WHITEPAPER

# ALLES WAT JE MOET WETEN OVER DE **NIS2-RICHTLIJN**

anbecom ICT

# INHOUD



anbecom ICT

# INLEIDING

De **NIS2-richtlijn** is sinds 17 oktober 2024 van kracht binnen de Europese Unie. Een belangrijk verschil met de eerste NIS1-richtlijn is dat organisaties automatisch onder de NIS2-richtlijn vallen als zij actief zijn in bepaalde sectoren.

Het is belangrijk om te weten binnen welke categorie (essentieel of belangrijk) jouw organisatie valt. Organisaties in de categorie essentieel worden namelijk proactief gecontroleerd op het naleven van de regels, zoals opgenomen in de NIS2-richtlijn.

In dit document gaan we dieper in op de belangrijkste aspecten van de NIS2-richtlijn en leggen we uit hoe je hier als organisatie mee te maken kunt krijgen vanaf het 2e kwartaal in 2026.

Bedankt voor het downloaden van onze whitepaper. Heb je na het lezen een vraag of behoefte aan meer informatie? Neem dan contact met ons op.

**LET OP:**
Valt jouw bedrijf **niet onder de NIS2-richtlijn**? Ook dan kun je hier toch mee te maken krijgen.

anbecom ICT

# WAT IS DE NIS2-RICHTLIJN?

Cybersecurity is ontzettend belangrijk voor het beschermen van de economie en onze samenleving. Om te zorgen voor meer samenhang binnen de Europese Unie (EU) werd in 2016 de NIS1-richtlijn (Network and Information Systems Directive) geïntroduceerd. Met de toenemende digitalisering en de grote hoeveelheid cyberaanvallen is de oude richtlijn herzien en verbeterd.

De **NIS2-richtlijn** (Network and Information Systems Directive 2) is een Europese regelgeving die de cyberbeveiliging van essentiële en belangrijke bedrijven versterkt. Met aangescherpte eisen rond risicobeheer, rapportageverplichtingen en verantwoordelijkheden voor bedrijfsleiding, breidt NIS2 het toepassingsgebied van de oorspronkelijke richtlijn uit.

## BELANGRIJKSTE WIJZIGINGEN

- **Uitgebreid toepassingsgebied:** Meer sectoren vallen onder de regelgeving, waaronder digitale aanbieders, voedselproductie en postdiensten.
- **Strengere beveiligingsvereisten:** Organisaties moeten proactieve maatregelen nemen, zoals risicobeheer en incidentpreventie.
- **Verhoogde verantwoordelijkheid voor bestuurders:** Leidinggevenden kunnen aansprakelijk worden gesteld bij tekortkomingen in cyberbeveiliging.
- **Snellere en strengere rapportageplicht:** Cyberincidenten moeten binnen 24 uur worden gemeld, met een gedetailleerd rapport binnen 72 uur.
- **Hogere sancties:** Niet-naleving kan leiden tot boetes en andere juridische consequenties.

# BELANGRIJKE CRITERIA

Organisaties die onder de NIS2-richtlijn vallen dienen hun cyberstrategie te herzien om te voldoen aan de nieuwe normen en sancties te vermijden. Deze aangepaste richtlijn treft ook organisaties die niet onder de NIS2-richtlijn vallen. Om te kunnen leveren aan organisaties die wél onder de NIS2-richtlijn vallen zal ook jouw organisatie aan bepaalde eisen voor cybersecurity moeten voldoen.

## CRITERIA NIS2-RICHTLIJN

De NIS2-richtlijn richt zich op grote- en middelgrote organisaties die actief zijn binnen bepaalde sectoren. Naast de grootte van de organisatie is ook de sector waarin je actief bent bepalend of je als essentieel of belangrijk wordt bestempeld.

- **Middelgrote organisaties**
  - 50 - 249 medewerkers
  - Jaaromzet: 10 - 50 miljoen euro (of een balanstotaal van 10 - 43 miljoen euro.
- **Grote organisaties**
  - > 250 medewerkers
  - Jaaromzet: > 50 miljoen euro (of een balanstotaal van > 43 miljoen euro.

## ZEER KRITIEKE SECTOREN - ESSENTIEEL

- Energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten (B2B), overheid en ruimtevaart.

## KRITIEKE SECTOREN - BELANGRIJK

- Post- en koeriersdiensten, afvalbeheer, chemische industrie, voedselproductie, -verwerking en -distributie, productie, digitale aanbieders, onderzoek en productie/distributie van essentiële geneesmiddelen en medische hulpmiddelen.

