INFOSENTRY

Whitepaper

NIS2, is jouw organisatie er klaar voor?

Inhoudsopgave

Inleiding: NIS Directive

De Europese Unie begrijpt al een tijd dat er meer inspanningen moeten worden geleverd om de veiligheid van de economie en het vertrouwen van de inwoners te verdedigen tegen cyberdreigingen. Dit bewustzijn heeft in 2016 geleid tot de NIS Directive (*Directive on Security of Network and Information Systems*).

Sinds de inwerkingtreding van deze eerste versie van de NIS Directive is het niveau van cybersecurity van de Europese Unie sterk verbeterd en is er een aanzienlijke mentaliteitsverandering. Bedrijven die onder het toepassingebied van NIS(1) vielen, moesten strategieën voor de beveiliging van netwerk- en informatiesystemen definiëren. De eerste versie van de NIS Directive heeft zeker bijgedragen tot een hogere cybersecurity maturiteit op het niveau van de Unie.

Ondanks deze verwezenlijkingen heeft de evaluatie van de NIS Directive inherente tekortkomingen aan het licht gebracht. Deze verhinderen dat de huidige en opkomende uitdagingen op het gebied van cyberbeveiliging doeltreffend worden aangepakt. Doordat de verplichtingen van de NIS richtlijn te algemeen waren beschreven, zijn de cyber beveiligingsniveaus tussen de deelstaten niet van een gelijke maturiteit. Ook was er onduidelijkheid over het toepassingsgebied voor essentiële diensten.

Van NIS naar NIS2

Als antwoord op deze tekortkomingen werd eind 2022 de NIS2 Directive in het leven geroepen. Deze nieuwe versie zorgt voor een aanzienlijke scope-uitbreiding van zowel organisaties die aan NIS2 moeten voldoen alsook het toezicht op naleving van de verplichtingen. NIS2 richt zich namelijk op sectoren en diensten die van vitaal belang zijn voor de maatschappij, de lidstaten of de Unie. Het aantal publieke en private organisaties die onder de richtlijn vallen wordt dus heel wat groter.

Een belangrijk verschil met de eerste NIS Directive is dat organisaties automatisch onder de NIS2 Directive vallen als zij actief zijn in één van de in de richtlijn vermelde sectoren. Lidstaten zijn dus niet langer verantwoordelijk voor het bepalen van de entiteiten die voldoen aan de criteria. Enkel voor de kleine en micro-ondernemingen zullen de lidstaten moeten bepalen of deze een sleutelrol vervullen voor de samenleving, de economie of voor bepaalde sectoren of soorten diensten.

Toepassingsgebied

De organisaties die aan de NIS2 Directive moeten voldoen, behoren tot sectoren vermeld in bijlage 1 en 2 van de richtlijn. Onderstaande tabel geeft een high-level overzicht.

Sectoren bijlage 1	Sectoren bijlage 2
• Energie • Transport • Bankwezen • Infrastructuur financiële markt • Gezondheidszorg • Drinkwater • Afvalwater • Digitale infrastructuur • Beheer van ICT diensten • Overheidsdiensten • Ruimtevaart	• Post- en koeriersdiensten • Afvalstoffenbeheer • Chemische stoffen • Levensmiddelen • Vervaardiging / manufacturing • Digitale aanbieders • Onderzoek

NIS2 maakt een onderscheid tussen tussen essentiële entiteiten en belangrijke entiteiten. Van essentiële entiteiten wordt over het algemeen aangenomen dat de uitval van hun diensten een grotere ontwrichtende impact heeft op de economie en samenleving dan uitval bij belangrijke entiteiten. Essentiële entiteiten vallen dan ook onder een intensiever regime van toezicht op de naleving van de verplichtingen, zowel proactief als reactief. Voor belangrijke entiteiten geldt een lichtere vorm van toezicht dat alleen plaatsvindt bij aanwijzingen voor niet-naleving of bij een incident.

