WithSecure Oyj

Lausunto

17.06.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Keskisuuri yritys

1.2 Pääasiallinen toimialanne

ICT-palvelut

1.3 KTL:n mukainen toimijatyyppi

Keskeinen toimija

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:

Kyberturvallisuuslaki on pääosin ymmärrettävä ja toimeenpantavissa. NIS2-direktiivi on itsessään kirjoitettu varsin korkealla abstraktiotasolla, mikä on aluksi aiheuttanut tulkintaepävarmuuksia siitä, miten velvoitteet käytännössä pannaan täytäntöön.

Tilanne on kuitenkin parantunut merkittävästi komission täytäntöönpanoasetuksen (EU) 2024/2690 myötä. Asetus täsmentää direktiivin 21 artiklan mukaisia teknisiä ja metodologisia vaatimuksia erityisesti hallituille palveluntarjoajille ja digitaalisen infrastruktuurin toimijoille, ja se on selvästi

helpottanut vaatimustenmukaisuuden käytännön toteuttamista. ENISA:n kesäkuussa 2025 julkaisema tekninen toimeenpano-ohjeistus on ollut hyödyllinen täydennys.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

2

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

2

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

2

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

3

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

3

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

WithSecure on toteuttanut tietoturvallisuuden hallintaa ja vaatimustenmukaisuutta jo pitkään. Tästä johtuen lain välittömät organisatoriset vaikutukset ovat olleet rajatut: merkittävä osa direktiivin 21 artiklan mukaisista riskienhallintakontrolleista, hallintamalleista ja toimittajaketjun tietoturvahallinnan prosesseista oli jo käytössä.

Keskeisin uusi elementti on ollut johdon vastuun ja sanktioriskin formalisoituminen direktiivin 20 artiklan myötä. Johto ymmärtää nyt eksplisiittisesti, että kyberturvallisuusvelvoitteiden laiminlyönnistä voi seurata merkittävä hallinnollinen seuraamus — tämä on nostanut kyberturvallisuuden prioriteettia johtotasolla.

Kokonaisuutena toimeenpanon vaikutus on ollut pikemminkin ryhdin vahvistaminen kuin perusteellinen uudelleenrakentaminen.

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

Sääntelyn haasteena on, että oleellisen toimijan (essential entity) kokonaiskynnysarvot — yli 250 työntekijää tai yli 50 miljoonan euron liikevaihto — ovat verrattain matalat. Tämä tarkoittaa käytännössä, että WithSecuren kaltaiset organisaatiot kuuluvat tiukimman valvontaregiiimin piiriin, vaikka niiden yhteiskunnallinen kriittisyys ja riski-profiili ei välttämättä edellytä samantasoista sääntelytaakkaa kuin esimerkiksi energiainfrastruktuurin tai terveydenhuollon toimijoilla.

Oleellisen toimijan velvoitteet — erityisesti ennakoiva valvonta (32 artikla) ja siihen liittyvät hallinnolliset vaatimukset — voivat muodostua suhteettoman raskaiksi organisaatioille, jotka täyttävät kokonaiskynnysarvot mutta joiden toiminta ei ole samalla tavoin yhteiskunnallisesti kriittistä. Tämä on laajempi haaste, joka koskee monia WithSecuren kokoluokan yrityksiä.

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

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

WithSecure, tietoturvayrityksenä on ollut jo ennestään hyvä kypsyystaso liittyen riskienhallintaan ja tietoturvan toteuttamiseen, joten sinänsä kyberturvalaki ei vaikuttanut merkittävästi toimintaan. Kuten yllä on kuvattu, lain velvoitteet ylemmälle johdolle ovat toki parantaneet ryhtiä yleisesti ottaen.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

2

4.1 Avoin tarkennus:

Hallinnollinen taakka ei ole merkittävästi lisääntynyt, koska valvova viranomainen ei ole tähän mennessä kohdistanut meihin ennakkovalvonnan toimenpiteitä.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Vähäiset

4.2 Avoin tarkennus:

Kyberturvallisuuslain toimeenpanosta ei ole aiheutunut merkittäviä lisäkustannuksia, koska tarvittavat kontrollit ja prosessit olivat pääosin jo käytössä ennen lain voimaantuloa.

