Finnish Information Security Cluster (FISC) – Kyberala ry

Lausunto

01.07.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Etujärjestö / toimialaliitto / muu edunvalvontatoimija

1.2 Pääasiallinen toimialanne

ICT-palvelut

1.3 KTL:n mukainen toimijatyyppi

Ei KTL:n soveltamisalaan kuuluva vastaaja

2. Lain soveltaminen ja velvoitteiden selkeys

2.1 Miten ymmärrettävästi riskienhallintaa ja raportointia koskevat velvoitteet on säädetty KTL-laissa?

4

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

4

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

Kyllä, ohjeistus on riittävää

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Kyberala ry ei ole kyberturvallisuuslain mukainen keskeinen tai tärkeä toimija, vaan vastaa kyselyyn jäsenyritystensä ja toimialansa näkökulmasta. Kyberala ry edustaa Suomessa toimivaa kyberturvallisuusalaa.

Keskeisin ”ohjeistus” on hyvän lainsäädännön kriteerit täyttävä laki. Yhtä keskeistä on, että Suomi poikkeaa mahdollisimman vähän säädöksen taustalla olevasta NIS2-direktiivistä, jotta kansainvälistä

kauppaa ja sisämarkkinahyötyjä tavoittelevat Suomeen sijoittautuneet yritykset voivat toimia tehokkaasti.

Keskeistä on myös, että valvovien viranomaisten välillä on yhteiset tulkintaohjeet soveltamisalaan kuuluville sektoreille. Soveltamisalaan kuuluvilla toimijoilla tulee olla mahdollisimman suuri ja myös kehittämisen salliva liikkumavara toteuttaa vaadittavat riskienhallintatoimet. Kyberturvallisuusteollisuus ja keskeiset tieto- ja viestintäteknologian palveluntarjoajilla tulee olla mahdollisuus tarjota ja edelleen kehittää soveltuvia ratkaisuja kilpailuperusteisesti. Tämä tarkoittaa sitä, että viranomaisen ei tule ohjeistaa keinoja, vaan korkeintaan selventää tavoitteita ja päämääriä niiden ollessa tulkinnanvaraisia.

Kaikki soveltamisalaan kuuluvat toimijat eivät käsityksemme mukaan vieläkään tiedä, että niiden tulisi ilmoittautua toimijaluetteloon. Tätä tulisi edistää aiempaa aktiivisemmin yhteistyössä niitä edustavien sektorijärjestöjen kanssa.

Joidenkin sektorien osalta odotettavissa on EU:n direktiivimuutos, jonka etenemisestä tulee tiedottaa aktiivisesti sitä koskevien sektoreiden toimijoille, jotka ovat jo ilmoittautuneet toimijaluetteloon sekä laajemmin näistä sektoreita edustaville järjestöille.

Koska Kyberalan jäsenyrityksiin kuuluu digitaalisen infrastruktuurin ja ICT-palvelujen toimijoita, joilla on jo SVPL 275 §:ään sekä Traficomin määräykseen perustuvia häiriöilmoitusvelvoitteita. Kyberturvallisuuslain 11 §:n mukainen poikkeamailmoitusvelvoite on osin rinnasteinen, jopa päällekkäinen, näiden kanssa, ja samasta tapahtumasta eri oikeusperustan nojalla tehtävien ilmoitusten suhde on epäselvä. Päällekkäisyys tulisi poistaa. Samaa tapahtumaa koskevan ilmoituksen tulisi täyttää sekä kyberturvallisuuslain että SVPL:n mukaiset ilmoitusvelvoitteet. Kyberturvallisuuskeskuksen ohjeet ja valvoville viranomaisille laaditut suositukset ovat hyödyllisiä, mutta poikkeamien ja kynnysarvojen määrittelyä tulee edelleen täsmentää yhdessä säänneltyjen toimialojen kanssa. Erityistä huomiota tulee kohdistaa siihen, että Suomi hyödyntää mahdolliset Komission täytäntöönpanosäädöksien kautta annettavat määräykset, eikä ainakaan luo poikkeavia ratkaisuja muihin jäsenvaltioihin verrattuna.