Essentiële entiteiten

Grote organisaties (meer dan 250 werknemers of een netto jaaromzet van meer dan € 50 miljoen en een balanstotaal van meer dan € 43 miljoen) die actief zijn in een sector uit bijlage 1 van de NIS2 Directive (zie bovenstaande tabel) worden gezien als essentiële entiteiten. Zij zullen dus moeten voldoen aan de verplichtingen die NIS2 oplegt aan essentiële entiteiten en mogen strenger toezicht verwachten.

Belangrijke entiteiten

Middelgrote organisaties (meer dan 50 werknemers of een netto jaaromzet of balanstotaal van meer dan € 10 miljoen) die actief zijn in een sector uit bijlage 1 van de NIS2 Directive (zie bovenstaande tabel) en organisaties die actief zijn in een sector uit bijlage 2 van de NIS2 Directive worden gezien als belangrijke entiteiten. Zij zullen dus moeten voldoen aan de verplichtingen die NIS2 oplegt aan belangrijke entiteiten.

Wat met kleine en micro-entiteiten?

Kleine en micro-entiteiten vallen in principe niet onder de NIS2 Directive. Lidstaten kunnen er echter wel voor kiezen om een kleine of micro-entiteit alsnog aan te wijzen op basis van een risicobeoordeling, bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de maatschappij of nationale economie. In dat geval worden deze bedrijven hierover geïnformeerd door de bevoegde overheidsdienst.

Daarnaast zijn er nog kleine en micro-entiteiten die wel automatisch onder de NIS2 Directive vallen. Het gaat dan om bedrijven die actief zijn als:

- Register voor topleveldomeinnamen;
- Aanbieder van vertrouwensdiensten;
- Verlener van domeinnaamregistratiediensten;
- Aanbieder van openbare elektronische communicatienetwerken; of
- Overheidsinstantie.

De tabel op volgende pagina geeft een detailoverzicht weer van de essentiële en belangrijke entiteiten per sector en grootte van organisatie. Op onze website vind je ook een self-assessment tool om te evalueren of jouw organisatie zal moeten voldoen aan NIS2 (via deze link).

<table>
<tr><th>Sector</th><th>Subsector</th><th>Grote entiteiten</th><th>Middelgrote entiteiten</th><th>Kleine en micro-entiteiten</th></tr>
<tr><td colspan="5">Bijlage 1: Zeer kritieke sectoren</td></tr>
<tr><td>1. Energie</td><td>Elektriciteit, stadsverwarming en -koeling, gas, olie, waterstof</td><td rowspan="6">Essentieel</td><td rowspan="6">Belangrijk, behalve indien geïdentificeerd als essentieel</td><td rowspan="6">Niet in het toepassingsgebied, behalve indien geïdentificeerd als essentieel of belangrijk</td></tr>
<tr><td>2. Transport</td><td>Lucht, spoor, water, weg</td></tr>
<tr><td>3. Bankwezen</td><td>Kredietinstellingen</td></tr>
<tr><td>4. Infrastructuur financiële markt</td><td>Handelsplatforms, centrale tegenpartijen</td></tr>
<tr><td>5. Gezondheidszorg</td><td>Gezondheidszorg biedt, EU-referentielaboratoria, farmaceutische productie, O&O van medische producten, …</td></tr>
<tr><td>6. Drinkwater</td><td></td></tr>
<tr><td>7. Afvalwater</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="8">8. Digitale infrastructuur</td><td>TLD-naamregisters, gekwalificeerde aanbieders van vertrouwensdiensten, DNS-dienstverleners</td><td colspan="3">Essentieel</td></tr>
<tr><td>Aanbieders van openbare elektronische communicatienetwerken</td><td colspan="2">Essentieel</td><td>Belangrijk, behalve indien geïdentificeerd als essentieel</td></tr>
<tr><td>Niet-gekwalificeerde aanbieder van vertrouwensdiensten</td><td rowspan="5">Essentieel</td><td rowspan="5">Belangrijk, behalve indien geïdentificeerd als essentieel</td><td rowspan="5">Niet in het toepassingsgebied, behalve indien geïdentificeerd als essentieel of belangrijk</td></tr>
<tr><td>Aanbieders van internetuitwisselingspunten</td></tr>
<tr><td>Dienstverleners van cloud computing</td></tr>
<tr><td>Aanbieders van datacentra</td></tr>
<tr><td>Aanbieders van content delivery netwerken</td></tr>
<tr><td>8a. ICT-dienstenbeheer</td><td>MSP, MSSP</td></tr>
<tr><td>9. Overheidsdiensten</td><td>Uitgezonderd rechterlijke macht, parlementen, centrale banken, defensie, nationale of openbare veiligheid</td><td colspan="3">Essentieel</td></tr>
<tr><td>10. Ruimtevaart</td><td>Exploitanten van infrastructuur op de grond</td><td>Essentieel</td><td>Belangrijk, behalve indien geïdentificeerd als essentieel</td><td>Niet in het toepassingsgebied, behalve indien geïdentificeerd als essentieel of belangrijk</td></tr>
<tr><td colspan="5">Bijlage 2: Andere kritieke sectoren</td></tr>
<tr><td>1. Post- en koeriersdiensten</td><td></td><td colspan="2"></td><td></td></tr>
</table>

