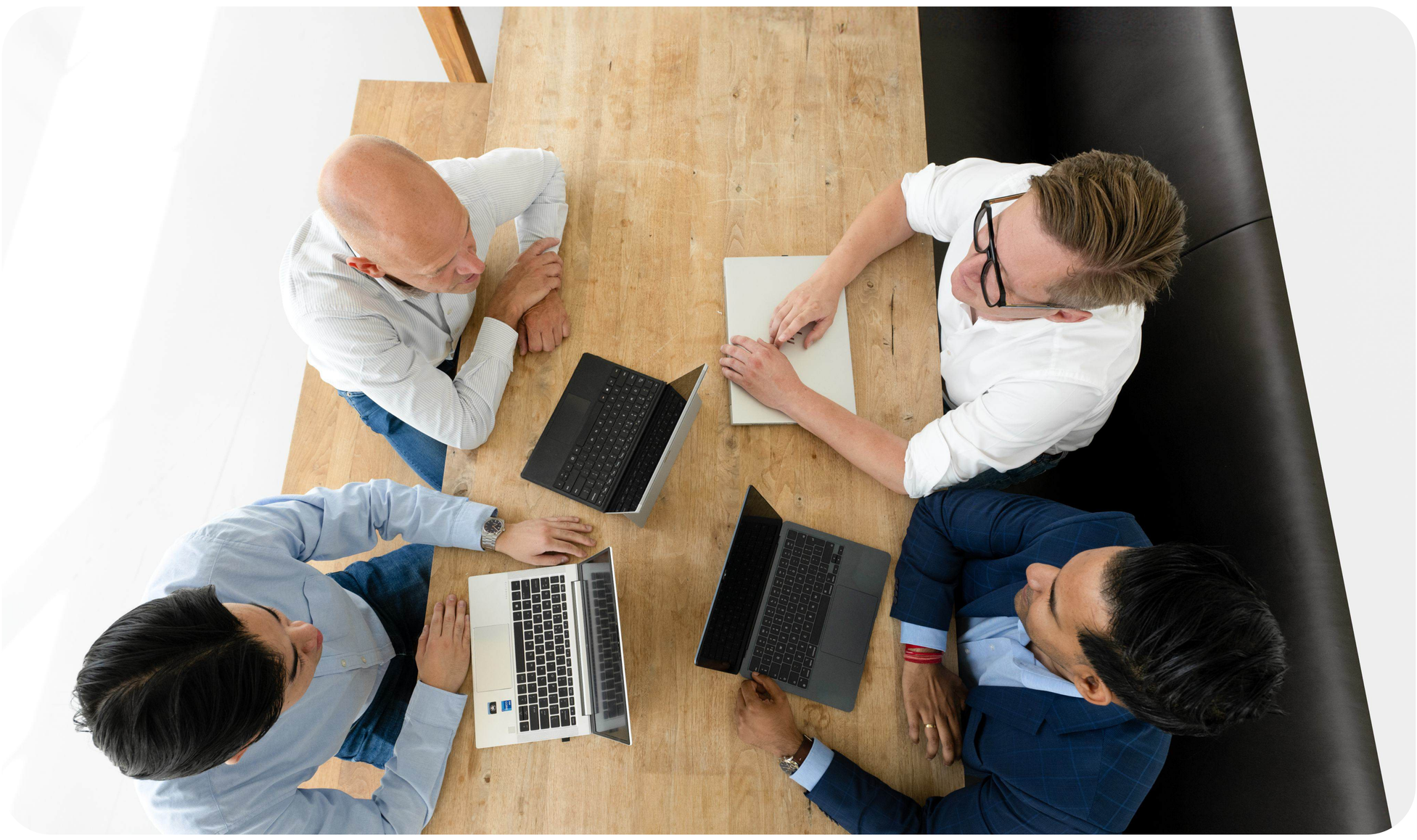
NIS2:
versterken van digitale veerkracht

De impact en implementatie
van NIS2 voor organisaties

HELIXIS
Cyber Security

Inhoudsopgave



Wat is NIS2?

De NIS2-richtlijn (Network and Information Security Directive 2) is de opvolger van de oorspronkelijke NIS-richtlijn uit 2016. Deze richtlijn was destijds de eerste Europese wetgeving die zich richtte op cyberbeveiliging binnen de EU. Het doel? Lidstaten en essentiële organisaties beter beschermen tegen digitale dreigingen.