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

Vähäiset

4.3 Avoin tarkennus:

Kyberturvallisuuslain toimeenpanosta ei ole aiheutunut merkittäviä lisäkustannuksia tai -investointeja, koska tarvittavat kontrollit ja prosessit olivat pääosin jo käytössä ennen lain voimaantuloa.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

3

5.1 Avoin tarkennus:

Organisaatiollamme ei ole toistaiseksi ollut tarvetta ilmoittaa poikkeamasta viranomaiselle, joten meillä ei ole käytännön kokemusta ilmoitusmenettelyn toimivuudesta.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Täytäntöönpanoasetus (EU) 2024/2690 antaa selkeän kuvan merkittävän poikkeaman kynnyksestä ja ilmoitusmenettelystä, mikä helpottaa velvoitteen käytännön soveltamista.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

4

5.3 Avoin tarkennus:

Traficomin Kyberturvallisuuskeskuksen sekä ENISAn julkaisema ohjeistus on ollut käytännöllinen ja hyödyllinen. Viranomaisdokumentaatio on tukenut velvoitteiden tulkintaa ja käytännön toimeenpanoa merkittävästi.

6. Lain tavoitteiden toteutuminen

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

2

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

2

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

2

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

2

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

3

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Lain tavoitteiden näkökulmasta arviomme on kaksitasoinen. WithSecuren kaltaiselle kyberturvallisuusyritykselle, jolla on ollut korkea tietoturvan taso, vahva riskienhallinta ja hyvä resilienssi jo ennen lain voimaantuloa, lain käytännön vaikutus on jäänyt vähäiseksi — tavoitteet olivat meillä jo pääosin toteutuneet.

Uskomme kuitenkin, että lain vaikutus on merkittävästi suurempi organisaatioille, jotka eivät toimi kyberturvallisuusalalla ja joilla kyberturvallisuuden hallinta ei ole ollut ydintoimintaa. Tältä osin lain

tavoite — kyberturvallisuuden yleisen tason nostaminen EU:ssa — on perusteltu ja todennäköisesti toteutuu parhaiten juuri näissä organisaatioissa.

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?

4

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Komission ehdottama uusi kategorialuokka – pienimuotoiset keskisuuret yritykset (small mid-cap: alle 750 työntekijää, enintään 150 miljoonan euron vuosiliikevaihto tai 129 miljoonan euron tase) – on perusteltu. Ehdotus varmistaa, että tähän kokoluokkaan kuuluvat organisaatiot luokitellaan enintään tärkeäksi toimijaksi (important entity) eikä oleelliseksi toimijaksi (essential entity).

Muutos on oikeasuhtainen: se vähentää tarpeettoman raskaan valvontataakan organisaatioilta, joiden yhteiskunnallinen kriittisyys ei edellytä oleellisen toimijan valvontaerää. Sääntelyn yleinen taso ei heikkene, koska tärkeät toimijat pysyvät edelleen velvoitteiden piirissä.

Post-kvanttikryptografia (PQC) on yksi kriittisimmistä tietoturvallisuuden kehityskohteista lähivuosikymmeninä. Kvanttilaskennan kehitys uhkaa nykyisin laajalti käytettäviä asymmetrisiä salausmenetelmiä, ja siirtymä PQC-algoritmeihin on aloitettava hyvissä ajoin ennen kuin uhka konkretisoituu.

Komission ehdottama vaatimus PQC-siirtymäpolitiikkojen sisällyttämisestä kansalliseen kyberturvallisuusstrategiaan – tavoitteena kriittisten käyttötapausten osalta vuosi 2030 ja laajemman käyttöönoton osalta vuosi 2035 – antaa tarvittavan poliittisen ohjaustason kansalliselle siirtymäsuunnittelulle. Suomen tulisi valmistautua tähän ja edistää PQC-siirtymää kansallisessa strategiassaan aktiivisesti jo ennen EU-tason velvoitteen voimaantuloa.

