Whitepaper

NIS2 in vogelvlucht

Alles wat je moet weten over deze nieuwe richtlijn.

Auteur: Linda van Woerkens
Versie: 1.1
Gepubliceerd: 28 september 2023 (update op 29 juli 2024)
Uitgegeven door: Cuccibu, Nederland

INHOUDSOPGAVE

Inleiding – Wat is de NIS2-richtlijn? 3
Welke organisaties vallen onder de NIS2 richtlijn? 3
Wat zijn straks jouw verplichtingen? 4
Wat zijn de gevolgen van de NIS2? 5
Wat kan je nu al doen? 6
Wat is de relatie met andere normenkader voor informatiebeveiliging? 6
Slotwoord 7

Inleiding – Wat is de NIS2-richtlijn?

In 2016 trad de eerste Network and Information Security directive, ofwel NIS-richtlijn, in werking: een richtlijn om de digitale weerbaarheid van de gehele Europese Unie (EU) te verbeteren. Door de snelle digitale transformatie van de afgelopen jaren heeft de EU sinds 2020 gewerkt aan een nieuwe versie van deze richtlijn: de NIS2. Het doel van de herziening van de NIS-richtlijn is om de weerbaarheid van onze samenleving te verbeteren evenals de **cyberbeveiliging**. De NIS2 draagt bij aan het realiseren van een basisniveau van beveiliging binnen de hele EU. Deze richtlijn moet uiterlijk 17 oktober 2024 door alle lidstaten worden omgezet in nationale wetgeving. In Nederland wordt deze vertaalslag gemaakt in de **Wet beveiliging netwerk en informatiesystemen** (Wbni). Deze whitepaper vertelt je alles wat je op dit moment moet weten over de NIS2 en de Nederlandse vertaling naar de Wbni.

Welke organisaties vallen onder de NIS2 richtlijn?

De NIS2 richt zich op verschillende sectoren. Naar verwachting heeft de richtlijn impact op 16.000 bedrijven en organisaties in Nederland. Organisaties vallen automatisch onder de NIS2 wanneer zij actief zijn in één van de achttien sectoren (zie tabel 1) en voldoen aan bepaalde omvangcriteria.

Daarbij worden organisaties die onder bijlage 1 en/of 2 vallen aangemerkt als essentiële entiteit of belangrijke entiteit. Het verschil tussen deze entiteiten zit hem in de mate van toezicht. Zo wordt er bij de essentiële entiteiten pro-actief toezicht gehouden op naleving van de richtlijn terwijl bij belangrijke entiteiten alleen toezicht plaatsvindt wanneer er aanwijzingen zijn voor het niet naleven van de richtlijn of wanneer een incident heeft plaatsgevonden.

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

Tabel 1 – Sectoren NIS2

Een organisatie is een **essentiële entiteit** wanneer zij werkzaam is binnen een sector genoemd in bijlage 1 van de NIS2-richtlijn en wordt aangemerkt als **groot** (meer dan 250 werknemers, een netto omzet van meer dan 50 miljoen euro of balanstotaal van meer dan 43 miljoen euro).

Een organisatie is een **belangrijke entiteit** wanneer zij werkzaam is binnen een sector genoemd in bijlage 1 en wordt aangemerkt als **middelgroot** (meer dan 50 werknemers of een jaaromzet of balanstotaal van meer dan 10 miljoen euro). Of wanneer de organisatie actief is in een sector uit bijlage 2 en wordt aangemerkt als **groot** óf **middelgroot**.

Er bestaan een aantal uitzonderingen op de regel:

- De minister die verantwoordelijk is voor een bepaalde sector kan er voor kiezen om een micro- of klein bedrijf alsnog aan te wijzen op basis van een risicobeoordeling. Bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de Nederlandse economie of maatschappij. In dat geval worden deze bedrijven hierover geïnformeerd door het desbetreffende ministerie.
- Er zijn micro- en kleine bedrijven die wel onder de NIS2-richtlijn vallen. Het betreft bedrijven die actief zijn als: aanbieder van vertrouwensdiensten, register voor topleveldomeinnamen, verleners van domeinnaamregistratiediensten, aanbieder van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten.
- Overheidsinstanties uit de genoemde sectoren vallen ook automatisch onder NIS2-richtlijn.

Wat zijn straks jouw verplichtingen?

Organisaties die onder de NIS2 vallen krijgen te maken met een tweetal verplichten, namelijk meldplicht en zorgplicht.

Meldplicht

Binnen **24 uur** dienen organisaties incidenten die aanzienlijke gevolgen (kunnen) hebben voor de verlening van hun diensten te melden bij de toezichthouder en het Nationaal Cybersecurity Centrum (NCSC). Het NCSC kan vervolgens steun en bijstand verlenen. De toezichthouder stelt vast of de organisatie de nodige technische en organisatorische maatregelen heeft genomen.

Binnen **72 uur** dient deze melding te worden opgevolgd met een gedetailleerd assessment. Hierin wordt de ernst en de impact van het incident omschreven, en indien mogelijk, welke maatregelen genomen worden.

