

Whitepaper

NIS2-richtlijn in Nederland

Zó ben je voorbereid op de nieuwe Cyberbeveiligingswet (CBW)

kader
Consultancy & Interim

Bekijk het op
kader.nl

In deze whitepaper vind je

Introductie 3

NIS2 in vogelvlucht 4

1. Van NIS naar NIS2 6

2. NIS2 in Nederland: wie valt onder de nieuwe richtlijn? 7

3. Mijn organisatie valt onder NIS2: waar moet ik aan voldoen? 10

4. Naar NIS2-compliance via ISO 7001-certificering 14

Contact
Heb je na het lezen van de informatie nog vragen, of wil je een offerte aanvragen?
Neem dan gerust contact met ons op.

Telefoonnummer 088 - 99 51 320
kader.nl | sales@kader.nl

Wij helpen je graag!

Introductie

Het rapport van Cybersecuritybeeld Nederland is duidelijk: de digitale veiligheid in Nederland is onderhevig aan turbulente tijden en onvoorziene effecten[1]. Steeds vaker wordt Nederland – en de rest van Europa – getroffen door cyberaanvallen. Geopolitieke omstandigheden, criminaliteit en de hogere mate van digitalisering dragen bij aan verhoogde cyberrisico's. Ook in het nieuws treden cyberaanvallen meer op de voorgrond: veel organisaties worden geraakt door DDoS-aanvallen, ransomware en diefstal van belangrijke data.

Het is een serieuze zorg voor de nationale veiligheid. Niet alleen omdat persoonsgevoelige data in handen van criminelen komt, maar ook omdat cyberaanvallen het werk kunnen verstoren van maatschappelijk belangrijke organisaties. Denk maar eens aan een apotheek groothandel die geen bestellingen kan ontvangen door een ransomware-aanval, of een ambulancepost met een communicatiestoring. Om nog maar te zwijgen over de gevolgen van een uitgeschakeld energienetwerk: hoe lang kan een ziekenhuis zonder stroom? Zijn we niet goed voorbereid, dan kan een cyberaanval desastreuze gevolgen hebben.

NIS2-richtlijn versterkt digitale weerbaarheid in Europa
Om de groeiende cyberdreiging in Europa te bestrijden, heeft de Europese Unie de NIS2-richtlijn opgesteld. Deze richtlijn is een vervolg op de eerdere NIS-regelgeving. NIS2 harmoniseert de bestaande wetgeving voor de lidstaten en tilt de cyberbeveiliging van Europa naar een hoger niveau. Daarbij worden flinke inspanningen verwacht van de sectoren die onder de NIS2-richtlijn vallen.

Toch dreigen duizenden organisaties nog omzet en klanten te verliezen door onvoldoende voorbereiding op deze nieuwe cyberbeveiligingswet[2]. En de tijd begint te dringen: sinds 17 oktober 2024 geldt de NIS2-richtlijn in de Europese Unie. Vanaf het derde kwartaal van 2025 wordt de richtlijn doorvertaald naar Nederlandse wetgeving en moeten Nederlandse organisaties die onder de richtlijn vallen aan NIS2 kunnen voldoen.

Wil jij goed voorbereid zijn op NIS2 en de digitale weerbaarheid van jouw organisatie versterken? In dit whitepaper beantwoorden we de volgende vragen:

- **Hoe verschilt NIS2 van de eerdere NIS-richtlijn?**
- **Welke sectoren moeten zich voorbereiden op NIS2?**
- **Welke stappen moet je zetten om te voldoen aan NIS2?**
- **Hoe zorgt ISO 27001-certificering voor NIS2-compliance?**

In dit whitepaper ontdek je de eisen waar een organisatie aan moet voldoen voor de nieuwe NIS2-richtlijn. Binnen de standaardmaatregelen van NIS2 zullen organisaties zich ook moeten voorbereiden op specifieke digitale veiligheidsrisico's. Ben je benieuwd wat de verplichtingen van NIS2 betekenen voor jouw organisatie? Neem gerust contact op met onze veiligheidsexperts!

