eshgro

# NIS2 en de impact op jouw organisatie

NIS2 en de impact op de (hele) keten

# Waarom NIS2?

Cyberaanvallen worden steeds geavanceerder en gerichter. Niet alleen grote organisaties, maar ook het mkb en hun toeleveranciers worden steeds vaker slachtoffer van digitale dreigingen. Landen zoals Rusland, Noord-Korea, Iran en China richten zich op supply chains, kritieke infrastructuur en bedrijven van alle groottes. Dit brengt enorme risico's met zich mee voor data, bedrijfsvoering en reputatie.

Om deze dreigingen tegen te gaan, heeft de Europese Unie de NIS2-richtlijn ingevoerd. Deze verplicht landen om hun cybersecurity naar een hoger niveau te tillen en risico's in hun keten te beheersen. NIS2 is niet alleen een juridische verplichting, maar ook een essentiële stap richting een veiliger en veerkrachtiger digitaal ecosysteem. Bedrijven die nu actie ondernemen, beschermen niet alleen zichzelf, maar versterken ook het vertrouwen bij hun klanten en partners.

# Inhoudsopgave

# NIS2 in het kort

Bron: Rijksinspectie Digitale Infrastructuur (RDI)

## “Nieuwe Europese richtlijn verplicht dat bedrijven hun cybersecurity op orde hebben.”

NIS2 staat voor Network and Information Security en heeft als doel de digitale weerbaarheid van essentiële en belangrijke sectoren in Europa te versterken. In Nederland wordt deze richtlijn omgezet in de **Cyberbeveiligingswet**. Dit betekent dat veel bedrijven verplicht maatregelen moeten nemen op het gebied van cybersecurity.

NIS2 plichtige bedrijven moeten hun digitale infrastructuur en systemen beveiligen, procedures opzetten voor het melden van incidenten, regelmatig beveiligingsprotocollen evalueren en bijwerken en actief samenwerken met overheidsinstanties en belanghebbenden.

## “Het is belangrijk dat alle NIS2 plichtige organisaties en bedrijven in de keten samenwerken.”

De NIS2-richtlijn beperkt zich niet tot de bedrijven die er direct onder vallen. **Ook hun leveranciers en partners** krijgen ermee te maken. De **ketenzorgplicht** van NIS2 eist dat organisaties niet alleen hun eigen beveiliging op orde hebben, maar ook actief bijdragen aan de digitale veiligheid van hun toeleveringsketen. Het NIS2-wetsartikel 21.2d stelt dat bedrijven verplicht zijn om risico’s binnen de keten te beheersen. Dit betekent dat leveranciers, vaak mkb-bedrijven, aantoonbaar moeten werken aan hun digitale veiligheid.

Als NIS2 plichtig bedrijf moet je er dus voor zorgen dat jouw leveranciers veilig werken, om cyberincidenten in de keten te voorkomen. Dit vereist heldere afspraken en naleving van strikte beveiligingsmaatregelen. Voor leveranciers betekent dit dat ze aan deze afspraken moeten voldoen. Zonder aantoonbare cybersecuritymaatregelen lopen zij het risico om klanten te verliezen.

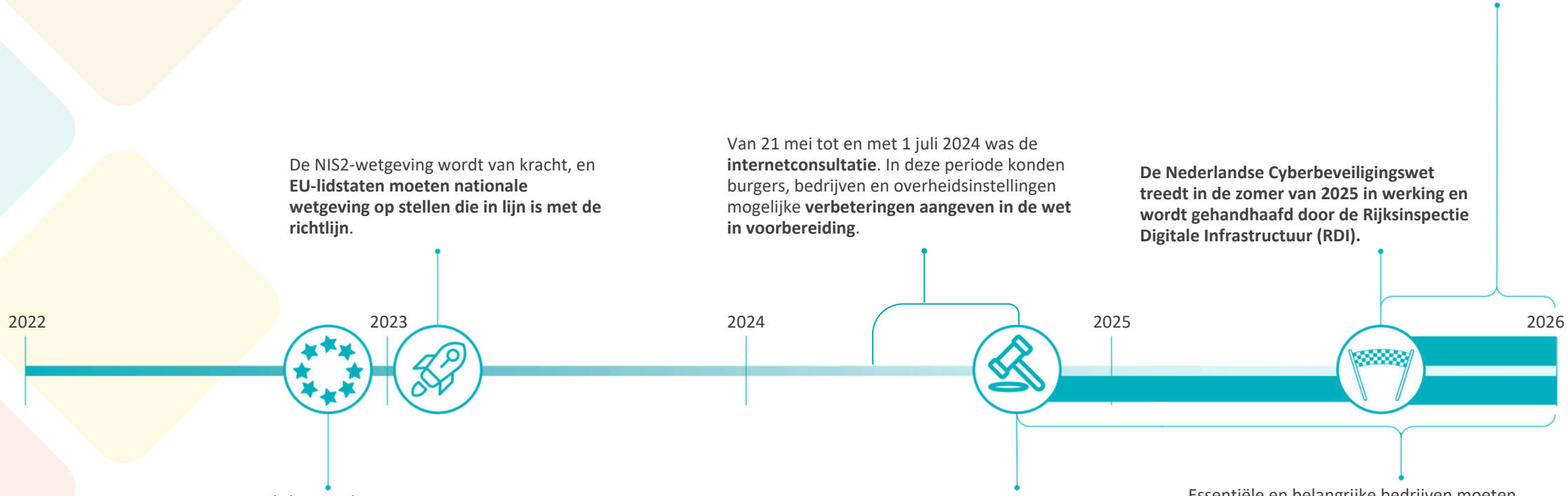
**De impact van NIS2 reikt dus verder dan alleen de bedrijven die onder de wet vallen. De hele keten wordt verantwoordelijk gehouden voor een hoger niveau van digitale veiligheid.**

