Opas NIS2

NIS2 – EU:n verkko- ja tietoturvadirektiivi **Opas NIS2-vaatimusten täyttämiseen ja kyberresilienssin vahvistamiseen**

Sisällysluettelo

Tiivistelmä

Opas NIS2-vaatimusten täyttämiseen ja kyberresilienssin vahvistamiseen

NIS2-direktiivi nostaa kyberturvallisuuden vaatimustasoa koko Euroopan unionissa ja laajentaa lakisääteiset velvoitteet huomattavasti aiempaa useammalle organisaatiolle. Direktiivin piiriin kuuluvien olennaisten ja tärkeiden toimijoiden on täytettävä selkeät riskienhallintaa koskevat vaatimukset, noudatettava määräaikaisia tietoturvaloukkausten ilmoitusvelvollisuuksia sekä varmistettava johdon aktiivinen osallistuminen kyberturvallisuuden johtamiseen.

Useimmille organisaatioille NIS2-vaatimusten täyttäminen ei ole yksittäinen projekti, vaan jatkuva kehittämisprosessi. Se kattaa muun muassa hallintamallit, toimitusketjun hallinnan, tekniset suojaustoimenpiteet ja henkilöstön koulutuksen. Organisaatiot, jotka hyödyntävät NIS2-direktiiviä mahdollisuutena kehittää kokonaisvaltaista tietoturvaansa, voivat muuttaa lakisääteiset velvoitteet pitkäjänteiseksi kilpailueduksi ja paremmaksi kyberresilienssiksi.

Tässä oppaassa kerrotaan:
- ketkä kuuluvat NIS2-direktiivin soveltamisalaan
- mitä vaatimuksia direktiivi asettaa organisaatioille
- miten DEKRA suosittelee lähestymään vaatimusten täyttämistä käytännössä.

Johdanto:

Uusi aikakausi kyberturvallisuuden velvoitteissa

Uudistettu EU:n verkko- ja tietoturvadirektiivi (NIS2) on merkittävä askel eteenpäin Euroopan unionin kyberturvallisuusstrategiassa. Direktiivin tavoitteena on vahvistaa yhteiskunnan kannalta kriittisten toimialojen kyberresilienssiä vastauksena jatkuvasti lisääntyviin ja kehittyviin kyberuhkiin.

NIS2 kohdistuu yhteiskunnan, talouden ja julkisten palveluiden kannalta keskeisiin toimialoihin. Monet näistä ylläpitävät kriittistä infrastruktuuria, minkä vuoksi organisaatioiden on omaksuttava vahva kyberturvallisuuden toimintakulttuuri ja edistettävä hyvää kyberhygieniaa koko organisaatiossa.

Direktiivin piiriin kuuluvien organisaatioiden tulee muun muassa:
- ottaa käyttöön tehokkaat tietoturvapoikkeamien hallinta- ja ilmoitusmenettelyt
- vahvistaa kyberturvallisuuden riskienhallintaa
- huolehtia toimitusketjun turvallisuudesta
- ehkäistä sellaisten tuotteiden ja palveluiden käyttöä, jotka voivat aiheuttaa haavoittuvuuksia kriittisiin järjestelmiin.

Lisäksi direktiivi sisältää kattavan valvonta- ja seuraamusjärjestelmän. Merkittävät seuraamukset korostavat ennakoivan kyberturvallisuuden johtamisen merkitystä.

Tämä opas tarjoaa yleiskatsauksen NIS2-direktiivin keskeisiin periaatteisiin ja vaatimuksiin sekä esittelee strategisen lähestymistavan vaatimusten täyttämiseen, ylläpitämiseen ja osoittamiseen.

Laajennettu soveltamisala:

Ketkä kuuluvat NIS2-direktiivin piiriin?

