EU:n kyberturvadirektiivi NIS-2-direktiivi osaksi Suomen lainsäädäntöä

Direktiivin esittely

Lokakuu 2023

Taloushallintoliitto
Janne Fredman
Johtava asiantuntija
janne.fredman@taloushallintoliitto.fi

NIS-2-direktiivi lyhyesti

- **NIS2 eli verkko- ja tietoturvadirektiivi** on EU:n laajuinen kyberturvallisuutta koskeva lakikokonaisuus
- Tavoitteena on yhtenäistää ja parantaa EU:n kyberturvallisuuden yleistä tasoa.
- NIS2 korvaa aiemman NIS-direktiivin laajentaen sen soveltamisalaa ja vaatimuksia.
- Direktiivi velvoittaa:
  - Määrättyjen toimialojen yrityksiä (esimerkiksi pilvipalvelun tarjoajat)
  - jotka täyttävät EU:n keskikokoisen yrityksen määritelmän

NIS-2-direktiivin voimaanpanosta

- NIS-2 direktiivi tuli voimaan tammikuussa 2023
- Direktiivi määrittää soveltamisalaan kuuluville organisaatioille yhtenäiset kyberturvallisuusriskien hallintatoimenpiteet, raportointivelvoitteet sekä valvontatoimenpiteet.
- Jokaisen EU:n jäsenmaan tulee sisällyttää NIS2-direktiivin säännökset kansalliseen lainsäädäntöön **lokakuuhun 2024** mennessä.
  - Suomessa direktiivin velvoitteet tulevat osaksi uutta lakia kyberturvallisuuden riskienhallinnasta
- Aiheesta on annettu luonnos hallituksen esityksestä kommenttikierrokselle

Keitä koskee – pilvipalvelun tarjoajat

- HE-luonnos *"Pilvipalvelulla tarkoitettaisiin digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja."*
- *"Tietotekninen resurssi voisi tarkoittaa siten esimerkiksi verkkoja, palvelimia ja muuta tietoteknistä infrastruktuuria, käyttöjärjestelmiä, ohjelmistoja, tallennustilaa, sovelluksia ja palveluja. Tarveperusteisella ohjauksella tarkoitettaisiin pilvipalvelun käyttäjän kykyä käyttää yksipuolisesti ja oma-aloitteisesti tietojenkäsittelyvalmiuksia ilman pilvipalveluntarjoajan inhimillistä panosta. Laajalla etäkäytöllä tarkoitettaisiin sitä, että resursseja tarjotaan verkossa ja niitä pääsee käyttämään erilaisten päätelaitteiden käytön mahdollistavien järjestelyjen ansiosta. Skaa-lautuvuus viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja voi teknisesti jakaa joustavasti kysynnän vaihtelun mukaan resurssien maantieteellisestä sijainnista riippumatta. Joustavaa joukolla tarkoitetaan tietoteknisiä resursseja, joita tarjotaan ja vapautetaan käyttöön kysynnän mukaan niin, että resursseja voidaan nopeasti lisätä ja vähentää kuormituksen perus-teella. Jaettavissa olevalla kuvataan tietoteknisiä resursseja, joita tarjotaan useille käyttäjille, joilla on yhteinen pääsy palveluun, jossa prosessointi on kuitenkin käyttäjäkohtaista, vaikka palvelu tarjotaan saman sähköisen laitteiston kautta. Hajautetulla viitataan tietoteknisiin resurs-seihin, jotka sijaitsevat erillisissä verkotetuissa tietokoneissa tai laitteissa ja jotka viestivät ja koordinoivat toimintaansa keskenään rakenteisella viestinvaihdolla."*

Traficomin kommentteja pilvipalvelun määritelmästä ja soveltamisesta

- *"Käsityksemme on, että pilvipalvelun määritelmä ei ole olennaisesti muuttunut NIS1- ja NIS2-direktiivien välillä. Olennainen ero kuitenkin on, että NIS1-direktiivin puitteissa pilvipalvelun tarjoajilla ei ollut velvoitetta ilmoittautua valvovalle viranomaiselle eikä toimijoista siten koostettu virallista luetteloa sääntelyn ja valvonnan piiriin kuuluvista yrityksistä. Tämä tulee muuttumaan NIS2-toimeenpanon myötä.*
- *Pilvipalvelun tarjoajaa koskevan kysymyksen osalta voidaan sanoa, että **pilvipalvelua kehittävä ja tuottava ohjelmistoyritys** on selvästi sääntelyn piirissä, mikäli kyseessä ei ole pieni yritys.*
- ***Palvelua välittävän toimijan (esim. tässä tilitoimiston)** kohdalla kyse olisi ns. cloud broker tyyppisestä toiminnasta, jonka osalta NIS-sääntelyn soveltuminen ei ole automaattista, vaan riippuu toiminnan luonteesta. Jos tilitoimisto huolehtii kuvatun typpisesti käyttäjien hallinnasta ja tarjoaa esim. osana omaa palvelukokonaisuuttaan alustan, jonka kautta pilvipalveluun pääsee, NIS-sääntely soveltuu tällöin myös tilitoimistoon. Jos taasen tilitoimisto toimii vain pilvipalvelun jälleenmyyjänä, eikä varsinaisesti hallinnoi mitään pilvipalvelun käyttöön liittyviä palveluita, tällöin tilitoimisto ei lähtökohtaisesti kuuluisi NIS-sääntelyn piiriin."*