# TREFT HET MIJN ORGANISATIE?

In principe vallen micro- en kleine bedrijven (<50 medewerkers met een jaaromzet of balanstotaal van minder dan 10 miljoen euro) niet onder de NIS2-richtlijn. Maar wanneer de dienstverlening van cruciaal belang is voor onze economie of de maatschappij kan een organisatie alsnog onder de NIS2-richtlijn vallen.

**Organisaties die actief zijn in onderstaande sectoren vallen altijd onder de NIS2-richtlijn**, ongeacht de grootte, de jaaromzet en de balanstotaal van de organisatie.

- Overheid, aanbieders van openbare elektronische communicatienetwerken en -diensten, aanbieders van vertrouwensdienstverleners, registers voor topleveldomeinnamen en DNS-dienstverleners.

## ZELF-EVALUATIETOOLS

Het is belangrijk te weten of jouw organisatie valt onder de NIS2-richtlijn. Om dit te achterhalen is het aanhouden van de eerder benoemde criteria niet (altijd) voldoende. Met behulp van de zelf-evaluatietool van de overheid wordt duidelijk of jouw organisatie valt onder de NIS2-richtlijn en wanneer het geval, of de organisatie wordt gekenmerkt als essentieel of belangrijk.

**Treft de NIS2-richtlijn mijn organisatie?**

- Gebruik hiervoor **de zelf-evaluatietool van de overheid**
- Controleer **jouw NIS2 Cyber Score** op Samen Digitaal Veilig

**Hulp nodig?**

Op zoek naar een ervaren partner bij het nemen van maatregelen om de cyberweerbaarheid van de organisatie te verhogen? Neem dan contact met ons op.

# CYBERSECURITY MAATREGELEN

Als jouw organisatie onder de NIS2-richtlijn valt of hiermee te maken heeft is het belangrijk om te weten welke maatregelen je moet nemen om aan deze richtlijn te voldoen.

## ZORGPLICHT

Organisaties moeten een risicobeoordeling uitvoeren en naar aanleiding daarvan maatregelen nemen om cyberdreigingen te beperken tot het minimum.

- Beveiliging van netwerk- en informatiesystemen.
- Toegangsbeheer en sterke authenticatieprocedures.
- Regelmatige updates en patchbeheer om kwetsbaarheden proactief te verhelpen.

## MELDPLICHT

Ernstige en kritieke cyberincidenten moeten binnen 24 uur gemeld worden aan de toezichthouder. Verder moet er na het binnen 72 uur een gedetailleerd rapport ingediend worden over de impact van het incident en de getroffen maatregelen.

## REGISTRATIEPLICHT

Alle organisaties (essentieel en belangrijk) die onder de NIS2-richtlijn vallen zijn wettelijk verplicht om zich te registreren bij de autoriteiten.

## KETENVERANTWOORDELIJKHEID

Leveranciers en partners van de organisatie die onder de NIS2-richtlijn valt moeten ook gaan voldoen aan de gestelde eisen in de richtlijn. Hierover zullen afspraken gemaakt moeten worden over de cybersecuritystandaarden, welke schriftelijk moeten worden vastgelegd.

## BEWUSTWORDING EN TRAINING

Organisaties moeten hun medewerkers actief en regelmatig te trainen om cyberaanvallen te herkennen om de kans daarop zo klein mogelijk te houden.

# BOETES & HANDHAVING

De manier waarop de EU gaat handhaven hangt af van de categorie (essentieel of belangrijk) waarin jouw organisatie valt. Organisaties in de categorie essentieel worden vanaf het 3e kwartaal in 2025 proactief gecontroleerd op het naleven van de NIS2-richtlijn.

Organisaties in de categorie belangrijk zullen bij een incident bij het in werking treden van de NIS2-richtlijn achteraf gecontroleerd worden op het naleven van de regels. Wanneer dat achteraf niet het geval blijkt te zijn zal de organisatie hiervoor een hoge boete opgelegd krijgen.

## BOETES

De maximale boetes voor organisaties die niet voldoen aan de NIS2-richtlijn kunnen hoog oplopen. Daarnaast kunnen er administratieve sancties worden opgelegd als een organisatie niet voldoet aan de zorg- of meldplicht. Dit kan leiden tot extra boetes en toezichtmaatregelen.

- **Belangrijke organisaties:** Een maximale boete van ten minste **7 miljoen euro** of ten minste **1,4% van de wereldwijde jaaromzet** in het volgende boekjaar; afhankelijk van welk bedrag hoger is.

