Eisen aan cyberveiligheid worden strenger en raken de hele keten

ABN·AMRO

Eisen aan cyberveiligheid worden strenger en raken de hele keten

Organisaties van kritisch maatschappelijk belang moeten vanaf oktober 2024 voldoen aan de Europese richtlijn NIS 2 die toeziet op informatiebeveiliging. De wet stelt dat deze organisaties hun digitale infrastructuur weerbaar maken tegen cyberaanvallen, incidenten binnen 24 uur melden, onder toezicht komen en flinke boetes krijgen bij overtredingen. Ook leveranciers die niet onder de wet vallen, moeten hun zaken op orde brengen. De onder toezicht gestelde organisatie zullen dit namelijk van hun leveranciers eisen, daar cyberveiligheid een zaak is van de hele keten.

De nieuwe richtlijn betekent een aanzienlijke verruiming van de oude NIS-richtlijn uit 2016. Het aantal sectoren dat als 'kritisch' wordt aangemerkt wordt uitgebreid, de vereisten aan de informatiebeveiliging zelf worden scherper en voor de handhaving worden verschillende toezichthouders aangewezen. De richtlijn wordt vanaf 17 oktober 2017 van kracht, al zal de implementatie naar Nederlandse regelgeving naar verwachting pas in 2025 plaatsvinden. Bedrijven die echter zaken doen met bedrijven uit onder meer Duitsland en België krijgen indirect wel vanaf oktober met de wet te maken, omdat de implementatie in die landen op schema ligt.

Doel en belang NIS2

De nieuwe Europese richtlijn NIS2 en toenemende integratie en automatisering binnen toeleveringsketens verhogen de noodzaak voor veel organisaties om aanvullende maatregelen op het gebied van informatiebeveiliging te nemen. De NIS2-richtlijn, een afkorting van Network and Information Security 2, is door de Europese Unie vastgesteld met de intentie om informatiebeveiliging beter te regelen en uiteindelijk alle EU-lidstaten digitaal weerbaarder te maken tegen cyberaanvallen.

Dankzij voortschrijdende digitalisering in toeleveringsketens kunnen organisaties steeds sneller en efficiënter opereren. Een neveneffect van het koppelen van data, processen, systemen en het uitwisselen van digitale gegevens en software met externe partners is dat het netwerk complexer wordt waardoor het aantal potentiële bedreigingen toeneemt.

Wereldwijd stijgt het aantal supply chain-aanvallen de afgelopen jaren fors. De eisen die ketenpartners aan elkaar stellen nemen dan ook snel toe. Organisaties willen voorkomen dat ze slachtoffer worden van cybercriminaliteit via ketenpartners. Het is daarom belangrijk om samen met uw partners de minder goed beveiligde elementen in de supply chain te identificeren en te voorkomen dat die door aanvallers kunnen worden misbruikt.

Moet mijn organisatie voldoen aan de NIS2-richtlijn?

Reeds gereguleerd onder NIS1 | Toegevoegd onder NIS2

Sectoren bijlage 1	Sectoren bijlage 2
Energievoorziening	Post- en koeriersdiensten
Vervoer	Afvalstoffenbeheer
Bankwezen en infrastructuur voor financiële markten	Levensmiddelenbedrijven
Gezondheidszorg	Productie-, verwerking en distributie van chemische stoffen
Digitale infrastructuur (waaronder communicatie-netwerken, datacenters en cloudaanbieders)	Productie van onder andere medische hulp-middelen, machines en transportmiddelen
Drinkwatervoorziening	Digitale aanbieders (onlinemarktplaatsen, zoekmachines en sociale media)
Afval- en afvalwaterverwerking	Onderzoek
Overheid	
Ruimtevaart	
Beheer van IT-diensten (B2B)	

Welke bedrijven moeten zich aan de nieuwe wetten houden?

