

PRAKTISCHE HANDLEIDING

WAT BETEKEN NIS2 VOOR UW ORGANISATIE?



“

OVERWEGING (1) NIS2-RICHTLIJN

‘Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad (4) heeft tot doel capaciteiten op het gebied van cyberbeveiliging in de hele Unie op te bouwen ... en aldus bij te dragen tot de veiligheid van de Unie.’



© 2024 Bureau Veritas | Secura en Masero Cyber Security. Alle rechten voorbehouden. Neem gerust contact met ons op voor toestemming of vragen over het gebruik van deze content. Dat kan via marketing@secura.com.

IN DEZE GIDS:

01. _____	2
Wat is NIS2 en waarom deze richtlijn?	
02. _____	3
Geldt NIS2 voor uw organisatie?	
03. _____	5
Vragen die klanten ons stellen over NIS2	
04. _____	6
Wat zijn de belangrijkste eisen van NIS2 voor bedrijven en wat betekenen deze in de praktijk?	
05. _____	11
Hoe verhoudt NIS2 zich tot standaarden als ISO 27001?	
06. _____	12
Hoe Masero en Secura u kunnen helpen bij het bereiken van NIS2 compliance	

“



‘De Europese samenleving beschermen tegen cyberdreigingen: dat is de belangrijkste reden voor de nieuwe Europese NIS2-richtlijn. Wat zijn de gevolgen van NIS2 voor u? Dit document geeft u een overzicht en achtergrondinformatie. Ik hoop dat deze inzichten u op weg helpen naar NIS2-compliance.’

Dirk Jan van den Heuvel - Algemeen Directeur Secura | BV



1. WAT IS NIS2 EN WAAROM DEZE RICHTLIJN?

De Network and Information Security 2-richtlijn, of NIS2-richtlijn, is Europese wetgeving die is ontworpen om Europese organisaties weerbaarder te maken tegen cyberdreigingen. De richtlijn is ook bedoeld om de samenwerking binnen de EU op het gebied van cyberbeveiliging te verbeteren. De richtlijn is van toepassing op meer dan **160.000 organisaties** in Europa. Lidstaten moeten NIS2 voor **17 oktober 2024** in hun nationale wetgeving hebben opgenomen. In Nederland zal NIS2 geïmplementeerd worden in de Cyberbeveiligingswet (Cbw). Het is nog niet bekend wanneer de Cbw in gaat.

De reden voor NIS2: kritieke sectoren beschermen tegen toenemende cyberdreigingen. ‘Cybercriminaliteit is *big business* geworden, met een hele illegale economie die is opgezet om cybercriminaliteit te ondersteunen met dienstverleners, ronselaars en financiële diensten,’ aldus Europols negende beoordeling van georganiseerde misdaad.

Volgens ENISA waren de grootste cyberdreigingen voor de EU in 2023 ransomware (goed voor 34% van de dreigingen), DDoS-aanvallen (28%) en dreigingen voor data (17%). Overheid, gezondheidszorg, digitale infrastructuur en de productiesector zijn het vaakst doelwit.

De NIS2-richtlijn schrijft beveiligingseisen voor. Lidstaten kunnen strenger zijn bij het omzetten van de richtlijn in nationale wetgeving.

EERSTE NIS-RICHTLIJN	NIS2, WIJZIGING VAN NIS
Van toepassing op <4.000 organisaties, voornamelijk kritieke infrastructuur en grote bedrijven	Van toepassing op >160.000 organisaties, van energie tot gezondheidszorg en postdiensten, ook op middelgrote bedrijven
Vereisten zijn op hoog niveau	Vereisten zijn specifiek
EU-richtlijn van kracht: 1 augustus 2016	EU-richtlijn van kracht: 16 januari 2023
Nationale wetten van kracht: 9 mei 2018	Nationale wetten van kracht: 17 oktober 2024



NIS2 was 2 jaar in de maak: het eerste NIS2-voorstel werd ingediend op 16 december 2020. De definitieve versie werd voorgelegd op 27 december 2022.

2. GELDT NIS2 VOOR UW ORGANISATIE?

Twee factoren bepalen of uw organisatie onder NIS2 valt. Als beide factoren gelden voor uw organisatie, kunt u ervan uitgaan dat NIS2 van toepassing is op u van toepassing is.

