Turvallisuus- ja kemikaalivirasto

Lausunto

28.11.2023 10638/00.00.01/2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

-

Soveltamisalaa koskevat huomiot

-

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Tiedonhallintalain muutosten toimeenpano merkitsee, että viranomaiset panostavat aikaisempaakin enemmän systemaattiseen riskienhallintaan ja johdon riskienhallintaosaamiseen sekä ylläpitävät kyberturvallisuuden riskienhallinnan toimintamallia. Esityksessä todetaan (s. 90), että uusista säännöksistä ei aiheutuisi viranomaisille ja tiedonhallintayksiköille sellaisia uusia velvoitteita ja vaatimuksia, jotka lisäisivät niiden työtä olennaisesti siitä, mihin jo voimassa oleva tiedonhallintalain

sääntely velvoittaa. On kuitenkin huomattava, että tiedonhallintalain voimaan saattaminen on toteutettu ilman tiedonhallintayksiköille osoitettuja lisäresursseja. Toimintaympäristön turvallisuusuhkien lisääntyessä tiedonhallintayksiköt käytännössä suuntaavat yhä enemmän resursseja tieto- ja kyberturvariskien hallintaan ja joutuvat priorisoimaan resurssiensa käyttöä niin, että riittävä kyberturvallisuuden taso voidaan saavuttaa.

Julkisen hallinnon edellytyksiä suoriutua uusista tehtävistä voitaisiin parantaa ja tehostaa esimerkiksi yhteisillä asiantuntijaresursseilla sekä järjestämällä säädöksen toimeenpanoa tukevaa koulutusta koordinoidusti julkisten organisaatioiden johdolle ja asiantuntijoille. Hallituksen esitystä olisi suositeltavaa täydentää yhteisten resurssien ja osaamisen koordinoinnin näkökulmasta.

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Yleistä

Tukes tukee esitettyä lakiehdotusta ja pitää sitä yleisesti ottaen hyvin laadittuna. Tukes pitää tärkeänä kyberturvallisuuteen liittyvien riskien järjestelmällistä tunnistamista ja niihin varautumista. Kyberturvallisuusriskien hallinnan merkitys korostuu samalla, kun halutaan vauhdittaa julkisen sektorin ja elinkeinoelämän digitalisoitumista. Kyberturvallisuusriskien ennakoinnin ja varautumisen tärkeys on entisestään korostunut nykyisessä turvallisuustilanteessa.

Kohta 4.4 Vaikutukset viranomaisten toimintaan: Vaikutukset Tukesin toimintaan ja resursseihin

Lakiehdotuksen vaikutuksia ja laajuutta yrityskenttään ei valmisteluvaiheessa ole kaikilta osin pystytty tunnistamaan tai arvioimaan. Arviointiin liittyvät epävarmuudet on otettu huomioon Tukesille esitettyjen resurssien arvioinnissa.

Hallituksen esitysluonnoksen lähtökohtana on, että Tukes valmistelisi ja käynnistäisi sille suunnitellut tehtävät 5 henkilötyövuoden resurssilla. Käynnistämisvaiheessa tarkentuisivat lain soveltamisalueeseen kuuluvat yritykset ja luotaisiin toimintamallit valvonnan toteuttamiseksi. Esityksessä todetaan, että määrärahaa arvioidaan uudelleen vuonna 2026, kun kokemusta toimijakentän laajuudesta ja valvontakentän haastavuudesta on karttunut. Lähtökohtana on, että

Tukesin valvonta osoittautuu arvioitua laajemmaksi ja resurssitarpeet tulisivat kasvamaan. Lisäresurssitarpeet arvioitaisiin viimeistään kolmen vuoden kuluttua lain toimeenpanosta.

