BLC Telecom Oy

Lausunto

02.07.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Keskisuuri yritys

1.2 Pääasiallinen toimialanne

Digitaalinen infrastruktuuri

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

Ohjeistus on riittävää joiltain osin

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Lain vaatimukset on tunnistettu keskeiseksi vaatimuksiksi, jotka olisi toteutettu ilman lakiakin.

Käytännössä epäselvyydet liittyvät enemänkin lain tulkinnan tasoon sekä osoitusvelvoillisuuteen esim. mikä taso tulkitaan riittäväksi, mitä pidetään hyväksyttävänä näyttönä, jne.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

3

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

3

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

Keskeisiin asioihin kiinnitetään enemmän huomiota. Asioita kuvataan entistä tarkemmin.

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

Pienillä yrityksillä haasteita lain määräysten täytäntöönpanossa.

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

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Kyberturvallisuuden taso on entisestään parantunut ja tietoisuus koko organisaatiossa lisääntynyt.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

3

4.1 Avoin tarkennus:

Kyberturvallisuustoimenpiteitä on tehty aiemminkin, nyt lain voimaan tulon jälkeen dokumentointi (näyttövelvollisuus) on lisännyt hallinnollista työtä.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Kohtalaiset

4.2 Avoin tarkennus:

Kustannukset syntyneet dokumentoinnin, auditointien ja koulutusten lisääntymisestä sekä tukijärjestelmän hankinnasta.

Hallinnollinen työ on lisääntynyt riskienhallinnan, raportoinnin, toimittajahallinnan ja vaatimustenmukaisuuden osoittamiseen liittyvän dokumentoinnin vuoksi

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

Kohtalaiset

4.3 Avoin tarkennus:

Normaalia investointia kyberturvallisuuden valmiuksien parantamiseksi, ei pelkästään lain vaatimusten täyttämiseksi,

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

4

5.1 Avoin tarkennus:

Organisaatiolla on ollut jo ennen KTL-lainsäädäntöä käytössä prosessit viranomaisille tehtävästä raportoinnista ja ilmoituksista. Uusia ilmoituksia ei ole ollut tarve lähettää KTL -lainsäädännön voimaantulon jälkeen, joten sen toimivuudesta ei ole vielä kokemusta.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

4

5.2 Avoin tarkennus:

KTL täsmentää joitakin raportointi- ja ilmoitusvelvollisuuksia, mutta ei lähtökohtaisesti muuta viranomaisyhteistyön perusrakennetta.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

3

5.3 Avoin tarkennus:

-

6. Lain tavoitteiden toteutuminen

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

4

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

3

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

4

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

3

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

4

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Parhaiten toteutuneita tavoitteita ovat olleet tietoturvakäytännöt, tekniset tietoturvakontrollit, poikkeamienhallinta sekä riskienhallinnan perusrakenteiden tarkennukset. Nämä toimintamallit olivat pääosin käytössä jo ennen KTL-lainsäädäntöä. Suurimmat kehitystarpeet ovat liittyneet dokumentoinnin laajuuteen, toimitusketjujen hallintaan, koulutusten systemaattisuuteen sekä vaatimustenmukaisuuden osoittamiseen.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Toimitusketjun hallinnan ulottaminen kaikkiin alihankkijoihin. Pienillä alihankkijoilla pienet resurssit toteuttaa asioita. Sopimusmuutosten päivittäminen hidasta.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

4

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Ei

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

-

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

4

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Sääntely on pääosin ajantasaista ja vastaa nykyiseen kyberturvallisuusympäristöön liittyviä uhkia ja tarpeita. KTL on selkeyttänyt organisaatioiden vastuuta kyberturvallisuuden riskienhallinnasta, jatkuvuudenhallinnasta sekä johdon vastuista.

Sääntelyn oikeasuhtaisuudessa on kuitenkin kehittämistarpeita erityisesti dokumentointi- ja osoitusvelvollisuuksien osalta. Jatkokehityksessä olisi hyödyllistä lisätä viranomaisten tarjoamaa käytännön ohjeistusta ja yhdenmukaistaa tulkintoja eri toimialojen välillä, jotta organisaatiot voivat kohdistaa resurssinsa tehokkaammin todelliseen riskienhallintaan ja kyberturvallisuuden kehittämiseen.

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

Nykyinen sääntelymalli luo tarpeellisen vähimmäistason kyberturvallisuudelle eikä sille ole näkyvissä suoraan vaihtoehtoa, joka kokonaisuutena toimisi merkittävästi paremmin. Kehittämismahdollisuuksia voisi olla kuitenkin erityisesti ohjauksen toteutustavassa.

Viranomaisohjauksessa voitaisiin nykyistä enemmän hyödyntää riskiperusteista lähestymistapaa, jossa painopiste olisi toteutuneessa kyberturvallisuuden hallinnassa ja jatkuvassa kehittämisessä yksityiskohtaisen dokumentaation sijaan. Viranomaisten tarjoamat käytännön ohjeet, toimialakohtaiset tulkinnat, mallipohjat ja hyvien käytäntöjen jakaminen voisivat monissa tapauksissa tuottaa paremman vaikuttavuuden kuin uusien velvoitteiden lisääminen.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

-

Pykäläinen Harri
BLC Telecom Oy