Asiantuntijalausunto eduskunnan talousvaliokunnalle

Allekirjoittanut kiittää mahdollisuudesta lausua kyberturvallisuuden asiantuntijan roolissa eduskunnan talousvaliokunnalle hallituksen esityksestä eduskunnalle laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 67/2024). Mainitun esityksen tarkoituksena on pääasiassa saattaa kansallinen finanssialaa koskeva lainsäädäntö yhdenmukaiseksi nk. EU:n DORA-asetuksen kanssa ja implementoida DORA-muutosdirektiivin tarvitsemat toimenpiteet rahoitustoimialalla. DORA-asetus ja muutosdirektiivi koskevat kyberturvallisuuden varautumisen (nk. kyberresilienssin) parantamista ja yhdenmukaistamista toimialallaan.

Rajaukset

Talousvaliokunta on jo saanut lausuntoja finanssitoimialan viranomaisilta ja pyytänyt kuultavaksi kattavasti toimialan muita toimijoita, joten pitäydyn tässä lausunnossani pääasiassa yleiseen kyberturvallisuuteen toimialan näkökulmasta katsottuna.

Lähitulevaisuuden muutostarpeista toimialan sääntelylle

Esityksessä on hyvin huomioitu muita olennaiset EU:n kyberturvallisuuden yhteismitallistamiseen tarkoitettuja jo voimassa olevia tai pian voimaantulevia asetuksia ja direktiivejä (kuten NIS2 ja CER). EU:lla on kuitenkin tulossa myös muita toimialan kyberturvallisuuteen vaikuttavaa lainsäädäntöä, kuten EU:n tekoälyasetus (tämänhetkinen ehdotus 206/2021), jonka astuu voimaan tämän vuoden kesällä ja muuttuu asteittain velvoittavaksi, viimeistään 24kk voimaanastumisesta.

Tekoälyasetus arvottaa erilaisten tekoälytoteutusten riskiä mm. toimialan perusteella. Tähän vaikuttavat esimerkiksi em. CER-direktiivin mukainen kriittinen toimiala ja tekoälyasetuksessa erikseen nimetyt, hyvinkin kapealla sektorilla tapahtuva toiminta. Jos tekoälyä käyttävä toiminta katsotaan asetuksessa suuririskiseksi, kyseiselle toteutukselle ja toimijalle seuraa erilaisia riskienhallinta- ja raportointivelvoitteita sekä sanktioita. Finanssitoimialalla luonnollisten henkilöiden luottokelpoisuuden arviointi ja riskiluokitus tietyissä vakuutustyypeissä katsotaan tällaiseksi[1]. Tällaisia järjestelmiä on jo Suomessa käytössä, ja näiden valvonta tulee erikseen velvoittavaksi EU:n kautta. Valiokuntaa pyydetään arvioimaan se, otetaanko näitä valvontavelvoitteita erikseen huomioon tässä lakimuutoksessa, vai jätetäänkö muiden muutosten varaan.

Esityksessä on käsitelty myös viranomaisyhteistyötä nykyisen lainsäädännön mukaisesti. Haluan kuitenkin tuoda esille sen, että äskettäin lausunnolle tullut, mm. NIS2-direktiivin edellyttämä kansallinen kyberturvallisuustrategia lähtee tilanteesta, jossa tunnustetaan entistä paremmin kyberuhkan lähde ja motivaatio, ja osallistetaan uhkatyypin mukaiset viranomaiset prosessiin. Haitallisia kybertapahtumia on pääasiassa kolmentyyppisiä: tahattomia ja tahallisia, joista jälkimmäiset voidaan vielä jakaa valtioiden (ei välttämättä pelkästään Suomen) sisäisessä toimintavallassa olevien toimijoiden aiheuttamiin uhkiin ja valtion ulkopuolisiin, valtiollisiin uhkiin. Suomen sisällä toimintavaltaa kyberturvallisuudessa ja varsinkin insidenttien selvittämisessä on jaettu pääasiassa Traficomin kyberturvallisuuskeskuksen (KTK) ja poliisin kesken. Kyberturvallisuusstrategia tulee todennäköisesti tunnistamaan kyberturvallisuuden operatiivisiksi viranomaisiksi myös puolustusvoimat ja suojelupoliisin, milloin kyse on epäillystä valtiollisesta vaikuttamisesta.

Finanssisektori on osa kriittistä infrastruktuuria ja tunnistettu valtiollisen hybridivaikuttamisen kohde- Tämän hetken esitys DORA-asetuksen kansallisista vaikutuksista antaa mahdollisuuden viranomaisyhteistyöhön myös puolustusvoimien kanssa, mutta muita asioita, esimerkiksi

[1] EU-asetusehdotus 206/2021, Liite III, kohdat 5b) ja 5c) (istuntoasiakirjan 15.4.2024 perusteella)

tiedonvaihtovelvoitteita ei ole määritelty samalla tasolla kuin esimerkiksi KTK:n kanssa. Esitetään harkittavaksi, jäävätkö kyberturvallisuusstrategiasta todennäköisesti seuraavat uudistustarpeet viranomaisyhteistyön laajentamiseksi tämän esityksen asiaksi.

