adesso

Insight into NIS2 Directive

INLEIDING

De laatste jaren is er wereldwijd een aanzienlijke toename van cyberdreigingen geweest. Mede door deze ontwikkeling werkt de Europese Unie sinds 2020 aan de Netwerk- en Informatiebeveiliging (NIS2) -richtlijn. Deze richtlijn heeft als doel de digitale veerkracht van Europese lidstaten te vergroten.

www.consilium.europa.eu/en/infographics/cyber-threats-eu/

De NIS2-richtlijn streeft naar een grotere Europese harmonisatie en een hoger niveau van cybersecurity voor bedrijven en organisaties. NIS2 is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB, die in 2016 is opgenomen in de Nederlandse Wet beveiliging netwerk- en informatiesystemen (Wbni).

De wereldwijde ransomware-pandemie benadrukt de urgentie van NIS2. Het is niet langer de vraag óf bedrijven worden aangevallen, maar wanneer ze worden aangevallen. De gevolgen van een cyberaanval kunnen rampzalig zijn voor bedrijven, waaronder datalekken, financiële verliezen, reputatieschade en verlies van vertrouwen onder klanten.

Hoe zal de NIS2-richtlijn de veerkracht van cybersecurity in alle Europese lidstaten versterken? Is het verplicht voor uw organisatie om aan deze richtlijn te voldoen? En welke maatregelen worden genomen voor handhaving en straffen met betrekking tot schendingen van NIS2? Na het lezen van deze whitepaper zult u antwoorden hebben op deze vragen.

"NIS2 zal leiden tot een betere samenwerking tussen de verschillende Europese lidstaten op het gebied van cybersecurity, aangezien het informatie delen gemakkelijker en efficiënter zal faciliteren."

JAN HEUKER
CEO | adesso Nederland

2. NIS2 IN HET KORT

De Netwerk- en Informatiesystemen (NIS)-richtlijn, oorspronkelijk aangenomen in juli 2016, had tot doel cybersecurity- en cyberveerkrachtcapaciteiten in de Europese Unie te verbeteren. Het doel was om beveiligingsmaatregelen vast te leggen voor digitale dienstverleners en operators om cyberrisico's te verminderen. Door de voortdurende evolutie en toename van cyberaanvallen, samen met de brede adoptie van cloud computing, bleek de NIS-richtlijn ontoereikend om het complexe landschap van bedrijfssystemen effectief aan te pakken.

