HE 27/2025 Lausunto

Liikenne- ja viestintävaliokunta

2025-05-23

WITH secure

PUBLIC

Versiohistoria

Versio	Päiväys	Tekijä	Muutos
1.0	2025-05-23	Artturi Lehtiö	Lopullinen versio
0.1	2025-05-20	Sari Lindroos (Head of Security Compliance)	Alustava versio.

Sisällys

1 Lausuntopyyntö....4

2 Lausunto....4

2.1 Valvovat viranomaiset ja valvontatoimenpiteet....5
2.2 Kriittisten toimijoiden määrittely....5
2.3 Rekisteröinti....5
2.4 Poikkeamailmoitukset....6

1 Lausuntopyyntö

Asia: HE 27/2025 vp Hallituksen esitys eduskunnalle laeiksi kyberturvallisuuslain ja julkisen hallinnon tiedonhallinnasta annetun lain 3 §:n muuttamisesta.

Ehdotetut muutokset koskevat NIS 2 direktiivin kansallisen lainsäädännön, kyberturvallisuuslain (HE 57/2024 vp) ja CER direktiivin kansallisen lainsäädännön, laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (HE 205/2024 vp), täydentämisestä siten, että kyberturvallisuutta koskevat velvoitteet soveltuisivat CER-direktiivin nojalla kriittisiksi toimijoiksi määritettäviin toimijoihin myös silloin, kun kriittinen toimija ei ennalta kuuluisi kyberturvallisuuslain tai julkishallinnon toimialan osalta tiedonhallintalain 4 a luvun soveltamisalaan.

NIS 2 direktiiviä koskeva lainsäädäntö tuli voimaan 8.4.2025. CER direktiiviä koskeva lainsäädäntö (HE 205/2024 vp) on vielä kesken. Ehdotetut lait on tarkoitettu tulemaan voimaan samanaikaisesti yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

WithSecure perustaa seuraavan lausuntonsa omaan kokemukseensa NIS2 direktiivin, muiden vastaavien velvoitteiden vaatimustenmukaisuuden arvioinnissa ja toteutuksessa, sekä lakivaliokunnan esitykseen HE_27+2025.pdf, joka toimitettiin WithSecurelle pohjamateriaaliksi.

2 Lausunto

Suomi tietoyhteiskuntana on äärimmäisen riippuvainen tietojärjestelmien ja tiedon saatavuudesta, eheyden ja luottamuksellisuuden jatkuvuudesta.

Olemme tänä päivänä jo tilanteessa, jossa voidaan ennemminkin keskustella siitä, milloin mahdollinen häiriö ilmaantuu kuin siitä, että niitä voitaisiin varmuudella estää. Häiriönsietokykyä pitää kehittää siitä näkökulmasta, että häiriön vaikutus pystytään minimoimaan ja häiriöstä pystytään toipumaan mahdollisimman nopeasti, tiedon eheys ja luottamuksellisuus säilyttäen. Tämä on suorassa yhteydessä ihmisten turvallisuudentunteeseen, yhteiskuntarauhaan ja yhteiskunnan toimintakykyyn.

WithSecuren näkökulmasta ehdotus on tervetullut laajennus ja edistysaskel yhteiskunnan tietoturvan ja häiriöiden sietokyvyn parantamisessa.

Tässä lausunnossa haluamme nostaa esiin muutamia käytännön osa-alueita, jotka olisi hyvä ottaa huomioon jo lainsäädäntövaiheessa.

2.1 Valvovat viranomaiset ja valvontatoimenpiteet

Lainsäädäntö ei ole tehokasta ilman valvontaa. CER- ja NIS 2 -direktiiveissä osoitetaan toimijalle valvova viranomainen ja tietyt velvoitteet esimerkiksi poikkeamailmoitusten osalta. Ehdotuksessa mainitaan, että valvovat viranomaiset olisivat pääosin samoja molempien lakien nojalla, mutta voi olla myös tilanteita, jossa tämä ei toteudu. Tämä tilanne aiheuttaa toimijalla lisätyötä ja kustannuksia vaatimusten toteuttamisessa (mahdollisesti kaksi eri prosessia poikkeamailmoituksiin, valvontatoimiin).

