DECLERCQ
Advocaten · Notariaat

Secura
A BUREAU VERITAS COMPANY

PRAKTISCHE HANDLEIDING

Wat betekent NIS2 voor uw organisatie?

BUREAU VERITAS
1828

INHOUD

INHOUDSOPGAVE

‘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 eerste 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.

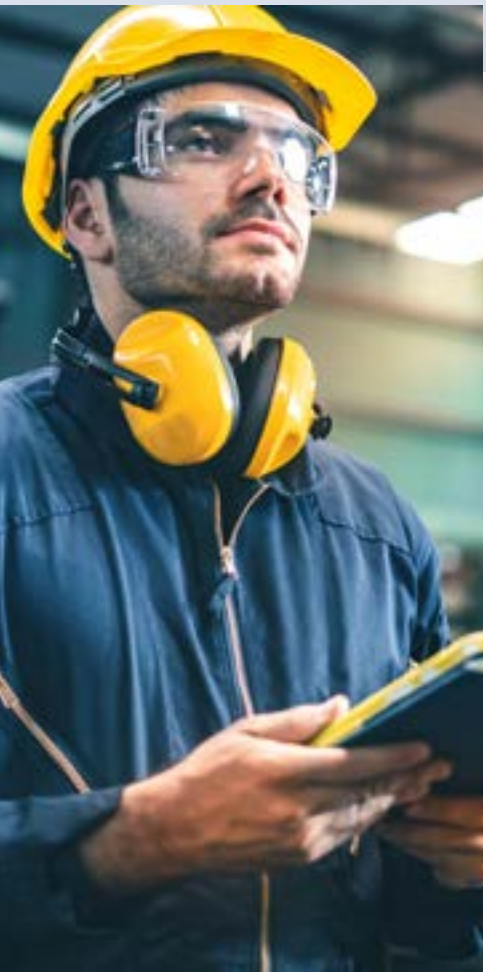
De reden voor NIS2: kritieke sectoren beschermen tegen toenemende cyberdreigingen. ‘Cybercriminaliteit is *big business* geworden, met een hele illegale economie die is opgezet om cybercriminaliteit te ondersteunen met dienstverleners, ronselaars en financiële diensten,' aldus Europols negende beoordeling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

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.

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 specifieker
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



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

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).

‘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.

3. 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.

NIS2 geldt voor meer dan 160.000 entiteiten in de EU.

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.

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

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 cybercybersecurity

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 Bram Blaauwendraad uit.

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 RISICOBEHEERSMAATREGELEN

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.

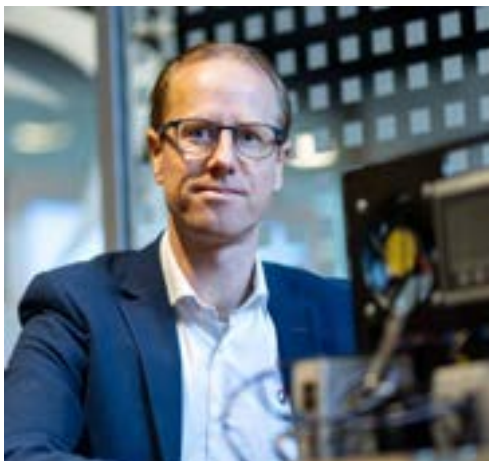
Het woord 'crisis' wordt 32 keer genoemd in de NIS2-tekst: de richtlijn geeft prioriteit aan het goed omgaan met incidenten.

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



4. 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.

5. Hoe serieus moet uw organisatie NIS2-compliance nemen?

Van organisaties wordt verwacht dat ze vanaf 18 oktober 2024 aan NIS2 voldoen. De gevolgen van niet-naleving zijn ernstiger voor essentiële entiteiten dan voor belangrijke entiteiten. De EU heeft benadrukt dat de handhaving van NIS2 serieuzer zal worden dan de handhaving op de huidige NIS-richtlijn. De artikelen 32 tot en met 34 gaan in op de sancties bij niet-naleving:

Essentiële entiteiten

- Meewerken aan willekeurige audits van bevoegde autoriteiten om er zeker van te zijn dat ze aan de regels voldoen.
- Mogelijke gevolgen zijn:
  - Zich houden aan bindende instructies
  - Extern toezicht
  - Management schorsen
  - Certificaten intrekken
- De maximale boete voor niet-naleving is 10 miljoen euro of 2% van de omzet

Belangrijke entiteiten

- Audits ondergaan na aanwijzingen van niet-naleving
- Mogelijke gevolgen zijn:
  - Zich houden aan bindende instructies

De maximale boete voor niet-naleving is 7 miljoen euro of 1,4% van de omzet

ARTIKEL 33 NIS2-RICHTLIJN

"Wanneer het bewijs, de aanwijzing of informatie wordt geleverd dat een belangrijke entiteit beweerdelijk deze richtlijn, en met name de artikelen 21 en 23, niet nakomt, zorgen de lidstaten ervoor dat de bevoegde autoriteiten zo nodig maatregelen nemen."