1. **Uw organisatie behoort tot een essentiële of belangrijke sector, zoals gedefinieerd in de NIS2-richtlijn.**
2. **Uw organisatie heeft meer dan 50 werknemers of een jaarlijkse omzet van 10 miljoen euro.** Kleinere organisaties vallen niet onder NIS2. Er zijn een paar uitzonderingen. Bijvoorbeeld: aanbieders van domeinnaamregistratiediensten worden aangemerkt als zeer kritisch en vallen onder NIS2, ongeacht hun grootte.

Sectoren opgenomen in NIS2

NIS2 heeft verschillende sectoren aangemerkt als vitaal voor de samenleving. Dit zijn **essentiële** en **belangrijke** entiteiten. Voor beide categorieën gelden dezelfde regels. Het belangrijkste verschil tussen de categorieën is de manier waarop een organisatie wordt gecontroleerd door toezichthouders en welke sancties kunnen worden verwacht bij niet-naleving. De lijst met sectoren is te vinden in [ANNEX I van de NIS2-tekst](#).



ESSENTIËLE ENTITEITEN 'zeer kritieke sectoren'



ENERGIE



TRANSPORT



**FINANCIËLE
INSTELLINGEN**



GEZONDHEID



WATER



**DIGITALE
INFRASTRUCTUUR**



**LOKALE
OVERHEID**



RUIMTEVAART

BELANGRIJKE ENTITEITEN 'andere kritieke sectoren'



**POST- EN
KOERIERSDIENSTEN**



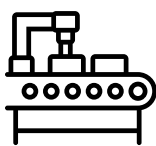
**AFVAL-
VERWERKING**



CHEMIE



VOEDSEL



**ALGEMENE
PRODUCTIE**



**DIGITALE
AANBIEDERS**



ONDERZOEK



3. VRAGEN DIE KLANTEN ONS STELLEN OVER NIS2



“
‘Waar kan ik zien of NIS2 voor mijn organisatie geldt?’

In de meeste gevallen kunt u afleiden of NIS2 van toepassing is op uw organisatie door de sectoren die als essentieel en belangrijk gemarkeerd zijn te controleren. Sommige Europese overheden hebben **tools voor zelf-assessment** gelanceerd om u te helpen. Bijvoorbeeld in Nederland: <https://regelhulpenvoorbedrijven.nl/NIS-2-NL/> en in Zweden: [Infosäkkollen \(msb.se\)](https://www.msb.se/infosakkollen).



“
‘Slechts een deel van mijn bedrijf valt in de categorie essentieel of belangrijk. Moet mijn hele organisatie voldoen aan NIS2?’



Misschien levert u verschillende diensten, die niet allemaal onder NIS2 vallen, of die in verschillende categorieën vallen. Bijvoorbeeld: een postdienst valt in de categorie ‘belangrijk’. Als hetzelfde postbedrijf ook transportdiensten aanbiedt, valt dit deel in de categorie ‘essentieel’. De Europese Commissie (EC) zal lidstaten richtlijnen geven over welke onderdelen van complexe organisaties onder het toepassingsgebied moeten vallen.



“
‘Ik weet niet zeker of NIS2 geldt voor mijn bedrijf; wat moet ik doen?’

Als u twijfelt, is het verstandig contact op te nemen met uw toezichthouder. Er zijn goede redenen om toch te streven naar compliance:

1. Als u een leverancier bent, kunnen uw klanten naleving eisen, zelfs als u technisch gezien niet onder NIS2 valt. Van hen wordt verwacht dat ze de beveiliging van hun toeleveringsketen controleren.
2. Van uw organisatie kan in de toekomst naleving worden geëist, bijvoorbeeld als u verwacht aanzienlijk in omvang en omzet te groeien.
3. Het uiteindelijke doel van NIS2 is om de cyberweerbaarheid van bedrijven in de hele EU te verhogen: door de richtlijn te gebruiken, versterkt u uw beveiliging, of de wetgeving nu wel of niet voor u geldt.



“
‘Mijn bedrijf heeft vestigingen in heel Europa. Als ik in Frankrijk voldoe aan NIS2, geldt dat dan ook voor vestigingen in Duitsland?’



Nationale wetten zijn meestal van toepassing op elke vestiging die fysiek in dat land aanwezig is. In complexe situaties zijn juridische expertise of EC-richtlijnen mogelijk nodig.