Yksi NIS2-direktiivin keskeisistä tavoitteista on laajentaa sen soveltamisalaa. Aiempi jako välttämättömien palvelujen tarjoajiin ja digitaalisten palvelujen tarjoajiin poistuu, ja sen sijaan direktiivin soveltamisalaan kuuluvat organisaatiot jaetaan kahteen pääryhmään:

- **Olennaiset toimijat (Essential entities)**
  Yhteiskunnan ja talouden kannalta kriittisillä toimialoilla toimivat organisaatiot, kuten energia-ala, liikenne, pankki- ja rahoitusmarkkinainfrastruktuuri, terveydenhuolto, vesihuolto, digitaalinen infrastruktuuri ja avaruussektori.
- **Tärkeät toimijat (Important entities)**
  Muita yhteiskunnan toiminnan kannalta merkittäviä toimialoja, kuten posti- ja kuriiripalvelut, jätehuolto, teollisuus ja tavaroiden valmistus, kemianteollisuus, elintarvikkeiden tuotanto ja jakelu, tietyt tutkimus- ja digitaaliset toimialat.

Organisaation luokittelu perustuu toimialaan, yrityksen kokoon sekä lainsäädännössä määriteltyihin poikkeuksiin. Useimmiten direktiivi koskee keskisuuria ja suuria yrityksiä, joissa on vähintään 50 työntekijää tai joiden vuosiliikevaihto tai taseen loppusumma on vähintään 10 miljoonaa euroa.

Soveltamisala ei kuitenkaan määräydy yksinomaan näiden kokorajojen perusteella, vaan siihen vaikuttavat myös kansallisen lainsäädännön määritelmät ja mahdolliset poikkeukset.

Ratkaisevia ovat kunkin jäsenvaltion NIS2-direktiivin kansalliseen lainsäädäntöön sisällyttämät määritelmät sekä niihin liittyvät velvoitteet, kuten rekisteröitymis- ja ilmoitusvaatimukset toimivaltaisille viranomaisille.

NIS2-vaatimusten ydin

Keskeiset hallintatoimenpiteet

NIS2-direktiivi täsmentää organisaatioiden kyberturvallisuuden riskienhallintaa koskevia vaatimuksia. Direktiivin soveltamisalaan kuuluvien organisaatioiden on toteutettava riskeihin nähden tarkoituksenmukaiset ja oikeasuhtaiset tekniset sekä organisatoriset toimenpiteet.

Nämä perustuvat NIS2-direktiivin 21 artiklassa määriteltyihin vähimmäisvaatimuksiin, joihin kuuluvat erityisesti seuraavat osa-alueet

1. **Riskianalyysi ja tietojärjestelmien turvallisuus**
   Organisaatiolla tulee olla dokumentoidut toimintamallit riskien tunnistamiseen, arviointiin ja hallintaan.
2. **Tietoturvapoikkeamien hallinta**
   Käyttöön on otettava tehokkaat menettelyt poikkeamien havaitsemiseksi, käsittelemiseksi sekä toiminnan palauttamiseksi normaaliksi.
3. **Liiketoiminnan jatkuvuus ja kriisinhallinta**
   Organisaation on varmistettava toimintansa jatkuvuus esimerkiksi varmuuskopioinnilla, palautumissuunnitelmilla ja kriisinhallintamenettelyillä.
4. **Toimitusketjun kyberturvallisuus**
   Kyberturvallisuusriskit tulee huomioida sekä toimitusketjussa että yhteistyössä palveluntarjoajien kanssa.
5. **Haavoittuvuuksien hallinta**
   Organisaatiolla tulee olla prosessit järjestelmien haavoittuvuuksien tunnistamiseen, käsittelyyn ja tarvittaessa niiden vastuulliseen ilmoittamiseen.
6. **Kyberturvallisuustoimenpiteiden arviointi**
   Kyberturvallisuustoimenpiteiden toimivuutta on testattava ja arvioitava säännöllisesti.
7. **Kyberhygienia ja henkilöstön koulutus**
   Organisaation tulee edistää hyviä kyberturvallisuuskäytäntöjä sekä järjestää henkilöstölle säännöllistä kyberturvallisuuskoulutusta.
8. **Salaus ja kryptografiset ratkaisut**
   Tietojen suojaamisessa on käytettävä salausmenetelmiä ja muita kryptografisia ratkaisuja aina, kun se on tarpeellista.
9. **Henkilöstöturvallisuus**
   Organisaation tulee huolehtia muun muassa käyttöoikeuksien hallinnasta, turvallisesta omaisuuden hallinnasta ja henkilöstöön liittyvistä tietoturvakäytännöistä.
10. **Monivaiheinen tunnistautuminen (MFA) ja turvallinen viestintä**
    Tarvittaessa on otettava käyttöön monivaiheinen tunnistautuminen (MFA) sekä suojattava organisaation sisäinen viestintä asianmukaisilla tietoturvaratkaisuilla.