Muilta osin laki on selkeä ja ymmärrettävä. Velvoitteet yrityksille on kuvattu selkeästi: kriittisten järjestelmien turvaaminen, riskienhallinta, häiriötilanteista raportointi, johdon vastuiden selkeyttäminen jne. Lain velvoitteiden operatiivinen toimeenpano voi kuitenkin olla haastavaa, erityisesti silloin kun palvelu- ja toimitusketjut ovat pitkiä ja jakautuvat useisiin maihin. Positiivista on, että laki määrittelee selkeästi toteutettavat velvoitteet. Tämä jämäköittää kyberturvallisuuteen suhtautumista verrattuna ISO 27xxx-tyyppisiin standardeihin, jotka ovat vapaaehtoisia ja joustavammin sovellettavia.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

3

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

4

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

-

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

-

3.5 Arvioikaa lain toimeenpanon vaikutuksia: Kumppanuus- ja toimitusketjuriskien hallinnan parantuminen organisaatiossanne

-

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Toimijaluetteloon on nähdäksemme ilmoittautunut toimijoita laajasti eri soveltamisalan sektoreilta. Tämä toimenpide on käynnistänyt systemaattisemman kyberturvallisuuden riskienhallinnan ja ohjannut näiden toimijoiden jatkuvuuden varmistamista. Mutta niin toimijoiden, kuin myös valvovien viranomaisten tulisi sisäistää kirkkaasti, että lopullinen päämäärä ei ole dokumentoitu vaatimuksenmukaisuus, vaan vähintään lain edellyttämä kyky hallita kyberturvallisuusriskejä päivittäistoiminnassa.

3.7 Kuvaus merkittävimmistä haasteista tai kielteisistä vaikutuksista, joita olette havainneet lain toimeenpanosta

Kyberturvallisuuden ”kypsyystaso” ei käsityksemme mukaan ole kollektiivisella tasolla edistynyt lain noudattamisen odotusarvon mukaisesti. Käsityksemme mukaan valvontaviranomaiset eivät ole toteuttaneet valvontatoimia siinä määrin, kuin lain voimaantulon jälkeen olisi asianmukaista odottaa. Erityisesti toimijaluetteloon ilmoittamatta jättäneihin tulisi kohdistaa valvontatoimia, sillä lain vaatimusten sivuuttaminen luo epäreiluja markkinaolosuhteita, kun vastuullisille kohdistuu selvästi enemmän hallinnollista taakkaa sekä kustannuksia. Aktiiviset valvontatoimet ovat sopiva ja yleistä kuuliaisuutta herättävä toimi.

3.8 Missä määrin arvioitte, että edellä kuvatut vaikutukset johtuvat nimenomaan KTL-laista?

5 = erittäin merkittävä vaikutus

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

-

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

3

4.1 Avoin tarkennus:

Pidämme selvänä, että lain vaatimusten tasoinen kyberturvallisuuden hallintamalli riskienhallintakeinoineen lisää hallinnollista taakkaa, mikäli riskien hallinnan taso ei ole aiemmin ylittänyt vaadittua tasoa. Monet toimijat, kuten kyberturvallisuusalan toimijat itse tai mm. huoltovarmuuden kannalta merkitykselliset toimija ovat toimeenpanneet laajasti riskienhallintatoimia ennen sääntelyn asettamia vaatimuksia. Hallitusohjelman tavoite yritysten hallinnollisen taakan kasvun välttämisestä tulee ottaa huomioon myös kyberturvallisuussääntelyn toimeenpanossa ja jatkokehittämisessä. Erityisesti on varmistettava, ettei sama tapahtuma tai vaatimustenmukaisuuden osoittaminen johda useisiin rinnakkaisiin prosesseihin

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Kohtalaiset

4.2 Avoin tarkennus:

Toistaiseksi käsityksemme on, että karkea tiedossamme oleva investointivaje eri sektoreilla ei ole merkittävästi korjaantunut. Muutosta kuitenkin on havaittu, mutta tilannetta on pidettävä edelleen dynaamisena. Kyberturvallisuusalan toimijoiden itsensä osalta käsityksemme on, että suorat kustannukset eivät ole olleet merkittäviä.

