

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Muu

1.2 Pääasiallinen toimialanne

Julkishallinto

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?

3

2.3 Arvio viranomaisohjeistuksen riittävydestä ja selkeydestä

Ohjeistus on riittävää joiltain osin

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Erityisesti toimitusketjujen riskien hallinta jää nykyisellä ohjeistuksella tulkinnanvaraiseksi, millä konkreettisin toimin voidaan tuotteiden ja palveluiden laatu, häiriönsietokyky, niiden hallintatoimenpiteet ja kyberturvallisuuskäytännöt riittävällä tavalla varmistaa.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

3

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

2

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

1 = ei vaikutusta

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

3

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

2

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Kyberturvallisuuden riskienhallintaan on kiinnitetty entistä paremmin huomiota ja siihen liittyvien menettelytapoja on kehitetty systemaattisempaan suuntaan. Myös johdon tietoisuus kyberturvallisuusriskeistä on kasvanut lain voimaantulon myötä.

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

Merkittävimmät haasteet ovat liittyneet resursointiin ja työmäärään, joka tarvitaan mm. riskienhallinnan menettelytapojen konkreettisten toimien suorittamiseksi.

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

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Organisaation tietoisuus kyberturvallisuuslain velvoitteista on lisääntynyt lain voimaantulon myötä.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

4

4.1 Avoin tarkennus:

Lain vaatimusten täyttäminen ja kyberturvallisuuden tilan (GAP-analyysi yms.) itsearviointi vaativat edelleen resursointitarpeita toiminnan jatkuvuuden varmistamiseksi.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Vähäiset

4.2 Avoin tarkennus:

Vain vähäisiä hankintoja/tarkastuksia on hankittu ulkoisilta toimijoilta ja velvoitteiden täyttymiseksi on käytetty pääasiassa vain viraston omia resursseja.

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

Vähäiset

4.3 Avoin tarkennus:

-

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

4

5.1 Avoin tarkennus:

Prosessi on käytännössä havaittu hyvin toimivaksi kanavaksi.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

2

5.2 Avoin tarkennus:

Merkittävän poikkeaman kriteerit ovat tulkinnanvaraisia ja joissakin tilanteissa organisaatio voi tehdä NIS2 mukaisen ilmoituksen ns. varmuuden vuoksi velvoitteen täyttämiseksi. Lisäksi Traficomilla on olemassa kaksi erillistä ilmoituskanavaa: NIS2 mukainen ilmoituskanava sekä tietoturvaloukkauksen ilmoituskanava. Toimijoille olisi selkeämpää jos ilmoitukset voitaisiin tehdä vain yhtä kanavaa käyttäen.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

3

5.3 Avoin tarkennus:

Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä auttaa varsin hyvällä tavalla kyberturvallisuusriskien hallinnan toteuttamisessa.

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

1 = erittäin vähäinen vaikutus

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Yleinen tietoisuuden lisääntyminen organisaatioissa sekä raportointivelvoitteen kautta parantunut tilannekuvan muodostuminen valvovilla viranomaisilla.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Toimitusketjujen kyberturvallisuusriskien arviointi ja hallintatoimien riittävyyden arviointi on tulkinnanvaraista ja voi johtaa hyvin erilaisiin tulkintoihin toimittajien kyberturvallisuuden tasosta, riippuen arvioitityötä tekevästä tahosta.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

3

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?

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisuudesta ja kehittämistarpeista

Lisääntyvä regulaatio asettaa sinänsä kannatettavia vaatimuksia toimijoille, mutta lisää samalla hallinnollista taakkaa velvoitteiden täyttämiseksi nykytilanteessa, jossa resursointi on haasteellista.

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

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

Kyberturvallisuus ja siitä huolehtiminen on jatkuvaa ja alati muuttuvaan toimintaa, laki tulisi kuitenkin olla riittävän geneerinen, jotta se kestää aikaa. Lainsäädäntöä tukemaan tulisi laatia sen soveltamiseen liittyvää ohjeistusta ja menettelytapoja, esimerkiksi valvovien viranomaisten taholta, joissa huomioitaisiin mm. kvanttiteknologian ja tekoälyn luomat haasteet kyberturvallisuudelle.

Rintamaa Janne
Terveiden ja hyvinvoinnin laitos THL