NIS2: Versterken van Digitale Veiligheid in Europa's Cyberspace

Nieuwe Europese wetgeving vereist proactieve cyberbeveiligingsmaatregelen

In een tijd van groeiende digitale afhankelijkheid en toenemende cyberdreigingen heeft de Europese Unie de Network and Information Security Directive herzien, resulterend in NIS2. Deze richtlijn, van kracht sinds januari 2023, versterkt de digitale weerbaarheid van lidstaten. Organisaties moeten zich voorbereiden op de eisen die in januari 2025 van kracht worden. Dit artikel onderzoekt de cruciale elementen van NIS2 en hoe organisaties er proactief aan kunnen voldoen, hun digitale veerkracht kunnen vergroten en de Europese digitale veiligheid kunnen verbeteren.

In het afgelopen decennium heeft een reeks ontwikkelingen geleid tot een toenemende druk op de digitale veiligheid van onze samenleving en economie. Dit is een gevolg van factoren zoals COVID-19, de voortdurende digitale transformatie en de groeiende dreiging van cyberaanvallen. Organisaties zijn steeds afhankelijker geworden van data en hebben zich ontwikkeld tot overwegend digitaal georiënteerde entiteiten. Deze afhankelijkheid gaat gepaard met het delen en verwerken van gegevens, wat het risico op ernstige bedrijfsstoringen verhoogt als deze gegevens of de bijbehorende verwerking niet beschikbaar zijn.

Bovendien worden deze gegevens niet alleen intern opgeslagen en verwerkt, maar ook bij hostingpartijen - cloudleveranciers - en gedeeld met diverse ketenpartijen, zoals leveranciers, dienstverleners en toezichthouders. Hoewel samenwerken met deze partners de focus op de kernactiviteiten van een organisatie vergroot, vereist het ook een centrale sturende rol in de beveiliging en betrouwbaarheid van de digitale gegevens.

Als reactie op deze dynamische ontwikkelingen heeft de Europese Unie sinds 2020 gewerkt aan de herziening van de Network and Information Security Directive (NIS) - de NIS2. Deze vernieuwde richtlijn trad op 16 januari 2023 in werking met als doel de digitale veerkracht van de lidstaten binnen Europa te versterken. Vanaf januari 2025 moeten organisaties die onder de NIS2 vallen, voldoen aan de eisen van deze wetgeving. Hoewel deze datum wellicht nog ver in de toekomst lijkt, bieden ervaringen met eerdere regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), waardevolle lessen over het belang van tijdige voorbereiding.

De NIS2 fungeert bovenal als een stimulans om de cyber- en informatiebeveiliging in de hele Europese Unie naar een hoger niveau te tillen - een doel dat elke organisatie zou moeten

omarmen. In dit artikel zullen we verkennen hoe organisaties proactief kunnen inspelen op de NIS2-vereisten. Bijvoorbeeld door de implementatie van ISO27001-richtlijnen, waarmee ze niet alleen aan de wetgeving voldoen, maar ook hun algehele digitale veerkracht versterken.

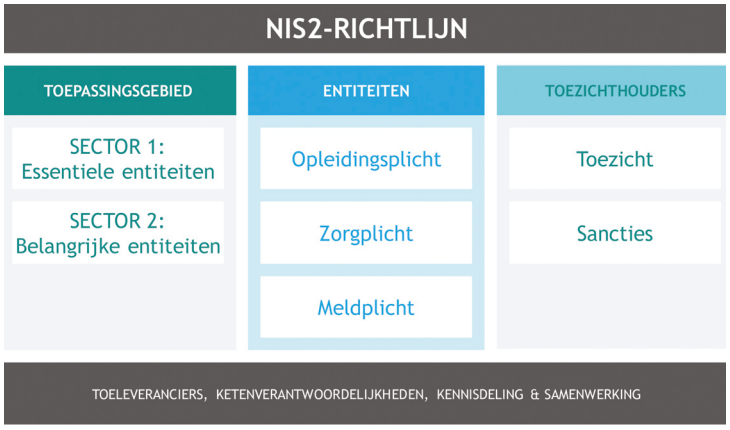
Wat is NIS2?

De NIS2-richtlijn, oftewel de 'Network and Information Security Directive', is de opvolger van de NIS-richtlijn: een belangrijke set regels en richtlijnen die bedoeld zijn om de digitale veiligheid en stabiliteit van essentiële diensten in de EU-lidstaten te waarborgen. De NIS2-richtlijn is opgesteld om ervoor te zorgen dat organisaties die vertrouwen op digitale systemen - zoals computers, netwerken en online diensten - robuuste beveiligingsmaatregelen implementeren. Ook streeft NIS2 naar het opzetten van een gemeenschappelijk kader voor de beveiliging van deze systemen, vooral die van kritieke sectoren zoals energie, transport, financiën en gezondheid. Dit is van cruciaal belang omdat cyberdreigingen, zoals hackers, malware en andere schadelijke activiteiten, steeds geavanceerder worden en de essentiële digitale infrastructuur kunnen verstoren of beschadigen.