Ilmoitusvelvollisuudet ja johdon vastuu

NIS2-direktiivi asettaa organisaatioille selkeät ja tiukat velvollisuudet merkittävien tietoturvapoikkeamien ilmoittamiseen. Direktiivin soveltamisalaan kuuluvien olennaisten ja tärkeiden toimijoiden on ilmoitettava merkittävistä tietoturvapoikkeamista kansallisille toimivaltaisille viranomaisille. Ilmoitusprosessi etenee yleensä vaiheittain:

- 24 tunnin kuluessa poikkeaman havaitsemisesta on toimitettava ennakkovaroitus.
- 72 tunnin kuluessa on tehtävä varsinainen ilmoitus, joka sisältää alustavan arvion poikkeaman vakavuudesta ja vaikutuksista.
- Tarvittaessa organisaation on toimitettava myös väliraportteja tilanteen etenemisestä.
- Lopullinen raportti on yleensä toimitettava kuukauden kuluessa.*

Direktiivi korostaa johdon vastuuta kyberturvallisuuden johtamisessa. Organisaation ylimmän johdon (C-tason johto) tehtävänä ei ole ainoastaan hyväksyä kyberturvallisuuden riskienhallintatoimenpiteet, vaan myös aktiivisesti valvoa niiden käyttöönottoa ja tehokasta toteuttamista koko organisaatiossa.

Lisäksi johdon vastuulla on edistää vahvaa kyberturvallisuuskulttuuria varmistamalla, että henkilöstö saa riittävää kyberturvallisuustietoisuuteen liittyvää koulutusta.

Myös ylimmän johdon jäsenten tulee osallistua säännöllisesti kyberturvallisuuskoulutuksiin, jotta he pysyvät ajan tasalla kyberuhista ja voivat hoitaa tehokkaasti johtamiseen, hallintoon ja riskienhallintaan liittyvät vastuunsa. Mikäli johto ei huolehdi riittävästä ohjauksesta, hallintamalleista ja strategisesta johtamisesta direktiivin vaatimusten täyttämiseksi, sen jäsenet voivat joutua henkilökohtaiseen vastuuseen.

*Huomio: Tarkat ilmoitusajat voivat vaihdella jäsenvaltioittain.

Seuraamukset vaatimusten laiminlyönnistä

NIS2-direktiivin vaatimusten noudattamatta jättämisestä voi seurata huomattavia taloudellisia seuraamuksia. Direktiivi velvoittaa jäsenvaltiot säätämään seuraamuksista, joiden suuruus riippuu siitä, onko organisaatio luokiteltu olennaiseksi vai tärkeäksi toimijaksi sekä rikkomuksen laadusta.

Seuraamukset voivat olla enintään:

- olennaisille toimijoille: 10 miljoonaa euroa tai 2 % maailmanlaajuisesta vuotuisesta liikevaihdosta sen mukaan, kumpi on suurempi
- tärkeille toimijoille: 7 miljoonaa euroa tai 1,4 % maailmanlaajuisesta vuotuisesta liikevaihdosta sen mukaan, kumpi on suurempi.

Sakkojen lisäksi valvontaviranomaiset voivat määrätä myös muita korjaavia toimenpiteitä, kuten sitovia määräyksiä, tietoturva-auditointeja tai määräyksiä vaatimusten täyttämisestä.*

Direktiivin velvoitteiden laiminlyönti voi johtaa merkittäviin hallinnollisiin seuraamuksiin ja taloudellisiin sanktioihin sen jäsenvaltion kansallisen lainsäädännön mukaisesti, jossa NIS2-direktiivi on saatettu voimaan.

* Huomio: Sakkojen tarkka määrä ja valvontamenettelyt määritellään kunkin jäsenvaltion kansallisessa lainsäädännössä.