De basis voor de NIS-richtlijn werd al in 2013 gelegd, toen de Europese Commissie de EU Cybersecurity Strategie presenteerde. Hierin werd het belang van een gezamenlijke aanpak van cybersecurity binnen Europa onderstreept. Drie jaar later keurden het Europees Parlement en de Raad de NIS-richtlijn goed.

In Nederland werd de richtlijn vertaald naar nationale wetgeving via de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Met de komst van NIS2 wordt de regelgeving verder aangescherpt.

NIS2 is geen verordening, maar een richtlijn. Dat betekent dat EU-lidstaten niet simpelweg de regels kunnen overnemen, maar zelf nationale wetgeving moeten opstellen om de doelen van NIS2 te bereiken.

Er geldt wel een ‘resultaatverplichting’: de einddoelen staan vast, maar hoe elk land die precies invult, is aan hen.

Waarom is NIS2 belangrijk?

Cyberveiligheid is van (inter)nationaal belang omdat een goed functionerende digitale infrastructuur de basis vormt voor veel essentiële sectoren, zoals energie, gezondheidszorg, transport en financiën. Een cyberaanval op deze systemen kan grote verstoringen veroorzaken, met maatschappelijke, economische en zelfs politieke gevolgen.

Afhankelijkheid van digitale infrastructuur maakt kwetsbaar. Cyberveiligheid is tegenwoordig belangrijker dan ooit, omdat digitale dreigingen steeds geavanceerder, omvangrijker en schadelijker worden.

Cybercriminelen gebruiken steeds slimmere technieken om geld, data of bedrijfsgeheimen te stelen. Hackers kunnen bedrijven platleggen met ransomware, waarbij losgeld wordt geëist om systemen weer toegankelijk te maken. Maar ook landen voeren cyberaanvallen uit, bijvoorbeeld om spionage te plegen of vitale infrastructuur te verstoren.

Cyberdreigingen vormen een directe bedreiging voor bedrijven, overheden en burgers. Een sterke cyberbeveiliging is essentieel om digitale aanvallen te voorkomen. NIS2 is een poging van de EU om lidstaten te helpen bij het versterken van hun cyberbeveiliging.

De belangrijkste veranderingen

NIS2 brengt ingrijpende veranderingen met zich mee ten opzichte van de oorspronkelijke NIS-richtlijn. De vernieuwde richtlijn breidt niet alleen het toepassingsgebied uit, maar scherpt ook de regels en toezichtmechanismen aan.

Aanscherping van beveiligingseisen
NIS2 stelt strengere eisen aan netwerk- en informatiebeveiliging. Dit omvat een breed scala aan maatregelen op het gebied van risicomanagement, incidentafhandeling, toeleveringsketenbeveiliging en cyberhygiëne.

Uitgebreidere reikwijdte
Waar NIS1 zich voornamelijk richtte op vitale sectoren zoals energie, transport en gezondheidszorg, geldt NIS2 voor een veel bredere groep organisaties. Ook ICT-dienstverleners, de maakindustrie en bedrijven die cruciaal zijn voor toeleveringsketens vallen nu onder de richtlijn. Dit betekent dat veel meer bedrijven te maken krijgen met strengere eisen op het gebied van cyberbeveiliging.

Onderverdeling essentiële en belangrijke organisaties
NIS2 maakt een duidelijk onderscheid tussen ‘essentiële’ en ‘belangrijke’ organisaties. Essentiële organisaties, zoals nutsbedrijven en zorginstellingen, hebben een kritische rol in de samenleving en vallen onder strenger toezicht, inclusief proactieve controles.

Actiever toezicht en handhaving
Voor essentiële organisaties geldt dat er proactieve controles plaatsvinden om naleving te waarborgen. Dit kunnen steekproefsgewijze inspecties zijn, maar ook diepgaande audits. Voor belangrijke organisaties wordt toezicht vooral reactief ingezet, bijvoorbeeld naar aanleiding van een beveiligingsincident of een melding van tekortkomingen.