Esityksessä arvioidaan Tukesin tietojärjestelmäinvestointeihin tarvittavaksi resurssiksi 200 000 € kertamenona vuodelle 2024 ja sen jälkeen vuosittain 60 000 euroa. Järjestelmäkehitykseen liittyvien tiedonhallintavaatimusten vuoksi Tukes tarkentaa resurssiarviotaan (s. 83 ja 87) siten, että käynnistämisvaiheessa tarvittavan henkilöresurssin määräksi arvioidaan 6 henkilötyövuotta ja 540 000 euroa henkilöstökuluihin, TAE-lisäys yhteensä 740 000 euroa vuonna 2024 ja 600 000 euroa vuodesta 2025 lähtien. Resurssitarvetta tarkasteltaisiin uudelleen vuonna 2026, kuten esityksessä on todettu.

Tukesilla ei ole aiempia kyberturvallisuuteen liittyviä tehtäviä, resursseja eikä tarvittavaa asiantuntemusta. Tukesille esitetyt resurssit ovat välttämättömiä, jotta virasto voi hankkia ja kehittää kyberturvallisuusvalvonnassa tarvittavaa osaamista.

Kyberturvallisuuteen liittyvää osaamista tullaan tarvitsemaan sekä elinkeinoelämässä että julkisella sektorilla. Kyberturvallisuuteen liittyvän teknisen ja juridisen osaamisen rekrytointi voi olla vaikeaa. Rekrytointien lisäksi virastossa tulisi varautua myös henkilöstön uudelleen kouluttamiseen kyberturvallisuuteen liittyvissä asioissa.

Organisointi

Lakiesityksessä kyberturvallisuuteen liittyviä tehtäviä jaetaan usealle eri viranomaiselle. Tukes esittää lakiesitystä täydennettäväksi siten, että nimettäisiin yksi viranomainen yhtenäistämään ja koordinoimaan eri viranomaisissa tehtävää valvontaa.

Tietojärjestelmäkehitykseen liittyvä yhteistyö

Esityksessä arvioidaan, että uusien valvontatehtävien hoitamisesta aiheutuu tietojärjestelmäkehityksestä kustannuksia lähes kaikille valvoville viranomaisille. Tukes esittää, että selvitettäisiin mahdollisuuksia laajentaa olemassa olevia NIS1-direktiivin täytäntöönpanoon liittyviä järjestelmiä valvovien viranomaisten yhteiseen käyttöön tai perustaa uusi yhteinen ratkaisu toimijaluetteloiden ylläpitoon ja poikkeamailmoitusten vastaanottamiseen ja käsittelyyn. Vastaavasti kyberturvallisuuden riskienhallinnasta annettavaan lakiin olisi tarpeen lisätä säännökset viranomaisten tietojärjestelmäyhteistyön mahdollistamiseksi.

Kemikaalin määritelmä ja toiminnanharjoittajiin kohdistuvat velvoitteet

Tukes esittää, että lakiesityksessä täsmennettäisiin kemikaalien määritelmää. Lakiesityksen liitteen II kohdassa 6, samoin kuin NIS2-direktiivin liitteen II kohdassa 3 viitataan ainoastaan REACH-asetuksen 3 artiklassa oleviin määritelmiin, joissa todetaan, että kemikaali on aine tai seos. Lakiesitys tarkoittaisi sitä, että riippumatta kemikaalin ominaisuuksista tai ”merkityksestä elinkeinoelämälle ”, niiden valmistusta tai jakelua harjoittava yritys kuuluisi sääntelyn piiriin, jos kokorajoitukset (50 henkeä ja 10 milj. liikevaihto) ylittyvät. Jos kaikki lukuisat kemikaalit lasketaan mukaan, niin on hyvin epäselvää, paljonko toimijoita tällöin tulisi sääntelyn piiriin. Lisäksi kaikki toimijat eivät todennäköisesti edes tunnistaisi valmistavansa kemikaalia.

Muut huomiot ja avoin palaute esityksestä

-

Levä Kirsi
Turvallisuus- ja kemikaalivirasto

Hautamäki Maiju
Turvallisuus- ja kemikaalivirasto