Kokorajat – keskisuuri tai sitä suurempi yritys

- Komission suosituksen 2003/361/EY kynnysarvojen mukainen keskisuuri yritys:
  - Palveluksessa on vähintään 50 työntekijää tai
  - vuosiliikevaihto **ja** taseen loppusumma ylittää 10 miljoonaa euroa.
- Keskisuuren rajat ylittävä yritys:
  - Palveluksessa on vähintään 250 työntekijää tai
  - vuosiliikevaihto ylittää 50 ja taseen loppusumma 43 miljoonaa euroa.

Direktiivin asettamat keskeiset velvoitteet

- Riskienhallinta
- Raportointi merkittävistä poikkeamista
- Toimijaluetteloon ilmoittautuminen

Riskinhallinta

Kyberturvallisuuden riskienhallinnan toimintamalli (8 §)

Kyberturvallisuuden riskienhallinnan toimenpiteet (9 §)

- Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään:
- 1) kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi;
- 2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;
- 3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;
- 4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
- 5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
- 6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;
- 7) pääsynhallinnan ja todentamisen menettelyt;
- 8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön;
- 9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;
- 10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö toimijan toiminnassa;
- 11) perustason kyberhygieniakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä
- 12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Raportointi merkittävistä poikkeamista

- Poikkeamailmoitukset viranomaiselle (11 §)
  - Ensi-ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta.
- Poikkeaman loppuraportti (13§)
  - Kuukauden kuluessa jatkoilmoituksen toimittamisesta tai pitkäkestoisen poikkeaman kohdalla kuukauden kuluessa sen käsittelyn päättymisestä.

    1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

    2) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi;

    3) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi; ja

    4) mahdolliset rajat ylittävät vaikutukset.
- Poikkeamasta ja kyberuhkasta ilmoittaminen muulle kuin viranomaiselle (14§)
  - Toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa toimijan palvelujen tarjoamista.

Toimijaluetteloon ilmoittautuminen ja viranomaisvalvonta

- Toimijan on ilmoittauduttava valvovalle viranomaiselle (pilvipalvelut, Traficom) toimijaluetteloon (43 §)
- Voimaan 1.1.2025
- Viranomainen voi kohdistaa keskeisiin toimijoihin ennakkovalvontaa (26§)
- Keskeisellä toimijalla tarkoitetaan mm. liitteessä I tarkoitettua toimijaa (pilvipalvelu), joka **ylittää** keskisuuren toimijan määritelmän (yli 250 henkeä tai liikevaihto 50 me **ja** tase yli 43 me)
- Valvovan viranomaisen toimivaltuuksia olisivat mm. tiedonsaantioikeus ja tietopyynnöt, tarkastus, turvallisuusauditoinnin teetättäminen, huomautus, varoitus ja korjaaviin toimiin velvoittaminen uhkasakon uhalla. Lisäksi viimesijainen toimivalta rajoittaa henkilön toimimista yrityksen johdossa.
- Pienemmillä yrityksille osa valvonta-aktiviteeteista (29–31 §) tehdään suoritetaan "vain, jos on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säädöksiä"

Vastuista ja sanktioista

- Seuraamusmaksut tietosuoja-asetuksesta tuttua suuruusluokkaa
- Johdon vastuusta 10§: Toimijan johto vastaa kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.
- Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa, toimitusjohtajaa, tai muussa niihin rinnastettavassa asemassa olevaa, sekä toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä, jotka ovat toimijan ylimpiä johtotehtäviä tai joissa tosiasiallisesti johdetaan sen toimintaa, toimivaa tahoa.
- NIS-2-direktiivi 20,1 artikla "Jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät näiden toimijoiden 21 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet ja valvovat mainitun artiklan täytäntöönpanoa ja että nämä hallintoelimet voidaan saattaa vastuuseen, jos toimijat rikkovat kyseistä artiklaa."

Janne Fredman
johtava asiantuntija
Taloushallintoliitto
janne.fredman@taloushallintoliitto.fi

talous
hallinto
liitto