Binnen **één maand** na het incident moet een eindverslag worden opgesteld. Dit is een rapport waarin precies wordt beschreven wat er is voorgevallen (wat was de oorzaak en hoe gedetecteerd?) en welke maatregelen zijn genomen (wat was de oplossing en wat zijn de lessons learned?).

Zorgplicht

De richtlijn verplicht organisaties om technische, operationele en organisatorische maatregelen te treffen om hun diensten zoveel mogelijk te waarborgen en de informatie te beschermen. Dit kan naar de Wbni onderhevig zijn aan verandering.

De volgende maatregelen worden benoemd in de NIS2 (art. 21):

- Risicobeoordeling voor beveiliging van informatiesystemen;
- Beleid en procedures voor beoordeling van effectiviteit van risicobeheersmaatregelen;
- Basisniveau van cyberhygiëne hanteren;
- Crisismanagement en operationele continuïteit bij een groot cyberincident;
- Veiligheid van de toeleveringsketen waarborgen;
- Waarborgen van veiligheid van netwerk- en informatiesystemen, waaronder het reageren op en communiceren van kwetsbaarheden;
- Zorgen voor digitale veiligheid van personeel, toegangsbeleid en het beveiligen van de digitale bedrijfsmiddelen;
- Gebruik van cryptografie en versleuteling;
- Toepassen van multifactor authenticatie en/of beveiligde communicatie;
- Reactieve monitoring na een incident en proactieve monitoring, ook buiten incidenten om.

Daarnaast zijn organisatie die onder de NIS2 vallen verplicht om zicht te registeren. Er geldt dus ook een registratieplicht.

Wat zijn de gevolgen van de NIS2?

Het toezicht op de naleving van de NIS2-richtlijn komt in handen van de Rijksinspectie Digitale Infrastructuur, het Nationaal Cyber Security Centrum en sectorspecifieke autoriteiten (zoals De Nederlandse Bank en Inspectie Gezondheidszorg en Jeugd). Zij zullen controleren om organisatie die aan de NIS2 moeten voldoen de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht, naleven.

Wanneer een organisatie voldoet aan de NIS2-richtlijn, brengt dit voordelen met zich:

- **Cyber Security** wordt naar een hoger niveau getild en de organisatie is beter beschermd tegen cyberaanvallen, wat bijdraagt aan de **bedrijfscontinuïteit** en reputatie van de organisatie.
- De organisatie laat zien dat het Cyber Security serieus neemt en zich inzet voor de bescherming van klanten en partners. Dit kan concurrentievoordeel opleveren.
- Het maakt de organisatie weerbaar. Het stelt de organisatie in staat om beter te reageren op het moment dat het toch fout gaat.

Wanneer een organisatie niet voldoet aan de vereisten van de richtlijn, kan dit lijden tot de volgende consequenties:

- Een boete van maximaal 10 miljoen euro of 2% van de totale wereldwijde jaaromzet voor essentiële diensten. Voor belangrijke entiteiten geldt een boete van maximaal 7 miljoen euro of 1,4% van de totale wereldwijde jaaromzet.
- Een verplichting om (onvoldoende beveiligde) diensten of de bedrijfsvoering te staken.
- Een verplichting om inbreuken op de richtlijn openbaar te maken, wat kan leiden tot verlies van vertrouwen van stakeholders en reputatieschade.
- Persoonlijke aansprakelijkheid van de bestuurder, die wettelijk bevoegd is om security-maatregelen te nemen, bij bewezen nalatigheid van cyberbeveiliging.

Wanneer treedt de NIS2 in werking?

Op 27 december 2022 is de definitieve versie van de NIS2 richtlijn in het publicatieblad van de EU gepubliceerd. Op 16 januari 2023 is deze richtlijn in werking getreden. Alle lidstaten hadden daarna 21 maanden (17 oktober 2024) de tijd om de richtlijn om te zetten in nationale wetgeving. Inmiddels is bekend dat Nederland deze deadline niet gaat halen. Naar verwachting treed de Nederlandse wetgeving van de NIS2 richtlijn in de zomer van 2025 in werking.

Wat kan je nu al doen?

Om te voldoen aan de vereisten van de NIS2-richtlijn, dienen de volgende stappen te worden gezet:

1. Breng je **landschap** in kaart en stel vast of je direct of indirect met de NIS2 te maken krijgt. Wanneer een organisatie in de toeleveringsketen van een essentiële of belangrijke entiteit opereert, kunnen door deze entiteit beveiligingseisen worden opgesteld voor hun leveranciers. Deze eisen kunnen dus ook aan een MKB-organisatie worden gesteld.
2. Voer een organisatiebrede **GAP-analyse** uit om in kaart te brengen welke onderdelen van NIS2 al zijn geïmplementeerd en welke nog niet.
3. Breng op basis van de uitkomsten de belangrijkste dreigingen en risico's voor de netwerken en systemen van de organisatie in kaart met behulp van een **risicoanalyse**.
4. Implementeer **beveiligingsmaatregelen** zoals genoemd in de zorgplicht van de NIS2-richtlijn. Prioriteer deze implementatie op basis van de gevonden risico's uit stap 2.
5. Zorg ervoor dat er bij deze maatregelen **aantoonbaar** gewerkt wordt: documenteer dus alle beveiligingsmaatregelen en procedures zodat de organisatie aantoonbaar aan de NIS2 voldoet.
6. **Controleer en evalueer**. De omgeving en informatiebeveiliging ontwikkelt zich, en je organisatie dus ook. Blijf de maatregelen controleren, evalueren en ontwikkelen. Naleving van de NIS2-richtlijn is een continu proces.

