Mika Linna
9.8.2024

LIIKENNE- JA VIESTINTÄMINISTERIÖLLE lausuntopalvelu.fi

Diaarinro VN/36693/2023

Finanssiala ry:n lausunto Suomen kyberturvallisuusstrategiasta

Liikenne- ja viestintäministeriö on pyytänyt Finanssiala ry:ltä (FA) lausuntoa valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiaksi.

1 FA pitää hyvänä, että valtioneuvoston kanslia on Petteri Orpon hallitusohjelman mukaisesti ryhtynyt toimenpiteisiin Suomen kyberturvallisuusstrategian uudistamiseksi. FA myös yhtyy pääosin strategiassa esitettyihin johtopäätöksiin ja toimenpiteisiin.

2 Hallitusohjelman kohdan 8.5. mukaisesti ”Kokonais- ja kyberturvallisuuden johtamisrakenne uudistetaan hallituskauden aikana. Uudistuksessa varmistetaan viranomaisten vastuunjaon ja toimivaltuuksien selkeys ja tiedonvaihdon tehokkuus sekä toteutetaan näiden edellyttämät lainsäädäntömuutokset. Hallitus laatii kyberpuolustusdoktriinin sekä selkeyttää ja tarkentaa Puolustusvoimien roolia kyberpuolustuksessa.” FA kiinnittää huomiota siihen, että kyberturvallisuusstrategia näyttää edelleen jäävän varsin yleisluontoiseksi eikä se myöskään kaikilta osin määrittele viranomaisia tai tahoja, joiden tehtävänä on huolehtia ja varmistaa strategiassa esiin tuotujen tehtävien ja tavoitteiden toteutuminen. FA esittääkin, että kyberturvallisuusstrategiaa näiltä osin tarkennettaisiin ja konkretisoitaisiin, jotta strategian toimeenpanoa ja toteutumista voitaisiin seurata tehokkaammin.

3 FA kiinnittää edelleen huomiota siihen, että mainitussa hallitusohjelman kirjauksessa johtamisrakenteen uudistaminen, viranomaisten vastuunjako ja toimivaltuudet, kyberpuolustusdoktriini ja Puolustusvoimien rooli kyberpuolustuksessa ovat kyberturvallisuusstrategian kannalta aivan keskeisiä elementtejä. FA:n mielestä johdonmukaista olisikin ollut, että strategian uudistaminen olisi toteutettu vasta sen jälkeen, kun mainittujen uudistusten ja muutosten sisältö on tiedossa – etenkin, kun strategiaa on haluttu linjata erittäin pitkälle tulevaisuuteen eli vuoteen 2035 asti

4 FA pitää tärkeänä, että Suomelle laadittaisiin mahdollisimman nopeasti kattava kyberpuolustusdoktriini, jossa selkeästi myös linjattaisiin Puolustusvoimien ja muiden viranomaisten rooleista kriittiseen siviili-infrastruktuuriin kohdistuvien hyökkäysten torjumisessa, selvittämisessä ja vaikutuksista toipumisessa. Yksityisellä sektorilla on keskeinen rooli yhteiskunnan kriittisen infrastruktuurin ja elintärkeiden palvelujen tuottajana, minkä vuoksi FA pitää selvänä, ettei niiden puolustamista esimerkiksi valtiollisessa kyberhyökkäyksessä voida jättää vain yksittäisten toimijoiden varaan.

5 Kyberturvallisuusstrategiassa uhkiin varautuminen ja reagoiminen on edelleen keskeisiltä osin hallinnonalakohtaista, mitä FA:n mielestä tulisi arvioida kriittisesti. FA:n kokemusten perusteella hallinnonalojen väliset erot kyberturvallisuuden johtamisessa ja hallinnassa ovat suuria, ja erojen kaventaminen näyttäisi edellyttävän selvästi nykyistä keskitetympää ohjausta ja johtamista.

6 Kyberturvallisuusstrategian lähtökohtana on, että valtiollisiin kyberoperaatioihin reagoidaan ja vastataan eri tavoin kuin tavanomaisiin kyberuhkiin. FA kiinnittää huomiota siihen, että valtiolliset toimijat yhä laajemmin hyödyntävät omissa hyökkäyksissään järjestäytyneitä rikollisryhmiä ja muita ei-valtiollisia toimijoita. Ei-valtiolliset hyökkäykset eivät myöskään kohteensa näkökulmasta useinkaan ole yhtään sen tavanomaisempia kuin valtiolliset hyökkäykset, vaan molemmat usein hyödyntävät täysin samoja menetelmiä ja haavoittuvuuksia. FA pitääkin välttämättömänä, että viranomaisten toimivaltuudet, yhteistyörakenteet ja johtovastuut määritellään kyberturvallisuusstrategiassa tai muulla tavoin niin yksiselitteisesti, että ne kaikissa tilanteissa varmistavat nopean, asianmukaisen ja riittävän reagoinnin kyberhyökkäykseen. Hyökkäyksen attribuutio eli syyksilukeminen on tärkeää, mutta kuitenkin toissijaista kriittiseen infrastruktuuriin tai palveluun kohdistuvan hyökkäyksen torjumiseen ja siitä toipumiseen nähden.

7 Lopuksi FA haluaa korostaa julkisen ja yksityisen sektorin välisen ja sisäisen tietojenvaihdon sekä yhteisen tilannekuvan tärkeyttä. Ns. pimeässä verkossa toimivien markkina-alustojen mahdollistama rikos palveluna -liiketoimintamalli tarjoaa sekä valtiollisille että ei-valtiollisille toimijoille jatkuvasti laajenevan valikoiman kehittyneitä välineitä, menetelmiä ja palveluja, joita ne voivat helposti hyödyntää omissa kyberhyökkäyksissään. Tämän vuoksi on tärkeää, ettei tietojenvaihtoa rajata vain toteutuneisiin tai käynnissä oleviin hyökkäyksiin tai esimerkiksi teknisiin haittaohjelma- tai haavoittuvuuskuvauksiin, vaan se voidaan ulottaa myös kyberhyökkäyksiä mahdollistaviin toimijoihin ja toimintaan. Tuloksellinen tilannekuvatoiminta edellyttää, että merkityksellinen tieto kulkee avoimesti ja mahdollisimman reaaliaikaisesti viranomaisilta myös yksityisen sektorin suuntaan. Näin ei valitettavasti aina ole, ja FA toivoo, että kyberturvallisuusstrategia osaltaan toisi kaivattua parannusta tilanteeseen.

FINANSSIALA RY
Taina Ahvenjärvi