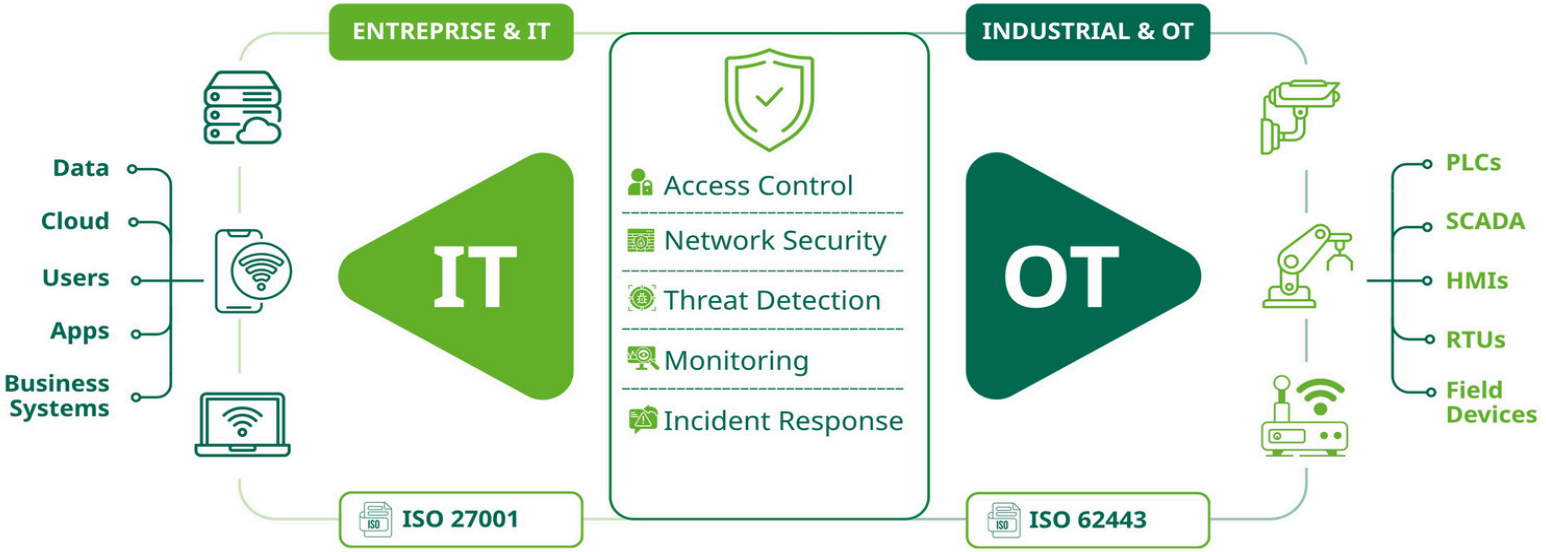
Tietotekniikka (IT) ja operatiivinen teknologia (OT)

Tietotekniikka (IT, Information Technology) keskittyy ensisijaisesti organisaatioiden toimisto- ja liiketoimintaympäristöissä käytettävien tietojärjestelmien suojaamiseen. Tavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja saatavuus.

ISO/IEC 27001 -standardi tukee tätä tarjoamalla viitekehyksen tietoturvan hallintaan, riskienhallintaan sekä tietoturvakontrollien toteuttamiseen.

Operatiivinen teknologia (OT, Operational Technology) puolestaan koostuu laitteista ja ohjelmistoista, joilla valvotaan ja ohjataan fyysisiä prosesseja. OT-järjestelmät ohjaavat laitteita ja infrastruktuuria, jotka vaikuttavat suoraan fyysiseen ympäristöön.

Esimerkkejä OT-ympäristöistä ovat mm. älykkäät rakennusautomaatiojärjestelmät, verkkoon liitetyt valaistusjärjestelmät, sähköverkot, vedenkäsittelylaitokset, liikennejärjestelmät ja teollisuuden tuotantolaitokset.