De implementatie van de richtlijn brengt mogelijk een aantal uitdagingen met zich mee. Bijvoorbeeld doordat het lastig is om voldoende middelen en expertise te vinden om de vereisten te implementeren. De **consultants van Cuccibu** hebben ervaring en helpen je graag verder.

Wat is de relatie met andere normenkader voor informatiebeveiliging?

Net zoals de NIS2 vraagt een standaard zoals **ISO 27001** om een structurele manier van werken aan informatiebeveiliging. In Nederland is voor de overheid op dit moment de **Baseline Informatiebeveiliging Overheid** (BIO) als uitgangspunt genomen voor de invulling van de zorgplicht. De BIO gaat op een aantal punten verder dan de ISO 27001. Voor overheidsinstanties geldt dat de invulling van de NIS2-zorgplicht zoveel mogelijk langs de bestaande kaders zal gebeuren. Instanties

die voorheen nog niet aan deze kaders voldeden, hebben hier vanuit de NIS2 nu wel verplichting toe. Om dit te realiseren zal de BIO waarschijnlijk met een aantal verplichtingen worden uitgebreid. Hoe dit er precies uit gaat zien, is nog niet bekend.

Voor niet-overheidsorganisaties is het raadzaam voorlopig de ISO 27001 te volgen, tenzij een branche-toezichthouder anders aanbeveelt. Zo kunnen zorgorganisaties nog de NEN 7510 aanhouden en onderwijsinstellingen het SURF-normenkader.

Het volgen van bestaande standaarden als de NEN 7510, ISO 27001 of de BIO een belangrijk beginpunt. Hierbij geldt wel dat bij inwerkingtreding van NIS2 hier aan voldoen dient te worden en het enkel en alleen werken volgens de bestaande standaarden mogelijk niet voldoende is.

Benieuwd naar de NIS2 in vergelijking met de andere normenkaders voor informatiebeveiliging? In een driedelige blogserie vertellen we meer over de maatregelen uit de NIS2 en hoe deze verschillen van de andere normenkaders. De volgende thema's komen daarbij aanbod: risicomanagement en incidentmanagement (**deel 1**), crisisbeheer, bedrijfscontinuïteit en leveranciersmanagement (**deel 2**), cyberhygiëne en awareness (**deel 3**).

Slotwoord

Heb je vragen over het voldoen aan de NIS2-richtlijn? Onze consultants helpen u graag. Naast het fungeren als sparringpartner voor de NIS2, bieden wij de volgende dienstverlening:

- **Uitvoeren GAP-analyse**: een GAP-analyse door Cuccibu geeft jouw organisatie inzicht in welke onderdelen van de NIS2 wel of niet zijn geïmplementeerd. Op basis van de uitkomst van de GAP-analyse kan jouw organisatie zelfstandig (of met ondersteuning van ons) aan de slag om de benodigde stappen te zetten om aantoonbaar te voldoen aan de NIS2.
- **Uitvoeren risicoanalyse**: het uitvoeren van een risicoanalyse is een vereiste vanuit de NIS2-richtlijn en een van de belangrijke stappen om te overwegen welke maatregelen jouw organisatie kan en wil treffen. Deze analyse zorgt niet alleen voor de basis om te voldoen aan de NIS2-richtlijn maar ook voor het beheersen van informatiebeveiligingsgerelateerde risico's.
- **Ondersteuning bij het implementeren van beveiligingsmaatregelen**: wij kunnen jouw organisatie helpen bij het uitvoeren van de juiste stappen met betrekking tot het implementeren van beveiligingsmaatregelen, zoals genoemd in de zorgplicht van de NIS2-richtlijn. Onze consultants doen dit aan de hand van een GAP-analyse. Daarna stemmen we gezamenlijk met jouw organisatie af wat deze stappen zijn en voeren deze uit conform planning.

Neem vrijblijvend **contact** met ons op en we vertellen je graag alles over de verschillende mogelijkheden. Wij zijn te bereiken via **085-3032984** of **sales@cuccibu.nl**

Reduce Risk, Create Value!

Bronnen

Publicatieblad van de Europese Unie, RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 december 2022
Digitale Overheid, NIS2-richtlijn
ACA IT-solutions, whitepaper NIS2

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security, QHSE en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!