Meldplicht voor cyberincidenten
NIS2 verplicht organisaties om ernstige cyberincidenten binnen een vastgestelde termijn te melden bij de bevoegde autoriteiten. Deze meldplicht draagt bij aan een snellere reactie op digitale dreigingen en bevordert de transparantie. Bovendien stimuleert het een betere samenwerking tussen bedrijven en overheden binnen de EU, wat essentieel is om cybercriminaliteit effectief aan te pakken.

Wat betekent het voor organisaties?

NIS2 verplicht organisaties om hun beveiligingsmaatregelen te versterken, en niet-naleving kan leiden tot hoge boetes en een groter risico op ernstige cyberincidenten. Hoewel NIS2 gericht is op bedrijven in kritieke en essentiële sectoren, heeft de richtlijn ook gevolgen voor andere organisaties.

Bedrijven moeten proactief investeren in cyber-weerbaarheid om risico's te beheersen en aan de nieuwe eisen te voldoen. NIS2 legt daarnaast de verantwoordelijkheid bij bestuurders om actief betrokken te zijn bij het goedkeuren van risicomanagement-maatregelen en het toezicht op de uitvoering daarvan. Dit houdt ook in dat zij trainingen moeten volgen om hun verantwoordelijkheden adequaat te kunnen vervullen.

Niet-naleving

Niet-naleving van NIS2 kan niet alleen leiden tot zware boetes, aanzienlijke reputatieschade en verstoringen in de bedrijfsvoering, maar ook tot bredere risico's voor de samenleving als geheel. Beveiligingsincidenten kunnen verregaande gevolgen hebben voor bedrijven, maar zelfs ook voor de economie en de openbare veiligheid.

Proactief investeren in cyberweerbaarheid helpt organisaties niet alleen om aan de nieuwe eisen te voldoen, maar ook om bredere risico's voor zichzelf en de samenleving te verkleinen en toekomstige problemen te voorkomen.

Welke verplichtingen gelden er?

NIS2 legt organisaties die onder de richtlijn vallen verschillende verplichtingen op, die grofweg te verdelen zijn in twee hoofdcomponenten: de zorgplicht en de meldplicht. De zorgplicht houdt in dat organisaties verantwoordelijk zijn voor het nemen van passende maatregelen om hun informatiesystemen en netwerken te beveiligen.

De meldplicht verplicht organisaties om cyberincidenten die een ernstige impact kunnen hebben, binnen een bepaalde tijd aan de bevoegde autoriteiten te rapporteren.

Zorgplicht

De **zorgplicht** vereist dat organisaties de juiste beveiligingsmaatregelen nemen om de digitale veiligheid en continuïteit van hun diensten te waarborgen. Hoewel NIS2 niet precies voorschrijft welke technologieën of oplossingen organisaties moeten inzetten, stelt de richtlijn dat ze 'passende en evenredige technische, operationele en organisatorische maatregelen' moeten treffen.

Onder de zorgplicht vallen onder meer de volgende verplichtingen:

1. Het uitvoeren van een risicoanalyse en het beveiligen van informatiesystemen.
2. Het opstellen van beleid en procedures voor incidentenbehandeling.
3. Het treffen van maatregelen voor bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningsplannen.
4. Het beveiligen van de toeleverancierskеten.
5. Het waarborgen van de veiligheid bij het ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief het reageren op en het bekendmaken van kwetsbaarheden.
6. Het opstellen van beleid en procedures om de effectiviteit van de genomen cyberbeveiligingsmaatregelen te beoordelen.
7. Basis cyberhygiëne en het bieden van trainingen op het gebied van cyberbeveiliging.
8. Beleid en procedures voor het gebruik van cryptografie en encryptie.
9. Het waarborgen van beveiliging op het gebied van personeel, toegangsbeheer en beheer van activa.
10. Het implementeren van MFA, beveiligde communicatiekanalen (spraak, video en tekst) en veilige nood-communicatiesystemen binnen de organisatie.

Meldplicht

NIS2 kent, in tegenstelling tot de oude NIS-richtlijn, een meldplicht voor organisaties die als belangrijke of essentiële entiteiten worden aangemerkt. Zij moeten grote incidenten melden bij het CSIRT en de toezichthouder. Door deze meldingen kunnen andere organisaties leren van gedeelde informatie en hun beveiliging verbeteren, wat bijdraagt aan een veiligere digitale omgeving binnen de EU.