www.consilium.europa.eu/en/infographics/cyber-threats-eu/

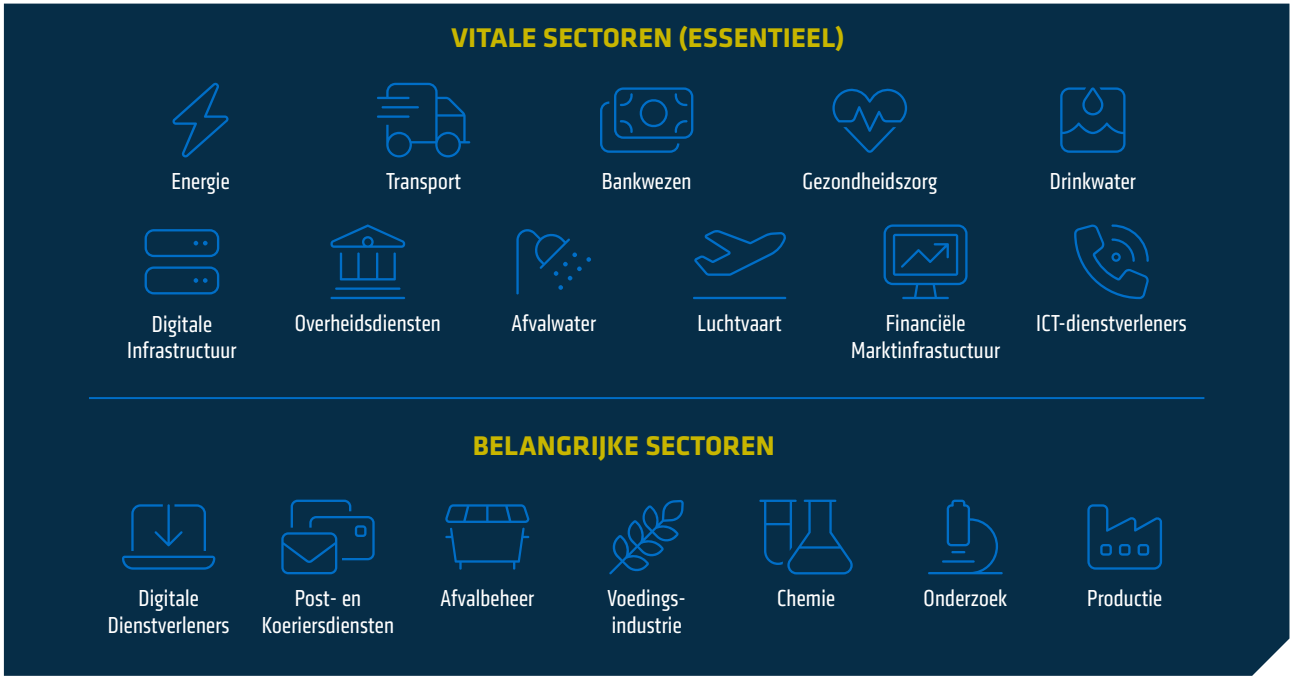
Als reactie hierop heeft de Europese Unie de NIS2-richtlijn geïntroduceerd. In tegenstelling tot de oorspronkelijke NIS-richtlijn stelt NIS2 strengere eisen en omvat het een breder scala van sectoren, met de nadruk op het waarborgen van de bedrijfscontinuïteit van getroffen organisaties. Tot medio 2024 hebben Europese lidstaten de tijd de NIS2-richtlijn in hun nationale wetgeving te implementeren. Conform de richtlijn dienen specifieke sectoren, zowel publieke als private organisaties, een zorgplicht en meldingsverplichting in hun beleid op te nemen. Het overkoepelende doel van de NIS2-richtlijn is het versterken van de cybersecuritystrategieën van organisaties en ze beter voorbereiden op mogelijke cyberdreigingen, en uiteindelijk een veiligere digitale omgeving creëren in reactie op de voortdurend veranderende aard van cyberdreigingen.

BELANGRIJKSTE PUNTEN VAN NIS2

- **Versterking van opgelegde beveiligingseisen.**
- **Aandacht voor de beveiliging van toeleveringsketens.**
- **Verbetering en stroomlijning van meldingsverplichtingen.**
- **Stricter toezicht.**
- **Invoering van handhavings-vereisten met geharmoniseerde sancties in alle Europese lidstaten.**

3. WELKE SECTOREN EN ORGANISATIES VALLEN ONDER DE NIS2-RICHTLIJN?

De NIS2-richtlijn richt zich op sectoren die al gedekt werden door de eerste NIS-richtlijn en op verschillende nieuwe industrieën. Dit betekent dat het aantal publieke en private organisaties dat onder de richtlijn valt, toeneemt. NIS2 maakt onderscheid tussen vitale sectoren, waarbij het belangrijkste verschil ligt in monitoring en naleving van de regels. De organisaties die onder de tweede NIS-richtlijn vallen, zijn onder andere:



3. WELKE SECTOREN EN ORGANISATIES VALLEN ONDER DE NIS2-RICHTLIJN?

ESSENTIËLE ENTITEITEN

Een organisatie wordt als groot beschouwd op basis van de volgende criteria:

ten minste 250 werknemers of

een jaarlijkse omzet van meer dan € 50 miljoen en

een balanstotaal van meer dan € 43 miljoen.

BELANGRIJKE ENTITEITEN

Een organisatie wordt als middelgroot beschouwd op basis van de volgende criteria:

ten minste 50 werknemers of

een jaarlijkse omzet van meer dan € 10 miljoen.

