Varsinais-Suomen hyvinvointialue

Lausunto

20.05.2026

VARHA/11095/03.00.00/2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Suuri yritys

1.2 Pääasiallinen toimialanne

Terveys

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?

3

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:

Merkittävän poikkeaman määritelmä on epätarkka.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

2

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

1 = ei vaikutusta

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

2

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

1 = ei vaikutusta

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

On huomattava, että IT-palveluntarjoajamme hoitaa tekniset häiriöt ja poikkeamat käyttäjätiedotuksineen automaattisesti ilman eri pyyntöä valvontajärjestelmissä havaittujen poikkeamien perusteella ja raportoi niistä meille, sekä pyytää tarvittaessa itse apua Kyberturvallisuuskeskukselta. Organisaatioomme perustettiin lain vaatimusten toteutumisen varmistamiseksi oma tietoturvapoikkeamien hallintaryhmä. Tämä on positiivinen asia, koska meillä on nyt säännöllisesti kokoontuva ryhmä, jossa voidaan keskustella tietoturvapoikkeamista eri näkökulmista, ja parantaa valmiuksia poikkeamatilanteissa toimimiseen ja viestintään.

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

Kolmen ilmoituksen tekeminen jokaisesta poikkeamasta on erittäin työlästä. Kyseessä ei ole pelkästään web-lomakkeiden täyttämisestä, vaan kopiot ilmoituksista pitää viedä myös asianhallintajärjestelmäämme ja jaella kolmeen kertaan. Lain lähtökohtana on ollut ilmoittaminen kyberhyökkäyksestä, mikä näkyy myös ilmoituslomakkeiden kysymyksissä. Käytännössä ilmoitettavat tapaukset ovat useimmiten sovelluspäivitysten aiheuttamia häiriöitä, jotka kuitenkin sisältyvät laissa kuvattuun merkittävän poikkeaman määritelmään. Niissä ei ole mitään ulkopuolista hyökkääjää. Erittäin suuri haaste on lain edellyttämä 24 tunnin kuluessa tehtävä ensi-ilmoitus. Vaikka toimimme 24 h, meillä ei ole tahoa, joka tekisi ensi-ilmoituksen viikonloppuisin ilman erityisjärjestelyjä. IT-palveluntarjoajamme hoitaa häiriöt 24h/7pv ja on tarvittaessa yhteydessä Kyberturvallisuuskeskukseen, mutta se ei voi tehdä viranomaisilmoituksia puolestamme.

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

5 = erittäin merkittävä vaikutus

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Raportointivelvollisuus valvovalle viranomaiselle ei ole vaikuttanut häiriöistä toipumiseen. Tietoturvapoikkeamien hallintaryhmän perustaminen lain vaatimusten toteuttamiseksi on kuitenkin vaikuttanut viestinnän ja operatiivisten toimintaohjeiden selkiyttämiseen häiriötilanteissa. Ensi-

ilmoituksen tekeminen mahdollistaminen 24 h kuluessa on vaatinut meiltä erityisjärjestelyjä, jotka eivät kuitenkaan auta häiriöstä toipumiseen.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

2

4.1 Avoin tarkennus:

Raportointivelvollisuus valvovalle viranomaiselle on vaatinut uuden prosessin luomista. Toimivan prosessin kehittäminen viikonloppuna tehtävien ensi-ilmoitusten osalta on ollut työlästä ottaen huomioon, ettei niillä ole häiriötilanteesta toipumisen kannalta mitään merkitystä. Mikäli kyse olisi todellisesta kyberhyökkäyksestä, IT-palveluntarjoajamme joka tapauksessa tekisi siitä ilmoituksen Kyberturvallisuuskeskukselle.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Vähäiset

4.2 Avoin tarkennus:

Muusta työstä pois, ei ulkopuolisia kustannuksia.

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

Vähäiset

4.3 Avoin tarkennus:

Ei investointeja.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

5 = erittäin hyvin toimiva

5.1 Avoin tarkennus:

Prosessi on kuvattu kirjallisesti ja se toimii.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

2

5.2 Avoin tarkennus:

Käsittääkseni kynnys ilmoittamiseen vaihtelee eri organisaatioissa eikä kaikilla ole selvää prosessia viikonloppuna tehtäviin ensi-ilmoituksiin.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

3

5.3 Avoin tarkennus:

LVV:lle tehtävistä ilmoituksista ei ole saatu mitään hyödyllistä palautetta eikä sitä ole odotettukaan. Kyberturvallisuuskeskus toimii loistavasti palautteen antajana.

6. Lain tavoitteiden toteutuminen

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

1 = erittäin vähäinen vaikutus

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

1 = erittäin vähäinen vaikutus

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

2

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

1 = erittäin vähäinen vaikutus

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

2

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Raportointi poikkeamista valvovalle viranomaiselle ja organisaation johdolle parantunut.

Tavoitteena lienee ollut tuottaa tilannekuvaa valvovalle viranomaiselle, joka on nyt toteutunut, joskin epämääräisten määritelmien takia, viranomaisten saama tietoa eri organisaatioilta ei liene tasalaatuista.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Vaikutukset riskienhallintaan, jota luonnollisesti tehdään, joskaan ei kyberturvallisuuslain pohjalta.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

2

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Ilmoitusvelvollisuuden keventäminen poikkeamista, jotka eivät ole kyberturvallisuuspoikkeamia vaan ainoastaan merkittäviä poikkeamia.

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

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Ilmoitusvelvollisuutta tulisi keventää niiden organisaatioiden osalta, joissa IT-palvelut tuottaa ulkopuolinen toimija, ja siirtää kyseiselle toimijalle. Ilmoitusten lukumäärää voitaisiin vähentää niiden tapausten osalta, jotka eivät ole ulkoisen tekijän aiheuttamia kyberhyökkäyksiä, vaan esim. ohjelmistopäivityksistä johtuvia katkoksia operatiivisessa toiminnassa.

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

Valvovan viranomaisen tulisi tehdä konkreettisia auditointeja valvomiinsa organisaatioihin sen sijaan, että valvonta perustuu pelkästään tulkinnallisiin kyselyihin.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

Ilmoituslomaketta tulisi kehittää niin, että se huomioisi paremmin muut merkittävät poikkeamat kuin juuri kyberhyökkäyksestä aiheutuneet poikkeamat, jotka lienevät harvinaisia. Voitaisiin lisätä vaikka sellainen kohta kuin, johtuiko poikkeama ohjelmistopäivityksestä? Näin saataisiin paremmin kategorioituja tilastoja siitä, miksi ilmoitukset tehtiin.

Satopää Jouni
Varsinais-Suomen hyvinvointialue - Konsernihallinnon hallintopalveluiden laki- ja asiantuntijapalvelut/Tietoturvapäällikkö