De meldplicht geldt voor ‘significante incidenten’, die ernstige verstoringen in diensten kunnen veroorzaken of financiële verliezen met zich mee kunnen brengen. Ook incidenten die materiële of immateriële schade bij andere organisaties veroorzaken, vallen hieronder. Daarnaast worden organisaties aangemoedigd om ook niet-significante incidenten of bijna-incidenten vrijwillig te melden.

Voor wie geldt NIS2?

NIS2 richt zich op organisaties en instellingen die een cruciale rol spelen in de samenleving. De richtlijn maakt een onderscheid tussen 'essentiële' en 'belangrijke' organisaties.

Essentiële organisaties zijn grotere bedrijven die een kritische rol spelen in het functioneren van de samenleving. Het gaat hierbij om organisaties met meer dan 250 medewerkers, een netto-omzet van meer dan 50 miljoen euro of een balanstotaal van meer dan 43 miljoen euro. Deze organisaties opereren binnen de volgende sectoren:

- Financiële marktinfrastructuur
- Ruimtevaart
- Overheid
- ICT-dienstverlening
- Digitale infrastructuur
- Transport
- Afvalwater
- Drinkwater
- Gezondheidszorg
- Bankwezen
- Energie

Belangrijke organisaties: Dit zijn middelgrote organisaties met minimaal 50 werknemers of een jaaromzet of balanstotaal van meer dan 10 miljoen euro. Deze organisaties opereren binnen de volgende sectoren:

- Chemische stoffen
- Maakindustrie
- Afvalbeheer
- Onderzoek
- Geneesmiddelen
- Medische apparatuur
- Levensmiddelen

Hoewel NIS2 van toepassing is op ondernemingen in kritieke en belangrijke sectoren, heeft de richtlijn ook implicaties voor bedrijven die er niet rechtstreeks onder vallen. Hiermee wordt bedoeld:

Ketenpartners van essentiële of belangrijke organisaties: Toeleveranciers en dienstverleners die niet in de genoemde sectoren actief zijn, maar een cruciale rol spelen in de toeleveringsketen van essentiële of belangrijke organisaties, kunnen onder NIS2 vallen.

Kleine bedrijven in de internetinfrastructuur: Bedrijven die een sleutelrol vervullen in de internetinfrastructuur kunnen strategische doelwitten voor cyberaanvallen zijn en vallen daarom ook onder NIS2.

Aparte aanwijzing door de overheid: De overheid kan specifieke organisaties aanwijzen die, ondanks dat ze niet standaard onder NIS2 vallen, toch verplicht zijn om aan de richtlijn te voldoen.

HELIXIS
Cyber Security

Is de NIS2 op jullie van toepassing?

Valt jouw organisatie binnen 1 van deze sectoren?

- Energie
- Transport
- Bankwezen
- Gezondheidszorg
- Drinkwater
- Afvalwater
- Financiële markt
- Digitale infrastructuur
- Chemische stoffen
- Overheid
- ICT-dienstverlening
- Ruimtevaart
- Afvalbeheer
- Levensmiddelen
- Maakindustrie
- Medische apparatuur
- Geneesmiddelen
- Onderzoek

Antwoord: Nee

Leveren jullie aan een of meer van bovenstaande sectoren?

Antwoord: Ja

Antwoord: Nee

Heeft jouw organisatie een belangrijke functie binnen de infrastructuur van het internet of binnen de overheid?

Antwoord: Nee

Jouw organisatie is **niet** verplicht om te voldoen aan de NIS2

Antwoord: Ja

Jouw organisatie is verplicht om te voldoen aan de NIS2

Antwoord: Ja

Hoeveel medewerkers heeft jouw organisatie?

Antwoord: meer dan 250

Antwoord: minder dan 250

Hoeveel omzet heeft jouw organisatie?

Antwoord: meer dan 10 miljoen

Antwoord: minder dan 10 miljoen

Jouw organisatie is **niet** verplicht om te voldoen aan de NIS2

Hulp nodig?