# NIS2 **tijdlijn**

Bronnen: NCSC & Digitale Overheid

**Essentiële en belangrijke bedrijven in Nederland moeten voldoen aan NIS2, anders riskeren ze aanzienlijke boetes (zie pagina 10)**

Daarnaast zijn Managed Service Providers (MSP's), zoals Eshgro, onder NIS2 verplicht om ervoor te zorgen dat hun klanten adequate en efficiënte beveiligingsmaatregelen hebben. MSP's hebben een 'zorgplicht', wat betekent dat ze (financieel) aansprakelijk kunnen worden gesteld als hun klanten slachtoffer worden van cyberaanvallen.



# Deze organisaties moeten voldoen aan NIS2

Bron: Digital Trust Center (DTC)

NIS2 richt zich op organisaties en instellingen met een belangrijke maatschappelijke functie.

**NIS2 is van toepassing op de volgende doelgroepen:**

1. Essentiële organisaties
2. Belangrijke organisaties
3. Ketenpartners van essentiële of belangrijke organisaties
4. Kleine bedrijven die vallen onder de uitzondering (strategische doelwitten)
5. Apart aangewezen organisaties

## 1. Essentiële entiteiten zijn grote* organisaties en bevinden zich in de volgende sectoren:


Energie


Vervoer


Bankwezen


Infrastructuur voor de financiële markt


Drinkwater


Afvalwater


Digitale infrastructuur


Beheer van ICT-diensten


Gezondheidszorg


Overheid


Ruimtevaart

*__Een organisatie is ‘groot’ als er:__ Min. 250 medewerkers zijn **of;** een jaaromzet van €50+ miljoen en een balanstotaal van €43+ miljoen.

## 2. Belangrijke entiteiten zijn grote of middelgrote* organisaties en bevinden zich in de volgende sectoren:


Post- en koeriersdiensten


Afvalstoffenbeheer


Levensmiddelen


Maakindustrie


Chemische stoffen


Onderzoek

**+ Alle middelgrote bedrijven in essentiële sectoren**

*__Een organisatie is ‘middelgroot’ als er:__ Min. 50 medewerkers zijn **of;** een jaaromzet van €10+ miljoen en een balanstotaal van €10+ miljoen.

### 3. Ketenpartners

Niet alleen grote bedrijven vallen onder de NIS2-richtlijn. **Ook leveranciers en dienstverleners die onderdeel zijn van de toeleveringsketen van een essentiële of belangrijke organisatie** moeten voldoen aan de nieuwe cybersecurity-eisen. Dit geldt zelfs voor bedrijven die zelf niet in een kritieke sector actief zijn of minder dan 50 medewerkers hebben. Waarom? Omdat cyberaanvallen vaak via de **zwakste schakel** binnenkomen. In het verleden zijn grote incidenten begonnen bij een leverancier met onvoldoende beveiliging. Daarom verplicht de NIS2 richtlijn bedrijven om strengere eisen te stellen aan hun partners. Dit betekent dat ook kleinere bedrijven aantoonbaar hun cybersecurity op orde moeten hebben – niet alleen om risico's te beperken, maar ook om te blijven voldoen aan de eisen van hun klanten.

### 4. Uitgezonderde kleine bedrijven

Sommige kleinere bedrijven vallen niet direct onder de standaard NIS2-categorieën, maar moeten alsnog aan de regelgeving voldoen. Dit geldt vooral voor organisaties die een belangrijke rol spelen in de digitale infrastructuur en daardoor een aantrekkelijk doelwit zijn voor cyberaanvallen. Denk aan bedrijven die toplevel-domeinnamen beheren, domeinnaamregistraties aanbieden, of openbare communicatienetwerken en -diensten leveren. Daarnaast vallen ook overheidsinstanties binnen deze sectoren automatisch onder NIS2.