2. Afvalstoffenbeheer		Belangrijk, behalve indien geïdentificeerd als essentieel	Niet in het toepassingsgebied, behalve indien geïdentificeerd als essentieel of belangrijk
3. Chemische stoffen	Vervaardiging, productie, distributie		
4. Levensmiddelen	Productie, verwerking en distributie		
5. Vervaardiging / manufacturing	Medische apparaten, computerelektronica, optische producten, motorvoertuigen, machines, transportmiddelen, …		
6. Digitale aanbieders	Online marktplaatsen, zoekmachines, sociale netwerken		
7. Onderzoek	Uitgezonderd onderwijsinstellingen		

Welke eisen stelt NIS2 aan essentiële en belangrijke entiteiten?

De NIS2 Directive verwacht van essentiële en belangrijke entiteiten om ten minste volgende maatregelen te implementeren (artikel 21):

a) Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) Procedures voor incidentenbehandeling;
c) Bedrijfscontinuïteit (bv. back-ups en noodvoorzieningen) en crisisbeheer;
d) Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten binnen relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e) Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f) Beleid en procedures om de doeltreffendheid van cyberbeveiligingsmaatregelen te beoordelen;
g) Elementaire cyberhygiënepraktijken en cyberbeveiligingsopleiding;
h) Beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Daarnaast worden ook eisen opgelegd aan het topmanagement van een entiteit (artikel 20). Niet alleen moeten maatregelen voor risicobeheer inzake cyberbeveiliging door het management worden genomen en goedgekeurd. Leden van beheersorganen moeten ook een opleiding volgen over risicobeheer op het gebied van cyberbeveiliging. Dit moet ertoe leiden dat het management voldoende kennis en vaardigheden heeft om risico's op het gebied van cyberbeveiliging en de gevolgen daarvan voor de entiteit te begrijpen en te beoordelen. *Infosentry heeft al vele jaren ervaring om management te helpen risico's te begrijpen om zo efficiënte keuzes te maken op vlak van cybersecurity.*

Rapportering van incidenten

Wanneer essentiële of belangrijke entiteiten kennis krijgen van een significant incident, moeten zij binnen 24 uur een **vroegtijdige waarschuwing** geven. Dit wil zeggen dat de entiteit de CSIRT of bevoegde autoriteit in kennis moeten stellen van elk cyberbeveiligingsincident die een significant effect heeft op de verlening van hun diensten. Deze vroegtijdige waarschuwing moet worden gevolgd door een kennisgeving van het incident. De betrokken entiteiten moeten zonder onnodige vertraging, en in ieder geval, binnen 72 uur na kennisname van het significante incident een **incidentmelding** indienen. Dit heeft als doel om de via de vroegtijdige waarschuwing verstrekte informatie te actualiseren. Zo kan er een eerste beoordeling gebeuren van het incident, inclusief de ernst, de gevolgen, indicatoren, …. Uiterlijk één maand na de melding van het incident moet een **eindverslag** worden ingediend.