Lähitulevaisuuden teknologiamurroksista

Useat teknologiset trendit vaikuttavat lähitulevaisuudessa kyberturvallisuuden eri osa-alueisiin yllättäviäkin reittejä. Näistä tekoälyn vaikutuksia finanssitoimialalle käsittelin jo edellä, mutta toinen merkittävä teknologiamurros sisältää kvanttilaskennan. Näiden teknologioiden edistyminen uhkaa tiettyjä tietoliikenneturvallisuuden perusteita, tarkoittaa myös sitä, että tietoturvan perusinfrastruktuuria joudutaan päivittämään jo viranomaisvaatimuksista johtuen keskipitkällä aikavälillä.

Kvanttilaskenta uhkaa kuitenkin suoremmin erilaisia hajautettuun tilikirjaan DLT pohjautuvia järjestelmiä, kuten esimerkiksi Bitcoin ja erilaiset kryptovaramarkkinoiden järjestelmät, mukaan lukien ”digi-Euro”. Onkin huomioitava, että tällaisten järjestelmien kybersietoisuudessa huomioidaan nk. kvanttikestävyys, eli teknologisten ratkaisuiden päivittäminen kvanttilaskennan kestäviksi riittävän ajoissa. Velvoittavuus kvanttikestävyydelle voi tulla viranomaisvaatimuksista jo paljon ennen itse uhkan realisoitumista.

Kyberuhat kehittyvät kiihtyvällä tahdilla myös kompleksisuuden osalta. Tämän hetken suurimpana haasteena ovat nk. kiristyshaittaohjelmat, joihin varautumisen ytimessä ovat erilaiset varakopiojärjestelyt. Tämäkin on kuitenkin eräänlaista kilpajuoksua, ja kiristyshaittaohjelmat pyrkivät olemaan esimerkiksi piilossa yli varakopioiden ottamisajan, jotta ne päätyvät myös luotettuina pidettyihin tieto- ja järjestelmävarantoihin. Organisaatioiden toipumissuunnitelmien tulisi siis olla riittävän pitkälle mietittyjä ja testattuja niin, että kyseessä ei ole vain yksi varautumiskerros. Lisäksi suunnitelmien tulisi aina kysyä: ”mitä jos tämä varasuunnitelma pettää?”.

Riskienhallinnan lähtötietojen epävarmuus kybertoimintaympäristössä

Organisaatioita (myös finanssialaa) velvoitetaan ottamaan kyberturvallisuuden riskienhallinta entistä tiiviimmin mukaan organisaation omaan riskienhallintaan. Tässä on huomioitava, että kybertoimintaympäristössä riskienhallinnan lähtötiedoissa on paljon suurempaa epävarmuutta kuin yleisessä toimintaympäristössä, koskien nimenomaan esimerkiksi tapahtumien todennäköisyyttä ja vaikuttavuutta, ja monimutkaisia ja pitkäkestoisia tapahtumaketjuja. Järjestelmiin tunkeutuminen havaitaan esimerkiksi keskimäärin vasta yli puolen vuoden kuluttua itse tapahtumasta, ja koko tapahtumaketjun paljastamiseen voi mennä niin ikään vuosi, jos kyseessä on edistyksellinen nk. APT-hyökkäys.

Tällä epävarmuudella on suoria seuraamuksia tapahtumista raportoinnin aikatauluihin ja poikkeaman vakavuuden arviointiin, esimerkiksi DORAn artiklan 18, kohdan 1b perusteella vaikuttavuutta arvioidaan poikkeaman kestolla. Jos poikkeamaksi lasketaan järjestelmään tunkeutuminen, on aivan viimeaikaistenkin tietomurtojen perusteella erittäin vaikeaa arvioida, kauanko poikkeama on kestänyt, ja lisäksi keston toteennäyttäminen ei välttämättä ole mahdollista. Tämä taas voi johtaa tilanteen kaunisteluun, jos organisaatiota uhkaavat erilaiset sanktiot. Esitetään harkittavaksi, tulisiko muutamia DORAn vaikuttavuuteen liittyviä kriteereitä täsmentää kansallisessa lainsäädännössä.

Lopuksi

Hallituksen esitys DORA-asetuksen kansalliseksi implementaatioksi on erittäin tervetullut lisäys osana EU:n tavoitetta parantaa ja yhdenmukaistaa kybersietoisuuden toteutusta ympäri Eurooppaa. On erityisen tärkeää, että puolustusmuuri täyttää joka puolelta vähintään tietyn minimitason, jos vaihtoehtona on keskittyä yksittäisten kohteiden korkeatasoiseen suojaukseen unohtaen kokonaan vähemmän tärkeiksi katsotut osat.

Suomi on perinteisesti suojannut järjestelmiään hyvin muihin maihin verrattuna, mutta ”perustason” määritelmä liikkuu koko ajan eteenpäin, ja integroituvaa kyberrikollisuuden ja valtiollisen vaikuttamisen ekosysteemiä vastaan voidaan puolustautua ainoastaan luomalla vastaava laaja ja hyvin yhteen toimiva kyberturvallisuuden ja -puolustuksen ekosysteemi myös järjestelmiä suojaavan tahon haltuun. Kyse ei ole siitä, onko nyt esityksessä oleva lainsäädäntömuutos tarpeellinen, vaan onko se riittävä.

Lahdessa, 18.6.2024. 

Kyberturvallisuuden työelämäprofessori Mikko Kiviharju
Tietotekniikan laitos
Perustieteiden korkeakoulu
Aalto-yliopisto
Sähköposti: mikko.kiviharju@aalto.fi