Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

14.9.2023

Eduskunta
Liikenne ja viestintävaliokunta

Viite: U 20/2023 vp, Valtioneuvoston kirjelmä eduskunnalle

Lausunto: komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen)

Teknologiateollisuus sekä Kyberala kiittävät mahdollisuudesta lausua asiasta. Lausunto on Teknologiateollisuuden ja Kyberalan yhteinen.

Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka tuottavat puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Haluamme kiinnittää huomiota seuraaviin seikkoihin:

Toimivaltakysymykset selvitettävä ja tarpeettomia rakenteita tulee purkaa, ei lisätä

Euroopan komissio antoi huhtikuussa 2023 esityksen Euroopan Unionin kybersolidaarisuussäädökseksi. Komissio ehdottaa lakiesityksessä kolmen EU-tason toiminnon perustamista: *yleiseurooppalaisia tietoturvavalvomopalveluita* (Security Operations Center, SOC) *ja niiden yhteistyöinfrastruktuurin käyttöönottoa* (European Cyber Shield, eurooppalainen kybersuojakilpi), *kyberhätämekanismia* ja luotettavista yksityisen sektorin palveluntarjoajista koostuvaa *kyberturvallisuusreserviä* sekä *kyberturvallisuuspoikkeamien arviointimekanismia.*

Esityksen tavoitteena on vahvistaa ja tehostaa unionin yhteisiä havainnointi- ja tilannekuvavalmiuksia sekä tukea jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa, niihin vastaamisessa ja niistä välittömästi toipumisessa. Esitettyjen toimintojen perustamista ehdotetaan tuettavaksi Digitaalinen Eurooppa-rahoitusohjelmasta, johon esitetään muutoksia tuen mahdollistamiseksi.

Haluamme painottaa, että koska esityksen tarkoituksena on lisätä kriittisillä ja erittäin kriittisillä aloilla toimivien kansalaisten, yritysten ja yhteisöjen sietokykyä kasvavia kyberturvallisuusuhkia vastaan, on vastuu sekä toiminnan, että omaisuuden hallinnan osalta tietoturvaloukkauksen kohteella itsellään omaisuuden suojaan liittyvien perusoikeuksien mukaisesti. Näin ollen on välttämätöntä varmistaa, ettei ehdotus synnytä kiertomekanismia tietoturvaloukkauksen hallintaan liittyvän päätös- tai ohjausvastuun siirtymisestä oikeudenomistajilta itseltään viranomaisille, eritoten millekään EU-virastolle tai toimielimelle. Tämä olisi selvä suhteellisuusperiaatteen sekä toissijaisuusperiaatteen vastainen tilanne.

Näemme komission esityksessä haasteita muutoinkin toimivallan sekä resurssien optimaalisen kohdentamisen osalta ja suhtaudumme siihen varauksellisesti. Suhteellisuusperiaate toteutuu esityksessä heikosti, minkä lisäksi esitys on tiedonvaihdon luottamuspohjaisuuden näkökulmasta ongelmallinen. Komission lakiehdotuksessa ehdotetut toimenpiteet eivät vastaa sen tavoitteita. Ehdotuksen erottelu kolmeen eri toimintoon ei paranna tietoturvaa. EU:ssa ei tarvita lisää uusia tiedonvaihdon verkostoja, vaan olemassa olevien verkostojen ja rakenteiden tehokkaampaa hyödyntämistä. Pidämme mahdollisena, että esitys kääntyisi tavoitteitaan vastaan, sillä hyvien käytäntöjen edistäminen ei edellytä uusia rakenteita. Uudet rakenteet aiheuttaisivat

Teknologiateollisuus ry
Kyberala ry

Eteläranta 10, P.O.Box 10, FI-00131 Helsinki
Telephone +358 9 192 31
www.techind.fi
Business ID: 0215289-2

lisäkustannuksia ja merkittävää toiminnallista viivettä sekä sekoittaisivat jo entisestään hankalasti hahmotettavaa [rakenteiden ja toimintojen] kokonaisuutta.

Kehittämisen tuleekin kohdistua olemassa olevien verkostojen ja rakenteiden kautta toteutettavaan vapaaehtoisen tiedonvaihdon toimintakulttuurin kehittämiseen sekä erikseen harkiten ja soveltuvin osin Unionin oikeusperustan mahdollistaman tiedonvaihdon kehittämiseen viranomaisten välillä. Katsomme, että Suomen ei tulisi kannattaa esitystä kuin valituilta osin noudattaen Valtioneuvoston arviota ehdotuksesta saavutettavien hyötyjen rajallisuudesta sekä huomioiden ehdotukseen jatkovalmistelussa tehtävät mahdolliset muutokset.

Komission esityksestä puuttuu vaikutusarviointi, ja on epäselvää, miltä osin ehdotus vaikuttaa tai on kytköksissä kansalliseen turvallisuuteen (joka kuuluu yksinomaan kunkin jäsenvaltion vastuulle). Lisäksi SOC-toiminnon hallinnollisiin rakenteisiin sekä arviointimekanismiin liittyen toissijaisuusperiaatetta ei voi arvioida luotettavasti. Esimerkiksi jäsenvaltiossa tapahtuva vakava ja laajamittainen tietoturvaloukkaus arvioidaan varmuudella kattavasti ja siitä syntyvä dokumentaatio olisi ilman ehdotettua säädösperustaakin jaettavissa muiden jäsenvaltioiden ja EU:n rakenteiden käyttöön. Ehdotuksesta kuitenkin seuraisi, että ENISAlle olisi luovutettava arvioinnin kohteena olevaa tietoa huomattavasti aiempaa laajemmin, vaikka tiedon alkuperäiset luovuttajat ovat useimmiten yksityisiä organisaatioita ja muutoinkin luottamuksellisuudesta säädetään jäsenvaltion tasolla. Saatavilla olevien tietojen perusteella näyttääkin vahvasti siltä, ettei ehdotuksessa edellytettävää toissijaisuusvaatimusta voida luotettavasti arvioida.