De vroegtijdige waarschuwing mag alleen informatie bevatten die nodig is om het CSIRT, of in voorkomend geval de bevoegde autoriteit, op de hoogte te brengen van het significante incident en de betrokken entiteit in staat te stellen zo nodig bijstand te vragen. Deze vroegtijdige waarschuwing moet aangeven of het significante incident vermoedelijk door onwettige of kwaadwillige handelingen is veroorzaakt en of het waarschijnlijk grensoverschrijdende gevolgen zal hebben. De vroegtijdige waarschuwing mag ook een vraag bevatten voor hulp van de lidstaat om te helpen bij het onderzoek.

Een incident wordt als significant beschouwd indien:

- het een ernstige verstoring van de dienstverlening of financieel verlies voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of
- het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

In België zal je een incident kunnen melden aan de CERT (zoals reeds mogelijk gemaakt door de eerste NIS Directive).

Toezicht en handhaving

Lidstaten zullen toezichthoudende autoriteiten moeten aanstellen die moeten toezien op naleving van NIS2 bij essentiële entiteiten (zowel preventief als reactief) en belangrijke entiteiten (reactief).

Toezicht voor essentiële entiteiten (ex ante en ex post)

Toezichthoudende autoriteiten kunnen essentiële entiteiten onderwerpen aan:

a) Inspecties ter plaatse en toezicht vanop afstand, met inbegrip van steekproefsgewijze controles;
b) Ad-hoc audits;
c) Beveiligingsscans op basis van beoordelingscriteria;
d) Verzoeken tot informatie om genomen cyberbeveiligingsmaatregelen te beoordelen;
e) Verzoeken om toegang tot gegevens, documenten of informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;
f) Verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de onderliggende bewijzen.

De bevoegde autoriteiten kunnen een termijn vaststellen waarbinnen de essentiële entiteit wordt verzocht de nodige maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van die autoriteiten te voldoen.

Toezicht voor belangrijke entiteiten (ex post)

Wanneer de lidstaten aanwijzingen krijgen dat een belangrijke entiteit de in de NIS2 neergelegde verplichtingen niet nakomt, moeten toezichthoudende autoriteiten maatregelen nemen en kunnen ze belangrijke entiteiten onderwerpen aan:

a) Inspecties ter plaatse en toezicht vanop afstand;
b) Gerichte beveiligingsaudits op basis van risicobeoordelingen;
c) Beveiligingsscans op basis van risicobeoordelingen;
d) Verzoeken tot informatie om genomen cyberbeveiligingsmaatregelen te beoordelen, met inbegrip van het gedocumenteerd cyberbeveiligingsbeleid;
e) Verzoeken om toegang tot gegevens, documenten of informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken.

Sancties en handhaving

Als de bevoegde autoriteit op de hoogte is van een aanzienlijke cyberdreiging of een dreigend risico, zal deze onmiddellijk handhavingsbesluiten kunnen nemen. De handhavingsmaatregelen moeten altijd proportioneel zijn aan het risico.