Essentiële bedrijven	Belangrijke bedrijven
Hieronder vallen **grote** organisaties actief in een van de sectoren onder 'bijlage 1'. Op deze bedrijven wordt proactief toezicht gehouden, dus middels audits en scans.	Hieronder vallen **grote** organisaties actief in een van de sectoren onder 'bijlage 2' en **middelgrote** organisaties actief in een van de sectoren onder 'bijlage 1' of 'bijlage 2'. Op deze bedrijven wordt reactief toezicht gehouden, wat betekent dat er enkel wordt ingegrepen als er aanwijzingen zijn dat iets niet goed gaat.
'**Groot**' houdt in: meer dan 250 werknemers of; een netto omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.	'**Middelgroot**' houdt in: minimaal 50 werknemers of; een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

***Kleinere bedrijven** vallen in principe niet onder de NIS2-richtlijn, maar kunnen wel individueel kunnen aangewezen op basis van een risicobeoordeling door het ministerie dat verantwoordelijk is voor de desbetreffende sector.*

Welke bedrijven worden indirect geraakt?

Leveranciers van essentiële- en belangrijke bedrijven

De bedrijven 'in scope' worden geacht kritisch naar de cyberveiligheid van hun leveranciers te kijken. Leveranciers krijgen dus via hun klanten te maken met de nieuwe wetten, ook als zij zelf niet in de categorie 'essentieel' of 'belangrijk' vallen. Dit betekent dat het speelveld ook voor kleinere bedrijven kan veranderen.

Vuistregel: Is uw een organisatie actief in een van bovengenoemde sectoren en heeft deze minimaal vijftig werknemers of een jaaromzet of balanstotaal van 10 miljoen euro of meer, dan valt uw organisatie hoogstwaarschijnlijk onder de NIS2-richtlijn.

Is de NIS2-richtlijn van toepassing op uw organisatie? Als hulpmiddel heeft de overheid een online tool ontwikkeld: de regelhulp voor bedrijven. Door middel van een zelf-evaluatie, bepaalt u of u een essentieel of belangrijk bedrijf hebt en dus binnen de scope van NIS2 valt.

Wat houdt de zorgplicht in?

Om uw organisatie goed te beschermen tegen cyberdreigingen zijn technische, operationele en organisatorische maatregelen noodzakelijk om de risico's op cyberincidenten te verkleinen en de bedrijfscontinuïteit te waarborgen. Zowel nationale normen zoals de Baseline Informatiebeveiliging Overheid (BIO) als internationale normenkaders zoals ISO 27001 bieden veel handvatten voor maatregelen om te voldoen aan de vereisten van de NIS2-richtlijn.

Voorbeelden van deze maatregelen zijn:

Cybercriminelen beginnen hun aanval steeds vaker door op bedrijfssystemen in te loggen met gebruikersnaam en wachtwoord. Hiermee wordt deze strategie inmiddels even vaak toegepast als phishing, dat juist aan populariteit inboette als initiële aanvalsmethode; in 2022 was phishing nog in maar liefst 41 procent van de gevallen het startpunt van een cyberaanval.

1.	Een risicoanalyse en beveiliging van informatiesystemen;	2.	Beleid en procedures over incidentenbehandeling;
3.	Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-up-beheer en noodvoorzieningenplannen;	4.	Beveiliging van de toeleverancierskete;
5.	Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons open bekend-making van kwetsbaarheden;	6.	Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen;
7.	Basis-cyberhygiëne en trainingen op het gebied van cyberbeveiliging;	8.	Beleid en procedures over het gebruik van cryptografie en encryptie;
9.	Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa;	10.	Het gebruik van Multi-Factor Authenticatie (MFA), beveiligde spraak-, video- en tekstcommunicatie en beveiligde nood-communicatiesystemen binnen de entiteit.

Cyberveiligheid en de toeleveringsketen

De cyberveiligheid van de toeleveringsketen is een van de sleutels om te kunnen voldoen aan de NIS2-vereisten. In de Europese NIS2-richtlijn hebben onder toezicht gestelde organisaties de zorgplicht voor de beveiliging van hun hele toeleveringsketen. Het gaat om beveiligingsaspecten met betrekking tot de relaties tussen elke organisatie en haar rechtstreekse leveranciers en dienstverleners.