**NIS2 geldt voor
meer dan 160.000
entiteiten in de EU.**



**De NIS2-richtlijn
heeft 46 artikelen.
De artikelen 20-24
bevatten
informatie over
specifieke
cybersecurity
maatregelen die
bedrijven moeten
nemen.**

4. WAT ZIJN DE BELANGRIJKSTE EISEN VAN NIS2 EN WAT BETEKENEN DEZE IN DE PRAKTIJK?

NIS2 beschrijft allerlei vereisten en de samenwerking tussen de lidstaten in detail. De belangrijkste vereisten voor bedrijven worden gespecificeerd in de artikelen 20-24. Dit zijn enkele van de meest opvallende vereisten.

ARTIKEL 20

Het management van uw organisatie is verantwoordelijk voor NIS2-compliance

NIS2 stelt hoger management van bedrijven verantwoordelijk voor de naleving van wetgeving op het gebied van cyberbeveiliging. Deze verantwoordelijkheid is verschoven naar het hoogste niveau van organisaties. Dit is een grote verandering ten opzichte van de oorspronkelijke NIS-richtlijn.

In de praktijk betekent dit dat de leden van uw directie en management moeten kunnen beoordelen welke cyberbeveiligingsmaatregelen gepast zijn. Daarom vereist NIS2 expliciet dat directieleden een cybersecuritytraining volgen, zodat zij dit kunnen beoordelen.



ARTIKEL 20 NIS2-RICHTLIJN

‘De lidstaten zorgen ervoor dat de leden van de leidinggevende organen van essentiële en belangrijke entiteiten verplicht zijn een opleiding te volgen, en moedigen essentiële en belangrijke entiteiten aan hun werknemers regelmatig soortgelijke opleidingen aan te bieden.’





‘Ik heb de afgelopen jaren 24/7 aan NIS2 gewerkt. We wilden cybersecurity *Chefsache* maken, zoals ze in Duitsland zeggen: een zaak voor de CEO. Te lang is cybersecurity een zaak geweest voor de IT-man, die op de achtergrond werkte. Ik ben blij dat NIS2 er een bestuurskwestie van heeft gemaakt.’

Rapporteur Bart Groothuis, die namens het Europees Parlement onderhandelde over NIS2
- in een [Secura webinar over NIS2](#)

ARTIKEL 21

Uw organisatie is verplicht om passende maatregelen te nemen voor risicobeheer rond cybersecurity

NIS2 verplicht u om maatregelen te implementeren voor risicobeheer op het gebied van cyberbeveiliging en deze regelmatig bij te werken. Het gaat hierbij om technische en organisatorische strategieën die cyberincidenten voorkomen en hun impact verkleinen. De tekst van de richtlijn beschrijft tien van deze maatregelen in detail.

‘Je zou kunnen zeggen dat deze maatregelen de kern vormen van wat NIS2 betekent voor individuele bedrijven. Deze zullen redelijk wat moeite kosten om te implementeren: ze houden namelijk in dat je je cyberbeveiliging over de hele linie op orde moet krijgen, van mens tot proces en technologie’, legt consultant Bram Blaauwendraad van Secura uit. Hij voert NIS2 Gap Assessments uit voor uiteenlopende klanten.



ARTIKEL 21 NIS2-RICHTLIJN

‘De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheren.’



