Sisäministeriö
Inrikesministeriet

Lausunto

4.10.2023

Hallintovaliokunta
HaV@eduskunta.fi

Asiantuntijalausunto valtioneuvoston kirjelmästä komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen, U 20/2023 vp)

Eduskunnan hallintovaliokunta on pyytänyt sisäministeriöltä asiantuntijalausuntoa valtioneuvoston kirjelmästä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi kybersolidaarisuussäädöksestä ja kyberturvallisuusasetuksen muuttamisesta (U 20/2023 vp). Sisäministeriö kiittää mahdollisuudesta lausua asiassa ja toteaa seuraavaa:

Sisäministeriö pitää tervetulleena komission aloitteellisuutta kyberturvallisuuden kehittämisessä. Turvallisuusympäristön muutokset, digitalisaatiokehitys ja teknologinen kehittyminen edellyttävät kyberturvallisuuden jatkuvaa kehittämistä ja aiempaa parempaa kykyä reagoida riittävän nopeasti vakaviin kyberpoikkeamiin. Kyberuhkien ja kyberpoikkeamien vaikutusten rajat ylittävä luonne edellyttää kotimaan kyberturvallisuuden kehittämistoimien lisäksi myös kansainvälisen yhteistyön tiivistämistä. Viranomaisyhteistyön ohella kyberuhkiin vastaamisessa keskeisessä roolissa ovat yksityisen sektorin tietoturvapalveluiden tuottajat.

Ehdotus sisältää kolme keskeistä elementtiä: eurooppalaisen kybersuojakilven perustamisen, kyberhätämekanismin ja kyberreservin luomisen. Ehdotetut muutokset eivät rajoita tai siirrä Suomen vastuuta kansallisesta turvallisuudestaan tai yleisestä turvallisuudesta ja järjestyksestä.

Kybersuojakilpi

Ehdotetun eurooppalaisen kybersuojakilven keskeisin elementti on kansallisten turvaoperaatiokeskusten, Security Operations Center, SOC (tai kyberturvallisuuden viitekehyksessä tietoturvavalvomo) verkoston perustaminen. Sen tavoitteena on tehostaa kyberuhkatiedon vaihtoa EU:n laajuisesti ja sitä kautta myös parantaa kybertilannekuvaa. Ehdotuksen mukaisesti jäsenmaat nimeäisivät kansalliset yhteyspisteet uudelle SOC-verkostolle. Verkoston olisi määrä hyödyntää kyberuhkatiedon ja -tilannekuvan tuottamisessa kehittynyttä teknologiaa ja uusia teknologisia ratkaisuja kuten tekoälyä. Näiden käyttöönottoon olisi tarkoitus hyödyntää kyberturvallisuuden eurooppalaisen osaamiskeskuksen (ECCC) yhteishankintoja ja niiden mahdollistamaa komission osarahoitustukea. Verkostossa tapahtuva tiedonvaihto noudattaisi voimassa olevaa EU-lainsäädäntöä.

Kirkkokatu 12, Helsinki
PL 26, 00023 Valtioneuvosto
Vaihde 0295 480 171 | kirjaamo@intermin.fi | www.intermin.fi

Kyberuhkien valtioiden rajat ylittävästä luonteesta johtuen kansainvälisen tiedonvaihdon tehostaminen kyberuhkista ja poikkeamista on sinällään kannatettavaa kansallisen turvallisuutemme näkökulmasta. Sisäministeriö pitää kuitenkin tärkeänä, ettei kybersuojakilven mukaisilla uusilla rakenteilla luoda päällekkäistä rakenteita suhteessa jo olemassa oleviin, vakiintuneisiin kansallisten kyberturvallisuusviranomaisten tiedonvaihtorakenteisiin ja mahdollisesti heikennetä tarkoituksettomasti näissä verkostoissa tapahtuvaa tiedonvaihtoa. Mikäli verkoston perustaminen loisi uusia kyberturvallisuustoimijoita, tulisi edellyttää vaikutusten arviointia siitä, millaista käytännön lisäarvoa uusi verkosto tuottaisi ja mitkä olisivat sen vaikutukset vakiintuneisiin tiedonvaihtorakenteisiin. Kuten valtioneuvoston kirjelmässäkin tuodaan esiin, tulisi lisäksi täsmentää millaista tietoa verkostossa on tosiasiallisesti määrä vaihtaa. Ehdotuksessa viitataan sopimusperustaiseen tietojen vaihtoon muun muassa liittyen haavoittuvuuksiin ja läheltä piti-tilanteisiin. Tämän kaltaisten tietotyyppien osalta syytä huomata, että tietojen jakamiseen saattaa liittyä myös kansallisen turvallisuuden riskejä, mikäli kyseisiä haavoittuvuuksia ja tietoturva-aukkoja ei ole korjattu ennen tietojen jakamista. Lisäksi kyberuhkista hankittava tieto voi osittain olla tiedustelupalveluiden hankkimaa tietoa, jonka jakamiseen on jatkossakin omat vakiintuneet yhteistyökanavansa. Näin ollen tietojen vaihdon ei voida edellyttää olevan automaattista, vaan tulee perustua aina kansallisen kyberturvallisuuden näkökulmasta tehtävään tarkoituksenmukaisuusharkintaan.

