FiCom ry

Lausunto

09.09.2024

Asia: VN/12457/2021

Lausuntopyyntö luonnoksesta Yhteiskunnan turvallisuusstrategiaksi 2024 (YTS2024)

Luku 1. Johdanto

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

Luku 2. Yhteiskunnan elintärkeät toiminnot

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

Luku 3. Yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

Luku 4. Yhteiskunnan elintärkeiden toimintojen turvaaminen

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

Luku 5. Kokonaisturvallisuuden toimijat

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

Luku 6. Kokonaisturvallisuuden tulevaisuus

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

-

OSA 2: Strategiset tehtävät

Kirjoita yksilöity palautteesi tähän. Merkitse strategisen tehtävän numero ja nimi sekä nimeä osio (Päämäärä ja tavoitteet; Toiminta-ajatus; Toimijat).

-

Yleiset kommentit strategialuonnokseen.

Kirjoita yleiset havaintosi strategialuonnoksesta.

Turvallisuuskomitea on pyytänyt lausuntoja luonnoksesta Yhteiskunnan turvallisuusstrategiaksi 2024 (YTS2024). Vaikka lausuntokierroksen tarkoituksena on kerätä kokonaisturvallisuuden toimijoilta mahdollisimman laaja-alaisesti näkemyksiä strategialuonnoksen kehittämiseksi ja viimeistelemiseksi, FiComilta ei ole pyydetty lausuntoa. Myös jakelulistan ulkopuoliset tahot voivat kuitenkin halutessaan antaa lausuntonsa, joten FiCom esittää kunnioittavasti seuraavaa:

Viime vuosina merkittävästi kehittyneen, kyberturvallisuuteen vaikuttavan EU-sääntelyn kansallinen täytäntöönpano ja organisaatioiden toiminnan mukauttaminen sen mukaisesti haastavat tulevina vuosina niin viranomaisia kuin elinkeinoelämääkin. EU:sta on tullut ja tuloillaan pelkästään kyberturvallisuuteen liittyviä velvoitteita mm. NIS2-direktiivin sekä sitä kansallisesti toimeenpanevan kyberturvallisuuslain, kriittistä infrastruktuuria koskevan CER-direktiivin sekä sitä kansallisesti toimeenpanevan yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain, kyberkestävyyssäädöksen, kyberturvallisuusasetuksen, ns. DORA-asetuksen ja kybersolidaarisuusasetuksen muodossa. Lisäksi yrityksiin kohdistuvaa uutta sääntelyä on tullut tai tuloillaan myös mm. datasäädöksestä, tekoälysäädöksestä ja digipalvelusäädöksestä. Parhaillaan vireillä olevasta valmiuslain kokonaisuudistuksesta on myös odotettavissa uutta kansallista sääntelyä.

Elinkeinoelämä omistaa merkittävän osan Suomen kriittisestä infrastruktuurista ja vastaa sen kyberturvallisuuden varmistamisesta. Kuten strategialuonnoksessakin todetaan, varautuminen häiriötilanteisiin ja poikkeusoloihin on osa toimialan normaalia toimintaa (s. 110). Taannoin lausunnoilla olleessa valtioneuvoston periaatepäätöksessä Suomen kyberturvallisuusstrategiasta 2024–2035 esitetyn varovaisen arvion mukaan elinkeinoelämän panostukset kyberturvallisuuteen ovat vähintään kymmenkertaisia verrattuna valtionhallinnon osoittamaan rahoitukseen. Myös huoltovarmuuden näkökulmasta yritysten käyttämät resurssit kyberturvallisuuteen ovat yhä tärkeämpiä, ja kyberturvallisuuteen investoidaan myös välillisesti. Varautumiskustannusten lisäksi myös poikkeusoloista ja normaaliolojen häiriötilanteista aiheutuva toipuminen aiheuttaa kustannuksia. Valmiuslaissa ei ole säännöksiä siitä, mitä tapahtuu ja tehdään, kun poikkeusolot ja normaaliolojen häiriötilanne ovat päättyneet. Valmiuslakia uudistettaessa olisikin hyvä arvioida varautumista, vastuita ja erityisesti korvauksia koskevia säännöksiä valmiuslain 128 §:ssä ja SVPL 298 §:ssä.

Yhteiskunnan toimivuuden kannalta kriittiset järjestelmät ja palvelut ovat yhä useammin lähes kokonaan yksityisen sektorin tuottamia, joten viranomaisten on siksi tehtävä entistä enemmän

yhteistyötä yritysten kanssa. Yhteiskunnan digitalisoituessa yritysten asema etenkin tieto- ja viestintäteknisten palveluiden tuottamisessa ja kybertoimintaympäristön turvaamisessa on muodostunut varsin keskeiseksi. Monet yhteiskunnan toiminnan kannalta elintärkeät palvelut, kuten maksuliikenteen välitys, sähköverkot ja vedenjakelu, ovat riippuvaisia viestintäpalveluiden ja -verkkojen toiminnasta. Keskinäisriippuvaisessa ja digitalisoituneessa yhteiskunnassa tulisi panostaa etenkin kansainvälisten yhteyksien ja logistiikkaketjujen toimivuuteen. Varautumisen kannalta on kriittistä, että meillä on mahdollisuus tukeutua Suomen ulkopuolella sijaitseviin resursseihin. On tärkeää varmistaa, että tälle ei aseteta lainsäädännöstä johtuvia tarpeettomia estettä.

Eri toimintojen ja toimijoiden välinen keskinäisriippuvuus esimerkiksi toimitusketjujen osalta sekä julkisen ja yksityisen sektorin yhteistyön tärkeys on hyvä tunnistaa. Yritykset tekevät yhteistyötä julkisen sektorin ohella myös laajasti yksityisen sektorin eri toimijoiden kanssa. Esimerkiksi sääntelyyn tai turvallisuusselvitysmenettelyihin liittyvät käytännön esteet voivat kuitenkin heikentää mahdollisuuksia yhteistyöhön. Rajat ylittävä yhteistyö niin julkisen kuin yksityisen sektorin toimijoiden kesken on kuitenkin tärkeää, jotta kyberturvallisuuden parantamiseksi saadaan paras tieto ja osaaminen. Turvallisuusselvitysprosessien yhdenmukaistamista Pohjoismaiden kesken tulisi arvioida siten, että tavoitteena on rajat ylittävä yhteistyö sekä julkisella että yksityisellä sektorilla. Yhdenmukaistetut turvallisuusselvitysprosessit Pohjoismaissa helpottaisivat sekä yksityisen että julkisen sektorin henkilöstön mahdollisuuksia jakaa tietoa ja parhaita käytänteitä, mikä parantaisi myös verkkoturvallisuutta yli rajojen.

Metsola Asko
FiCom ry