Neem gerust contact met mij op

martijn@helixis.nl
06 289 55 857

Implementatie

De implementatie van NIS2 is een uitgebreid proces dat zorgvuldig moet worden voorbereid. De volgende stappen helpen organisaties om zich goed voor te bereiden en de richtlijn effectief toe te passen:

1. Risico-inventarisatie

Begin met een grondige analyse van de huidige beveiligingsmaatregelen en identificeer de potentiële risico's en bedreigingen voor de informatiebeveiliging.

Evalueer de impact van deze risico's op de vertrouwelijkheid, integriteit en beschikbaarheid van data en systemen.

Prioriteer de risico's op basis van hun waarschijnlijkheid en de mogelijke gevolgen voor de organisatie en de bredere samenleving.

2. Implementatiestrategie

Ontwikkel praktische en uitvoerbare plannen voor netwerk- en informatiebeveiliging, waarbij je de geschikte technische en organisatorische maatregelen kiest op basis van de geïdentificeerde risico's.

Zorg ervoor dat de implementatie voldoet aan de vereisten van de NIS2-richtlijn en dat de genomen maatregelen effectief bijdragen aan het waarborgen van de digitale veiligheid.

3. Uitvoering

Zorg voor efficiënte processen voor de detectie, rapportage en opvolging van incidenten.

Ontwikkel incident-responseplannen die duidelijke rollen en verantwoordelijkheden voor medewerkers definiëren.

Beveilig de toeleveringsketen door te zorgen dat ook jouw leveranciers voldoen aan de beveiligingseisen. Betrek hen in het proces en zorg ervoor dat ze zich bewust zijn van de risico's en maatregelen die van toepassing zijn op de samenwerking.

4. Training & awareness

Zorg ervoor dat medewerkers goed getraind zijn om de incident-response plannen uit te voeren.

Creeër bewustwording en training van jouw team en bestuur, zodat iedereen op de hoogte is van de risico's, beveiligingsmaatregelen en procedures rondom incidentmanagement.

Hiermee versterk je de organisatie als geheel en zorg je ervoor dat alle medewerkers bijdragen aan de naleving van NIS2.

Kortom

De NIS2-richtlijn is de opvolger van de NIS-richtlijn uit 2016 en richt zich op het versterken van de cyberbeveiliging binnen de EU. Het doel is organisaties beter te beschermen tegen digitale dreigingen, aangezien de afhankelijkheid van digitale infrastructuur steeds groter wordt. NIS2 breidt de regelgeving uit, stelt strengere beveiligingseisen en verhoogt het toezicht. Essentiële organisaties krijgen strikter toezicht, inclusief proactieve controles, terwijl belangrijke organisaties reactief worden gecontroleerd. De richtlijn verplicht organisaties om ernstige cyberincidenten te melden bij de autoriteiten en legt nadruk op het versterken van risicomanagement, incidentafhandeling en toeleveringsketenbeveiliging.

Voor organisaties betekent NIS2 dat ze verplicht zijn te investeren in cyberweerbaarheid. Niet-naleving kan leiden tot zware boetes en ernstige gevolgen voor de organisatie en zelfs voor de samenleving. De richtlijn richt zich op grote bedrijven in kritieke sectoren zoals energie, gezondheidszorg en transport, maar ook op kleinere bedrijven in de internetinfrastructuur en ketenpartners van essentiële organisaties. Bedrijven moeten risico's inventariseren, een implementatiestrategie ontwikkelen en hun leveranciers en medewerkers betrekken bij het waarborgen van de digitale veiligheid.

Heb je vragen over NIS2 of hulp nodig bij de implementatie van de NIS2-richtlijn binnen jouw bedrijf? Bij Helixis staan we klaar om jouw organisatie te begeleiden en beschermen tegen hedendaagse cyberdreigingen: van strategisch advies tot hands-on implementatie. Met ruim 40 jaar ervaring is Helixis jouw partner voor al je cybersecurity uitdagingen.

Neem gerust contact op met ons op.