Mogelijke sancties zijn:

a) Waarschuwingen;
b) Verplichting om vastgestelde tekortkomingen te verhelpen;
c) Openbaar maken van niet-naleving van de verplichtingen van de organisatie; of
d) Administratieve geldboetes.

a. Voor essentiële entiteiten zijn geldboetes mogelijk tot € 10 miljoen of 2% van de totale wereldwijde jaaromzet;
b. Voor belangrijke entiteiten zijn geldboetes mogelijk tot € 7 miljoen of 1,4% van de totale wereldwijde jaaromzet;

Essentiële entiteiten kunnen ook een toezichthoudende ambtenaar aangewezen krijgen met duidelijk omschreven taken gedurende een bepaalde periode die zal toezien op de naleving van hun verplichtingen.

Als essentiële entiteiten de gevraagde maatregelen niet nemen of de geïmplementeerde maatregelen inefficiënt blijken, kunnen ook volgende maatregelen genomen worden:

a) Schorsing van een deel of alle relevante diensten of activiteiten die door een essentiële entiteit worden verricht; of
b) Schorsing van personen die leidinggevende verantwoordelijkheden uitoefenen op het niveau van CEO of wettelijk vertegenwoordiger.

Europese cyberbeveiligingscertificaten

De Europese Commissie krijgt de mogelijkheid om te eisen dat bepaalde categorieën essentiële of belangrijke entiteiten gecertificeerde ICT-producten, -diensten en -processen moeten gebruiken of zelf een cyberbeveiligingscertificaat moeten behalen. NIS2 specifieert vandaag echter nog geen goedgekeurd certificaat. De Europese Unie ontwikkelt daarom via ENISA een EU-cyberbeveiligingscertificaat dat moet aantonen dat een entiteit een bepaald vertrouwensniveau naleeft. De verwachting is dat dit certificaat sterk gebaseerd zal zijn op internationale norm ISO27001, waardoor het raadzaam is om alvast een information security management systeem (ISMS) te implementeren volgens de bepalingen van ISO27001.

Informatiedeling

De Europese Unie wil inzetten op maximale informatiedeling. Hiervoor worden in NIS2 enkele nieuwe iniatieven genomen. Naast verplichte rapporteringen voor organisaties die onder NIS2 vallen (bv. bij incidenten), wil de Europese Unie ook informatiedeling voor organisaties die niet in het toepassingsgebied van NIS2 vallen mogelijk maken. Door mogelijkheden te bieden om (vrijwillig) relevante informatie over cyberbeveiliging uit te wisselen (bv. cyberdreigingen, kwetsbaarheden, informatie over specifieke technieken, …) wil de Unie cyberaanvallen sneller opsporen, incidenten voorkomen en het algemeen niveau van cyberbeveiliging binnen de Unie verhogen.

Cyber security incident response team (CSIRT)

Bij de eerste NIS Directive is het CSIRTs-netwerk opgericht "om bij te dragen tot de ontwikkeling van vertrouwen tussen de lidstaten en om een snelle en doeltreffende operationele samenwerking te bevorderen". Het CSIRTs-netwerk is een netwerk dat bestaat uit door de EU-lidstaten aangewezen CSIRT's en CERT-EU. ENISA (European Network and Information Security Agency) heeft als taak de samenwerking tussen de CSIRT's actief te ondersteunen en op verzoek actieve steun te verlenen voor de coördinatie van incidenten.

NIS2 verwacht nu dat CSIRT's gaan optreden als vertrouwenspersoon tussen de rapporterende persoon en de fabrikant of aanbieder van het IT-product en/of dienst die is of zal worden getroffen door de kwetsbaarheid.

In België is de CERT aangesteld als nationale CSIRT.

Vulnerability databank

Er zal een Europese databank aangelegd worden met kwetsbaarheden waarin entiteiten (ongeacht of zij binnen of buiten het toepassingsgebied van NIS2 vallen), hun leveranciers van netwerk- en informatiesystemen, alsook de bevoegde autoriteiten en de CSIRT's op vrijwillige basis algemeen bekende kwetsbaarheden kunnen melden en registreren. Dit om ervoor te zorgen dat gebruikers passende risicobeperkende maatregelen kunnen nemen. Deze databank zal worden beheerd door ENISA en moet voor meer transparantie zorgen.

