Suomen Taloushallintoliitto ry

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

Suomen Taloushallintoliitto ry. edustaa suomalaisia taloushallintoalan palveluyrityksiä. Yhdistyksen jäseninä on sekä yrityskentän että julkisen hallinnon palveluntuottajia. Tietoturvan merkitys yhteiskunnassa ja taloushallintopalveluissa kasvaa ja säätelyllä on mahdollistaa yhdenmukaistaa ja kehittää tietoturvaa ja tietosuojaa tukevia toimintamalleja. Pidämme direktiivin ja kansallisen lainsäädäntöhankkeen tavoitteita ja sisältöä kannatettavana huomioiden jäljempänä esittämämme varaumat ja selvennyspyynnöt.

Taloushallintopalvelujen tuottaminen nojaa nykyään melkein täysin pilvipalveluihin ja niiden perustana oleviin datakeskuspalveluihin. Käytännössä taloushallintopalvelujen tuottajilla ja niiden asiakasorganisaatioilla ei ole vaikutusmahdollisuuksia siihen, miten pilvipalvelujen tuottajat toteuttavat riskienhallinnan toimenpiteet eivätkä ne myöskään voi yleensä vaikuttaa siihen, miten nämä raportoivat poikkeamista. Uskomme, että direktiivin ja lainsäädännön säätely parantaa tietoturvan tasoa sekä taloushallintopalvelujen tuottajien ja niiden asiakkaiden oikeusturvaa.

Soveltamisalaa koskevat huomiot

Tässä esitetyt näkemyksemme arvoketjun ja sen eri toimijoiden roolin huomioimisesta liittyvät toimialoihin pilvipalvelut ja datakeskuspalvelut. Vastaavia tulkintatilanteita löytyy todennäköisesti myös muiltakin toimialoilta.

TULKINTA ONKO YRITYS TOIMIALALLA JA SITEN LAINSÄÄDÄNNÖN PIIRISSÄ

Suuri joukko suomalaisia ja kansainvälisiä ohjelmistoyrityksiä kehittää Suomessa ja EU-alueella pilvipalveluna myytäviä ohjelmistoja, joita kyseiset yritykset ylläpitävät joko omissa datakeskuksissaan tai datakeskuspalvelujen tarjoajien datakeskuksissa. Näiden yritysten osalta toimiala pilvipalvelut on ilmeinen. Lukuisa joukko muita yrityksiä, esimerkiksi taloushallintopalvelun tarjoajia osallistuu näiden pilvipalvelujen myymiseen ja/tai palvelutuotantoon eri rooleissa ja erilaisilla toimintamalleilla. Alla esimerkkejä:

- yritys myy edelleen pilvipalvelujen tuottajan pilvipalvelua osallistumatta muuten palvelujen tuottamiseen

- yritys myy edelleen pilvipalveluja ja osallistuu palvelujen tuottamiseen hoitamalla rajallista roolia. Se hoitaa esimerkiksi loppukäyttäjien hallintaa pilvipalvelun tuottajan ohjeistuksen mukaisesti.

- yritys myy edelleen pilvipalveluja ja osallistuu palvelujen tuottamiseen hoitamalla laajempaa roolia. Se hoitaa esimerkiksi loppukäyttäjien hallintaa pilvipalvelun tuottajan ohjeistuksen mukaisesti, pilvipalvelun neuvontaa sekä pilvipalveluohjelmiston pääkäyttäjätehtäviä omien asiakkaidensa osalta.

- yritys ei itse myy pilvipalveluja vaan pilvipalvelujen tuottaja myy ne suoraan asiakkaille. Yritys kuitenkin hoitaa esimerkiksi pilvipalvelun käyttäjähallintaa, neuvontaa sekä pääkäyttäjätoimia omille asiakkailleen.

Yritysten oikeusturva huomioiden esimerkiksi seuraamusmaksut ja johdon vastuu edellyttää, että yritykselle on mahdollisuus saada selkeä viranomaisohjeistus siitä, onko yritys toimialan piirissä. Ohjeistus tulisi antaa esimerkiksi lakia alemman tasoisella säätelyllä. Lisäksi jokaisella yrityksellä tulisi olla mahdollisuus saada itseään koskeva viranomaistulkinta siitä, onko se toimialan osalta lainsäädännön piirissä.

Näkemyksemme on, että jos esimerkiksi pilvipalvelujen arvoketjussa tietyn yrityksen rooli ei ole kokonaisuuden ja riskinhallinnan osalta olennainen, sen ei tulisi katsoa olevan toimialan piirissä. Näin esimerkiksi tilanteessa, jossa yritys myy edelleen pilvipalvelun tuottajan palvelua ja se hoitaa palvelun tuottamisessa vain rajattua tehtävänkuvaa, esimerkiksi käyttäjien hallintaa pilvipalvelun tuottajan ohjeistuksen mukaisesti. Tämä yritys ei muilta osin voi vaikuttaa riskihallintavelvoitteen toteutumiseen pilvipalvelun tuottajan osalta eikä käytännössä edes yksityiskohtaisesti tiedä, miten tämä velvoitteet toteuttaa.

KONSERNIN TAI TOSIASIALLISEN MÄÄRÄYSVALLAN HUOMIOIMINEN KOKORAJOISSA

Ymmärryksemme mukaan yritysten kokorajojen määrittely perustuu yhtiökohtaiseen käsittelyyn. Jos kuitenkin tietyissä tilanteissa tulee tai voi tulla sovellettavaksi konserniin tai tosiasialliseen määräysvaltaan perustuva käsittely, asia tulisi ohjeistaa selkeästi lainsäädännössä.

Riskienhallintavelvoitetta koskevat huomiot

Kunkin arvoketjussa toimivan yrityksen tulee omalta osaltaan toteuttaa relevantit riskienhallinnan toimenpiteet. Osa säädösluonnoksen 9§ ” Kyberturvallisuuden riskienhallinnan toimenpiteet” toimenpiteistä ei kuitenkaan ole relevantteja kaikille arvoketjun yrityksille.

Lainsäädännön tulisi mahdollistaa toimintamalli, jossa arvoketjun yritykset voivat toteuttaa yhdessä 9§ toimenpiteet, jolloin myös vastuukysymykset koskisivat vain kustakin toimenpiteestä vastaavaa yritystä. Mielestämme ei ole kohtuullista, että lainsäädännön kautta arvoketjussa toimivat yritykset joutuisivat tosiasiallisesti yhteisvastuuseen ja joutuisivat vastaamaan myös sellaisista toimista, joihin niillä ei ole tosiasiallista mahdollisuutta vaikuttaa.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoitteen toteuttamisessa tulisi huomioida myös arvoketjussa toimivien yritysten rooli, tiedonsaanti ja vastuu. Kukin yritys voi olla vastuussa poikkeamien raportoinnista vain siltä osin kuin se on saanut tai sillä on ollut tosiasiallinen mahdollisuus saada tieto poikkeamasta.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

Mielestämme lain yhdenmukainen soveltaminen edellyttää tarkentavia toimialakohtaisia keskusteluja arvoketjun yritysten ja ohjeistavien/valvovien viranomaisten kesken. Näiden keskustelujen pohjalta tulisi laatia esimerkiksi toimialojen yritysten yhteisiä toimintamalleja ja suosituksia, joissa olisi huomioitu viranomaisen näkemykset ja vaatimukset. Esimerkiksi Traficom voisi järjestää soveltamista käsitteleviä työpajoja toimialan ”digitaalinen infrastruktuuri” yrityksille.

Fredman Janne
Suomen Taloushallintoliitto ry