Contact

1. Meer informatie lees je in het rapport van Cybersecuritybeeld Nederland 2024
2. Emerce Duizenden bedrijven dreigen klanten kwijt te raken door onvoldoende compliance aan NIS2, 19-07-2024

NIS2 in vogelvlucht

De NIS2-richtlijn:

- Maakt Europa weerbaarder tegen cyberaanvallen uit criminele en statelijke hoek.
- Richt zich op een breder aantal sectoren. Deze essentiële en belangrijke sectoren moeten zich zo snel mogelijk voorbereiden op de verplichtingen van deze nieuwe regelgeving.
- Behandelt de complete toeleveringsketen. Bedrijven die onder NIS2 vallen, moeten zorg dragen dat de diensten van hun zakenpartners de richtlijnen volgen. Ook als deze partners niet onder de richtlijn vallen.
- Ziet strenger toe op het volgen van de maatregelen en stelt het bestuur van bedrijven aansprakelijk bij onvoldoende naleving.

Nederlandse organisaties die vallen onder NIS2:

- Moeten voor Q3 2025 voldoen aan de richtlijnen
- Komen onder strenger toezicht voor het volgen van de veiligheidsmaatregelen
- Zijn verplicht te voldoen aan een zorgplicht (met risicoanalyse), meldplicht en een registratieplicht



1. Van NIS naar NIS2

Er bestaat al sinds 2016 een NIS-richtlijn. Deze richtlijn is in Nederland opgenomen in de Wbni (Wet beveiliging netwerk- en informatiesystemen). De Wbni richt zich op het versterken van de digitale weerbaarheid van Europa, onder andere via een meldplicht van digitale incidenten en een zorgplicht voor het treffen van beveiligingsmaatregelen.

De huidige wet kent ook onduidelijkheden: zo wordt er onvoldoende gecontroleerd of organisaties de richtlijnen volgen. Ook werken organisaties samen met zakenpartners die niet onder de Wbni vallen. Deze partners hoeven zich niet aan dezelfde veiligheidsstandaarden te houden. Dat betekent dat hun diensten en producten een digitaal veiligheidsrisico kunnen worden voor de organisaties die wél onder de richtlijn vallen.

De NIS2-richtlijn verdiept de veiligheidsmaatregelen en controleert strenger op de naleving ervan. Meer organisaties en sectoren zijn verplicht om de regelgeving te volgen en bij onvoldoende naleving worden de sancties verhoogd. Reden genoeg voor organisaties om hun cyberbeveiliging zo snel mogelijk te versterken. Wat zijn de belangrijkste veranderingen van NIS2? We delen hier een overzicht.

Meer organisaties vallen onder de richtlijn
De doelgroep van de NIS2-richtlijn is uitgebreid ten opzichte van de Wbni. Alle middelgrote en grote organisaties die vallen onder de 'essentiële' en 'belangrijke' sectoren moeten voldoen aan de nieuwe regelgeving. Dit zijn hoofdzakelijk aanbieders van essentiële en digitale diensten, zoals energie, transport, gezondheid, infrastructuur, maar bijvoorbeeld ook fabrikanten van digitale apparatuur. Ontdek hier of jouw organisatie valt onder de NIS2-richtlijn.

Meer aansprakelijkheid
Als een essentiële of belangrijke onderneming niet aan de NIS2-richtlijn voldoet, dan is het bestuur van de organisatie aansprakelijk. Hiermee hoopt NIS2 het digitale veiligheidsbewustzijn van organisaties te versterken vanaf de toplaag; niet alleen vanuit de IT-afdeling. Het MT moet er dus voor zorgen dat digitale veiligheid geïntegreerd wordt in de organisatie én dat er meldingen worden gedaan van incidenten. Doet het bestuur dat niet, dan riskeert de organisatie strengere sancties en boetes.