Toisin kuin IT-järjestelmät, OT-ympäristöt toimivat usein etänä ja pitkälti ilman jatkuvaa ihmisen valvontaa. IT-järjestelmään kohdistuva kyberhyökkäys voi aiheuttaa häiriöitä liiketoiminnalle, mutta onnistunut hyökkäys OT-järjestelmään voi keskeyttää yhteiskunnan kannalta välttämättömiä palveluita, vahingoittaa laitteistoa, aiheuttaa ympäristövahinkoja tai jopa vaarantaa ihmisten turvallisuuden. Esimerkiksi yrityksen sähköpostipalvelimen häiriö on yleensä liiketoiminnallinen ongelma, mutta sähköverkon osan toiminnan keskeytyminen voi vaikuttaa laajasti koko yhteiskuntaan. Tämän vuoksi OT-ympäristöjen kyberturvallisuudessa korostuvat erityisesti: turvallisuus, toiminnan jatkuvuus, häiriönsietokyky ja turvalliset käyttöprosessit. IEC 62443 -standardisarja tukee OT-ympäristöjen turvallista suunnittelua, käyttöönottoa ja ylläpitoa.

DEKRAn näkökulma:
Vaatimustenmukaisuudesta kilpailueduksi

Monet organisaatiot lähestyvät NIS2-direktiiviä erillisenä sääntelyvaatimuksena, joka ei liity niiden nykyisiin tietoturvan tai teollisuuden kyberturvallisuuden hallintajärjestelmiin. DEKRAn kokemuksen mukaan huomattavasti enemmän hyötyä saavutetaan, kun NIS2 integroidaan osaksi organisaation olemassa olevia toimintamalleja. NIS2-direktiivi, ISO/IEC 27001 ja IEC 62443-2-1 tähtäävät kaikki samaan tavoitteeseen – kyberturvallisuusriskien järjestelmälliseen hallintaan – mutta eri näkökulmista.

NIS2 määrittelee lakisääteiset vaatimukset kyberturvallisuudelle, hallintamalleille ja tietoturvapoikkeamien ilmoittamiselle. ISO/IEC 27001 tarjoaa johtamisjärjestelmän organisaation IT-ympäristön tietoturvan hallintaan. IEC 62443-2-1 määrittelee vaatimukset teollisten automaatio- ja ohjausjärjestelmien (IACS) kyberturvallisuuden hallintajärjestelmälle.

Organisaatioissa kehittämistarpeita havaitaan useimmiten seuraavilla osa-alueilla:

- **Johdon aktiivisempi osallistuminen:** Kyberturvallisuuden riskien hallinnan tulee olla aktiivisesti johdettua ja todennettavissa käytännössä, ei pelkästään dokumentoitua.
- **Toimitusketjun näkyvyyden parantaminen:** Monet organisaatiot hallitsevat omat tietoturvakäytäntönsä hyvin, mutta näkyvyys toimittajien kyberturvallisuuteen on usein rajallinen. Toimitusketjun turvallisuus on kuitenkin yksi NIS2-direktiivin keskeisistä vaatimuksista.
- **Tietoturvapoikkeamien toimintamallien testaaminen:** Tietoturvapoikkeamien hallintaa tulee harjoitella säännöllisesti, jotta esimerkiksi 24 tunnin ilmoitusvelvollisuus voidaan täyttää myös todellisessa häiriötilanteessa.

Organisaatiot, joilla on käytössä ISO/IEC 27001 -sertifioitu tietoturvallisuuden hallintajärjestelmä (ISMS) ja tarvittaessa IEC 62443-2-1 -standardin mukainen teollisuuden kyberturvallisuuden hallintajärjestelmä (CSMS), ovat yleensä jo hyvässä asemassa täyttämään suuren osan NIS2-direktiivin asettamista hallinnon, riskienhallinnan ja kyberturvallisuuden vaatimuksista sekä IT- että OT-ympäristöissä.

