Valtioneuvoston kirjelmä (U 20/2023 vp) kybersolidaarisuussäädös

Liikenne- ja viestintävaliokunta 15.9.2023

Valtioneuvoston kanta on hyvin perusteltu

- Esityksen tavoite on ymmärrettävä, mutta se on kiireessä laadittu, monimutkainen ja epäselvä. Iso ongelma on vaikutusarvioinnin puute.
- Valtioneuvoston kanta on kannatettava ja erittäin hyvin perusteltu.
- Kansallisen viranomaisen resursseista on huolehdittava, jos ja kun sille tulee esityksen myötä uusia tehtäviä, mutta hallinnollista taakkaa ei saa lisätä.
- Kyberturvallisuuden operatiiviset tehtävät unionin tasolla kuuluu säilyttää ensisijaisesti ENISAlla, mutta sen tulee toiminnassaan välttää päällekkäisyyksiä kansallisten viranomaisten toimintojen kanssa. Ei ole syytä luoda uutta hallinnollista orgaania tai kerrosta esimerkiksi komissiolle
- Jos viranomaisille esitetään uusia toimivaltuuksia tai velvoitteita, esitykseen tulee kirjata suhteellisuus- ja välttämättömyysperiaatteet.

Yritysten tietojen luovuttaminen ulkomaille

- Kyberhätätilanteiden mekanismi ja kyberturvallisuusreservi edistävät suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia, mutta kyberturvallisuusreserviin pääsyn edellytykset tulee olla mahdollisimman selkeitä ja tasapuolisia.
- Valtaosa yhteiskunnan kriittisistä toiminnoista – verkot, palvelut, järjestelmät ja ohjelmistot – ovat pääasiassa yksityisten yritysten omistamia ja tarjoamia. Yritykset vastaavat näiden kyberturvallisuudesta, ja toimintojen keskeinen lähtökohta on luottamus. Vahvin kyberturvallisuus rakentuu yritysten ja viranomaisten hyvällä ja luottamuksellisella yhteistyöllä.
- **Yrityksille on aina ilmoitettava, jos kotimaiselle viranomaiselle annettuja tietoja luovutetaan ulkomaille** tai jos säädöksen tarkoittama ”merkittävä tai laaja-alainen kyberturvallisuuspoikkeama” **annetaan ENISA:n arvioitavaksi.**
- Tiedonvaihdon ja luottamuksellisuuden problematiikkaa on avattu hyvin U-kirjelmän s 12.