NIS2-direktiivi, haasteista yrityksen voimavaraksi

Tammikuussa 2023 voimaan tulleen kyberturvallisuusdirektiivin eli NIS2-direktiivin tavoitteena on parantaa tietoturvallisuutta koko EU:n alueella. NIS2-direktiivi korvaa aikaisemman verkko- ja tietoturvadirektiivin (NIS1) ja määrittää soveltamisalaan kuuluville organisaatioille yhtenäiset kyberturvallisuusriskien hallintatoimenpiteet, raportointivelvoitteet sekä valvontatoimenpiteet.

Siirtymisajan puitteissa jokaisen EU:n jäsenmaan tulee sisällyttää NIS2-direktiivin säännökset kansalliseen lainsäädäntöön lokakuuhun 2024 mennessä. Suomessa direktiivin velvoitteet tulevat osaksi uutta lakia kyberturvallisuuden riskienhallinnasta. Lakiin tullaan keskittämään yhteiskunnan toiminnan kannalta kriittisiin toimijoihin kohdistuvat kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet.

Kriittisiin toimialoihin kuuluvat liikenne (satamat, rautatiet, lentoliikenne ja maantiekuljetukset), energia (sähköntuotanto, jakelu ja varastointi), pankit ja muut rahoituspalvelut, kriittiset palveluntarjoajat (terveydenhuolto, vesihuolto, elintarviketeollisuus), teleoperaattorit sekä julkishallinto (ministeriöt, kunnat ja muut julkiset organisaatiot). Lisäksi yritykset, joissa on yli 250 työntekijää, tai joiden liikevaihto ylittää 10 miljoonaa euroa kuuluvat tulevan lainsäädännön piiriin.

NIS2-direktiivissä edellytetään, että yritykset investoivat enemmän kyberturvallisuuteen, noudattavat uusia sääntöjä, standardeja ja velvoitteita, kuten poikkeamista ilmoittamista, riskinarviointien tekemistä, turvatoimien toteuttamista ja yhteistyötä kansallisten viranomaisten kanssa.

Yritysten tulisi tunnistaa NIS2-direktiivin mukainen rooli ja velvollisuudet sekä arvioida yrityksen kyberturvallisuuden nykyinen taso sekä tunnistaa mahdolliset aukot ja heikkoudet. Näiden tunnistamisen jälkeen yritysten tulisi ottaa käyttöön asianmukaiset turvatoimet ja käytännöt järjestelmien ja tietojen suojaamiseksi erilaisilta kyberuhilta sekä varmistaa, että turvatoimet ovat oikeassa suhteessa yrityksen kohtaamaan riskitasoon nähden. Kaikki tämä vaatii yrityksiltä riskiperusteisen lähestymistavan omaksumista.

NIS2-direktiivin raportointivelvoite vaatii yrityksiä raportoimaan huomattavista tai merkittävistä tietoturvapoikkeamista kansallisille viranomaisille ja Euroopan unionin verkko- ja tietoturvavirasto ENISAlle.

Edelleen NIS2-direktiivi vaatii yrityksiä tekemään yhteistyötä kansallisten viranomaisten ja muiden sidosryhmien kanssa. Yritysten tulee tulevaisuudessa osallistua kansallisten viranomaisten säännöllisiin auditointeihin ja tarkastuksiin sekä jaettava tietoja ja parhaita käytäntöjä muiden alan toimijoiden kanssa tai eri alojen kesken.

Yrityksen täyttäessä NIS2-direktiivin vaatimukset, yrityksen luotettavuus paranee, eli sillä on vaikutus yrityksen maineeseen, liiketoimintaan ja kilpailukykyyn, NIS2:n noudattaminen voi myös tuoda etuja, kuten

parempaa resilienssiä, innovaatioita ja markkinamahdollisuuksia. NIS2-direktiiviä ei kannata nähdä vain haasteena, vaan mahdollisuutena yrityksen johdolle osoittaa johtajuutensa ja sitoutumisensa kyberturvallisuuteen.

Ismo Turve

Kirjoittaja on kyberturvallisuus orientoitunut heinolalainen Tietojenkäsittelyn lehtori Hämeen ammattikorkeakoulusta.