BLAUWHUYS

NIS2
WHITEPAPER

+31 85 369 6058
INFO@BLAUWHUYS.NU
KARL WEISBARDSTRAAT 181-201, ROTTERDAM

INHOUDSOPGAVE

BLAUWHUYS

Wat is de NIS2?

De NIS2 richtlijn is het nieuwe Europese kader voor cybersecurity en risicobeheer. De richtlijn verplicht een groot aantal organisaties om hun digitale weerbaarheid te versterken, incidenten sneller te melden en bestuurders nadrukkelijker verantwoordelijk te maken voor beveiligingsmaatregelen.

NIS2 (Network and Information Security Directive 2) is een Europese cybersecurityrichtlijn die organisaties verplicht om hun digitale beveiliging te verbeteren en cyberincidenten snel te melden. Deze richtlijn is bedoeld om:

- Cyberrisico's te verkleinen.
- Kritieke sectoren beter te beschermen.
- De samenwerking tussen EU-lidstaten te verbeteren.
- Strengere eisen te stellen aan bestuurders en leveranciers.

NIS2 vervangt de oorspronkelijke NIS-richtlijn uit 2016. Deze wetgeving treed naar verwachting in het tweede kwartaal van 2026 in. De NIS2-richtlijn wordt in Nederland omgezet in de nationale Cyberbeveiligingswet (Cbw). De Cbw vervangt de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

Voor wie geldt de NIS2?

De NIS2-richtlijn is bedoeld om de digitale weerbaarheid binnen Europa fors te versterken. Daarom geldt de wet voor een brede groep organisaties die een cruciale of maatschappelijk belangrijke rol vervullen. In Nederland bepaalt de combinatie van de sector en de omvang of een organisatie onder de NIS2 valt. Onderstaand is beschreven waar een organisatie aan moet voldoen:

- De organisatie is in een essentiële of belangrijke sector actief én
- De organisatie voldoet aan de groottecriteria, óf
- De organisatie is door een ministerie specifiek aangewezen.

Mocht u direct inzicht willen over waar uw organisatie onder valt, dan kunt u onze NIS2-beslisboom raadplegen. Klik hier voor de beslisboom.

Verplichtingen onder de NIS2

Registreren
Organisaties die onder de NIS2-richtlijn vallen, zijn verplicht zich te registreren bij het nationale register. Deze registratie is bedoeld om toezichthouders een actueel overzicht te geven van alle essentiële en belangrijke entiteiten binnen de scope van de wet.

Zorgplicht
Een van de kernverplichtingen van de NIS2-richtlijn is de zorgplicht. Organisaties die onder deze wetgeving vallen moeten kunnen aantonen dat zij doordachte en passende technische, organisatorische en operationele maatregelen hebben getroffen om hun IT- en informatiesystemen te beschermen tegen ernstige digitale verstoringen. Deze maatregelen moeten aansluiten bij de huidige technologische mogelijkheden, relevante internationale standaarden en de specifieke risicoprofielen van de organisatie. De zorgplicht vereist dat organisaties onder meer:

- Een risicoanalyse uitvoeren en hun beveiliging daarop afstemmen.
- Zorgen voor incidentrespons en bedrijfscontinuïteit, zoals back-ups en crisisplannen.
- De toeleveringsketen beveiligen, inclusief ICT-dienstverleners.
- Processen rondom ontwikkeling, onderhoud en verwerving van IT-systemen beveiligen.
- De effectiviteit van genomen maatregelen periodiek meten en evalueren.
- Investeren in cyberhygiëne en opleiding van personeel.
- Duidelijke procedures voor cryptografie, toegangsbeheer en personeelsbeveiliging hanteren.

Het doel van deze zorgplicht is dat de beveiligingsmaatregelen proportioneel zijn aan de risico's die zich binnen de organisatie voordoen en dat entiteiten hun digitale weerbaarheid structureel verhogen.

