Olli Haukkovaara

Lausunto

26.05.2026 VN/11135/2026

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

Tärkeä toimija

2. Lain soveltaminen ja velvoitteiden selkeys

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

5 = erittäin ymmärrettävästi

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

5 = erittäin selkeinä

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

Kyllä, ohjeistus on riittävää

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Velvoitteet ovat selkeät - mutta monet sen piirissä olevat pienet yritykset eivät edelleenkään toteuta lain vaatimuksia.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

2

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

Tietyt kumppanit ovat selkeästi parantaneet tietoturvansa ja riskienhallintansa tasoa.

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

PK yrityksillä haasteita löytää tietoturva- ja riskienhallintaosaajia laittamaan asiat kuntoon.

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

5 = erittäin merkittävä vaikutus

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Ylin johto sitoutuu aiempaa paremmin tietoturvaan.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

2

4.1 Avoin tarkennus:

Hallinnollinen taakka on suht pieni.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Kohtalaiset

4.2 Avoin tarkennus:

Alihankintaketjun tietoturvan arviointi / seuranta kasvattanut työkuormaa / kustannuksia.

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

Kohtalaiset

4.3 Avoin tarkennus:

Investointeja kyberturvallisuuteen tulisi lisätä edelleen.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

1 = erittäin huonosti toimiva

5.1 Avoin tarkennus:

Rikosilmoitus poliisille vaatii organisaation virallisen nimenkirjoitusoikeuden, eli esim. tietohallintojohtaja, tietoturvapäällikkö tai tietosuojavastaava ei voi yleensä tehdä rikosilmoitusta, vaan se jää esim. toimitusjohtajan tehtäväksi, joka puolestaan ei välttämättä tiedä tapahtuneesta rikoksesta riittävästi.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Tämä kohta ei ole minulle ihan selkeä.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

5 = erittäin hyödyllisiä

5.3 Avoin tarkennus:

Ilman tukea ja ohjeistuksia lain noudattaminen oikein aiheuttaisi ongelmia organisaatioille.

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

3

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

2

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Valtaosa lain vaatimuksista on organisaatiossamme toteutettu jo ISO 27001 sertifikaatin myötä. Ainoastaan kyberriskienhallinnan puitteissa on tapahtunut positiivista kehitystä.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Kaikki tavoitteet ovat toteutuneet.

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?

Tulevaisuus tulisi huomioida paremmin, esim. PQC alkaa olla jo arkipäivää esim. VPN palveluissa. Kaikkien organisaatioiden tulisi aloittaa välittömästi kryptoinventaario.

Samoin ransomware hyökkäyksiin tulisi jokaisen organisaation varautua nopeasti, koska globaalisti kiristyshaittaohjelmahyökkäysten riski on kriittisen korkea, sillä jopa 73 % organisaatioista raportoi kokeneensa vähintään yhden kiristyshaittaohjelmahyökkäyksen edellisen vuoden aikana.

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

5 = oikeasuhtaisia ja toteuttamiskelpoisia

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Kuten edellä sanoin kohdassa 7.2. tiettyjä alueita on syytä kehittää.

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

Selkeät ohjekirjat organisaatioille esim. kryptoinventaarion luomiseksi ja ransomware hyökkäykseen varautumiseksi ja muiden vastaavien asioiden maaliin saattamiseksi.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

NIS2 vaatimukset on hyvin huomioitu mutta esim. CRA, CER, ja AI Act regulaatioiden nostamia kyberturvallisuus vaatimuksia ei ole riittävästi huomioitu.

Olli Haukkovaara
CISO Sofigate Oy