Nykyinen tilanne, jossa jäsenvaltiot voivat täydentää komission 21(5) artiklan mukaisia teknisiä vaatimuksia kansallisilla lisävaatimuksilla, aiheuttaa käytännössä merkittävää sääntelyjännitettä ja hallinnollista kuormaa erityisesti rajat ylittäviä palveluja tarjoaville toimijoille.

Ehdotettu maksimiharmonisointi – jossa jäsenvaltiot eivät voisi asettaa tiukempia kansallisia vaatimuksia komission täytäntöönpanosäädösten kattamilta osilta – poistaisi tämän epäjohdonmukaisuuden. Se helpottaisi vaatimustenmukaisuuden hallintaa, vähentäisi kustannuksia ja vahvistaisi yhtenäisen eurooppalaisen kyberturvallisuussääntelyn tavoitetta. Suomen tulisi kannattaa tätä muutosta EU-neuvotteluissa.

Nykyinen tilanne, jossa jäsenvaltiot voivat täydentää komission 21(5) artiklan mukaisia teknisiä vaatimuksia kansallisilla lisävaatimuksilla, aiheuttaa käytännössä merkittävää sääntelyjännitettä ja hallinnollista kuormaa erityisesti rajat ylittäviä palveluja tarjoaville toimijoille.

Ehdotettu maksimiharmonisointi – jossa jäsenvaltiot eivät voisi asettaa tiukempia kansallisia vaatimuksia komission täytäntöönpanosäädösten kattamilta osilta – poistaisi tämän epäjohdonmukaisuuden. Se helpottaisi vaatimustenmukaisuuden hallintaa, vähentäisi kustannuksia ja vahvistaisi yhtenäisen eurooppalaisen kyberturvallisuussääntelyn tavoitetta. Suomen tulisi kannattaa tätä muutosta EU-neuvotteluissa.

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

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Kyberturvallisuuslaki on pääosin ajantasainen ja sen tavoitteet ovat oikeansuuntaiset. Sääntelyn kehittämisen näkökulmasta keskeinen haaste liittyy kuitenkin velvoitteiden oikeasuhtaisuuteen suhteessa toimialan riskeihin ja organisaatioiden resursseihin.

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

Pidemmällä aikavälillä tehokkain keino vähentää sääntelypirstaloitumista olisi siirtyä direktiiveistä suoraan sovellettaviin EU-asetuksiin. Asetus on sellaisenaan velvoittava kaikissa jäsenvaltioissa ilman kansallista täytäntöönpanoa, mikä poistaisi jäsenvaltiokohtaiset poikkeamat ja tulkintaerot. Tämä helpottaisi merkittävästi erityisesti rajat ylittäviä palveluja tarjoavien organisaatioiden vaatimustenmukaisuuden hallintaa, kun sovellettava sääntely olisi yhtenäinen koko EU:n alueella.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

WithSecure on kyberturvallisuusalan yritys, jonka näkökulma kyberturvallisuuslakiin poikkeaa monesta muusta lain soveltamisalaan kuuluvasta organisaatiosta. Tietoturva on ydintoimintaamme, ja olemme rakentaneet kyberturvallisuuden hallinnan, riskienhallinnan ja resilienssin vuosien kuluessa hyvälle tasolle. Laki ei ole meille ensisijaisesti ohjannut toimintaa uuteen suuntaan, vaan formalisoinut jo olemassa olevan käytännön.

Tästä asemasta käsin haluamme kuitenkin nostaa esiin laajemman havainnon: kyberturvallisuuslaki on tärkeä ja oikeansuuntainen instrumentti erityisesti toimialoilla, joilla tietoturvan hallinta ei ole perinteisesti ollut ydintoimintaa. Juuri näissä organisaatioissa lain vaikutus on todennäköisesti merkittävin ja yhteiskunnallinen hyöty suurin.

Sääntelykehyksen pitkän aikavälin kehittämisessä suosittelemme harkitsemaan siirtymistä direktiivimallista suoraan sovellettaviin EU-asetuksiin, velvoitteiden oikeasuhtaisuuden parempaa huomioimista suhteessa organisaatioiden resursseihin ja toimialakohtaisiin riskeihin.

Lindroos Sari
WithSecure Oyj - Head of Security Compliance