In de praktijk betekent dit dat onder toezicht gestelde organisaties intensief in overleg moeten met hun leveranciers die ICT-diensten leveren of waarmee ze bestanden uitwisselen. Ze moeten zich ervan vergewissen dat hun leveranciers hun technologie, processen en personeel op orde hebben. De keten is immers zo sterk als de zwakste schakel.

Wat houdt de meldplicht in?

De NIS2-richtlijn verplicht organisaties om incidenten in de digitale dienstverlening binnen 24 uur te melden bij de toezichthouder. Of een incident meldingswaardig is hangt af van de tijdsduur van het incident, het aantal personen dat is geraakt en de financiële verliezen. Het is overigens nog niet bekend welke instanties als toezichthouder zullen optreden.

Een incident moet tevens worden gemeld bij het Computer Security Incident Response Team (CSIRT), dat vervolgens bijstand kan leveren. Indien er in uw sector geen CSIRT is, kan melding worden gedaan bij het Nationaal Cyber Security Centrum (NCSC). Na de initiële melding moet binnen 72 uur een verslag worden opgesteld met een gedetailleerde beschrijving van het incident en de mogelijke oorzaak van het incident. Binnen een maand na het incident moet een eindverslag worden ingeleverd waarin de maatregelen staan die zijn getroffen om de schade te beperken en herhaling te voorkomen.

Het is belangrijk om een procedure op te stellen voor het melden en afhandelen van incidenten die de organisatie in staat stelt om te voldoen aan de eisen van de NIS2-richtlijn. De ervaring die u heeft opgedaan bij de implementatie van de AVG-richtlijn kan hierbij helpen.

Wat houdt het toezicht in?

Organisaties die onder de NIS2-richtlijn vallen, moeten zich registeren en komen onder toezicht te staan. De toezichthouder controleert of de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht, worden nageleefd. De toezichthouder kan uw organisatie onderwerpen aan on-site inspecties, verzoeken om bewijsmateriaal, steekproefsgewijze controles en gerichte audits. Voor organisaties die als ‘essentieel’ worden aangemerkt, vindt het toezicht continu plaats. Voor ‘belangrijke’ organisaties vinden toezichtmaatregelen in geval van niet-naleving achteraf plaats.

Zodra de NIS2-richtlijn is omgezet in nationale wetgeving, kan de toezichthouder boetes opleggen bij het niet naleven van de verplichtingen. Het management van de organisatie is verplicht om ervoor te zorgen dat aan de vereisten van de NIS2-richtlijn wordt voldaan. Is dit niet het geval, dan kunnen de verantwoordelijke managers persoonlijk aansprakelijk worden gesteld en kan de organisatie boetes krijgen die kunnen oplopen tot 10 miljoen euro of een percentage van de jaaromzet.

Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in 3 stappen

1 **Maak een risico-analyse**
Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld een kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 **Neem adequate maatregelen**
Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:
- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te bepalen en te nemen.

3 **Stel een Cyber Response Plan op**
Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Cyber Trends Rapport 2024 (Lees het complete rapport)
Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Lees alle feiten en ontwikkelingen in het jaarlijkse rapport 'Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

Sectorspecifieke infosheets (Bekijk alle sectorspecifieke info)
Elke sector kent verschillende cyberrisico's. In de industrie sector is vaak de productie het doelwit van cybercriminelen, terwijl zij in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Whitepaper over Employee Awareness (Download onze Whitepaper)
Cybercriminelen komen vaak via medewerkers binnen in uw digitale systemen. Houd uw medewerkers scherp en maak hen bewust van de risico's van cybercrime – gebruik hiervoor onze whitepaper.

Third-Party Risk Management Checklist (Bekijk de checklist)
Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden.
Met Third-Party Risk Management brengt u deze in kaart.
- Identificeer mogelijke cyberrisico's
- Deel de checklist met uw klanten en leve- ranciers voor meer veiligheid

Cyber Response Plan (Maak uw Cyber Response Plan)
Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.
- Stel uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

Zo helpt ABN AMRO u

Cyber Veilig & Zeker van MMOX
Voor midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid
- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering
Voor zakelijke klanten die zich willen indekken tegen cyberschade
- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek
IVoor ondernemers die willen weten hoe zij ervoor staan op het gebied van cyberveiligheid
- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief