

10.9.2024

Eduskunta
Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Asia: HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuudirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Päivittäistavarakauppa ry:ltä (PTY) kirjallista asiantuntijalausuntoa otsikkoasiassa.
PTY kiittää ja lausuu asiassa seuraavaa:

Direktiivin tavoitteet ovat hyviä ja tukevat kansallista huoltovarmuutta parantamalla toimialojen kyberturvallisuutta ja jatkuvuudenhallintaa organisaatiokohtaisesti sekä osana laajempaa verkostoa. Sen asettamat vaatimukset ovat kuitenkin joiltain osin tulkinnanvaraisia. Vaatimuksia olisi näiltä osin syytä tarkentaa, jotta yritykset voivat paremmin tunnistaa niihin kohdistuvat vaatimukset.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallintavelvoitteen mukaan riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Velvoitteessa tulisi ottaa huomioon myös jäännösriskit sekä riskin siirtäminen ja pitäminen.

Se, mille toimijoille oikeushenkilön sisällä henkilökohtainen vastuu kohdentuu, tulee olla täsmällinen. Yhtiöoikeudellinen vastuu koskee osakeyhtiön toimitelimiä eli hallitusta, mahdollista hallintoneuvostoa ja toimitusjohtajaa. Yhtiöoikeudellisesti hallitus (tai hallintoneuvosto) nimittää toimitusjohtajan ja valvoo hänen toimintaansa.

Raportointivelvoitetta koskevat huomiot

Poikkeamatilanteessa toimija on hyvin työllistetty ja erilaiset raportoinnit nähdään helposti lisätyönä. Valvovan viranomaisen tulisi järjestää raportointi mahdollisimman suoraviivaiseksi ja automatisoiduksi, jotta siitä ei koituisi toimijalle kohtuutonta työmäärää poikkeamatilanteessa, jossa resurssit kuitenkin kohdennetaan poikkeaman tai häiriön selvittämiseen, korjaamiseen ja ratkaisemiseen.

Luonnoksen mukaan poikkeamailmoitus tulee tehdä vakavasta toimintahäiriöstä. Vakavan toimintahäiriön määritelmää olisi hyvä tarkentaa. Nyt sen määrittely jätetään toimijan vastuulle.

Luonnoksen 14 §:n mukaan toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa. Merkittävällä kyberuhkalla tarkoitettaisiin lakiesityksen 2 §:ssä määriteltyä kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti toimijan viestintäverkkoihin ja tietojärjestelmiin tai

10.9.2024

toimijan palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Tämänkin määrittely jää käytännössä toimijan vastuulle.

Viranomaisten resurssit tulee turvata

Osalle valvovista viranomaisista kybersäädöksen valvontavastuut poikkeavat merkittävästi sen muusta osaamisalasta. On kiinnitettävä erityistä huomioita osaamiseen ja varmistettava riittävät resurssit.

Valvovilla viranomaisilla olisi velvollisuus vastata poikkeaman raportoineelle yritykselle ja tukea sitä ongelman selvittämisessä, luonnoksen mukaan niiden tulisi vastata poikkeamailmoituksen tehneelle taholle "viivytyksettä ja mahdollisuuksien mukaan 24 tunnin kuluessa, mutta kuitenkin virka-aikojen puitteissa". Samalla kuitenkin soveltamisalan yrityksiltä edellyttäisiin käytännössä välitöntä raportointikyvykkyyttä riippumatta poikkeaman havaintohetkestä. Tämä ei ole kohtuullista. Jos lainsäädännöllä luodaan vaatimuksia sekä yrityksille että niitä valvoville viranomaisille, on huolehdittava siitä, että viranomaiset myös kykenevät vasteen antamaan silloin, kun sitä tarvitaan.

Liikenne- ja viestintäviraston nykyinen valtionhallinnolle ja huoltovarmuuskriittisille toimijoille tarkoitettu 24/7- päivystys tulee säilyttää ja myös toimialakohtaisilla valvovilla viranomaisilla tulisi olla velvollisuus päivystyksen järjestämiseen.

Seuraamusmaksun määrittäminen

Esityksen 35 §:ssä säädetään hallinnollisesta seuraamusmaksusta. Pykälän 1 momentissa määriteltäisiin teot, joista hallinnollinen seuraamusmaksu voitaisiin määrätä toimijalle. Seuraamusmaksu voitaisiin määrätä riskienhallintavelvoitteen laiminlyönnistä, riskienhallintatoimenpiteiden toteuttamisen laiminlyönnistä, velvoittavien poikkeamailmoitusten ja -raporttien tekemisen laiminlyönnistä tai toimijaluetteloon ilmoittautumisen laiminlyönnistä.

Hallinnollisen seuraamusmaksun määrä perustuisi kokonaisarviointiin. Seuraamusmaksu on huomattavan suuri, minkä vuoksi on kiinnitettävä huomiota moitittavien tekojen perusteluihin ja täsmälliseen yksilöintiin. Toimijan oikeussuojan kannalta on keskeistä, että toimija noudattaessaan lainsäädäntöä ja viranomaismääräyksiä, pysyy luottamaan toiminnan laillisuuteen ja pysyvyyteen.

Lakiesityksen mukaan seuraamusmaksun määrittämisessä huomioitavat seikat vastaisivat NIS2-direktiivin 32 artiklan 7 kohdassa säädettyjä seikkoja, jotka sen 34 artiklan 3 kohta edellyttää vähintään otettavan huomioon seuraamusmaksua määrättäessä. Tekoja ei ole perusteltu lausuttavana olevassa toimeenpanolaissa.

Lopuksi

NIS2-direktiivi on tärkeä ja yhdessä CER-direktiivin kanssa kyseessä ovat tärkeimmät laajaa elinkeinoelämän kriittisen yritysjoukon riskienhallintaa ja turvallisuutta koskevat lainsäädäntökokonaisuudet.

On erittäin tärkeää, että ne implementoidaan Suomen lainsäädäntöön huomioiden kansalliset erityispiirteet, kuten, että huoltovarmuutemme on vuosikymmeniä

10.9.2024

perustunut siihen osallistuvien yritysten kannalta ennen kaikkea osapuolten keskinäiseen luottamukseen sekä omaehtoiseen, sitoutuneeseen ja sopimusperusteiseen kehittämiseen, eikä velvoittavaan regulaatioon.

Kunnioittavasti

Päivittäistavarakauppa ry

Merja Söderström
Asiantuntija, VT

merja.soderstrom@pty.fi
050 5600350

www.pty.fi