Sisäministeriö nostaa myös esiin sisäministeriön ja puolustusministeriön yhteisen, huhtikuussa 2023 julkaistun kyberselvityshankkeen kehittämistoimenpide-ehdotukset (VN/2434/2022). Selvityksessä tunnistettiin yhdeksi keskeiseksi kehittämistarpeeksi kotimaan kyberturvallisuusviranomaisten välisen tiedonvaihdon esteiden poistaminen. Kansainvälisen tiedonvaihdon kehittämisellä on oma arvonsa, mutta Suomen kansallisen kyberturvallisuuden kannalta viranomaisten kybertiedonvaihdon esteiden purkaminen on ensisijaista. Tätä tukee hallitusohjelman kirjaus tiedonvaihdon esteiden poistamisesta kansallisen turvallisuuden ja järjestäytyneen yhteiskunnan suojaamiseksi.

Kyberhäiriötilanteiden mekanismi ja kyberturvallisuusreservi

Ehdotetulla kyberhäiriötilanteiden mekanismilla toteutettaisiin kyberturvallisuuden varautumis- ja valmiustoimenpiteitä (ml. mahdollinen varautumistestaus) sekä reagoitaisiin kyberhäiriötilanteisiin mukaan lukien jäsenmaalta toiselle pyynnöstä annettava apu. Kyberturvallisuusreservin koostuisi puolestaan sertifioiduista tietoturvallisuuspalveluntarjoajista, joiden palveluilta kyberhätämekanismin kautta voisivat hyödyntää EU:n instituutioiden, virastojen ja toimielimien lisäksi jäsenvaltioiden kriittisten alojen toimijat kyberpoikkeamatilanteista toipumisessa.

Sisäministeriö pitää lähtökohtaisesti kannatettavana kyberturvallisuuden valmius- ja varautumistoiminnan sekä reagointikyvyn kehittämistä huomioiden EU:n kyberturvallisuusdirektiivin NIS2:n vaatimukset. Kyberturvallisuuden kanssa työskentelevien viranomaisten lisäksi luonnollisesti yksityisen sektorin toimijoilla on merkittävää kyberosaamista ja kyberturvallisuuskyvykkyyttä. Kyberturvallisuusreservi voikin jossain määrin edistää tietoturvallisuuspalvelutuottajien liiketoimintamahdollisuuksia ja siten kasvattaa toimia-alan kapasiteettia ja käytettävyyttä vakavista kyberpoikkeamatilanteisiin reagointiin ja niistä toipumiseen.

Ehdotuksessa mahdollistettaisiin avun pyytäminen ja kyberreservin hyödyntäminen myös kolmansille maille. Yhteiskuntamme resilienssi on osittain kytköksissä muun muassa rajat ylittävään energiainfrastruktuuriin kuten unioniin kuulumattoman Norjan vesivoimakapasiteettiin, jolloin kolmansille maille annettava mahdollisuus saada kyberhätämekanismin kautta apua esimerkiksi energiainfrastruktuuriin kohdistetusta kyberhyökkäyksestä toipumiseen, on kansallisen turvallisuutemme intressien mukainen.

Komissio ehdottaa myös kyberhäiriötilanteiden jälkitarkastelumekanismia, joka mahdollistaisi EU:n kyberturvallisuusvirasto ENISA:lle mahdollisuuden arvioida tapahtuneita kyberturvallisuushäiriötilanteita, tilanteisiin johtaneita syitä ja haavoittuvuuksia. Sisäministeriön näkemyksen mukaan vakavien kyberhäiriötilanteiden jälkikäteinen arviointi voisi parantaa kyberuhkiin varautumista. Oleellista on arvioinnissa saatujen tietojen hyödyntämisen ohella tietojen luottamuksellisuuden tarkoituksenmukainen suojaaminen.

Yhteenveto

Sisäministeriön katsoo kybersolidaarisuussäädösehdotuksen voivan jossain määrin parantaa kyberturvallisuutta EU-tasolla. Sisäministeriö yhtyy valtioneuvoston kirjelmässäkin esiin nostettuihin huoliin mahdollisesta päällekkäisen tiedonvaihtoverkoston luomisesta suhteessa jo vakiintuneisiin, jäsenmaiden välisiin kybertiedonvaihtokanaviin ja nostaa esiin tarpeen vaikutusten arvioinnille. Sisäministeriön näkemyksen mukaan kybersolidaarisuussäädösehdotuksen jatkovalmistelua olisi tarkoituksenmukaista vielä jatkaa. Kyberturvallisuutta ylläpidetään ja kehitetään jatkuvasti niin kotimaan viranomaistoimenpitein kuin kansainvälisessä yhteistyössä, ja tässä mielessä kybersolidaarisuussäädöksen voimaan saattamiselle ei ole akuuttia kiirettä.

Erityisasiantuntija Hannu Kotipelto

Sisäministeriö
Kansallisen turvallisuuden yksikkö

Jakelu Hallintovaliokunta

Tiedoksi Sisäministeri Mari Rantanen
Valtiosihteeri Juha Martelius, SM
Erityisavustaja Timo Kerttula, SM
Johtava asiantuntija Katarine Lindstedt, SM
Johdon sihteeri Jaana Söderman, SM
Johdon sihteeri Tiina Landström, SM
Kansainvälisten asioiden yksikkö, SM
Erityisasiantuntija Emma Hokkanen, LVM