Meldplicht
De NIS2-richtlijn introduceert een strikte meldplicht voor organisaties die onder de wetgeving vallen. Dit betekent dat significante cyberincidenten verplicht en binnen duidelijke termijnen moeten worden gemeld bij het Nationaal Cyber Security Centrum (NCSC) en de toezichthouder. Het doel hiervan is om snel zicht te krijgen op digitale dreigingen en om verdere schade in de keten te voorkomen. Hierin moet een incident in 3 fases gemeld worden:

1. Vroegtijdige melding (binnen 24 uur): Een eerste inschatting van het incident, inclusief de impact en aard van de verstoring.
2. Vervolgmelding (binnen 72 uur): Aanvullende informatie, zoals vermoedelijke oorzaak, omvang, getroffen systemen en genomen maatregelen.
3. Eindverslag (binnen 1 maand): Een definitieve rapportage met een volledig incidentoverzicht, inclusief gevolgen, definitieve analyse en structurele verbeteracties.

De gevolgen van de NIS2-richtlijn

Het naleven van de NIS2-richtlijn wordt in Nederland bewaakt door verschillende instanties die verantwoordelijk zijn voor digitale veiligheid en sectorspecifiek toezicht. Deze organisaties houden in de gaten of bedrijven die onder de wetgeving vallen daadwerkelijk voldoen aan de verplichtingen, waaronder het nemen van passende beveiligingsmaatregelen en het tijdig melden van cyberincidenten.

Wanneer een organisatie de NIS2-eisen op orde heeft, levert dat diverse voordelen op:

- Het niveau van digitale beveiliging stijgt aanzienlijk, waardoor het risico op cyberaanvallen afneemt en zowel de continuïteit als de reputatie van de organisatie beter wordt beschermd.
- Het toont aan dat de organisatie serieus werk maakt van cybersecurity en zich inzet voor de veiligheid van klanten, partners en ketenpartijen.

Het niet naleven van de NIS2-richtlijn kan daarentegen grote gevolgen hebben, waaronder:

- Financiële sancties die kunnen oplopen tot 10 miljoen euro of 2% van de wereldwijde omzet voor essentiële entiteiten, en tot 7 miljoen euro of 1,4% van de omzet voor belangrijke entiteiten.
- Het (tijdelijk) stopzetten van diensten of bedrijfsprocessen wanneer deze onvoldoende beveiligd blijken.
- Persoonlijke aansprakelijkheid van bestuurders wanneer wordt vastgesteld dat zij nalatig zijn geweest in het treffen van noodzakelijke beveiligingsmaatregelen.

Informatiebeveiligingsstandaarden als fundament voor NIS2-compliance

De NIS2-richtlijn vraagt van organisaties dat zij informatiebeveiliging op een gestructureerde, aantoonbare en risico gestuurde manier organiseren. Dit sluit nauw aan bij bestaande internationale normen zoals ISO 27001, die al jaren dienen als raamwerk voor het opzetten en beheren van een Information Security Management System (ISMS).

Binnen de Nederlandse overheid vormt momenteel de Baseline Informatiebeveiliging Overheid (BIO) het primaire kader voor de invulling van de zorgplicht. De BIO bevat in verschillende opzichten uitgebreidere eisen dan ISO 27001 en fungeert als leidraad voor overheidsinstellingen die hun digitale weerbaarheid willen versterken in lijn met de NIS2-richtlijn.

Omdat NIS2 volledig aansluit op het principe van risico gestuurd werken, ligt het voor de hand dat publieke organisaties de nieuwe verplichtingen zoveel mogelijk binnen de bestaande BIO-structuur implementeren. Voor overheidsinstanties die deze norm nog niet of slechts gedeeltelijk toepasten, ontstaat door NIS2 nu wél een wettelijke verplichting om dit te borgen.

Voor organisaties buiten de overheid biedt ISO 27001 vooralsnog het meest logische vertrekpunt. Sectorale normen blijven daarnaast relevant, zoals de NEN 7510 voor zorginstellingen en het SURF-normenkader voor het onderwijs. Deze standaarden bieden een solide basis om het beveiligingsniveau op orde te brengen en vormen een waardevolle opstap richting NIS2-compliance.

Belangrijk is echter te benadrukken dat werken volgens ISO 27001, NEN 7510 of de BIO op zichzelf niet voldoende garantie biedt voor volledige naleving van de NIS2-richtlijn. De NIS2 introduceert aanvullende verplichtingen op het gebied van governance, ketenverantwoordelijkheid, meldprocedures en aantoonbaarheid. Organisaties zullen daarom bestaande normen moeten aanvullen met gerichte maatregelen om te voldoen aan de nieuwe wettelijke eisen.

Waar kan Blauwhuys in ondersteunen?