NIS2 raakt de complete toeleveringsketen
Val je niet onder NIS2, maar werk je wel samen met sectoren die onder de nieuwe richtlijn vallen? Dan is het ook raadzaam om voorbereidingen te treffen voor NIS2. Organisaties die onder NIS2 vallen, worden namelijk ook verantwoordelijk gesteld als hun zakenpartners de security niet op orde hebben. Dit is belangrijk, omdat organisaties die onder NIS2 vallen in grote mate afhankelijk kunnen zijn van specifieke zakenpartners. Organisaties zijn verplicht om deze zakenpartners mee te nemen in een risicoanalyse, zodat veiligheidsmaatregelen effectief doorvertaald worden in de relatie tussen organisatie en zakenpartner.

Strenger toezicht
Organisaties worden strenger gecontroleerd door de overheid en zijn verplicht zelf een risicobeoordeling uit te voeren en passende veiligheidsmaatregelen te nemen. Grote incidenten moeten binnen 24 uur gemeld worden bij het Nationaal Cyber Security Centrum (NCSC). Ook wordt er strenger gehandhaafd op het voldoen van rapportageverplichtingen.

2. NIS2 in Nederland: wie valt onder de nieuwe richtlijn?

De NIS2-richtlijn moet nog worden overgezet naar de Nederlandse wetgeving: de Cyberbeveiligingswet (Cbw / NIS2) en de Wet weerbaarheid kritieke entiteiten (Wwke/CER)[3]. Naar verwachting treden de nieuwe wetten in vanaf het **derde kwartaal van 2025**. Valt jouw organisatie onder deze Nederlandse NIS2-richtlijn?

Deze sectoren vallen onder NIS2[4]

De NIS2-richtlijn breidt de reikwijdte uit naar meer sectoren. De sectoren die onder NIS2 vallen, worden gedefinieerd als **essentieel** en **belangrijk**. Dit zijn veelal sectoren met een grote maatschappelijke impact. Dat is belangrijk om de nationale veiligheid te kunnen waarborgen: denk bijvoorbeeld aan de gevolgen voor de maatschappij als een bank een groot datalek heeft, of als er operationele storingen worden veroorzaakt bij een drinkwaterbedrijf. Dergelijke risico's voor de nationale veiligheid moeten zo veel mogelijk voorkomen worden of - in het ergste geval - zo snel mogelijk worden gemeld.

In onderstaand schema ontdek je welke sectoren vallen onder de NIS2-richtlijn. Liever zelf evalueren? Met de NIS2-vragenlijst opgesteld door de Rijksoverheid ontdek je of jouw organisatie onder de richtlijn valt.

Essentiële en belangrijke sectoren	
Energie - levering, distributie, transmissie en verkoop van elektriciteit, gas, olie, verwarming/ koeling, waterstof, exploitanten van EV-oplaadpunten	**Essentieel**
Transport - via lucht, spoor, weg en water (inclusief rederijen en havenfaciliteiten)	**Essentieel**
Bankieren/financiën – krediet, handel, markt en infrastructuur	**Essentieel**
Gezondheid - zorgverleners, onderzoekslaboratoria, farmaceutica, productie van medische hulpmiddelen	**Essentieel**
Water - drinkwaterleveranciers en afvalwaterbeheerders	**Essentieel**
Digitale infrastructuur en IT-diensten - DNS, naamregisters, vertrouwensdiensten, datacenters, cloud computing, elektronische communicatiediensten, beheerde diensten en beheerde veiligheidsdiensten	**Essentieel**
Openbaar bestuur - (centraal, regio's + lokaal optioneel)	**Essentieel**
Space - exploitanten van infrastructuur op de grond	**Essentieel**
Post- en koeriersdiensten aanbieders	**Belangrijk**
Afvalbeheer	**Belangrijk**
Chemische producten - productie en distributie	**Belangrijk**
Voedsel - distributie en productie	**Belangrijk**
Fabrikanten - medische/diagnostische apparaten, computers, elektronica, optica, machines, motorvoertuigen, aanhangwagens, opleggers, andere transportmiddelen	**Belangrijk**
Digitale aanbieders - online marktplaatsen, zoekmachines, sociale platforms	**Belangrijk**
Onderzoeksorganisaties	**Belangrijk**

3. Voor consistentie refereren we in dit whitepaper naar 'NIS2' als het gaat om de Nederlandse wetgeving.
4. Meer informatie over de sectoren die onder de NIS2-richtlijn vallen, vind je op de website van het NCTV.

Essentieel en belangrijk: wat is het verschil?[5]

Essentiële en belangrijke entiteiten moeten allebei voldoen aan dezelfde verplichtingen van NIS2. Het verschil zit 'm in de controle. Essentiële entiteiten worden sneller, strenger en nauwkeuriger gecontroleerd door de overheid. Ook vallen de boetes voor essentiële entiteiten hoger uit dan voor belangrijke entiteiten. De sector en grootte bepalen of een organisatie een essentiële of belangrijke entiteit is.

Type organisatie	Essentieel of belangrijk voor NIS2?
Grote organisaties • Minimaal 250 medewerkers of • een jaaromzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro	Behoor je tot een essentiële sector? Dan ben je een essentiële entiteit. Behoor je tot een belangrijke sector? Dan ben je een belangrijke entiteit.
Middelgrote organisaties • Minimaal 50 medewerkers of • een jaaromzet van meer dan 10 miljoen euro en een balanstotaal van meer dan 10 miljoen euro	Middelgrote organisaties onder de NIS2-richtlijn zijn altijd een belangrijke entiteit. Ook als jouw organisatie behoort tot een essentiële sector.
Micro- en kleinbedrijven • Minder dan 50 werknemers • Een jaaromzet van hooguit 2 miljoen euro en een balanstotaal kleiner of gelijk aan 2 miljoen euro	Je valt niet onder de NIS2-richtlijn. Bij uitzondering neemt het ministerie contact op met jouw organisatie voor een risicobeoordeling.

5. We hanteren de definitie zoals gesteld door de Europese Unie. Bij overgang naar de Nederlandse wetgeving kan deze definitie nog aangepast worden.



3. Mijn organisatie valt onder NIS2: waar moet ik aan voldoen?

Valt jouw organisatie onder de NIS2-richtlijn of werk je samen met organisaties die onder de richtlijn vallen? Dan is het raadzaam om je zo snel mogelijk voor te bereiden op de vereisten van deze nieuwe wetgeving. De voorbereidingen voor de NIS2-richtlijn zijn samengevat in drie plichten:

- Registratieplicht
- Zorgplicht
- Meldplicht

We behandelen de algemene stappen die je moet nemen om aan de plichten te kunnen voldoen. De exacte veiligheidsmaatregelen verschillen per bedrijf. Bedenk dus hoe NIS2-richtlijn van toepassing is op jouw organisatie. Uiteraard kunnen de veiligheidsexperts van Kader altijd ondersteunen en adviseren in het pad naar NIS2-compliance.

1. Registratieplicht: snelle communicatie binnen de sector

Alle essentiële en belangrijke organisaties moeten zich verplicht registreren in het entiteiten register van het Nationaal Cyber Security Centrum (NSCS). Zo heeft dit centrale orgaan de contactgegevens van alle essentiële organisaties overzichtelijk. Dat biedt verschillende voordelen: snelle communicatie binnen de sector én meer inzicht in de cyberdreigingen per sector!

Wordt een energiecentrale geraakt door een cyberaanval? Dan kunnen de autoriteiten direct alle organisaties binnen de energiesector waarschuwen. Op lange termijn kunnen deze aanvallen doorvertaald worden naar learnings voor de rest van de sector. Welke dreigingen komen het meest voor en hoe kunnen organisaties hierop nog beter anticiperen? Doordat entiteiten van alle lidstaten zich moeten registreren, levert de registratieplicht ook een Europees beeld op van alle organisaties die onder NIS2 vallen.

Voorbereiding
Registreren doe je via de website van het Nationaal Cyber Security Centrum (NSCS). Dit is verplicht zodra de Nederlandse wetgeving in 2025 in werking treedt. Organisaties kunnen zich nu al vrijwillig registreren, dus je kunt je tijdig voorbereiden op de registratieplicht. Een NIS2-registratie vraagt om een aantal specifieke organisatie- en netwerkgegevens. Goed voorbereid voldoen aan de registratieplicht? Met de checklist van het NSCS ontdek je alle details over het verzamelen en registreren van de nodige gegevens.

2. Zorgplicht: bescherm netwerk- en informatiesystemen tegen incidenten

De zorgplicht stelt tien standaard veiligheidsmaatregelen waar organisaties in ieder geval aan moeten voldoen. Van het maken van een risicoanalyse, tot het zorgdragen dat medewerkers opgeleid worden om cyberrisico's te kunnen spotten en voorkomen. Onder de zorgplicht valt ook de aansprakelijkheid van het bestuur. Dat betekent dat het bestuur verantwoordelijk wordt gehouden voor de digitale veiligheid van de organisatie.

Voorbereiding

Maak een risicoanalyse.

NIS2 verplicht organisaties om een risicoanalyse te maken van de veiligheidsbelangen, dreigingen en de huidige weerbaarheid van de organisatie. Je ontdekt welke risico's de organisatie heeft, en hoe je daarmee moet omgaan. Een risicoanalyse is specifiek: de uitdagingen voor jouw organisatie zullen verschillen van andere organisaties.

Neem maatregelen op basis van de analyse.

De risico's van jouw organisatie zijn in kaart gebracht. Nu is het belangrijk om passende maatregelen te nemen. Uiteindelijk moet jouw organisatie voldoen aan de 10 standaardmaatregelen, maar misschien zijn een aantal maatregelen al voorbereid. Misschien is jouw interne digitale veiligheid op orde, maar is de toeleverancierskеten onvoldoende op de hoogte. En hoe zit het met de kennis van jouw medewerkers omtrent informatiebeveiliging?

Ontwikkel een noodplan.

Maak een actieplan waarmee medewerkers een storing snel kunnen signaleren en communiceren: dit is een incident respons plan. Wie is er verantwoordelijk voor het uitroepen van het incident? Moeten externe IT partners op de hoogte gesteld worden van je storingsbeleid en hoe maak je dat realistisch binnen 24 uur? En wie voldoet aan de rapportageplicht nadat een incident heeft plaatsgevonden?

Onthoud ook dat jouw externe partners misschien niet aan de NIS2-richtlijn hoeven te voldoen. NIS2 stelt je verantwoordelijk om je maatregelen en risico's door te vertalen naar de ketens waarmee je samenwerkt. Neem je bijvoorbeeld digitale elektronica af van een fabrikant? Zorg dan dat je risicogebaseerde maatregelen doorvertaalt aan de fabrikant.

Onder de zorgplicht vallen de volgende 10 maatregelen[6]

Maatregel 1: 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;

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 en beveiligde noodcommunicatiesystemen;

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

6. De voorbereidingsmaatregelen voor de NIS2 zorgplicht zijn afkomstig van het National Cyber Security Centrum.

3. Meldplicht: meld significante incidenten binnen 24 uur

Alle geregistreerde entiteiten moeten binnen 24 uur melding doen van een storing als er sprake is van een 'significant incident'. Dit zijn incidenten die een ernstige operationele verstoring veroorzaken of zorgen voor grote financiële verliezen van de organisatie. Deze storingen moeten gemeld worden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Dit expertiseteam kan hulp verlenen bij de storing.

Voorbereiding
Bij de voorbereiding van de zorgplicht heb je een incident respons plan gemaakt. Dit plan is een structureel protocol dat je helpt bij het maken van de melding. Zorg er dus voor dat er intern duidelijke richtlijnen zijn over het signaleren en communiceren van mogelijke incidenten.

Daarnaast stelt de meldplicht een aantal vereisten:

- Bij een significant incident (een storing met grote operationele of financiële gevolgen) moet je binnen 24 uur een melding maken bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder.
- Alle andere incidenten moeten binnen 72 uur gemeld worden
- Binnen één maand moet er een eindrapportage opgesteld zijn aan de hand van het incident. Is het incident nog gaande? Dan volstaat een voortgangsverslag.

Ook krijg je als organisatie de mogelijkheid om incidenten vrijwillig te melden bij het CSIRT, zodat je altijd kunt rekenen op extra professionele ondersteuning bij een cyberincident.





4. Naar NIS2-compliance via ISO 27001-certificering

De NIS2-richtlijn verplicht een flinke reeks veiligheidsmaatregelen voor essentiële en belangrijke sectoren. Dat kan overweldigend zijn, want elke organisatie loopt tegen specifieke uitdagingen aan rond informatiebeveiliging. Ook als je samenwerkt met organisaties die onder NIS2 vallen, wil je kunnen aantonen dat jouw bedrijf voldoet aan de laatste veiligheidsmaatregelen. Één manier om dat goed aantoonbaar te maken, is via **ISO 27001-certificering**.

ISO 27001: voldoe aan de internationale norm voor informatiebeveiliging
Met een ISO 27001-certificaat laat je zien dat jouw organisatie voldoet aan alle eisen rondom informatiebeveiliging. Een organisatie met ISO 27001-certificering heeft een weerbaar Information Security Management System (ISMS). Dat betekent dat jouw organisatie zorgvuldig met persoonlijke gegevens omgaat, informatieprocessen beheerst en de veiligheid van bedrijfskritische informatie waarborgt.

Veel procedures en processen die je doorloopt voor ISO 27001, zoals beveiligingsbeoordelingen, risicobeoordelingen en audits, zijn ook vereist voor NIS2. Een organisatie met een ISO 27001-certificaat is dus goed op weg naar NIS2-compliance en hoeft nog maar enkele stappen te doorlopen.

Informatiebeveiliging via ISO 27001-certificering

- Voldoe aan de laatste vereisten rondom wet- en regelgeving (zoals NIS2)
- Maak gebruik van een weerbaar informatiebeveiligsmanagementsysteem die grip geeft op je belangrijkste veiligheidsrisico's
- Integreer digitale veiligheid topdown door de hele organisatie, zodat medewerkers bewust leren omgaan met informatie en digitale veiligheid
- Toon aan instanties en zakenpartners dat jouw bedrijf voldoet aan de laatste internationale standaarden voor informatiebeveiliging
- Toepasbaar op verschillende soorten organisaties, ongeacht grootte, sector of locatie

Liever in gesprek met een adviseur over NIS2?
Het behalen van ISO 27001-certificering is een van de mogelijke paden naar de NIS2-richtlijn. De route naar NIS2 is voor iedere organisatie anders. Of je nu loopt tegen uitdagingen rond digitalisering, het beschermen van belangrijke informatie of het maken van een actieplan. Onze veiligheidsexperts denken graag met je mee en komen met oplossingen die aansluiten op jouw organisatie. Zodat jouw organisatie niet alleen voldoet aan de aankomende verplichtingen van NIS2, maar ook een informatiesysteem bouwt dat voorbereid is op de digitale toekomst.

Contact



Over Kader en BMGRIP

Kader helpt organisaties verantwoord te moderniseren. Met consultancy & interim, opleidingen en software versterken wij de zes Kader Kapitalen: medewerkerswelzijn, arbeidsveiligheid, technische veiligheid, organisatiekwaliteit, informatiebeveiliging en duurzaamheid. Zo bouwen we samen aan moderne, veerkrachtige organisaties die klaar zijn voor de toekomst. Met ruim 400 professionals en meer dan 30 jaar ervaring creëren we dagelijks duurzame waarde voor mens, milieu en maatschappij.

BMGRIP is expert op het gebied van integrale informatiebeveiliging en privacy. Als onderdeel van de Kader Group helpen we organisaties verantwoord te moderniseren.

Bekijk het op
kader.nl

kader.nl | sales@kader.nl

© 2025 Kader Group B.V. Deze whitepaper is met de grootst mogelijke zorgvuldigheid samengesteld. Kader behoudt zich het recht voor zonder enige verplichtingen naar of jegens derden aanpassingen aan deze whitepaper door te voeren.

V.0826