Gregor Abbas en Martijn Uunk

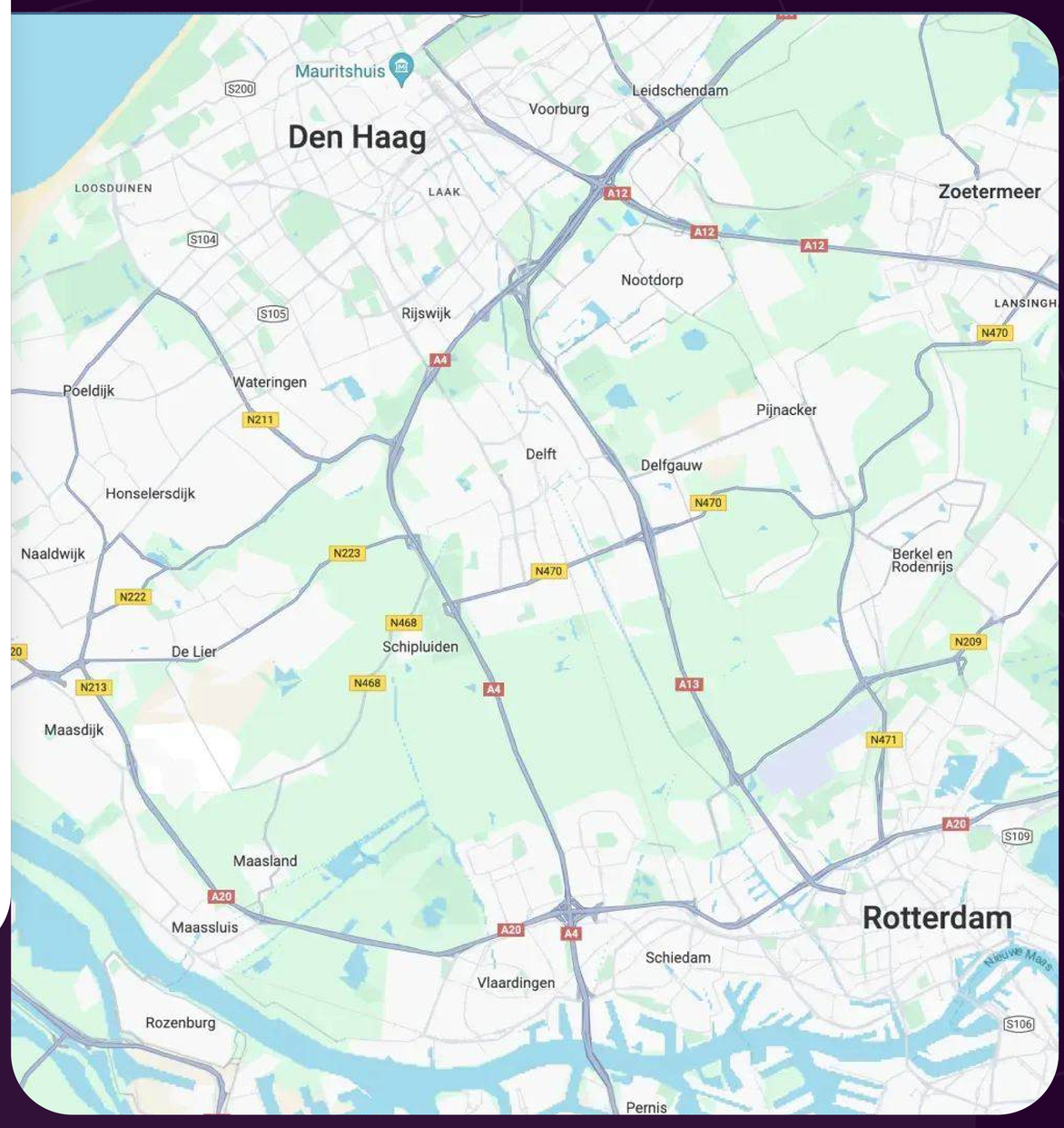
HELIXIS
Cyber Security

CONTACT

Heb je vragen over NIS2?

Onze specialisten staan klaar om je te ondersteunen tijdens een gratis vragenuurtje. Natuurlijk bespreken we ook graag de mogelijkheden voor samenwerking.

Wij zorgen ervoor dat jouw organisatie klaar is voor een digitaal veilige toekomst. Ben jij er klaar voor?



Contactgegevens

Helixis B.V.
Spaces Air Offices
Rode Zand 80, 4de verdieping
3011 AN Rotterdam
Zuid-Holland

T: 06 289 55 857
E: info@helixis.nl

www.helixis.nl