De NIS2-richtlijn vraagt van organisaties een aantoonbaar hogere mate van digitale weerbaarheid. Dat betekent: structurele risicobeheersing, duidelijke governance, robuuste beveiligingsmaatregelen en een gestroomlijnde incidentrespons. Voor veel organisaties vormt dit een ingrijpende veranderopgave. Blauwhuys biedt een aanpak die deze complexiteit terugbrengt tot heldere stappen, onderbouwde keuzes en praktisch uitvoerbare maatregelen.

Inzicht creëren
Blauwhuys voert een gestructureerde NIS2-analyse uit waarin alle relevante domeinen worden beoordeeld, variërend van governance en beleid tot technische maatregelen en ketenbeveiliging. Dit gebeurt via een gestructureerde workshopaanpak en een eigen NIS2-beoordelingstool, waarmee de organisatie direct inzicht krijgt in sterktes, risico's en gaten in compliance. De resultaten worden uitgewerkt in een duidelijk volwassenheidsmodel, zodat direct zichtbaar wordt waar verbetermaatregelen noodzakelijk zijn.

Praktische en uitvoerbare aanbevelingen
Op basis van de analyse levert Blauwhuys een concreet adviesrapport met gerichte acties, prioriteiten en een roadmap richting volledige naleving van de richtlijn. Dit rapport is ontworpen voor besluitvorming op directie- en managementniveau en maakt inzichtelijk wat er moet gebeuren, waarom, en binnen welke termijnen. Deze aanpak is bewust pragmatisch: geen dikke rapporten, maar heldere aanbevelingen die direct in de organisatie kunnen worden toegepast.

Begeleiding bij implementatie
Niet elke organisatie beschikt over de interne capaciteit of expertise om de benodigde maatregelen door te voeren. Blauwhuys ondersteunt daarom niet alleen in analyse, maar ook in implementatie:

- Het opstellen en actualiseren van beleid en procedures.
- Het inrichten of verbeteren van processen, van incidentrespons tot leveranciersbeheer.
- Het borgen van governance, rollen en verantwoordelijkheden.
- Het opzetten van training en bewustwording.

Waar nodig helpt Blauwhuys bij het modelleren, verbeteren en optimaliseren van informatiestromen en procesketens, zodat beveiligingsmaatregelen niet alleen op papier bestaan, maar ook daadwerkelijk ingebed zijn in de dagelijkse praktijk.

Waar kan Blauwhuys in ondersteunen?

Training & bewustwording voor bestuurders en teams
NIS2 stelt bestuurders expliciet verantwoordelijk voor cybersecurity. Blauwhuys helpt organisaties hierbij met gerichte sessies, waaronder:

- Kennissessies voor bestuurders
- Trainingen voor medewerkers en securityteams
- Sectorgerichte workshops en awarenessprogramma's

Zo wordt niet alleen aan de wettelijke verplichtingen voldaan, maar wordt ook de interne draagkracht versterkt om cybersecurity structureel te verbeteren.

Een toekomstbestendige aanpak
Blauwhuys benadert NIS2 vanuit de organisatie in plaats van uitsluitend vanuit techniek. Daarmee sluiten we aan op de kern van de richtlijn: structurele, risico gestuurde en organisatie-brede digitale weerbaarheid. De ondersteuning is ontworpen om direct resultaat te leveren, maar ook om organisaties blijvend sterker te maken.

