

GRATIS E-BOOK

NIS2

Wat je echt moet regelen

Het begrijpelijke NIS2-overzicht voor bestuurders en IT,
zonder juridisch jargon.

ACTUEEL

De Cyberbeveiligingswet is aangenomen en treedt op 15 augustus 2026 in werking.

Een uitgave van

Leasa IT

leasa-it.nl

Het begrijpelijke NIS2-overzicht voor bestuurders en IT - zonder juridisch jargon

Een gratis uitgave van Leasa IT

Voor wie is dit e-book? Voor bestuurders, directeuren, IT-managers en compliance-verantwoordelijken die weten dat NIS2 nu wet is, maar door de bomen het bos niet meer zien. Geen juristentaal, wel concrete antwoorden: geldt het voor mij, wat moet ik regelen, en waar begin ik?

Voorwoord - waarom NIS2, en waarom nu

Actueel: Op 7 juli 2026 nam de Eerste Kamer de Cyberbeveiligingswet aan, de Nederlandse invulling van NIS2. De wet treedt in werking op **15 augustus 2026, zonder overgangperiode**. Vanaf dat moment gelden de verplichtingen direct. Voorbereiden kan dus niet langer wachten.

Cyberincidenten zijn niet langer iets dat "andere bedrijven" overkomt. Een gegijzeld netwerk, een datalek met patiëntgegevens, een leverancier die gehackt wordt en jou meesleurt - het is dagelijkse realiteit geworden. De Europese Unie trekt daarom de teugels aan met een nieuwe richtlijn: **NIS2**.

Het doel is simpel: organisaties die belangrijk zijn voor de samenleving en economie moeten hun digitale weerbaarheid op orde hebben. Niet vrijblijvend, maar als wettelijke plicht, met toezicht, boetes en persoonlijke verantwoordelijkheid voor bestuurders.

De grootste misvatting? Dat NIS2 "iets voor de IT-afdeling" is. Dat is het niet. NIS2 is een **bestuurskwestie** geworden. En de tijd om je voor te bereiden is **nú** - niet als de toezichthouder voor de deur staat.

In dit e-book leggen we in begrijpelijke taal uit wat NIS2 van je vraagt, of het op jouw organisatie van toepassing is, en welke stappen je concreet kunt zetten.

Disclaimer: Dit e-book is bedoeld als praktische introductie en vormt geen juridisch advies. Wetgeving en exacte data kunnen wijzigen. Laat je specifieke situatie altijd toetsen door een deskundige.

1. NIS2 in het kort

NIS2 staat voor de tweede **Network and Information Security**- richtlijn van de Europese Unie. Het is de opvolger van de eerste NIS-richtlijn uit 2016, die te beperkt en te vrijblijvend bleek.

De kern in drie zinnen:

1. NIS2 verplicht organisaties om passende maatregelen te nemen tegen cyberrisico's.
2. NIS2 verplicht je om ernstige incidenten te melden bij de toezichthouder.
3. NIS2 maakt het **bestuur** verantwoordelijk en aansprakelijk voor naleving.

Een richtlijn, een nationale wet. NIS2 is een Europese richtlijn. Elk land vertaalt die naar eigen wetgeving. In Nederland gebeurt dat via de **Cyberbeveiligingswet** (CBW- de opvolger van de Wet beveiliging netwerk- en informatiesystemen). Deze wet is op 7 juli 2026 aangenomen en treedt in werking op **15 augustus 2026, zonder overgangsperiode**. De plichten die we in dit e-book beschrijven, gelden via die Nederlandse wet.

Twee categorieën organisaties. NIS2 maakt onderscheid tussen:

- **Essentiële entiteiten** - de zwaarste categorie (bijv. energie, drinkwater, gezondheidszorg, digitale infrastructuur). Strenger toezicht, hogere boetes.
- **Belangrijke entiteiten** - eveneens verplicht, maar met iets lichter toezicht (bijv. post, afvalbeheer, levensmiddelen, bepaalde productie en digitale aanbieders).