EU CyCLONe

The Cyber Crisis Liaison Organisation Network (EU CyCLONe) is een samenwerkingsnetwerk voor de nationale autoriteiten in de lidstaten die belast zijn met het beheer van cybercrises.

Om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en crises op operationeel niveau te ondersteunen en te zorgen voor de regelmatige uitwisseling van relevante informatie tussen lidstaten en instellingen, organen en agentschappen van de Unie, is de Europese verbindingsorganisatie (EU CyCLONe) opgericht.

Dankzij EU CyCLONe kunnen zij informatie delen en bewustzijn ontwikkelen op basis van instrumenten en ondersteuning van ENISA, dat als secretariaat van het netwerk fungeert.

Elke lidstaat wijst één of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor het beheer van grootschalige cyberincidenten en -crises. Elke lidstaat moet een nationaal plan uitwerken voor de respons op incidenten en crises op het gebied van cyberbeveiliging. Dit plan zal worden voorgelegd aan de Commissie en EU CyCLONe. In België zal de CERT worden aangeduid als autoriteit om grootschalige cyberincidenten en -crises te beheren.

Tijdslijn en inwerkingtreding

Op 27 december 2022 is de NIS2 Directive gepubliceerd in de Official Journal van de Europese Unie als Directive EU 2022/2555. Vervolgens is een implementatietermijn van 21 maanden gestart, waarin de richtlijn moet worden opgenomen in nationale wetgeving. Volgende deadlines zijn van toepassing:

- 17 oktober 2024: Deadline voor de lidstaten om de NIS2 Directive om te zetten in nationale wetgeving;
- 17 april 2025: Deadline voor de lidstaten om de lijst vast te leggen van essentiële en belangrijke entiteiten;

Ervan uitgaande dat België haar deadline haalt en NIS2 tegen 17 oktober 2024 heeft omgezet in Belgische wetgeving, zullen Belgische essentiële en belangrijke entiteiten dus tegen eind 2024 moeten voldoen aan de verplichtingen van NIS2.

Hoe kan Infosentry helpen?

Infosentry heeft al meer dan 15 jaar ervaring met governance, risk en compliance diensten binnen onder meer informatiebeveiliging, privacy en business continuity management. In de aanloop naar GDPR, die in werking trad op 25 mei 2018 en ook een aanloop had van 2 jaar, hebben we meer dan 100 organisatie geholpen om zich in regel te stellen met de compliance verplichtingen die de Europese privacywetgeving met zich meebracht. Daarnaast zijn we experten in ISO27001 implementaties (tot en met certificering), cyber security auditing, security project management en zelfs CISOaaS. Kortom, we zijn een ideale partner om uw organisatie van A tot Z te helpen om zich in regel te brengen met NIS2.

Een standaard traject zou bestaan uit:

1) **Assessment** en roadmap creatie met duidelijk actieplan van de nog te implementeren verplichtingen die NIS2 oplegt;
2) **Implementatie** van de roadmap, met inbegrip van risicomanagement, definiëren en implementeren van vereiste policies en procedures, training en awareness (incl. aan management), supply chain auditing, …
3) **Follow-up** om op lange termijn compliant te blijven met NIS2 (door middel van interne audits, workshops, coaching of zelfs het opnemen van de rol van Security Officer of CISO binnen uw organisatie).

We kunnen uw organisatie zoveel mogelijk ontzorgen of eerder ad hoc ondersteuning bieden. We stellen ons steeds flexibel en pragmatisch op en kijken graag samen met u welke noden uw organisatie heeft in aanloop naar NIS2 en welke toegevoegde waarde wij kunnen bieden.

Voor meer informatie over NIS2 en onze diensten, contacteer ons via:

info@infosentry.be

of bezoek onze website:

www.infosentry.be