Tulisi pyrkiä tilanteeseen, jolloin toimijalla olisi yksi viranomainen (single point of contact), jonka kanssa luoda yhteistyösuhde, jolle poikkeamailmoitukset tehdään ja joka hoitaa valvontatoimet keskitetysti tilanteessa, jossa toimijalle olisi osoitettu kaksi eri valvovaa viranomaista. Tällä tavoin saavutetaan resursseja säästävää synergiaa toimijoiden osalta, mutta myös valvovien viranomaisten resurssien osalta. Suositus olisi siis panostaa valvovien viranomaisyhteistyön ja tiedonvaihdon tehokkuuteen.

2.2 Kriittisten toimijoiden määrittely

Ehdotus lähtee siitä olettamasta, että CER direktiivin nojalla kriittisiksi määritellyt toimijat kuuluisivat jo NIS 2 direktiivin soveltamisalaan keskeisinä toimijoina. Oletus on perusteltu, mutta ehdotuksessa pitäisi silti ottaa kantaa tilanteeseen, jossa kyberturvallisuuslain soveltamisalaa koskevan keskisuuren yrityksen kokokynnyksen alittava toimija määriteltäisiin kriittiseksi CER direktiivin nojalla.

Tällä hetkellä NIS 2-direktiivin soveltamisalaan kuuluvilla organisaatioilla on ollut haasteita vaatimustenmukaisuuden arvioinnissa ja toteutuksessa niin osaamisen kuin resurssien osalta. Jos kooltaan pien- tai mikroyritys määritellään kriittiseksi ja toimija velvoitetaan toteuttamaan NIS 2 vaatimukset, tulee yhteiskunnan varautua antamaan merkittävää tukea direktiivien velvoitteiden toteuttamisessa. Tässä tilanteessa olisi myös hyvä harkita ehdotuksessa määriteltyjen siirtymäaikojen (rekisteröinti, poikkeamista ilmoittaminen ja NIS 2 vaatimusten toteuttaminen) pidentämistä.

2.3 Rekisteröinti

Ehdotuksessa määritellään toimijalle velvoite rekisteröityä valvovalle viranomaiselle kuukauden kuluessa siitä, kun toimijalle on annettu tiedoksi päätös kriittiseksi toimijaksi määrittämisestä.

NIS 2-direktiivin vaatima rekisteröinti kaikkien toimijoiden osalta ei toteutunut kuukauden sisällä (Lähde: Traficom Webinaari: Kyberturvallisuuslaki tuli voimaan - mikä muuttui? : 12.5.2025). Tätä määräaikaa suositellaan pidennettäväksi vähintään kolmeen kuukauteen.

WithSecure suosittelee myös viranomaisyhteistyötä siten, että jos toimija on jo rekisteröitynyt NIS 2 direktiivin vaatimusten mukaisesti valvovalle viranomaiselle, tämä rekisteröinti kattaisi myös CER -direktiivin vaatimukset.

2.4 Poikkeamailmoitukset

Velvoite toteuttaa poikkemailmoituksiin vaadittavat velvoitteet kuukauden kuluessa siitä, kun toimijalle on annettu tiedoksi päätös kriittiseksi toimijaksi määrittämisestä on haastava. Sama velvoite liittyi myös NIS 2 direktiiviin, mutta tällöin toimijalla oli jo etukäteen tieto vaatimuksen soveltamisesta organisaatioon. Tässä ehdotuksessa vaatimus kattaa mahdollisen uuden toimintatavan kehittämisen ja resurssoinnin yhdessä kuukaudessa, koska se perustuu viranomaisen ilmoitukseen.

WithSecure suosittelee poikkeamailmoituksiin vaadittavien velvoitteiden soveltamiseen pidempää siirtymäaikaa (vähintään 3kk) etenkin, jos kyseessä on toimija, joka ei ole jo ollut NIS 2 soveltamisalassa ja/tai WithSecuren ehdotusta kappaleessa 2.1 viranomaisyhteistyöstä poikkeamailmoittamisessa ei voida toteuttaa.

Lausunnon antaja

Sari Lindroos
Head of Security Compliance
WithSecure

Artturi Lehtiö
Vice President, Partner Success
WithSecure

Jakelu 2025-05-23 Liikenne- ja viestintävaliokunta, Eduskunta