ARTIKEL 21 | 10 RISICOBEBEERSMAATREGELEN

- 1** **Beleid voor risicoanalyse**
NIS2 vraagt van u dat u een framework heeft voor risicobeheer en een beleid opstelt voor de beveiliging van informatiesystemen.
- 2** **Incident response**
U moet kunnen aantonen dat uw organisatie een cyberincident technisch aankan. Bijvoorbeeld: bestaat er een incident response plan?
- 3** **Bedrijfscontinuïteit**
Als het noodlot toeslaat, hoe gaat uw bedrijf er dan mee om? De richtlijn vereist dat u kunt laten zien dat u voorbereid bent op een crisis. In de tekst wordt specifiek gesproken over back-upbeheer, noodherstel en crisisbeheer.
- 4** **Beveiliging van de toeleveringsketen**
NIS2 verwacht van u dat u de beveiliging van uw supply chain controleert. Dit kan betekenen: weten hoe veilig uw leveranciers zijn en welke cybersecurity maatregelen zij nemen.
- 5** **Netwerk- en systeembeveiliging**
U moet kunnen aantonen dat uw netwerken en informatiesystemen veilig zijn, wanneer u ze koopt, ontwikkelt of onderhoudt.
- 6** **Beleid om effectiviteit te beoordelen**
Werken uw risicobeheersmaatregelen in de praktijk? NIS2 vraagt dat u dit kunt aantonen, bijvoorbeeld door tests en audits.
- 7** **Basis cyberhygiëne**
Uw organisatie is verplicht om de basis cyberhygiëne na te volgen. De richtlijn vereist ook dat u werknemers cybersecuritytraining aanbiedt.
- 8** **Cryptografie**
NIS2 verplicht u om beleid en procedures te hebben met betrekking tot het gebruik van cryptografie en, indien van toepassing, encryptie.
- 9** **Toegangsbeheer**
Wie heeft toegang tot de systemen? Hoe gaat u om met het in en uit dienst treden van werknemers? Hoe beheert u bedrijfsmiddelen? Dit zijn vragen die u zult moeten beantwoorden.
- 10** **Gebruik van multi-factor authenticatie**
NIS2 vereist dat u waar nodig MFA of andere authenticatieoplossingen gebruikt. Van de noodcommunicatiesystemen binnen uw organisatie wordt verwacht dat ze veilig zijn.

ARTIKEL 23

U bent verplicht om cyberincidenten te melden

Cybercriminelen stoppen niet bij landsgrenzen. Daarom wil NIS2 de samenwerking en informatie-uitwisseling rond cyberincidenten in de hele EU verbeteren. Dat betekent dat van u wordt verwacht dat u belangrijke incidenten binnen een bepaalde tijd meldt bij de relevante autoriteiten. Welke autoriteiten dat zijn, bepalen de lidstaten zelf.

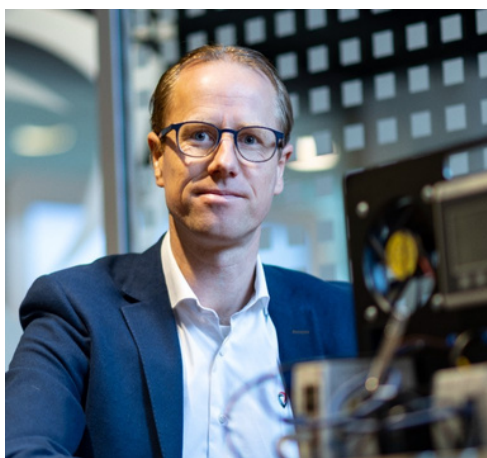
- Eerste melding binnen 24 uur
- Eerste rapport binnen 72 uur
- Volledig rapport binnen een maand na melding

Het melden van incidenten klinkt simpel, maar deze vereiste heeft vergaande gevolgen. Om goed te kunnen rapporteren, heeft u immers goede detectie nodig, inclusief follow-up: denk aan incident response en forensisch onderzoek. Het is ook belangrijk dat u weet of deze maatregelen goed werken. Dit betekent een investering in procedures voor business continuity of crisisoefeningen.

“

ARTIKEL 23 NIS2-RICHTLIJN

“Elke lidstaat zorgt ervoor dat essentiële en belangrijke entiteiten hun CSIRT of, indien van toepassing, hun bevoegde autoriteit zonder onnodige vertraging in kennis stellen van elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten.”



“

‘Deze vereisten zijn eigenlijk dingen die voor elk bedrijf slim zijn om te doen. Zelfs als uw bedrijf niet onder NIS2 valt, is het een goed idee om deze vereisten te gebruiken om weerbaarder te worden tegen cyberaanvallen.’

Sjoerd Peerlkamp
Manager Industriële Marktgroep Secura



Het woord 'crisis' wordt 32 keer genoemd in de NIS2-tekst: de richtlijn geeft prioriteit aan het goed omgaan met incidenten.



‘Het is nog niet volledig duidelijk hoe de Europese richtlijnen door Nederland zullen worden geïnterpreteerd. Wel is duidelijk dat het beveiligingsniveau van veel ondernemingen omhoog moet. Onze 24x7 monitoring en response dienst (SOC) biedt een complete en toegankelijke oplossing voor het MKB, die aansluit op de doelstellingen van NIS2. Hierdoor kan het MKB, ondanks beperktere middelen, effectief beschermd worden tegen cyberdreigingen.

