FINIB
A Gallagher Company

NIS2-DIREKTIIVI

Mitä NIS2 tarkoittaa?

NIS2-direktiivi perustuu vuoden 2016 alkuperäiseen NIS1-direktiiviin, jonka tavoitteena on vahvistaa Euroopan kriittisen infrastruktuurin kyberturvallisuutta. Sen tarkoituksena on parantaa häiriönsietokykyä, vähentää kyberriskejä sekä vahvistaa yritysten ja kansallisten viranomaisten välistä yhteistyötä uhkiin vastaamisessa.

NIS2 tuo sääntelyn piiriin aiempaa suuremman joukon yrityksiä. Sen laajempi soveltamisala tarkoittaa, että yhä useammat organisaatiot hyötyvät tarkemmista kyberturvallisuusohjeistuksista, joiden avulla ne voivat ennaltaehkäistä kyberhyökkäyksiä ja samalla täyttää NIS2-direktiivin kansalliseen lainsäädäntöön sisällytettävät vaatimukset.

Yrityksille, jotka jo noudattavat NIS1-vaatimuksia, NIS2 tarjoaa mahdollisuuden kehittää kyberturvallisuuttaan entistä kattavammilla riskienhallinta- ja reagointimenettelyillä. Uusille toimialoille se puolestaan tarjoaa keinot vahvistaa resilienssiä digitaalisten uhkien lisääntyessä.

Olennaiset ja tärkeät toimijat: velvollisuuksien ymmärtäminen

NIS2 jakaa organisaatiot kahteen pääluokkaan: olennaisiin toimijoihin (Essential Entities) ja tärkeisiin toimijoihin (Important Entities). Oman luokituksen ymmärtäminen on keskeistä, sillä se määrittää organisaation vaatimukset, valvonnan toteutustavan ja mahdolliset seuraamukset.

• **Olennaiset toimijat:** Organisaatiot, jotka tarjoavat kriittisiä palveluja ja joiden toiminnan häiriintyminen voisi aiheuttaa merkittäviä yhteiskunnallisia tai taloudellisia vaikutuksia. Näitä ovat esimerkiksi energia-, pankki-, terveydenhuolto-, rahoitus- ja liikennesektorit sekä muut kriittiset toimialat. Näiltä toimijoilta edellytetään ennakoivia kyberturvallisuuden riskienhallintatoimenpiteitä, kuten poikkeamien raportointia ja palautumissuunnitelmia.

• **Tärkeät toimijat:** Tähän luokkaan kuuluvat yritykset ovat myös merkittäviä, mutta niiden toiminnan häiriöiden vaikutukset eivät yleensä ole yhtä laaja-alaisia. Näitä toimialoja ovat esimerkiksi valmistava teollisuus, tutkimus, elintarviketuotanto, jätehuolto ja postipalvelut. Näidenkin organisaatioiden on kuitenkin otettava käyttöön asianmukaiset kyberturvallisuuskäytännöt riskien vähentämiseksi ja liiketoiminnan jatkuvuuden turvaamiseksi.

On tärkeää huomata, että olennaisten ja tärkeiden toimijoiden velvoitteet ovat pääosin samat. Ero liittyy ennen kaikkea valvonnan toteuttamiseen sekä mahdollisiin seuraamuksiin.

FINIB
A Gallagher Company

NIS2:n keskeiset vaatimukset: mitä organisaation tulee tehdä?

NIS2:n piiriin kuuluvien eurooppalaisten organisaatioiden on otettava käyttöön tiettyjä kyberturvallisuuden käytäntöjä ja toimintamalleja. Keskeiset vaatimukset ovat seuraavat:

- **Tehostettu kyberturvallisuuden riskienhallinta:** Organisaation tulee ottaa käyttöön kattava kyberturvallisuuden riskienhallintakehys, johon sisältyvät muun muassa säännölliset haavoittuvuusarvioinnit sekä tietoturvatoimenpiteet, kuten salaus ja monivaiheinen tunnistautuminen.
- **Kyberpoikkeamien ilmoittaminen 24 tunnin kuluessa:** Kyberpoikkeamista on ilmoitettava toimivaltaisille viranomaisille 24 tunnin kuluessa. Merkittävistä tietoturvaloukkauksista, jotka vaikuttavat palvelujen saatavuuteen tai luottamuksellisuuteen, on toimitettava alustava ilmoitus 24 tunnin kuluessa, tarkennettu raportti 72 tunnin kuluessa sekä lopullinen raportti yhden kuukauden kuluessa.
- **Vahvempi toimitusketjun turvallisuus:** Yritysten on arvioitava kolmansien osapuolten toimittajiaan ja varmistettava, että nämä täyttävät NIS2-vaatimukset eivätkä vaaranna organisaation vaatimustenmukaisuutta.
- **Johdon vastuu:** Yritysjohdon on otettava vastuu kyberturvallisuusstrategioista ja -käytännöistä. Vakavissa tietoturvaloukkauksissa ylimmän johdon edustajat voidaan saattaa henkilökohtaiseen vastuuseen, mikä voi vaikuttaa myös johdon vastuuvakuutuksiin.