6. Waar te beginnen met NIS2-compliance?

NIS2 compliance omvat niet alleen cybersecurity-issues, maar heeft een sterke juridische component. Daarom werken Secura en De Clercq Advocaten en Notariaat veel samen rond NIS2. De Clercq specialiseert zich onder meer in wetgeving rond cybersecurity.

Wilt u erachter komen hoe u NIS2-compliance bereikt, dan helpt het als u zichzelf de volgende vragen stelt, adviseert Natascha van Duuren, partner bij De Clercq:

- Valt mijn organisatie in de ‘zeer kritieke’ of ‘andere kritieke’ categorie die NIS2 heeft aangewezen?
- Kwalificeer ik als een middelgrote onderneming volgens de EU-wetgeving?
- Is er sectorspecifieke wet- en regelgeving van de EU van toepassing op mijn organisatie op het gebied van cyberbeveiliging?
- Val ik onder de rechtsbevoegdheid van één lidstaat of onder de afzonderlijke en gelijktijdige rechtsbevoegdheid van meerdere lidstaten?
- Welke van mijn activiteiten en diensten moeten binnen het bereik van mijn risicoanalyses vallen?
- Hoe zorg ik ervoor dat de risicobeheersmaatregelen die ik neem als passend en evenredig worden beschouwd?

“

‘Wij kunnen u helpen bij het beantwoorden van al deze vragen, zodat u weet waar u aan toe bent en gericht en efficiënt kunt werken aan de naleving van NIS2.’

Natascha van Duuren
Advocaat en partner - De Clercq Advocaten en Notariaat

In 5 stappen starten met compliance

Als u er vrij zeker van bent dat uw bedrijf onder NIS2 valt, kunt u een paar dingen doen om u voor te bereiden op naleving. Omdat de vereisten als geheel tamelijk complex zijn, raden we u aan om voldoende tijd te nemen om deze te implementeren.

1. Betrek het management

Zorg ervoor dat de directie en het management op de hoogte zijn van NIS2 en zich ervan bewust zijn dat ze verantwoordelijk zijn voor naleving. Als eerste stap kunt u wellicht voorstellen dat de directie een training volgt.

2. Voer een gap assessment uit

Zijn er hiaten tussen uw bestaande beveiligingsmaatregelen en de NIS2-eisen voor organisaties die de artikelen 21-24 voorschrijven? Een inventarisatie van deze verschillen is een goed startpunt. Dit is ook iets om met het management af te stemmen.

3. Maak een roadmap

Om naleving te bereiken, is het van belang dat u eventuele tekortkomingen aanpakt. De volgende stap kan daarom zijn om een concrete roadmap op te stellen waarin staat hoe en wanneer u deze hiaten wilt oplossen.

4. Kom meer te weten over uw toezichthouder en uw rapportageverplichtingen

Welke instantie houdt toezicht op uw organisatie? Bij welke instantie bent u verplicht om cyberincidenten te melden? Het is verstandig om dit onderzoek nu uit te voeren. U kunt uw toezichthouder vinden met behulp van de tool voor NIS-richtlijnen van ENISA. Deze tool zal naar verwachting worden bijgewerkt voor NIS2.

5. Discussieer met branchegenoten

Welke maatregelen nemen andere bedrijven in uw sector om naleving te bereiken? Hoe hebben zij eventuele problemen opgelost? Discussiëren met collega's kan u waardevolle inzichten opleveren.

7. Hoe wij u kunnen helpen bij het bereiken van NIS2 compliance

Het vertalen van de eisen van de NIS2-richtlijn naar praktische en passende maatregelen vereist specifieke expertise. Wij kunnen u helpen NIS2-compliance te bereiken. Dit doen wij al voor een aantal klanten. U heeft de keuze uit de volgende NIS2-services:

NIS2 Boardroom Training

Deze eendaagse training helpt uw management bij het beoordelen welke maatregelen nodig zijn om uw organisatie te beschermen tegen cyberdreigingen. We bieden deze training aan in samenwerking met De Clercq Advocaten en Notariaat. 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.

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

Over De Clercq Advocaten en Notariaat

De Clercq Advocaten en Notariaat is onder meer gespecialiseerd in IT, Privacy & Cybersecurity. De Clercq begeleidt cliënten bij compliancy trajecten op het gebied van privacy en security. Daarnaast maakt De Clercq regelmatig onderdeel uit van een incident response team, waarbij zij de lead heeft in de afhandeling van de juridische aspecten van een cyberincident.

Neem contact op

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

n.vanduuren@declercq.com

+31 (0)71-581 53 08