Wolter Buijs, eigenaar Masero



Overweging (56)

De EU wil dat MKB-bedrijven extra aandacht krijgen

In de 46 wetsartikelen gaat het over ‘vereisten’ en ‘verplichtingen.’ In de uitgebreide toelichting op de wettekst van NIS2, met 144 overwegingen, legt de EU de motivatie uit achter de richtlijn. Een opvallende overweging is nummer 56. Daarin stelt de EU vast dat kleine en middelgrote ondernemingen steeds vaker het doelwit worden van aanvallen op de toeleveringsketen, omdat zij minder strenge maatregelen voor het beheer van cyberbeveiligingsrisico’s en aanvalsbeheer nemen, en omdat zij beperkte beveiligingsmiddelen hebben. Een aanval op een MKB-bedrijf kan zo leiden tot een aanval op een groter bedrijf, als een sneeuwbal.

Daarom roept de EU lidstaten op om via hun nationale cyberbeveiligingsstrategieën kleine en middelgrote ondernemingen helpen de uitdagingen in hun toeleveringsketen aan te pakken.



OVERWEGING (56) NIS2-RICHTLIJN

‘De lidstaten moeten in hun nationale cyberbeveiligingsstrategieën rekening houden met de specifieke behoeften van kleine en middelgrote ondernemingen op het gebied van cyberbeveiliging.’



5. Hoe verhoudt NIS2 zich tot standaarden als ISO 27001?

De kans is groot dat uw organisatie al een cyberbeveiligingsnorm gebruikt om risico's te beheren, bijvoorbeeld ISO 27001. 'Het is zinvol om een internationaal erkende standaard als ISO 27001 te gebruiken als benchmark om NIS2-compliance te bereiken', zegt Bram Blaauwendraad. 'Er is ook veel overlap tussen de NIS2-richtlijn en de ISO 27001-norm: 80 tot 90% van de NIS2-compliance wordt waarschijnlijk gedekt als u ISO 27001-gecertificeerd bent.'

Maar een ISO 27001-certificering betekent niet automatisch dat u NIS2-compliant bent. De scope van uw ISO 27001-certificering kan te beperkt zijn voor NIS2-compliance. Er zijn ook verschillende NIS2-vereisten die niet worden gedekt door ISO 27001, bijvoorbeeld de verantwoordelijkheid van de directie of de monitoring die van u wordt verwacht rond de security van uw toeleveringsketen. Dit betekent dat het verstandig is om controleren op hiaten tussen de NIS2-richtlijn en de norm die u gebruikt.



Hoe verhoudt NIS2 zich tot andere cybersecurity standaarden?

ISO 27001 is niet de enige norm die kan worden gebruikt om de naleving van NIS2 te meten. Het maakt niet veel uit welke standaard u kiest, zolang u kunt beargumenteren dat deze standaard het meest relevant is voor uw organisatie en dat de standaard van voldoende kwaliteit is.

Er zijn verschillende tools beschikbaar om de vereisten van NIS2 tegen de verschillende standaarden te leggen. [ENISA heeft een hulpmiddel](#) om de verschillende beveiligingsmaatregelen van de huidige NIS-richtlijn in kaart te brengen met standaarden zoals ISO 27001, NIST CSF en ISA/IEC 62443. Naar verwachting zal deze tool worden bijgewerkt zodat deze ook de NIS2-richtlijn omvat.

6. Hoe Masero en Secura u helpen bij het bereiken van NIS2 compliance

Het vertalen van de eisen van de NIS2-richtlijn naar praktische en passende maatregelen vereist specifieke expertise. Secura en Masero kunnen u helpen NIS2-compliance te bereiken. Dit doen wij al voor een groot aantal klanten.

Masero biedt u een complete SOC-dienst, zodat u uw detectie en respons verbetert.

Hierdoor worden incidenten real-time gedetecteerd en veelal in de kiem gesmoord, voordat serieuze schade ontstaat.



1. Actieve dreigingsdetectie en respons

Masero's monitoringdiensten detecteren en analyseren voortdurend mogelijke dreigingen in real-time. Dit stelt ons in staat om niet alleen snel op aanvallen te reageren, maar ook om aanvallen te voorkomen door afwijkend gedrag vroegtijdig te herkennen.



2. Gebruik van geavanceerde opsporingstools

Masero maakt gebruik van moderne opsporingsinstrumenten, die specifiek gericht zijn op de risico's waar het MKB mee te maken heeft. Deze tools zijn ontworpen om de beveiliging van netwerken te verbeteren en inbreuken te voorkomen.



3. Snelle respons en beperking van schade

Bij detectie van een dreiging biedt Masero's SOC-dienst direct responsmaatregelen, zoals het isoleren van systemen of het neutraliseren van bedreigingen, wat het risico op schade minimaliseert. Daarnaast zorgen we voor post-incident rapportages en analyse, zodat u uw cyberstrategie verder kunt versterken.

“De diensten van Masero zijn toegankelijk, betaalbaar en afgestemd op de behoeften van het MKB. Door de schaalbaarheid van onze SOC-dienst profiteert het MKB van dezelfde technologieën als grote organisaties, zonder de hoge kosten die hier meestal bijhoren.”

Elmer Evers, Sales Directeur Masero



Secura biedt u trainingen en assessments om stappen te zetten naar NIS2 compliance.



NIS2 Boardroom Training

Deze eendaagse training helpt uw management bij het beoordelen welke maatregelen nodig zijn om uw organisatie te beschermen tegen cyberdreigingen. Na het volgen van deze 1-daagse training voldoet uw directie aan de NIS2 trainingseis en ontvangt u een certificaat.



NIS2 Gap Assessment

U kunt ook een NIS2 Gap Assessment uitvoeren. Wat is het beveiligingsniveau van uw organisatie? Welke hiaten zijn er op het gebied van NIS2-compliance en welke stappen zijn nodig om deze te overbruggen? Als u dat wilt, kunnen wij een concrete routekaart naar compliance voor u opstellen.



Breed aanbod aan cybersecuritydiensten

Het overbruggen van de hiaten vereist verschillende acties voor elke organisatie. Wij kunnen u helpen met een breed scala aan diensten op het gebied van cyberbeveiliging.

Misschien blijkt dat een investering nodig is in awareness: wij bieden een SAFE Awareness Programma. Heeft u een incident response-plan nodig? Incident Response PRO kan u daarbij helpen. U kunt ook technische penetratietests en vulnerability assessments uitvoeren, om ervoor te zorgen dat uw netwerken en systemen veilig zijn.



Wat onze klanten zeggen

“Gelukkig zijn we op tijd gestart”

“We dachten dat er wel waren voor NIS2, want we zijn ISO 27001 gecertificeerd. Maar uit het Gap Assessment van Secura bleek dat onze ISO certificering sommige kritieke processen niet dekte.”



MASERO

CYBER SECURITY

Over Masero

Masero Cyber Security helpt organisaties om zich te beschermen tegen cyberdreigingen en dataverlies. We adviseren organisaties op het gebied van beleid en procedures die nodig zijn voor een hoogwaardige cybersecuritystrategie. Masero geeft u inzicht in de status van uw cyber-veiligheid, zowel technisch als organisatorisch en biedt daarnaast een 7x24 uur monitoring & response dienst (SOC, in Nederland) om uw omgeving continu te bewaken. Ons team van SOC-analisten staat 7x24 paraat om cybersecurity-incidenten van elk formaat vroegtijdig te detecteren, te analyseren en te mitigeren zodat uw kostbare bedrijfsinformatie geen gevaar loopt.



Neem contact op

Wilt u meer weten over hoe Masero u helpt met NIS2? Neem contact met ons op.



elmer.evers@masero.nl



+31 (0)6 50 697 439



Over Bureau Veritas / Secura

Secura is een gespecialiseerd security-bedrijf. Wij bieden organisaties waardevol inzicht in hun digitale beveiliging, met aandacht voor mens, proces en technologie. Secura biedt audit-, test- en certificeringsdiensten in de wereld van IT, IoT en OT. We voeren onze audits en tests uit volgens internationale normenkaders en standaarden. Secura is uw onafhankelijke, betrouwbare security-partner. Secura is onderdeel van de internationale Bureau Veritas Group.



Neem contact op

Wilt u meer weten over hoe Secura u helpt met NIS2? Neem contact met ons op.



info@secura.com



+31 (0) 88 888 3100