa kriittisten toimijoiden valmiuksia koko EU:ssa ja vahvistaa solidaarisuutta kehittämällä yhteisiä kyberturvallisuusviranomaisten ja yksityisen sektorin toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalle.

Ehdotuksessa esitetään yleiseurooppalaisen turvaoperaatiokeskusten (Security Operations Center, SOC) infrastruktuurin käyttöönottoa yhteisten kyberhavainnointivalmiuksien rakentamiseksi ja tehostamiseksi. Lisäksi ehdotuksessa esitetään kyberhätätilanteiden mekanismin ja luotettavista yksityisen sektorin palveluntarjoajista koostuvan kyberturvallisuusreservin perustamista jäsenvaltioiden tukemiseksi merkittäviin ja laajamittaisiin

kyberturvallisuuspoikkeamiin varautumisessa, niihin vastaamisessa ja niistä välittömästi toipumisessa.

Lisäksi ehdotuksessa esitetään kyberturvallisuuspoikkeamien arviointimekanismin perustamista tiettyjen merkittävien tai laajamittaisten poikkeamien tarkastelua ja jälkiarviointia varten. SOC-infrastruktuuria, kyberhätätilanteiden mekanismia sekä kyberturvallisuusreserviä esitetään tuettavaksi Digitaalinen Eurooppa -rahoituksesta, jonka sääntelyyn esitetään muutoksia soveltuvin osin.

Ehdotuksen mukaan sillä ei rajoiteta jäsenvaltioiden ensisijaista vastuuta kansallisesta turvallisuudesta, yleisestä turvallisuudesta sekä rikosten ehkäisemisestä, tutkimisesta, paljastamisesta ja syytteeseenpanosta.

Ehdotuksen vaikutukset

Komissio ei ole tehnyt ehdotuksesta vaikutustenarviointia sen sisällön kiireellisyydestä johtuen. Liikenne- ja viestintäministeriö pitää EU-tason vaikutusarviointien puuttumista valitettavana. Vaikutusarvioinnin puuttumisen vuoksi ehdotuksen kansallisten vaikutusten arviointi on haastavaa.

Kansalliselle turvaoperaatiokeskukselle (SOC) esitetyt tehtävät ovat osittain samoja kuin kyberturvallisuusdirektiivin (NIS2-direktiivi) mukaisille CSIRT-yksiköille (tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt) esitetyt tehtävät. Siten Suomen kansalliseksi SOC-yhteyspisteeksi esitettäneen nimettäväksi Liikenne-ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Kansallinen SOC-yhteyspiste voisi tehdä yhteistyötä kansallisesti viranomaisten (esimerkiksi Puolustusvoimien) ja yksityisen sektorin välillä muun muassa välittämällä ajankohtaista tietoa kyberturvallisuuden tilannekuvasta. On kuitenkin huomioitava, että kyberturvallisuuden verkostojen toiminta perustuu useimmiten velvoittavan sääntelyn sijaan osallistujien vapaaehtoiseen ja luottamukselliseen yhteistyöhön, jonka vuoksi luottamukseen perustuvan yhteistyön vaaliminen on jatkossakin tärkeää. Liikenne- ja viestintäministeriö huomauttaa, että ehdotettu SOC-yhteistyörakenne sisältää useita päällekkäisyyksiä nykyisen kyberturvallisuuden toimintaympäristön kanssa.

Kyberhätätilanteiden mekanismin osalta Suomi voisi pyytää tukea kyberreservistä merkittävän tai laaja-alaisen kyberpoikkeaman sattuessa kriittisille toimialoille. Tämä voi pienentää kyberpoikkeaman haitallisia vaikutuksia sekä ehkäistä häiriön leviämistä kansallisesti tai rajojen yli. Hätätilanteiden mekanismilla voidaan myös suorittaa ennakollisia varautumistestauksia kriittisille toimialoille. Kyberturvallisuuspoikkeamien jälkitarkastelumekanismilla voidaan arvioida tapahtuneita poikkeamia, niihin johtaneita syitä sekä auttaa ennaltaehkäisemään vastaavia poikkeamia jatkossa.

