september 2023

WAT BETEKENT DE NIEUWE NIS2 WETGEVING VOOR JOUW ORGANISATIE?

WAT IS DE NIEUWE NIS2 WETGEVING?

De afgelopen jaren zien we dat diverse ontwikkelingen in toenemende mate de veiligheid van onze maatschappij en economie onder druk zetten. In het licht van deze ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de Network and Information Security (NIS2) directive. Deze richtlijn is gericht op een verbetering van de fysieke, digitale en economische weerbaarheid van Europese lidstaten.

De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van NIS2-richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. De NIS2 is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Naar verwachting zal de wet in oktober 2024 in werking treden nadat deze door het parlement is behandeld. De organisaties die onder de NIS2-richtlijn vallen moeten vanaf dat moment aan de zorgplicht en meldplicht voldoen.

BESTUURLIJKE AANSPRAKELIJKHEID

De NIS2-richtlijn stelt eisen aan het bestuur, risicobeheer, bedrijfscontinuïteit en de rapportage van dreigingen en incidenten aan de autoriteiten. Zo moet het management van een organisatie bekend zijn met de eisen van de NIS2 en de inspanningen op het gebied van risicobeheer. Bestuursleden moeten er bovendien op toezien dat regels worden nageleefd. Ze worden straks ook hoofdelijk aansprakelijk wanneer verplichtingen niet worden nageleefd.

Dit betekent dat directie en bestuur van een organisatie over voldoende kennis en vaardigheden moet beschikken om te kunnen inschatten welke gevolgen een cyberincident voor hun organisatie kan hebben. Daarnaast moeten ze concreet inzichtelijk hebben welke securitymaatregelen het bedrijf heeft genomen en of deze voldoen aan de wettelijke verplichtingen. Door het Nationaal Cyber Security Centrum en het Ministerie van Justitie en Veiligheid is een handreiking opgesteld waarin de minimum vereiste maatregelen uiteen worden gezet.

MELDPLICHT, DATALEKKEN EN BOETES

Er komt met NIS2 bovendien strenger toezicht op governance. Organisaties die de vereiste maatregelen niet voldoende implementeren, kunnen flinke boetes tegemoetzien. Gebrekkige naleving wordt niet alleen gecontroleerd door toezichthouders, organisaties hebben onder de nieuwe wet- en regelgeving zelf een meldplicht, vergelijkbaar met de meldplicht wanneer er een datalek geconstateerd is. Een NIS2-melding moet binnen 24 uur worden gedaan, gevolgd door een eindverslag, uiterlijk een maand later.

Daarnaast worden bedrijven die onder de NIS2-wetgeving vallen verplicht om binnen 24 uur een melding te maken van alle incidenten en datalekken waardoor zij geen dienstverlening meer kunnen uitoefenen. Ook zijn zij verplicht binnen een maand, na het afhandelen van het incident, een rapportage aan te leveren.

De NIS2 bevat ook een boeteclausule voor bedrijven. Voor bedrijven die als essentieel zijn aangemerkt, kan dit oplopen tot 10 miljoen euro of 2 procent van de totale jaaromzet. Voor bedrijven die als belangrijk worden beschouwd, kan de boete oplopen tot 7 miljoen euro of 4 procent van de jaaromzet. Zeker met het oog op deze boeteclausule is het voor bedrijven belangrijk te weten of zij moeten voldoen aan de NIS2. Er is echter geen kant-en-klare lijst waarin staat welke bedrijven hieronder vallen. Bedrijven zullen daarom zelf moeten kijken of zij aan de criteria voldoen.

WELKE ORGANISATIES VALLEN ONDER DE NIS2-RICHTLIJN?