HET VERSCHIL TUSSEN ESSENTIEEL EN BELANGRIJK:

Organisaties kunnen worden ingedeeld als 'essentieel' of 'belangrijk', het belangrijkste verschil ligt in toezicht en naleving van regelgeving. Daarom verschilt de handhavingsaanpak tussen deze twee categorieën. Voor essentiële organisaties die opereren in vitale sectoren, zal het toezicht proactief zijn. Dit betekent dat de overheid actief zal monitoren om ervoor te zorgen dat deze organisaties voldoen aan de wettelijke vereisten. Voor essentiële aanbieders daarentegen vindt het toezicht retrospectief plaats, bijvoorbeeld wanneer er een incident optreedt. Deze organisaties kunnen ook gevolgen ondervinden als wordt vastgesteld dat ze niet juist hebben gehandeld en de nodige stappen hebben ondernomen.

"Essentiële entiteiten hebben een grotere impact op de samenleving in geval van falen dan belangrijke entiteiten. Essentiële entiteiten zijn daarom onderhevig aan intensiever toezicht, zowel proactief als retrospectief. Belangrijke entiteiten daarentegen worden alleen retrospectief gecontroleerd, meestal in gevallen van aanwijzingen van niet-naleving of na een incident."

JAN HEUKER
CEO | adesso Nederland

4. WELKE ORGANISATIES MOETEN VOLDOEN AAN

Alle organisaties die onder de NIS2-richtlijn vallen, moeten voldoen aan hun zorgplicht, met inbegrip van een lijst van vereiste maatregelen. Enkele voorbeelden van deze maatregelen zijn:

> Risicobeoordeling: Zorgen dat een organisatie voldoende aandacht besteedt aan de beveiliging van informatiesystemen.
> Crisismanagement en operationele continuïteit bij een aanzienlijk cyberincident.
> Zorgen voor de beveiliging van de toeleverings-keten en netwerk- en informatiesystemen.
> Het gebruik van cryptografie en versleuteling.
> Het hebben van beleid en procedures om de effectiviteit van risicobeheersingsmaatregelen te beoordelen.

Bovendien schrijft de NIS2-wetgeving rapportage-verplichtingen voor voor alle organisaties die onder deze regeling vallen. Dit betekent dat organisaties verplicht zijn incidenten binnen 24 uur na bewustwording te melden. Binnen één maand na de melding moet een uitgebreider rapport worden ingediend. Een belangrijke verandering is dat de gehele leiding van zowel vitale als essentiële organisaties gezamenlijk aansprakelijk is als de organisatie wordt getroffen door ransomware en wordt geconstateerd dat onvoldoende preventieve maatregelen zijn genomen.