Contact

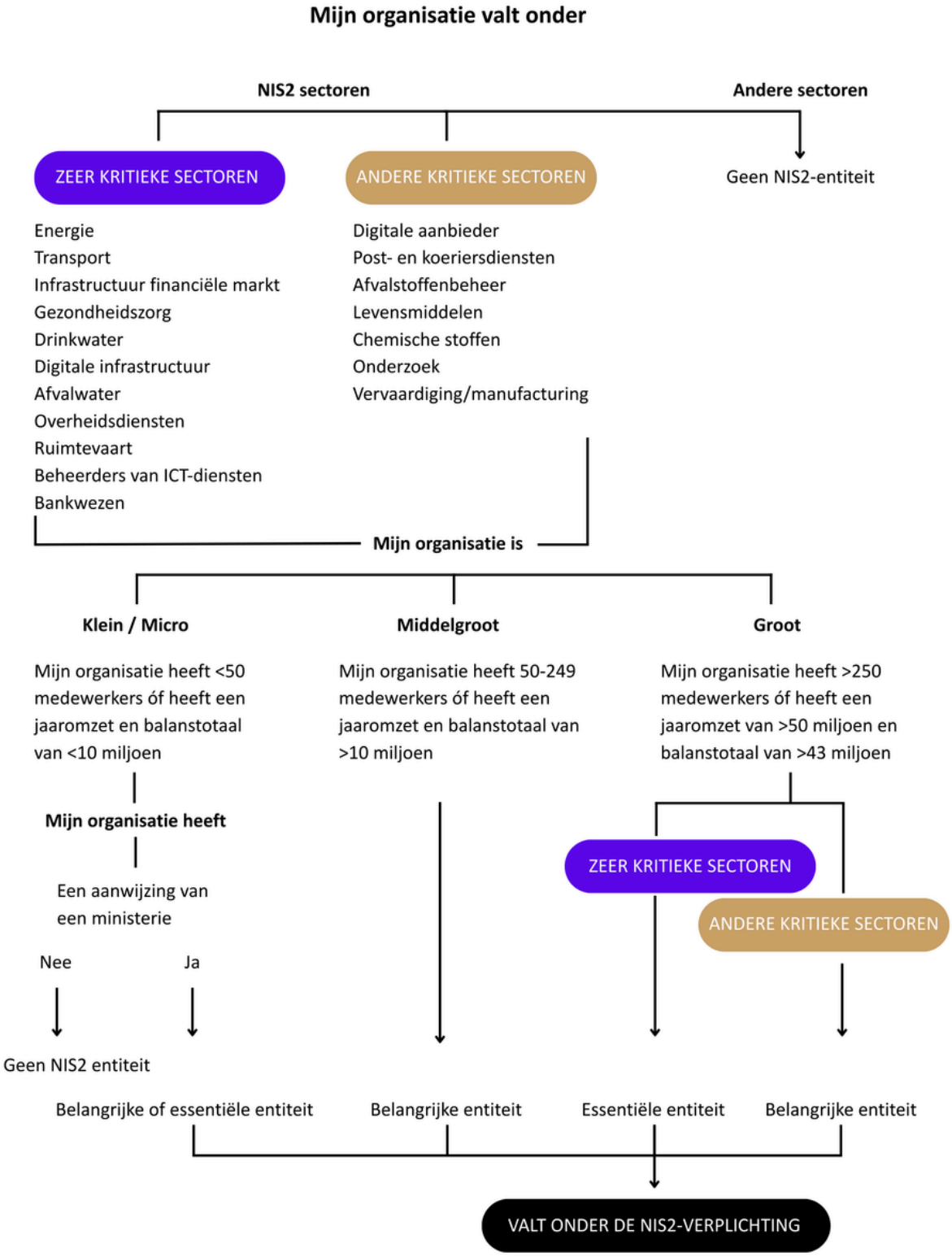
Wilt u sparren over de impact van NIS2 op jouw organisatie of bent u benieuwd hoe Blauwhuys u kan ondersteunen richting aantoonbare compliance? Ons team staat klaar om u verder te helpen. Neem gerust contact met ons op voor een vrijblijvend gesprek, een kennissessie of meer informatie over onze diensten.

Karl Weisbardstraat 181–201, 3015 GM Rotterdam
E-mail: info@blauwhuys.nu
Telefoon: 085 369 60 58

Samen bouwen we aan een veiligere en toekomstbestendige digitale omgeving.

Bijlage 1. Beslisboom

In onderstaande beslisboom kunt u in één oogopslag zien of uw organisatie onder de NIS2-verplichting valt.



Bijlage 1. Beslisboom

Uitzonderingen

- Rijksoverheid, gekwalificeerde vertrouwensdienstverleners (QTSP), registers voor topleveldomeinnamen en verleners van domeinnaamregistratiediensten zijn, ongeacht de grootte van de organisatie essentiële entiteiten.
- Middelgrote aanbieders van openbare elektronische communicatienetwerken zijn essentiële entiteiten.
- Micro- en kleinbedrijven die openbare elektronische communicatienetwerken aanbieden en aanbieders van niet gekwalificeerde vertrouwensdienstverleners zijn belangrijke entiteiten.
- Organisaties die volgens de CER-richtlijn zijn aangewezen als kritieke entiteit zijn automatisch een essentiële entiteit volgens de NIS2-richtlijn.