NIS2 vs. NIS1: mitä on muuttunut?

- Laajempi soveltamisala: NIS2 koskee aiempaa useampia toimialoja, erityisesti kriittisen infrastruktuurin piiriin kuuluvia organisaatioita. Seuraavat toimialat kuuluvat direktiivin soveltamisalaan joko palveluntarjoajina tai toimitusketjun osana (direktiivi kattaa myös muita toimialoja):
  - **Olennaiset toimijat**
    - Energia (sähkö, kaasu, öljy)
    - Liikenne (ilmailu, rautatie-, meri- ja maantieliikenne)
    - Terveydenhuolto (sairaalat, lääketeollisuus)
    - Digitaalinen infrastruktuuri (pilvipalvelut, datakeskukset ja internetin vaihtopisteet)
    - Julkishallinto
  - **Tärkeät toimijat**
    - Elintarvikehuolto
    - Postipalvelut
    - Valmistava teollisuus
    - Tutkimus
    - Jätehuolto
- **Tiukempi valvonta ja sanktiot:** Uusi direktiivi vahvistaa valvontaa ja tuo merkittäviä seuraamuksia vaatimusten laiminlyönnistä. Olennaisille toimijoille seuraamus voi olla enintään 10 miljoonaa euroa tai 2 % maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi on suurempi. Tärkeille toimijoille seuraamus voi olla enintään 7 miljoonaa euroa tai 1,4 % maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi on suurempi.

FINIB
A Gallagher Company

- **Tiiviimpi yhteistyö:** NIS2 edellyttää tiiviimpää yhteistyötä kansallisten viranomaisten kanssa. Tavoitteena on mahdollistaa nopeampi ja paremmin koordinoitu reagointi kyberuhkiin koko Euroopan unionin alueella.

Miten Gallagher voi auttaa?

Gallagherin kyberriskienhallintaan erikoistunut asiantuntijatiimi voi auttaa organisaatiotanne arvioimaan NIS2-velvoitteitanne, arvioimaan tietoturvan nykytilaa suhteessa viitekehykseen, tunnistamaan riskejä ja puutteita sekä tukemaan tarvittavien hallintatoimenpiteiden käyttöönotossa vaatimustenmukaisuuden saavuttamiseksi.

Riskienhallintatiimimme voi auttaa saavuttamaan seuraavat keskeiset tavoitteet:

- Riskien arviointi ja puuteanalyysi
- Riskien käsittelysuunnitelma ja toteutuksen tiekartta
- Tuki NIS2:n käyttöönotossa, sisältäen:
  - Kyberpoikkeamien hallinta ja liiketoiminnan jatkuvuussuunnittelu
  - Kyberturvallisuustietoisuuden koulutus
  - Tietoturvapolitiikat ja -menettelyt
  - Toimitusketjun riskienhallinta
  - Hallinto- ja raportointimenettelyt
- NIS2-sisäisen auditoinnin toteuttaminen
- Poikkeamien ja korjaavien toimenpiteiden määrittäminen

Ota yhteyttä asiantuntijoihimme

Aldo Borsani

Head of Financial Lines and Cyber Europe

Puhelin: +39 349 889 4284

Sähköposti: aldo_borsani@ajg.com

Tom Mooney

Global Head of Cyber Defence

Puhelin: +44 7752 470 418

Sähköposti: tom_mooney@ajg.com

Sources:

1"Article 3 — Essential and important entities," NIS2 Directive, accessed 15 Nov. 2024.

2"Chapter II — Coordinated Cybersecurity Frameworks," NIS2 Directive, accessed 15 Nov. 2024.

3"Article 23 — Reporting Obligations," NIS2 Directive, accessed 15 Nov. 2024.

4"Chapter VIII — Delegated and Implementing Acts," NIS2 Directive, accessed 15 Nov. 2024.

5"NIS2 Fines: Get an Overview of The Potential Penalties for NIS2 Non-Compliance," NIS2 Directive, accessed 15 Nov. 2024.

6"Chapter III — Cooperation at Union and International Level," NIS2 Directive, accessed 15 Nov. 2024

AJG.com/uk | The Gallagher Way. Since 1927.