Beide categorieën moeten aan dezelfde zorgplicht en meldplicht voldoen. Het verschil zit vooral in de zwaarte van het toezicht en de sancties.

2. Geldt NIS2 voor mijn organisatie?

Veel organisaties denken "dat zal voor ons wel niet gelden" - en hebben het mis. NIS2 raakt veel meer sectoren dan de eerste richtlijn. Loop deze beslisboom door:

Stap 1 - Zit mijn sector erin?

NIS2 dekt onder meer: energie, transport, bankwezen en financiële markten, **gezondheidszorg**, drinkwater en afvalwater, digitale infrastructuur, ICT-dienstverlening, overheid, ruimtevaart, post- en koeriersdiensten, afvalbeheer, chemie, levensmiddelen, productie/maakindustrie, digitale aanbieders (zoals online platforms en clouddiensten) en onderzoek.

Stap 2 - Ben ik groot genoeg?

NIS2 geldt in beginsel voor **middelgrote en grote** organisaties. De vuistregel:

- **50 of meer medewerkers, óf**
- meer dan **EUR 10 miljoen** jaaromzet én balanstotaal.

Stap 3 - Geldt er een uitzondering?

Sommige organisaties vallen er ongeacht hun omvang onder, omdat ze cruciaal zijn (bijvoorbeeld bepaalde aanbieders van digitale infrastructuur of de enige aanbieder van een dienst in een regio). Twijfel je, ga dan uit van "waarschijnlijk wel" en laat het toetsen.

Let op de keten. Ook als je zelf nét buiten de scope valt, kun je er indirect mee te maken krijgen. Want organisaties die wél onder NIS2 vallen, moeten de **veiligheid van hun toeleveranciers** waarborgen. Grote kans dat je klanten dan eisen aan jou gaan stellen. NIS2 werkt door in de hele keten.

Registratieplicht. Organisaties die onder NIS2 vallen, moeten zich registreren bij de bevoegde toezichthouder. Wachten tot je "ontdekt" wordt is geen strategie - de plicht ligt bij jou.

3. Wat eist NIS2 concreet?

NIS2 rust op drie pijlers: de zorgplicht, de meldplicht en de bestuursverantwoordelijkheid.

Pijler 1 - De zorgplicht (risicomaatregelen)

Je moet "passende en evenredige" maatregelen nemen om je netwerk- en informatiesystemen te beveiligen. De wet noemt onder andere:

- **Risicoanalyse en informatiebeveiligingsbeleid** - weet welke risico's je loopt en leg beleid vast.
- **Incidentafhandeling** - processen om incidenten te detecteren, te beheersen en op te lossen.
- **Bedrijfscontinuïteit** - back-ups, herstelplannen, crisismanagement.
- **Beveiliging van de toeleveringsketen** - afspraken met leveranciers over hun beveiliging.
- **Veiligheid bij aanschaf, ontwikkeling en onderhoud** van systemen (inclusief omgang met kwetsbaarheden).
- **Beleid om de effectiviteit** van maatregelen te toetsen.
- **Basale cyberhygiëne en bewustwordingstraining** voor medewerkers.
- **Cryptografie en versleuteling** waar passend.
- **Toegangsbeleid** en beheer van bevoegdheden.
- **Multifactor-authenticatie (MFA)** en beveiligde communicatie.

Kort samengevat: techniek, processen én mensen, alle drie.

Pijler 2 - De meldplicht (incidenten melden)

Bij een **significant incident** gelden strakke termijnen:

- **Binnen 24 uur:** een eerste melding (vroegtijdige waarschuwing).
- **Binnen 72 uur:** een vollediger incidentmelding met eerste beoordeling.
- **Binnen 1 maand:** een eindrapportage.

Een incident is "significant" als het ernstige operationele verstoring of financiële schade veroorzaakt, of andere personen/organisaties raakt. Je moet dus vooraf weten wie wat meldt, en hoe anders haal je die 24 uur nooit.