Markkinatermit ja lainsäätäjiä harhauttavat kuvailut eivät kuulu lainsäädäntöehdotuksiin

Huomautamme komissiota harhaanjohtavien ”markkinointitermien” käytöstä. Ehdotus ei vastaa mielikuvaa ”European Cyber Shield, eurooppalaisesta kybersuojakilvestä” – eritoten, koska kyberuhkatietojen käsittely ei sinällään ”torju” tietoturvaloukkauksia eli toiminta ei täytä tehokkaiden riskienhallintatoimien edellytyksiä. Lisäksi ei ole asianmukaista sekoittaa alan vakiintuneihin käytänteisiin liittyvää ”SOC”-termiä ehdotuksen tavoitteisiin. Pikemminkin tulisi korostaa, että kyse on kansallisten julkisen viranomaisen toimintojen kehittämisestä ja mahdollisesti uusista viranomaistehtävistä, joita rahoitettaisiin Unionin varoista. Kyseessä oleviin kansallisiin viranomaistoimintoihin ei viitata termillä ”Security Operations Center”, vaan CSIRT (Computer Security Incident Response Teams) tai esim. NCSC (National Cyber Security Center). Tämä olisi jo selvyydenkin vuoksi perustelua.

Sertifiointi lisäisi hallinnollista takkaa sekä yrityksille, että kansallisille viranomaisille ja heikentäisi ENISAn toimintakykyä entisestään

Katsomme, että esitetty luotettujen toimijoiden sertifiointikehys lisäisi pienten ja keskisuurten alan yritysten hallinnollista ja taloudellista taakkaa ja heikentäisi niiden liiketoimintamahdollisuuksia, vaikka yhtenäistämisestä voisikin olla myös hyötyä. Kuitenkin käytäntö on osoittanut, että vaatimusten pohjiksi päätyvät useimmiten suuren jäsenvaltioiden kansalliset mallit, minkä lisäksi Suomessa on kansallisestikin suhteellisen haastava tilanne yritysten halukkuudessa investoida kustannuksiltaan raskaisiin lupamenettelyihin (ml. sertifiointi).

Pidämme komission esitykseen sisältyvää vaatimusta palveluiden tuottamisesta kohdemaan kielellä ongelmallisena ja arvioimme sen heikentävän suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia muissa jäsenmaissa. Katsomme, että kohdemaan kielivaatimuksesta tulee luopua, sillä laadukkaiden ylikansallisesti toimivien luotettujen yritysten (trusted providers) täytyy voida työskennellä monikansallisessa ympäristössä tietoturva-alan vakiintuneiden

Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

käytänteiden mukaisesti englannin kielellä. Muussa tapauksessa ehdotus johtaisi vain sisämarkkinoiden sirpaloitumiseen ja kansallisten markkinoiden keskittymiseen entisestään.

Katsomme, että jatkovalmistelussa tulee selvittää luotettujen palveluntarjoajien (trusted providers) vaikutus markkinoiden toimintaan. Mekanismin ei tule aiheuttaa markkinahäiriötä kansallisesti tai Unionin sisämarkkinoilla. Selvittämisintressi on myös sen osalta, miten kustannukset korvattaisiin avunpyyntötilanteessa (kulukorvausperustaisuus vs. liiketoimintaperusteinen hinnoittelu). Lisäksi on huomioitava, että vahingon kohteeksi joutuneella ja mahdollisella vakuutusyhtiöllä on sopimusvapauden perusteella oikeus päättää palveluntarjoajasta, mikäli tapahtuma kuuluu toimijan vakuutussuojan piiriin.

Siviili-sotilasyhteistyö on vähimmäisvaatimus

Katsomme, että mikäli kyberhätämekanismin avulla täydennettäisiin EU:n yhteisen ulko- ja turvallisuuspolitiikan tai yhteisen turvallisuus- ja puolustuspolitiikan yhteydessä annettavaa apua, myös nopean kybertoiminnan joukkojen (Cyber Rapid Response Teams) kautta, tulee näiden rakentua puolustushallintoon rajaamisen sijaan laaja-alaisen siviili-sotilasyhteistyön varaan. Useat lähteet vahvistavat, että esimerkiksi Ukrainassa siviilitoimijoiden osallistuminen ei ole pelkästään menestystekijä, vaan edellytys digitaalisen infrastruktuurin ja palveluiden kriisinhallintatoimissa. On perustelua korostaa ehdotuksen kytkentää EU:n pelastuspalvelumekanismiin, sillä mekanismin soveltamisalalla on kehitetty pitkään hyviä käytänteitä sekä oikeusperustaa.

EU:n tukirahoitusinstrumenttien temaattinen koherenssi heikosti perusteltu

Suhtaudumme varauksella ehdotettuun muutokseen Digitaalinen Eurooppa -ohjelman sisäisiin allokointeihin (luku 3.1.5 Loppusäännökset), erityisen ongelmallinen on esitetty 285 M€ vähennys tekoälyyn. Pidämme välttämättömänä, että tekoälyn kehittämiseen ohjataan riittävästi varoja, jotta eritoten eurooppalaisiin arvoihin nojautuva tekoälyn kehittäminen voi jatkua korkeatasoisena.

Lisätiedot

Peter Sund, Kyberala ry, +358 50 565 0621, peter.sund@teknologiateollisuus.fi