Kustannuksia aiheutuu muun muassa riskienhallinnan dokumentoinnista, raportointiprosesseista, auditoinneista ja päällekkäisestä vaatimustenmukaisuuden osoittamisesta. Tarkastuksissa tulisi hyödyntää sertifiointeja, auditointiraportteja ja muita vakiintuneita osoituskeinoja päällekkäisen hallinnollisen taakan välttämiseksi.

Korostamme, että kansallisesta tai EU-tason sertifioinnista ei kuitenkaan tule muodostua tosiasiallisesti. Vaatimustenmukaisuuden osoittamisen tulee olla oikeasuhtaista toimijan riskeihin, kokoon ja toiminnan luonteeseen nähden.

4.3 Miten arvioitte KTL-lain soveltamisen aikaista investointien tasoa kyberturvallisuuden kehittämiseen organisaatiossanne?

-

4.3 Avoin tarkennus:

Vaikka palveluntuottaja täyttää NIS2-vaatimukset, se ei automaattisesti tarkoita asiakkaalle NIS2-yhteensopivaa palvelua ilman erillisiä sopimuksia. Tämä voi luoda välillisiä riskejä toimitusketjuissa ja luonnollisesti synnyttää myös kustannusvaikutuksia.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

3

5.1 Avoin tarkennus:

Viranomaisraportointi ei edelleenkään ole elinkeinoelämän toimijoille optimaalinen, koska merkittävä hyöty kokonaisuudessaan lisääntyneistä raportointivelvoitteista saavutetaan vasta, kun kaikki kyberturvallisuuspoikkeamaan liittyvät, eri lainsäädäntöön perustuvat ja eri viranomaisille toimitettavat ilmoitukset voidaan tehdä yhdellä kertaa yhdessä ja samassa palveluportaalissa.

Palveluportaalin olisi tarpeen tarjota myös ns. API-rajapinta sekä mahdollisesti myös agenttisten tekoälyohjelmistoille sopiva rajapinta tai muotosisältö.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Kyberturvallisuuslaki ei tarjoa kattavaa vastausta kysymykseen, vaan olennaista merkitystä on Euroopan komission antamilla täytäntöönpanoasetuksilla. Tätä tietoisuutta tulisi aktiivisemmin edistää esim. kyberturvallisuuden hallintapalveluita edustavien järjestöjen kanssa paremman vaikuttavuuden ja resurssien käytön tehostamiseksi. Kansallinen kyberturvallisuusviranomainen on edelleen osin tarpeettoman itseriittoinen ja rajaava (esim. nojautuminen ISAC-ryhmiin) kyberturvallisuuslain soveltamiseen liittyvissä toimissa.

Merkittävän poikkeaman kynnys on osin tulkinnanvarainen. Merkittävä ero tietyissä tilanteissa kriteerien suhteen syntyy huomioon komission täytäntöönpanoasetuksen (EU) 2024/2690 kautta eräiden toimijatyyppien osalta.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

3

5.3 Avoin tarkennus:

Ohjeistus on riittävää ja pääosin hyvin laadukasta.

6. Lain tavoitteiden toteutuminen

6.1 Arvio KTL-lain tavoitteiden toteutumisesta: Kyberturvallisuuden tason nousu organisaatiossanne

3

6.2 Arvio KTL-lain tavoitteiden toteutumisesta: Toimintaan vaikuttavien poikkeamien ennaltaehkäisy organisaatiossanne

-

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

-

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

3

6.5 Arvio KTL-lain tavoitteiden toteutumisesta: Raportoinnin laadun parantuminen organisaatiossanne

-

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Käsityksemme mukaan sääntelyn vaikutukset ovat realisoituneet vasta osittain. Tämä voi johtua osin talouden suhdannetilanteesta, uusien sektorien tietämättömyydestä, viranomaisvalvonnan joustavasta suuntaamisesta, joskin samalla myös valvonnan todennäköisyyden aliarvioimisesta.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

-

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

3

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Lain kyberturvallisuuden (teknishallinnolliset) riskienhallintavaatimuksien ei voi missään tilanteessa olettaa olevan riittäviä teknologisen kehitykseen ja pahantahtoisen toiminnan kehittymiseen liittyvistä syistä. On selvää, että mm. tekoälyjärjestelmien käyttöönotto ja kyberturvallisuutta vaarantavat tehostetut kyvyt muuttavat riskienhallintakeinojen tarvetta.