Pijler 3 - De bestuursverantwoordelijkheid

Dit is de grote verandering ten opzichte van vroeger. Het bestuur moet de risicomatregelen **goedkeuren, toezicht houden op de uitvoering**, en mag zich niet verschuilen achter de IT-afdeling. Bovendien moeten bestuurders **scholing** volgen om cyberrisico's te kunnen beoordelen. Hierover meer in het volgende hoofdstuk.

4. De bestuurder is aansprakelijk - wat dat betekent

Onder NIS2 verschuift cybersecurity van de serverruimte naar de bestuurstafel. Concreet:

- **Het bestuur keurt de maatregelen goed en houdt er toezicht op.** Niet de IT-manager, maar de bestuurder is eindverantwoordelijk.
- **Bestuurders kunnen persoonlijk aansprakelijk worden gesteld** bij nalatigheid. Voor essentiële entiteiten kan een toezichthouder zelfs verdergaande maatregelen treffen richting leidinggevenden.
- **Bestuurders moeten training volgen** om cyberrisico's te begrijpen en af te wegen.
- **De boetes zijn fors.** Voor essentiële entiteiten kunnen ze oplopen tot in de orde van **EUR 10 miljoen of 2% van de wereldwijde jaaromzet** (het hoogste van de twee); voor belangrijke entiteiten ligt het iets lager. Maar het echte risico is breder: reputatieschade, aansprakelijkheid en verlies van klanten die compliance van je eisen.

De boodschap voor de bestuurskamer: "dat regelt IT wel" is geen verdediging meer. Wie nu niets doet, neemt een persoonlijk risico.

5. NIS2 vs. NEN 7510 vs. ISO 27001 - hoe verhouden ze zich?

Veel organisaties - zeker in de zorg - werken al met **NEN 7510** of **ISO 27001**. Goede basis. Maar dekt dat NIS2? Gedeeltelijk. Het verschil in één tabel:

	NIS2	ISO 27001	NEN 7510
Wat is het?	Europese wet/richtlijn	Internationale norm (certificeerbaar)	Nederlandse norm voor de zorg
Verplicht?	Ja, bij wet (in scope)	Nee, vrijwillig	Feitelijk verplicht in de zorg
Focus	Wettelijke plichten: zorgplicht, meldplicht, bestuur	Managementsysteem voor informatiebeveiliging (ISMS)	ISMS specifiek voor patiënt-/gezondheidsdata
Meldplicht aan toezichthouder?	Ja (24u/72u/1mnd)	Nee	Nee
Bestuurs-aansprakelijkheid ?	Ja, expliciet	Nee	Nee

De kern: ISO 27001 en NEN 7510 geven je een sterk raamwerk (een managementsysteem) dat een groot deel van de NIS2-zorgplicht invult. Maar ze dekken **niet** de wettelijke extra's van NIS2: de registratieplicht, de meldplicht met harde termijnen, en de bestuursverantwoordelijkheid.

Met andere woorden: ben je ISO- of NEN-gecertificeerd, dan heb je een voorsprong - maar je bent er niet automatisch mee NIS2-compliant. (In aparte e-books gaan we dieper in op NEN 7510 en ISO 27001 - houd onze kanalen in de gaten.)

6. De 10 meest gemaakte fouten

1. **"NIS2 geldt niet voor ons" - zonder het te checken.** De scope is breder dan gedacht, en de keten trekt je er alsnog in.
2. **Het zien als een IT-project.** Het is een bestuurs- en organisatievraagstuk.
3. **De leverancierketen vergeten.** Je bent zo zwak als je zwakste toeleverancier.
4. **Geen meldproces klaar hebben.** Zonder draaiboek haal je de 24-uurstermijn nooit.
5. **Alleen techniek aanpakken, mensen overslaan.** De meeste incidenten beginnen bij een medewerker.
6. **Bestuur niet betrekken of trainen.** Terwijl de wet dat juist eist.
7. **Denken dat je nog tijd hebt.** De Cyberbeveiligingswet is aangenomen en gaat 15 augustus 2026 in, zonder overgangsperiode. De maatregelen kosten maanden; uitstel is risico.
8. **Geen aantoonbaarheid.** Maatregelen die je niet kunt documenteren, tellen bij een audit niet mee.
9. **Eenmalig "afvinken".** Compliance is een doorlopend proces, geen project met einddatum.
10. **Alles zelf willen doen, zonder capaciteit.** Onderschatting van tijd en kennis is de grootste valkuil.