De NIS2-richtlijn richt zich op sectoren die al onder de eerste NIS-richtlijn vallen en op een aantal nieuwe sectoren. De organisaties die onder de NIS2-richtlijn vallen behoren tot:

Essentiële entiteiten	**Belangrijke entiteiten**
Grote organisaties die actief zijn in onderstaande sectoren:	*Middelgrote* organisaties die actief zijn in een sector uit de eerste kolom en middelgrote en grote organisaties die actief zijn in onderstaande sectoren:
• Energie • Transport • Bankwezen • Infrastructuur financiële markt • Gezondheidszorg • Drinkwater • Digitale infrastructuur • Beheerders van ICT-diensten • Afvalwater • Overheidsdiensten • Ruimtevaart	• Digitale aanbieders • Post- en koeriersdiensten • Afvalstoffenbeheer • Levensmiddelen • Chemische stoffen • Onderzoek • Vervaardiging / manufacturing
Een organisatie is *groot* op basis van de volgende criteria: • minimaal 250 werknemers of; • een jaaromzet van meer dan € 50 miljoen en een balanstotaal van meer dan € 43 miljoen.	Een organisatie is *middelgroot* op basis van de volgende criteria: • minimaal 50 werknemers of; • een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

Micro- en kleine bedrijven vallen in principe niet onder de NIS2-richtlijn. De minister die verantwoordelijk is voor een bepaalde sector kan er echter wel voor kiezen om een micro- of klein bedrijf alsnog aan te wijzen op basis van een risicobeoordeling, bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de Nederlandse economie of maatschappij. In dat geval worden deze bedrijven hierover geïnformeerd door het desbetreffende ministerie.

Daarnaast zijn er nog micro- en kleine bedrijven die wel onder de NIS2-richtlijn vallen. Het gaat dan om bedrijven die actief zijn als aanbieder van vertrouwensdiensten, als register voor topleveldomeinnamen, als verleners van domeinnaamregistratiediensten of als aanbieder van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten, vallen wél automatisch onder

de NIS2-richtlijn. Overheidsinstanties uit de bovenstaande sectoren vallen ook automatisch onder NIS2-richtlijn.

WELKE MAATREGELEN MOETEN ORGANISATIES NEMEN?

Op het moment van schrijven (september 2023) is het nog steeds onduidelijk welke onderliggende beveiligingsmaatregelen het NIS2-risicobeheer omvat, omdat er geen verwijzing is naar specifieke beveiligingscontroles of een verwijzing naar een onderliggend raamwerk zoals ISO 27001 of CIS-controles. Dit betekent dat het enigszins onduidelijk blijft wat er onder NIS2 vereist is.

De letterlijke vertaling van de NIS2 richtlijn onder artikel 21 subparagraaf 2 stelt het volgende:

..[] een benadering die alle risico's omvat en die erop gericht is netwerk- en informatiesystemen en de fysieke omgeving van die systemen te beschermen tegen incidenten, en zal ten minste het volgende omvatten:

a. *beleid over risicoanalyse en informatiebeveiliging;*
b. *afhandeling van incidenten;*
c. *bedrijfscontinuïteit, zoals back-upbeheer en rampenherstel, en crisismanagement;*
d. *beveiliging van de toeleveringsketen, inclusief beveiligingsgerelateerde aspecten betreffende de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners;*
e. *beveiliging bij de verwerving, ontwikkeling en onderhoud van netwerk- en informatiesystemen, inclusief het omgaan met en openbaar maken van kwetsbaarheden;*
f. *beleid en procedures om de effectiviteit van cybersecurity risicobeheermaatregelen te beoordelen;*
g. *basispraktijken voor cyberhygiëne en training in cybersecurity;*
h. *beleid en procedures met betrekking tot het gebruik van cryptografie en, waar passend, encryptie;*
i. *beveiliging van human resources, toegangsbeheerbeleid en assetmanagement;*
j. *het gebruik van multi-factor authenticatie of continue authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit, waar passend.*

Echter op basis van de huidige NIS regelgeving en publicaties van het Nationaal Cyber Security Centrum en het Nationaal Coördinator Terrorismebestrijding en Veiligheid van de overheid, kan worden gesteld dat organisaties ten minste de volgende risicobeheersmaatregelen dienen te nemen:

- *In kaart brengen van de gebruikte netwerk- en informatiesystemen*
- *Inventariseren en analyseren van risico's*
- *Opstellen van bedrijfscontinuïteitplannen en protocollen voor crisisbeheersing en het organiseren van incident response.*
- *Identificeren van alternatieve toeleveringsketens*
- *Bewustwording van personeel van risico's en te nemen maatregelen*
- *In kaart brengen van de eigen assests (dus de eigen netwerk- en informatiesystemen)*
- *Richt risicomanagement in*
- *Pas sterke authenticatie toe*
- *Bepaal wie toegang heeft tot uw data en diensten*
- *Beperk het aanvalsoppervlak*
- *Gebruik versleuteling*
- *Bescherm uw organisatie tegen verlies van gegevens*
- *Richt patchmanagement in*
- *Centraliseer en analyseer loginformatie*

NIS2 COMPLIANCY OPLOSSING VAN OBI VOOR ORGANISATIES

De risicobeheersmaatregelen die in de richtlijn zijn vast gesteld, overlappen grotendeels met het raamwerk van de *OBI ICT scan* die wij periodiek uitvoeren bij klanten als onderdeel van de standaard ICT dienstverlening om de veiligheid van het computernetwerk te waarborgen. De *OBI ICT scan* bestaat uit een risicobeoordeling met daaraan gekoppeld technische beheersmaatregelen om een computernetwerk als veilig te kunnen bestempelen.

De NIS2 richtlijn voorziet echter ook een Informatiebeveiligings management systeem. Dit betekent een Informatie beveiligingsstrategie, risico analyse en organisatorische beheersmaatregelen. Om u hierbij te helpen heeft OBI de *OBI NIS2 scan* ontwikkeld.

De *OBI NIS2 scan* helpt uw organisatie inzchtelijk te maken in hoeverre u voldoet aan de NIS2 wetgeving. Consultants van OBI helpen u vervolgens verder een strategie, een risicoanalyse en maatregelen te implementeren binnen uw organisatie om zo te voldoen aan de nieuwe NIS2 wetgeving. Denk hierbij aan een risico inventarisatie, een gedragscode met een IB beleid, on- en offboarding protocollen, een Business Continuïty Plan (BCP) en een Cyber Security Awareness programma voor uw medewerkers.

Wilt u ze zelf alvast aan de slag? Dan voorziet de overheid hierin met onderstaande tool:

NIS 2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)

OVER OBI

OBI is gespecialiseerd in volledige outsourcing van uw ICT. Dat betekent het bouwen, beheren en bewaken van uw ICT omgeving bij u op uw eigen locatie in combinatie met de laatste cloud-ontwikkelingen op gebied van Microsoft 365 en Microsoft Azure.

OBI ondersteunt uw medewerkers met een vriendelijke supportdesk en hoog opgeleide systeembeheerders. Om de beveiliging van uw computernetwerk te waarborgen maken wij gebruik van de laatste technieken op gebied van periodieke ICT scans en -audits, ticketsoftware en server bewaking- en monitoringsystemen om de kans op downtime, hack aanvallen en ransomware te minimaliseren.

Daarnaast ondersteunt OBI met het helpen voldoen aan de AVG privacywetgeving en de nieuwe NIS2 wetgeving met security officers die u helpen de juiste organisatorische beheersmaatregelen te implementeren, zoals een risico inventarisatie, een gedragscode met een IB beleid, on- en offboarding protocollen, een BCP en een Cyber Security Awareness programma voor uw medewerkers.

OBI bestaat sinds 01-01-2001 en bestaat uit een team van 20 mensen. OBI is ISO27001 gecertificeerd en heeft een brede klantenkring opgebouwd van organisaties tussen de 20 en 300 computerwerkplekken, wat een hoge continuïteit van dienstverlening garandeerd.

BRONNEN

Voor dit artikel zijn als bron de volgende websites gebruikt van overheidsinstanties:

- https://www.nctv.nl/onderwerpen/implementatie-cer-nis2
- https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie
- https://www.digitaltrustcenter.nl/wat-gaat-de-nis2-richtlijn-betekenen-voor-jouw-organisatie
- https://digital-strategy.ec.europa.eu/nl/policies/nis2-directive

- https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen
- https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555 (NL vertaling NIS2 richtlijn)

OBI Automatisering www.obi.nl
Insulindelaan 111 +31(0)889008100
5642 CV Eindhoven www.linkedin.com/company/OBI-automatisering
Nederland KvK: 17130973 | BTW: NL 8093.61.048.B01