Liikenne- ja viestintäministeriö katsoo, että ehdotuksessa mainitut toimenpiteet voivat parantaa kyberturvallisuutta koko Euroopan unionissa ja Suomessa sekä tukea jo käynnissä olevia kansallisia toimenpiteitä kybervarautumisen kehittämiseksi. Ehdotettujen toimien vapaaehtoisuus antaa kansallista liikkumavaraa. Liikenne- ja viestintäministeriö myös katsoo, että on tärkeää varmistaa, ettei ehdottettuihin uusiin mekanismeihin

osallistuessa luovuteta sellaisia tietoja, jotka voivat vaarantaa kansallista turvallisuutta.

Käsittelyvaihe

Kybersolidaarisuussäädöstä koskevan ehdotuksen käsittely on käynnissä Euroopan unionin neuvoston horisontaalisessa kybertyöryhmässä. Puheenjohtajamaa Espanja käsittelee ehdotusta nopealla aikataululla ja pyrkii yleisnäkemykseen vuoden 2023 loppuun mennessä.

Ehdotuksesta on annettu ensimmäinen kompromissiesitys, jossa ehdotuksen suhdetta kansalliseen turvallisuuteen on tarkennettu valtioneuvoston kannan mukaisesti. Myös jäsenvaltioiden harkintavallan rajoituksista SOC-toimijan nimeämisessä on luovuttu. Ehdotusta on myös tarkennettu siten, että ehdotetut toimenpiteet olisivat jäsenmaille vapaaehtoisia. Myös Euroopan unionin neuvoston oikeuspalvelu on pyytänyt valtioneuvoston kannan mukaisesti tarkentamaan ehdotuksen sisältöä vastaamaan paremmin ehdotuksen oikeusperustaa.

Valtioneuvoston kanta ehdotukseen

Valtioneuvosto kannattaa ehdotuksen tavoitetta ja katsoo, että on Suomen edun mukaista vahvistaa kyberturvallisuutta myös EU:n yhteisillä toimilla. EU:n kriisinkestävyyden kokonaisvaltainen kehittäminen on keskeistä. Kriittisten toimijoiden fyysisen ja digitaalista kriisinkestävyyden ja varautumisen edistäminen EU:ssa on erityisen tärkeää.

Valtioneuvosto kannattaa toimia, jotka edistävät jäsenmaiden välistä tietojenvaihtoa kyberturvallisuuspoikkeamista, mutta toteaa, että uusien tilannekuva- ja tiedonvaihtotoimintojen perustamisessa tulee välttää päällekkäisyyksiä jo olemassa olevien toimintojen kanssa. Kansallisten SOC-toimijoiden ja rajat ylittävien SOC-yhteenliittymien välisestä tietojenvaihdosta sekä komissiolle annettavasta toimivallan siirrosta tarvitaan lisätietoja.

Kyberhätätilanteiden mekanismin osalta valtioneuvosto suhtautuu myönteisesti toimiin, joilla pyritään koordinoidusti vahvistamaan kriittisten toimialojen varautumista kyberhäiriötilanteisiin.

Valtioneuvosto toteaa, että ehdotuksen suhdetta kansalliseen turvallisuuteen pitää arvioida tarkemmin. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti.

Kyberturvallisuusasetuksen muuttaminen

Kyberturvallisuusasetukseen ehdotettujen muutosten osalta luotettujen palveluntarjoajien lisäämistä soveltamisalaan voidaan pitää kannatettava siltä osin kuin sääntelyllä pyrittäisiin lisäämään luottamusta digitaalisille sisämarkkinoille, vähentämään yrityksille sertifioinnista aiheutuvia kuluja ja parantamaan kyberturvallisuuspalveluiden laatua ja turvallisuutta.