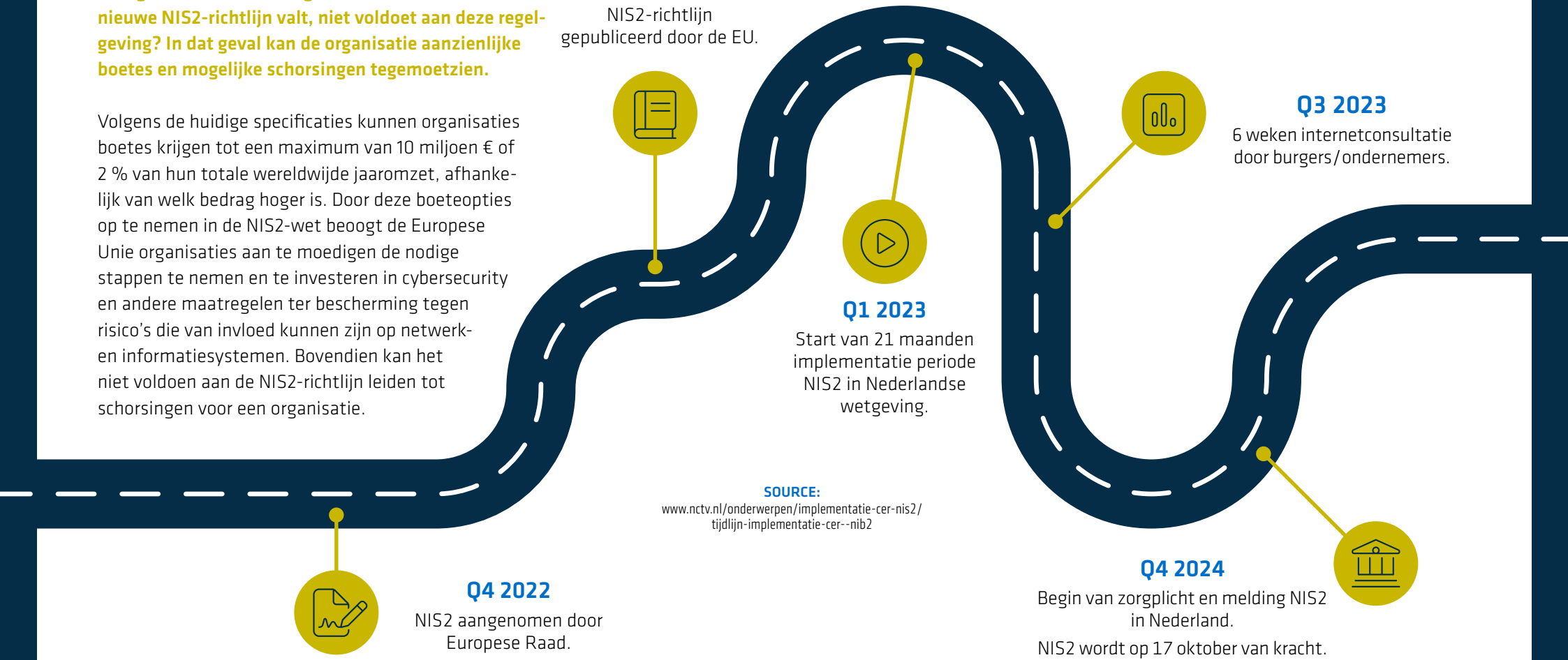
"Het feit dat de gehele leiding gezamenlijk aansprakelijk is, benadrukt het belang en de urgentie van het voldoen aan de vereisten van NIS2."

JAN HEUKER
CEO | adesso Nederland

5. BOETES EN SCHORSINGEN

Wat gebeurt er als een organisatie die onder de nieuwe NIS2-richtlijn valt, niet voldoet aan deze regelgeving? In dat geval kan de organisatie aanzienlijke boetes en mogelijke schorsingen tegemoetzien.

Volgens de huidige specificaties kunnen organisaties boetes krijgen tot een maximum van 10 miljoen € of 2 % van hun totale wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is. Door deze boeteopties op te nemen in de NIS2-wet beoogt de Europese Unie organisaties aan te moedigen de nodige stappen te nemen en te investeren in cybersecurity en andere maatregelen ter bescherming tegen risico's die van invloed kunnen zijn op netwerk- en informatiesystemen. Bovendien kan het niet voldoen aan de NIS2-richtlijn leiden tot schorsingen voor een organisatie.



Q4 2022
NIS2-richtlijn gepubliceerd door de EU.

Q1 2023
Start van 21 maanden implementatie periode NIS2 in Nederlandse wetgeving.

Q3 2023
6 weken internetconsultatie door burgers/ondernemers.