Toisaalta samalla on niin, että asianmukainen lain tarkoituksen täyttävän riskienhallintamallin avulla myös kehittyviä ja uusia riskejä voidaan hallita. Sääntelyn jatkuva ja epävarmuutta luova muuttaminen ei ole tehokas tapa, vaan tuleekin arvioida, onko kansallisen sääntelyn taustalla oleva EU-sääntely hyvän lainsäädäntötavan kriteerit täyttävä erityisesti niiltä osin, että kyberturvallisuuden hallintaan liittyviä velvoitteita pyrittäisiin sääntelemään tulos- tai

päämääräperusteisesti sen sijaan, että toimijoita edellytetään soveltamaan tiettyjä yksittäisiä riskienhallinnan keinoja.

Eräs yllä mainitusta erikseen esille nostettava esimerkki: Ns. aiempaan sääntelyyn perustuvissa ilmoituksissa on tullut erikseen luokitella tietojen julkisuus. Raportoivien yritysten näkökulmasta NIS2-raporttien tulisi olla oletusarvoisesti salassa pidettäviä, ellei toisin ilmoiteta.

Lisäksi on huomioitava se tosiasia, että NIS2-direktiiviin on ehdotettu muutoksia, jotka toteutuessaan todennäköisesti johtaisivat kansallisen täytäntöönpanolain muuttamiseen.

7.3 Minkälaisia KTL:n velvoitteet ovat suhteessa arvioonne toimialanne riskeistä ja organisaationne resursseista?

-

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Kyberturvallisuuslaki on käsityksemme mukaan yksi parhaiten muotoilluista täytäntöönpanolaista EU:n jäsenvaltioissa. Keskeistä on, että Suomi poikkeaa mahdollisimman vähän säädöksen taustalla olevasta NIS2-direktiivistä, jotta kansainvälistä kauppaa ja sisämarkkinahyötyjä tavoittelevat Suomeen sijoittautuneet yritykset voivat toimia tehokkaasti. Vaatimuksia ei voi liian korkeina, sillä teknologinen kehitys ja pahantahtoinen toiminta on intensiivistä ja edelleen nopeasti kehittyvää. On selvää, että mm. tekoälyjärjestelmien käyttöönotto ja kyberturvallisuutta vaarantavat tehostetut kyvyt muuttavat riskienhallintakeinojen tarvetta. Kyberturvallisuuslain keskeisin ja samalla oikeasuhtainen päämäärä on hyvän kyberturvallisuuden perustason saavuttaminen ja sen myötä ”kerrosteisen” riskienhallintamallin soveltaminen. Tällä tavalla on mahdollista säilyttää kyberturvallisuuden riskienhallintataso ja systeemiset ulkoisvaikutukset kohtuullisena.

Samalla on todettava, että sääntelyä on toki välttämätöntä kehittää, kun EU-tason sääntely (NIS2-direktiiviä) muutetaan. Siksi tärkein tavoite on pyrkiä saavuttamaan mahdollisimman hyvä yhteiseurooppalaisen sääntelyn sisältö turvallisuuden, kilpailukyvyn ja toimintavapauden välillä.

7.4 Näettekö vaihtoehtoisia sääntely- tai ohjauskeinoja, jotka voisivat toimia paremmin kuin nykyinen malli?

Kuten aiemmin olemme todenneet, käsityksemme mukaan soveltamisalaan kuuluvia sektoreita ja eritoten kyberturvallisuuden toimialaa edustavien järjestöjen välistä yhteistyötä tulisi lisätä sen sijaan, että valvovat viranomaiset pyrkivät omin toimin saavuttamaan kaikki tavoitteensa ja samalla käyttämään kohtuuttoman paljon julkisia resursseja vuorovaikutuksen ja tietoisuuden saavuttamiseksi.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

-

Sund Peter
Finnish Information Security Cluster (FISC) – Kyberala ry