- **Essentiële organisaties:** Een maximale boete van ten minste **10 miljoen euro** of ten minste **2% van de wereldwijde jaaromzet** in het volgende boekjaar; afhankelijk van welk bedrag hoger is.

## EXTRA SANCTIES

Als een organisatie in de categorie essentieel niet voldoet aan de NIS2-richtlijn kan dat leiden tot het (tijdelijk) intrekken van vergunningen. Daarnaast kunnen natuurlijke personen (directeuren) bij het in werking treden van de aangepaste richtlijn geschorst of persoonlijk aansprakelijk gesteld worden.

# TOEKOMST NIS2-RICHTLIJN

Op dit moment zijn er 18 verschillende sectoren opgenomen, verdeeld in de categorieën essentieel en belangrijk in de NIS2-richtlijn. In de komende jaren zal de Europese Commissie de richtlijn blijven evalueren en verder uitbreiden.

## NIEUWE SECTOREN

Hoewel er nog geen officiële lijst is van sectoren die in de komende jaren worden toegevoegd, zullen onderstaande sectoren in de komende jaren naar alle waarschijnlijkheid extra aandacht krijgen.

- **Financiële marktinfrastructuren** (uitbreiding van de DORA-vereisten)
- **Productie en distributie van essentiële geneesmiddelen en medische hulpmiddelen**
- **Onderzoek en ontwikkeling** (met focus op digitale innovatie)
- **Managed Service Providers (MSP's) en IT-bedrijven** als digitale aanbieders

## STRENGERE REGELS

In de toekomst zal de NIS2-richtlijn verder aangescherpt worden om de digitale weerbaarheid van bedrijven en overheden te verbeteren.

- **Strengere eisen voor toeleveranciers:** bedrijven zullen hun leveranciersketen beter moeten beschermen om cyberaanvallen via zwakke schakels te voorkomen.
- **Nadruk op ketenveiligheid:** grote organisaties gaan kleinere partners verplichten om het cybersecuritybeleid verder aan te scherpen.
- **Certificeringen en kwaliteitsstandaarden:** bedrijven moeten kunnen aantonen dat ze voldoen aan de NIS2-richtlijn met bijvoorbeeld het NIS2 Quality Certificaat.

# STAPPENPLAN NIS2-RICHTLIJN

In een tijdperk waarin digitale dreigingen steeds geavanceerder worden, is het naleven van de NIS2-richtlijn cruciaal voor organisaties die essentiële- en belangrijke diensten leveren. Onderstaand stappenplan kan gehanteerd worden om de cyberweerbaarheid te verhogen om de continuïteit van de organisatie en haar diensten te waarborgen.

## ORIËNTATIEFASE

De oriëntatiefase omvat het begrijpen van de NIS2-richtlijn en de impact ervan op de organisatie. Dit begint met het identificeren van de essentiële en belangrijke entiteiten binnen de organisatie die onder de richtlijn vallen. Vervolgens wordt er een overzicht gemaakt van de huidige cybersecuritymaatregelen en -processen.

## RISICOBEOORDELING

In de risicobeoordelingsfase voert de organisatie een gedetailleerde risicoanalyse uit. Hierbij dient gekeken te worden naar de (potentiële) dreigingen, kwetsbaarheden en de impact van mogelijke incidenten. Het is belangrijk dat deze beoordeling periodiek opnieuw wordt uitgevoerd om de organisatie te kunnen beschermen tegen nieuwe cyberdreigingen.

## IMPLEMENTATIES NIS2-RICHTLIJN

Tijdens de implementatiefase worden de geïdentificeerde maatregelen uit de risicobeoordeling daadwerkelijk ingevoerd. Dit kan variëren van technische oplossingen zoals firewalls en encryptie tot organisatorische maatregelen zoals training van personeel en het opstellen van noodplannen.

## AUDIT

De auditfase omvat het voorbereiden op en het uitvoeren van (externe) audits om te controleren of de organisatie voldoet aan de NIS2-richtlijn. Dit omvat het verzamelen van documentatie, het testen van systemen en processen, en het identificeren van eventuele tekortkomingen.


Dank voor het lezen van onze whitepaper over de NIS2-richtlijn. Behoefte aan meer informatie of hulp nodig bij de technische inrichting om te voldoen aan de NIS2-richtlijn?

Neem dan contact met ons op voor een vrijblijvend advies.

BTU9XvUic7s8RNIf

NIS2 QUALITY MARK

DigiTrust ISO 27001 MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING

DigiTrust NEN 7510 MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING IN DE ZORG

Volg jij ons al?