### 5. Apart aangewezen uitzonderingen

Val je niet in een van de eerder genoemde categorieën? Dan is het alsnog mogelijk dat je te maken krijgt met NIS2. De overheid kan namelijk organisaties aanwijzen die bij uitzondering toch hieraan moeten voldoen.

## Waarom raakt NIS2 ons allemaal?

NIS2-bedrijven zijn sterk afhankelijk van de veiligheid van hun toeleveranciers. Een cyberincident bij één partij kan grote gevolgen hebben voor de hele keten. Daarom stelt NIS2 strengere eisen aan leveranciers om verstoringen te voorkomen. Uit onderzoek van SamenVeiligDigitaal blijkt dat **70.000 mkb bedrijven NIS2-leverancier zijn.** Dit betekent dat veel bedrijven – zelfs als ze zelf geen NIS2-entiteit zijn – toch te maken krijgen met de strengere beveiligingsregels.



### "Elk cyberincident kan de keten verstoren."

De supply chain is het meest kwetsbaar op de zwakste plek. En dat is precies waar hackers naar zoeken. Zelfs een klein foutje bij een leverancier kan grote gevolgen hebben voor een bedrijf met een belangrijke functie in onze samenleving.

# NIS2 plichten

## Registratieplicht

Bedrijven die onder NIS2 vallen, zijn verplicht zich te registreren in het entiteitenregister. Dit register geeft inzicht in welke organisaties onder de wetgeving vallen en of ze voldoen aan de juiste cybersecurity-eisen. Het Nationaal Cyber Security Centrum (NCSC) biedt hiervoor een online registratievoorziening. Sinds 17 oktober 2024 is vrijwillige registratie mogelijk via www.ncsc.nl, maar dit wordt met ingang van NIS2 verplicht.

Meer informatie: NCSC Infosheet Registratieplicht

## Zorgplicht

De Cyberbeveiligingswet verplicht organisaties om een risicoanalyse uit te voeren en op basis daarvan passende beveiligingsmaatregelen te nemen voor hun netwerk- en informatiesystemen. (zie volgende pagina) Dit betekent dat bedrijven actief hun digitale weerbaarheid moeten verbeteren.

Meer informatie: NCSC Infosheet Zorgplicht

## Meldplicht

Onder NIS2 moeten organisaties significante incidenten binnen 24 uur melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Binnen 72 uur volgt een gedetailleerd rapport en na een maand een eindverslag.
Het Nationaal Cyber Security Centrum (NCSC) heeft hiervoor een Meldportaal ingericht. Dit is ook geschikt voor vrijwillige meldingen van minder ernstige incidenten of bijna-incidenten. De exacte drempelwaarden voor meldplichtige incidenten worden nog verder uitgewerkt.

Meer informatie: NCSC Infosheet Meldplicht

## Toezicht

Op organisaties die onder de Cyberbeveiligingswet vallen wordt toezicht gehouden. Hierbij wordt gekeken naar de naleving van de verplichtingen uit de Cyberbeveiligingswet, zoals de zorg- en meldplicht. Sancties richten zich tot de entiteit maar kunnen in een uiterst geval ook de individuele bestuurders raken.

# Zorgplicht

Bron: Nationaal Cyber Security Centrum

**Maatregel 1** Een risicoanalyse en beveiliging van informatiesystemen;

**Maatregel 2** Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets;

**Maatregel 3** Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen;

**Maatregel 4** Incidentenbehandeling;

**Maatregel 5** Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging;

**Maatregel 6** Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden, met 24/7 monitoring en beveiliging.

**Maatregel 7** Beveiliging van de toeleverancierskеten;

**Maatregel 8** Beleid en procedures over het gebruik van cryptografie en encryptie;

**Maatregel 9** Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie

**Maatregel 10** Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen.

## Boetes

Voldoet een organisatie niet aan de NIS2-richtlijn? Dan kan de sectorale toezichthouder boetes opleggen. De hoogte van deze boetes wordt bepaald door de ernst van de overtreding en kan fors oplopen:

Essentiële organisaties: minimaal €10 miljoen of 2% van de wereldwijde jaaromzet (het hoogste bedrag geldt).
Belangrijke organisaties: minimaal €7 miljoen of 1,4% van de wereldwijde jaaromzet.

**Bestuurders persoonlijk aansprakelijk**

Een belangrijke wijziging onder NIS2 is dat bestuurders hoofdelijk aansprakelijk zijn voor naleving van de wetgeving. Dit betekent dat zij niet kunnen terugvallen op beslissingen van anderen – de verantwoordelijkheid ligt direct bij het bestuur. NIS2 is daarmee niet alleen een IT-vraagstuk, maar een strategische prioriteit voor de hele organisatie.

# Klaar voor NIS2?

Samen met Eshgro zet je de stappen om te voldoen aan de minimale NIS2-eisen en je IT-omgeving optimaal te beschermen tegen toenemende cyberdreigingen. Wij zorgen ervoor dat je security up-to-date blijft, zodat jij je kunt focussen op je business.