Strategiset suositukset käyttöönottoon

NIS2-direktiivin vaatimusten täyttäminen edellyttää strategista ja koko organisaation kattavaa lähestymistapaa. Keskeiset vaiheet ovat:

- **Toteuta IT- ja OT-ympäristöjen GAP-analyysi:** Arvioi organisaatiosi nykyinen kyberturvallisuuden taso suhteessa NIS2-direktiivin vaatimuksiin. Näin tunnistat kehityskohteet ja voit laatia suunnitelman vaatimusten täyttämiseksi.
- **Vahvista kyberturvallisuuden perustaa:** Keskity toimenpiteisiin, jotka luovat vakaan perustan organisaation kyberresilienssille. Vahva perusta auttaa suojaamaan organisaatiota luvattomalta pääsyltä sekä erilaisilta kyberhyökkäyksiltä.
- **Tarkista toimitusketjun sopimukset:** Varmista, että toimittajien ja yhteistyökumppaneiden kanssa tehdyt sopimukset sisältävät selkeät kyberturvallisuutta ja tietoturvapoikkeamien ilmoittamista koskevat vastuut. Myös IEC 62443-2-1- ja IEC 62443-2-4 -standardien mukainen sertifiointi voi tukea toimitusketjun kyberturvallisuuden hallintaa.
- **Kouluta ja sitouta ylin johto:** Varmista, että organisaation johto ymmärtää NIS2-direktiivin mukaiset lakisääteiset velvollisuutensa ja oman roolinsa kyberturvallisuuden johtamisessa.
- **Testaa toimintasuunnitelmat säännöllisesti:** Harjoittele tietoturvapoikkeamien hallintaa ja liiketoiminnan jatkuvuussuunnitelmia säännöllisesti esimerkiksi simulaatioiden avulla. Näin varmistat, että organisaatio pystyy toimimaan tehokkaasti myös todellisissa häiriötilanteissa.

Miten DEKRA voi tukea organisaatiotasi?

DEKRA tarjoaa asiantuntemusta ja ratkaisuja, joiden avulla organisaatiot voivat täyttää NIS2-direktiivin vaatimukset ja vahvistaa kyberresilienssiään.

Palveluihimme kuuluvat muun muassa:

- Nykytila-analyysit ja kyberturvallisuuden riskien arvioinnit.
- Tuki tietoturvapoikkeamien hallinta- ja liiketoiminnan jatkuvuussuunnitelmien laatimisessa, jotta kriittiset liiketoimintaprosessit voidaan palauttaa nopeasti häiriötilanteissa.
- Kohdennetut koulutukset tekniselle henkilöstölle ja ylimmälle johdolle.
- OT-standardeihin perustuvat koulutukset.
- IEC 62443 -standardisarjan mukaiset arviointi- ja sertifiointipalvelut (IEC 62443-2-1, IEC 62443-2-4 ja IEC 62443-3-3).

Yhteenveto:
Vaatimustenmukaisuudesta kyberresilienssiin

NIS2-direktiivi on paljon enemmän kuin pelkkä lakisääteinen velvoite – se tarjoaa organisaatioille mahdollisuuden rakentaa turvallisempaa ja toimintakykyisempää liiketoimintaa.

Kun NIS2-vaatimuksiin suhtaudutaan mahdollisuutena vahvistaa organisaation kyberturvallisuuden perustaa, organisaatio voi samalla pienentää taloudellisten seuraamusten riskiä, parantaa kykyään ehkäistä kyberhyökkäyksiä ja toipua niistä tehokkaasti sekä suojata liiketoimintaansa, mainettaan ja asiakkaitaan. Kyberturvallisuuden kehittäminen ei ole vain vaatimusten täyttämistä, vaan investointi organisaation pitkäjänteiseen toimintavarmuuteen ja kilpailukykyyn.

Haluatko lisätietoja? Ota yhteyttä!

Huomio: Tämä opas käsittelee EU:n NIS2-direktiivin (EU 2022/2555) keskeisiä vaatimuksia. Koska NIS2 on EU-direktiivi, kukin jäsenvaltio saattaa sen osaksi omaa kansallista lainsäädäntöään. Tämän vuoksi esimerkiksi toimivaltaiset viranomaiset, ilmoitusajat, seuraamukset ja yksityiskohtaiset velvoitteet voivat vaihdella jäsenvaltioittain. Useassa EU-maassa toimivien organisaatioiden tulee huomioida kunkin toimintamaan kansallinen lainsäädäntö