GRATIS E-BOOK

NIS2

Wat je echt moet regelen

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

Een uitgave van

Leasa IT

leasa-it.nl

> Voor wie is dit e-book? Voor bestuurders, directeuren, IT-managers en compliance-verantwoordelijken die weten dat NIS2 eraan komt, 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

Cyberincidenten zijn niet langer iets dat 'andere bedrijven' overkomt. Een gegijzeld netwerk, een datalek met patientgegevens, 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 nu - 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:

- NIS2 verplicht organisaties om passende maatregelen te nemen tegen cyberrisico's.
- NIS2 verplicht je om ernstige incidenten te melden bij de toezichthouder.
- 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 (de opvolger van de Wet beveiliging netwerk- en informatiesystemen). De plichten die we hier beschrijven, gelden via die Nederlandse wet.

Twee categorieen organisaties. NIS2 onderscheidt essentiele entiteiten (de zwaarste categorie - bijv. energie, drinkwater, gezondheidszorg, digitale infrastructuur; strenger toezicht, hogere boetes) en belangrijke entiteiten (eveneens verplicht, iets lichter toezicht - bijv. post, afvalbeheer, levensmiddelen, bepaalde productie). Beide moeten aan dezelfde zorgplicht en meldplicht voldoen.

2. Geldt NIS2 voor mijn organisatie?

Veel organisaties denken 'dat zal voor ons wel niet gelden' - en hebben het mis. Loop deze stappen door:

Stap 1 - Zit mijn sector erin?

NIS2 dekt onder meer: energie, transport, bankwezen en financiele markten, gezondheidszorg, drinkwater en afvalwater, digitale infrastructuur, ICT-dienstverlening, overheid, ruimtevaart, post- en koeriersdiensten, afvalbeheer, chemie, levensmiddelen, productie/maakindustrie, digitale aanbieders

en onderzoek.

Stap 2 - Ben ik groot genoeg?

NIS2 geldt in beginsel voor middelgrote en grote organisaties. De vuistregel: 50 of meer medewerkers, OF meer dan EUR 10 miljoen jaaromzet en balanstotaal.

Stap 3 - Geldt er een uitzondering?

Sommige organisaties vallen er ongeacht hun omvang onder, omdat ze cruciaal zijn. Twijfel je, ga dan uit van 'waarschijnlijk wel' en laat het toetsen.

> Let op de keten. Ook als je zelf net buiten de scope valt, kun je er indirect mee te maken krijgen. Organisaties die wel 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. De wet noemt onder andere:

- Risicoanalyse en informatiebeveiligingsbeleid.
- Incidentafhandeling - detecteren, beheersen en oplossen.
- Bedrijfscontinuiteit - back-ups, herstelplannen, crisismanagement.
- Beveiliging van de toeleveringsketen - afspraken met leveranciers.
- Veiligheid bij aanschaf, ontwikkeling en onderhoud van systemen.
- Beleid om de effectiviteit van maatregelen te toetsen.
- Basale cyberhygiene en bewustwordingstraining voor medewerkers.
- Cryptografie en versleuteling waar passend.
- Toegangsbeleid, multifactor-authenticatie (MFA) en beveiligde communicatie.

Kort samengevat: techniek, processen en 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 volledigere incidentmelding met eerste beoordeling.
- Binnen 1 maand: een eindrapportage.

Je moet dus vooraf weten wie wat meldt, en hoe - anders haal je die 24 uur nooit.

Pijler 3 - De bestuursverantwoordelijkheid

Het bestuur moet de risicomaatregelen 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.

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 - de bestuurder is eindverantwoordelijk.
- Bestuurders kunnen persoonlijk aansprakelijk worden gesteld bij nalatigheid.
- Bestuurders moeten training volgen om cyberrisico's te begrijpen en af te wegen.
- De boetes zijn fors: voor essentiele entiteiten tot in de orde van EUR 10 miljoen of 2% van de wereldwijde jaaromzet; voor belangrijke entiteiten iets lager.

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

Veel organisaties werken al met NEN 7510 of ISO 27001. Goede basis. Maar dekt dat NIS2? Gedeeltelijk. Het verschil per onderwerp:

Wat is het? NIS2: een Europese wet/richtlijn. ISO 27001: een internationale norm (certificeerbaar). NEN 7510: een Nederlandse norm voor de zorg.

Verplicht? NIS2: ja, bij wet (in scope). ISO 27001: nee, vrijwillig. NEN 7510: feitelijk verplicht in de zorg.

Focus. NIS2: wettelijke plichten (zorgplicht, meldplicht, bestuur). ISO 27001: een managementsysteem voor informatiebeveiliging. NEN 7510: hetzelfde, specifiek voor zorgdata.

Meldplicht aan toezichthouder? Alleen NIS2 (24u / 72u / 1 maand).

Bestuursaansprakelijkheid? Alleen NIS2, expliciet.

> De kern: ISO 27001 en NEN 7510 geven je een sterk raamwerk 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. Ben je gecertificeerd, dan heb je een voorsprong - maar je bent niet automatisch NIS2-compliant.

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. Wachten tot de wet 'definitief' is. 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 actiepunt.

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.

8. Van weten naar aantoonbaar voldoen

Na 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 - voldoend aan NEN 7510 en NIS2. Daarbij ondersteunen we met:

- Gap- en projecttooling om helder te krijgen waar je 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 wel voor actie. De organisaties die nu 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 half uur brengen we samen in kaart waar je staat ten opzichte van NIS2 - zonder verplichtingen.

Plan je gesprek op leasa-it.nl

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