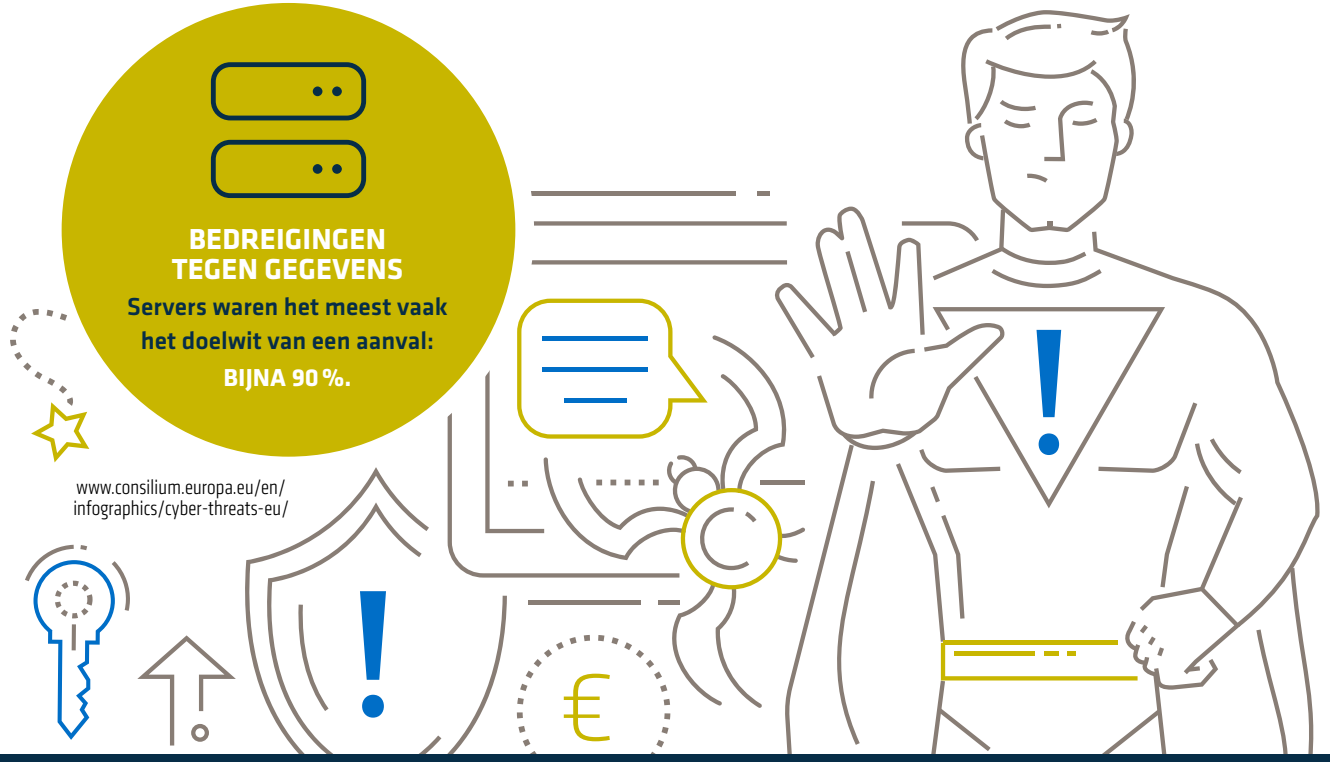
Q4 2022
NIS2 aangenomen door Europese Raad.

Q4 2024
Begin van zorgplicht en melding NIS2 in Nederland.
NIS2 wordt op 17 oktober van kracht.

SOURCE:
www.nctv.nl/onderwerpen/implementatie-cer-nis2/tijdlijn-implementatie-cer--nib2

6. WAT KUNNEN ORGANISATIES VOORAF DOEN TER VOORBEREIDING?

In afwachting van nationale wetgeving kunnen organisaties proactief stappen ondernemen om te voldoen aan hun zorgplicht door de beveiliging en veerkracht van hun processen en diensten te verbeteren. Op de websites van het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center worden verschillende maatregelen beschreven die organisaties kunnen implementeren om zich beter te beschermen tegen de risico's en schade veroorzaakt door cyberaanvallen. Enkele voorbeelden zijn:



- Het in kaart brengen van gebruikte netwerk- en informatiesystemen.
- Identificatie en analyse van risico's.
- Ontwikkeling van bedrijfscontinuïteitsplannen en protocollen voor crisismanagement en incidentrespons.
- Identificatie van alternatieve toeleveringsketens.
- Bewustwording van personeel met betrekking tot risico's en benodigde maatregelen.
- In kaart brengen van hun eigen activa, inclusief netwerk- en informatiesystemen.