7. Praktische checklist - ben ik NIS2-klaar?

Loop deze lijst door. Elke "nee" is een actiepoint.

Scope & organisatie

- ☐ Ik weet of mijn organisatie onder NIS2 valt (sector + omvang).
- ☐ Ik ben (indien nodig) geregistreerd bij de toezichthouder.
- ☐ Het bestuur is betrokken en op de hoogte van zijn verantwoordelijkheid.
- ☐ Bestuurders hebben (basis)scholing over cyberrisico's gehad.

Zorgplicht (maatregelen)

- ☐ Er is een actuele risicoanalyse en informatiebeveiligingsbeleid.
- ☐ Back-up- en herstelplannen zijn aanwezig en getest.
- ☐ MFA en toegangsbeleid zijn ingevoerd.
- ☐ Afspraken met leveranciers over beveiliging zijn vastgelegd.
- ☐ Medewerkers krijgen bewustwordings-/awarenesstraining.
- ☐ Maatregelen worden periodiek op effectiviteit getoetst.

Meldplicht

- ☐ Er is een incident-meldproces met duidelijke rollen.
- ☐ Iedereen weet wie binnen 24 uur de melding doet.

Aantoonbaarheid

- ☐ Alle maatregelen zijn gedocumenteerd en actueel.
- ☐ Ik kan bij een audit aantonen dat het beleid ook echt wordt uitgevoerd.

Vink je hier niet alles aan? Dan is er werk aan de winkel en dat is precies waar het volgende hoofdstuk over gaat.

8. Van weten naar aantoonbaar voldoen

Hier zit de echte uitdaging. Ná het lezen van dit e-book begrijp je NIS2. Maar begrijpen is iets anders dan **aantoonbaar voldoen**. Het verschil:

- **Weten** is een checklist doorlopen.
- **Doen** is beleid schrijven, techniek inrichten, leveranciers contracteren, medewerkers en bestuur trainen, een meldproces opzetten - en dat allemaal documenteren zodat het een audit doorstaat. En het vervolgens blijven onderhouden.

Voor de meeste organisaties is dat maanden werk, met kennis en capaciteit die er intern vaak niet (volledig) is. En juist daar zit het risico: de tijd dringt, de aansprakelijkheid ligt bij het bestuur, en half werk telt bij een toezichthouder niet.

Hoe Leasa IT hierbij helpt. Wij leveren werkplekken als dienst waarin beveiliging en compliance van begin af aan zijn ingebouwd - voldoende aan NEN 7510 en NIS2. Daarbij ondersteunen we met:

- **Gap- en projecttooling** om helder te krijgen waar je nu staat en wat er nog moet gebeuren.
- **Bestuurderstrainingen** zodat je voldoet aan de scholingsplicht.
- **Awareness-/securitytrainingen** voor je medewerkers - de menselijke firewall.
- **Beheer, monitoring en updates** zodat compliance geen eenmalig project is, maar geborgd blijft.

Zo verschuift de last van "alles zelf uitzoeken en bijhouden" naar "het is geregeld, en aantoonbaar".

9. De volgende stap

NIS2 is geen reden voor paniek, maar wél voor actie. De organisaties die nú beginnen, zijn straks klaar zonder stress en stralen vertrouwen uit naar klanten en toezichthouders.

Wil je weten waar jouw organisatie staat?

Plan een **gratis, vrijblijvend gap-gesprek** met Leasa IT. In een halfuur brengen we samen in kaart waar je nu staat ten opzichte van NIS2, en wat de meest logische volgende stappen zijn - zonder verplichtingen.

Plan je gratis gap-gesprek op leasa-it.nl

Leasa IT - Veilige, compliant werkplekken zonder gedoe. Van device tot bestuurskamer.