Minna Rintala

Lausunto

29.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Yrityksen digitalous -hanke (myöhemmin YD-hanke) näkee EU:n NIS2-direktiivin tavoitteet ja tarkoituksen erittäin tarpeellisina. Tietoturvaa ja riskienhallintaa koskevan sääntelyn ulottaminen aiempaa laajemmin digitaalisten palveluiden tarjoajiin ja datan välittäjiin mahdollistaa YD-hankkeen digitaalisen talouden ekosysteemin kriittisten toimijoiden tietoturvan ja riskienhallinnan minimitason varmistamisen sekä siten tukee syntyvän ekosysteemin luotettavuutta. Direktiivin jalkauttaminen kansalliseen lainsäädäntöön myös vähentää potentiaalisten häiriöiden vaikutuksia digitaalisen talouden verkostoissa.

Yrityksen digitalouden luonteeltaan kehittyvän ja muuttuvan digitaalisen ekosysteemin kannalta lakiesitykseen sisällytetty mahdollisuus ulottaa lain velvoitteet tarvittaessa kaikkiin kriittisiksi tunnistettuihin toimijoihin valtioneuvoston asetuksella on tarpeellinen. Uusien teknologioiden kehittyminen ja niiden käyttöönotto synnyttävät uudenlaista liiketoimintaa, muokkaavat ekosysteemejä sekä tuovat niiden osaksi uusia toimijoita. Koska kehitystä on haasteellista ennakoida, varmistetaan tällä mahdollisuudella kyky reagoida muutoksiin ja ylläpitää kyberturvallisuuden korkeaa tasoa.

Lakiesityksessä tulee huomioida EU:n tulevan eIDAS2-asetuksen vaikutukset sähköisiin luottamuspalveluihin, erityisesti digitaalisten lompakkopalveluiden tarjoajien osalta, joista osa voi olla yksityisten toimijoiden omistamia ja kooltaan pieniä yrityksiä.

Soveltamisalaa koskevat huomiot

NIS2-direktiivissä ja hallituksen esityksessä laista kyberturvallisuuden riskienhallinnasta velvoitteet laajennetaan koskemaan kattavasti digitaalisten palveluiden tarjoajia siten, että käytännössä kaikki

suuret ja keskisuuret toimijat sisältyvät velvoitteiden piiriin. Digitaalisten palveluiden osalta soveltamisalan löyhä määrittely aiheuttaa ongelman liiallisen tulkinnanvaran suhteen, jota tulisi selkeyttää esimerkeillä etenkin, kun lakiesityksessä mainitaan yrityksen velvoite tunnistaa itse olevansa lain velvoitteiden piirissä ja ilmoittautua.

Myös hallituksen esityksessä oleva toimijoiden kriittisyyden nykyinen määrittelytapa on epätarkka, ja määrittelytapaa tulisi jatkovalmistelussa tarkastella edelleen ja tarvittaessa täydentää. Määrittelyssä ei tunnisteta esimerkiksi vaikutuksia, jotka aiheutuvat häiriötilanteessa koskien toimijan käsittelemiä arkaluontoisia, liiketaloudellisesti merkittäviä tai kriittisiä tietoja eikä toimijan myöntämiä varmenteita.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintavelvoite on kattava ja huomioi laajasti turvallisuuden eri osa-alueet mukaillen yleisten standardien sisältämiä kokonaisuuksia. Näemme myös erinomaisena asiana valvovan viranomaisen mahdollisuuden tarkentaa teknisiä vaatimuksia.

Raportointivelvoitetta koskevat huomiot

Ei lausuttavaa.

Valvontaa koskevat huomiot

Valvonta on jaoteltu loogisesti soveltamisalueittain. Valvonnassa on huomioitava realistinen resursointi suhteessa käytännön toimenpiteisiin, niin valvontaan kuin toimijoiden neuvontaakin, etenkin alkuvaiheessa.

Seuraamusmaksua koskevat huomiot

Ei lausuttavaa.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei lausuttavaa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei lausuttavaa.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Tällä hetkellä HE-luonnoksesta ei käy selvästi ilmi, että onko NIS2-direktiivin kansallisella implementaatiolla vaikutuksia verkkolaskujen ja muiden sanomien (sähköiset tilaukset, katalogit,

lähetysilmoitukset jne.) välittäjiin. Sanomavälitys on kansainvälistä, esimerkkeinä Peppol-verkosto, EESPA ja eFTI-verkosto. Jos suomalainen lainsäädäntö tai sen tulkinta on tiukempi kuin muiden maiden lainsäädäntö, niin on mahdollista, että lainsäädännöllä ei saavuteta aukottomasti haluttua hyötyä, koska verkoston muilla toimijoilla ei ole samanlaisia kriteeristöjä toiminnalleen. On myös mahdollista, että tällöin suomalaiset palveluntarjoajat asetetaan kilpailullisesti epäedulliseen asemaan. Tästä syystä soveltamisalan tulkinnassa tulisi huomioida vaikutusten arviointi.

Vaikutusten arvioinnissa tulisi huomioida:

- Mitä vaikutuksia NIS 2 -direktiivin soveltamisella on sanomavälitykseen ja sanomavälittäjiin?

- Mitä vaikutuksia soveltamattomuudella em. toimijoihin olisi?

- Mitä vaikutuksia loppukäyttäjille seuraa?

Nousevatko sanomavälityksen hinnat?

Onko vaikutusta pienten yritysten digitalisoitumiseen?

Vaikuttavuusarviointi on tärkeää huomioida koko yrityksen digitalouden ekosysteemin verkostojen toimijoiden näkökulmasta, jossa on sanomanvälittäjien lisäksi kysymys myös esimerkiksi verkkolaskuoperaattoreista ja muiden luottamuspalveluiden kuin digitaalisten lompakoiden tarjoajista. Vaikutusarvioinnissa tulee huomioida kriittisiä tehtäviä toteuttaville toimijoille aiheutuvat kustannukset ja hallinnollinen kuorma.

Muut huomiot ja avoin palaute esityksestä

Koska hallituksen esityksessä on mainittu toimijan velvollisuudesta tunnistaa itse olevansa lain velvoitteiden kohteena, tulee tiedottaminen yrityksen digitalouden verkostojen jäsenille koordinoida digitaalisia palveluita valvovan LVM:n ja yrityksen digitalouden ekosysteemin osien vastuuviranomaisten välillä, esimerkiksi Valtiokonttorin Peppol-viranomaisen. Tiedottaminen ja sen yhteensovittaminen eri toimijoiden välillä vaativat riittävien resurssien varmistamista.

Rintala Minna
Minna Rintala, Yrityksen digitalous -hankkeen hankejohtaja; Janne Kastepohja, Yrityksen digitalous -hankkeen turvallisuus- ja riskienhallintatiimin johtaja; Yrityksen digitalous -hankkeen turvallisuus- ja riskienhallintatiimin jäsenet