Het is ook raadzaam om het budget en de middelen toe te wijzen die nodig zijn om te voldoen aan de richtlijnen.

7. ADESSO EN NIS2: HOE ONDERSTEUNEN WIJ BEDRIJVEN

Ontdek hoe adesso uw bedrijf kan helpen om te voldoen aan de NIS2-richtlijnen, zowel nu als in de toekomst. Als strategische partner zijn we gespecialiseerd in het ondersteunen van organisaties bij het voldoen aan hun NIS2-compliance-eisen. Onze uitgebreide diensten variëren van advies tot een geautomatiseerde NIS2-gereedheidsbeoordeling, waarmee uw traject naar NIS2-compliance wordt gestroomlijnd.

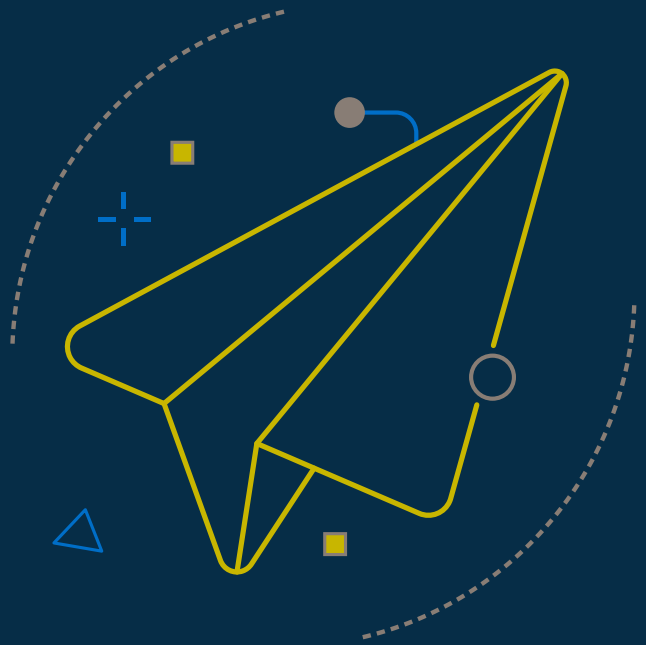
Ons team biedt de expertise die nodig is om de complexiteiten van NIS2 te doorgronden, aangevuld met een geavanceerd beoordelingsinstrument dat ervoor zorgt dat uw IT-omgeving volledig is voorbereid om aan alle NIS2-vereisten te voldoen.

https://www.adesso.nl/NIS2readiness

Meer weten?
Neem contact op:

PIETER KUIJER
Business Manager
adesso NL

Pieter.Kuijer@adesso.nl
+31 6 2741871
linkedin.com/in/pieterkuijer
www.adesso.nl



Zijn er vragen?

info@adesso.nl | www.adesso.nl

adesso Nederland

Zoomstede 21 A
3431 HK Nieuwegein

info@adesso.nl
www.adesso.nl
www.linkedin.com/company/adesso-netherlands/
www.instagram.com/adesso_nl/
www.facebook.com/adessoNL/

DISCLAIMER

Deze whitepaper dient alleen ter informatie en vormt geen juridisch advies. Entiteiten dienen juridische en cybersecurityprofessionals te raadplegen voor uitgebreide begeleiding over NIS2-compliance.

SOURCES

www.nctv.nl/onderwerpen/implementatie-cer-nis2/critical-entities-resilience-directive-cer
www.nctv.nl/onderwerpen/implementatie-cer-nis2/network-and-information-security-directive-nis2
www.nctv.nl/onderwerpen/implementatie-cer-nis2/tijdlijn-implementatie-cer--nib2
www.kvk.nl/advies-en-informatie/veiligzakendoen/cybersecurity/europese-cyberwetten-dit-gaan-ze-voor-je-bedrijf-betekenen/