De NIS-richtlijn is door de Nederlandse staat verwerkt naar nationale wetgeving. De Wet Beveiliging Netwerk- en Informatiesystemen (WBNI) is de Nederlandse wet die is opgesteld om te voldoen aan de verplichtingen van de NIS-richtlijn. De WBNI vertaalt de eisen en principes van de NIS-richtlijn naar nationale wetgeving en is bedoeld om de digitale veiligheid in Nederland te versterken. Met het herzien van de NIS-richtlijn ligt er dus een herziening van de WBNI in het verschiet en zullen herziene elementen uit de richtlijn nader moeten worden ingevuld of uitgewerkt. De omzetting en uitwerking van de NIS2-richtlijn in nationale wetgeving dient eind 2024 gereed te zijn, zodat entiteiten per januari 2025 kunnen en moeten voldoen aan de NIS2.

De NIS2-richtlijn omvat verplichtingen voor de Nederlandse staat om deze te verwerken naar nationale wetgeving, maar tevens verplichtingen om nadere invulling en verwerking vorm te geven. Bijvoorbeeld door het optuigen van toezicht en verantwoordingsstructuur, het faciliteren in een meldpunt voor incidenten (bij een zogeheten CSIRT – Computer Security Incident Response Team) en het faciliteren van samenwerkingen en kennisdeling.

Voor wie/wat is de NIS2 van toepassing?



Figuur 1: overzicht werking NIS2-richtlijn.

De NIS2 richt zich op organisaties die als essentieel of belangrijk worden beschouwd voor de continuïteit van vitale diensten en de digitale infrastructuur. Meer specifiek geldt dit voor die sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten.

De NIS2 is uitgebreider dan de NIS-richtlijn en beslaat een groter aantal organisaties waarop de richtlijn van toepassing is. De NIS maakt een onderscheid tussen essentiële en belangrijke entiteiten, verdeeld over twee categorieën/sectoren. Of een entiteit binnen een categorie/sector valt en wordt aangewezen

als essentieel of belangrijk, wordt mede bepaald door de omvang van de organisatie. Echter, wanneer een organisatie niet aan deze criteria voldoet, betekent dit niet dat deze niet hoeft te voldoen aan de NIS2. De Nederlandse overheid moet ervoor zorgen dat ook kleine ondernemingen en micro-ondernemingen voldoen aan de NIS2-richtlijn, wanneer deze een sleutelrol spelen in de samenleving of economie.

Hieronder staan de criteria die bepalen of een organisatie als belangrijk of essentieel wordt beschouwd:

SECTOREN - BIJLAGE I	SECTOREN - BIJLAGE II
Energie	Digitale aanbieders
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Vervaardiging/manufacturing
Beheerders van ICT-diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	
Beheer van ICT-diensten	

Figuur 2: essentieel en/of van belang zijnde beoordelingscriteria.

Essentiële entiteiten zijn grote organisaties die actief zijn in een sector uit Bijlage I van de NIS2-richtlijn. Een organisatie is groot op basis van de volgende criteria: minimaal 250 werknemers of een jaaromzet van vijftig miljoen euro of meer en een balanstotaal van 43 miljoen euro of meer.

Belangrijke entiteiten zijn middelgrote organisaties die actief zijn in een sector uit Bijlage I en middelgrote en grote organisaties die actief zijn in een sector uit Bijlage II. Een organisatie is middelgroot op basis van de volgende criteria: vijftig of meer werknemers of een jaaromzet en balanstotaal van tien miljoen euro of meer.

Essentiële of belangrijke organisaties moeten als zodanig worden aangewezen door de Nederlandse overheid en/of toezichthouders die namens hen toezicht houden. Omdat de huidige criteria nog niet verder zijn uitgewerkt, is een expliciete aanwijzing nog niet bekend. Het is echter duidelijk dat de huidige categorisering op basis van de SBI-codering (Standaard BedrijfsIndeling) niet een-op-een zal worden toegepast.

Het is ook mogelijk dat een organisatie die niet aan de bovengenoemde criteria voldoet en niet wordt aangewezen als een essentiële of belangrijke entiteit, toch moet voldoen aan vereisten uit de NIS2. De NIS2 benadrukt namelijk ook de verantwoordelijkheden van een organisatie in de keten en samenwerkingen. Organisaties zonder directe aanwijzing zullen dus door opdrachtgevers of samenwerkingsverbanden de vereisten uit de NIS2 opgelegd krijgen, bijvoorbeeld in contractuele voorwaarden en/of verantwoordingsverplichtingen. Denk hierbij bijvoorbeeld aan een producent van verpakkingsmaterialen voor medische producten of een transporteur van levensmiddelen.

De impact en belangrijke veranderingen als gevolg van NIS 2

Hoewel de volledige uitwerking van NIS2 in nationale wetgeving nog moet worden bekrachtigd en eind 2024 moet worden afgerond, en de definitieve aanwijzing van organisaties die onder de NIS2 vallen nog moet plaatsvinden, is nu al duidelijk welke impact de NIS2 zal hebben en wat deze van organisaties zal vragen. Kort samengevat stelt de NIS2 dat:

- Organisaties moeten voldoen aan een **opleidingsplicht**;
- Organisaties hebben een **zorgplicht** met betrekking tot informatie- en cyberbeveiliging;
- Organisaties hebben een **meldplicht** om incidenten binnen gestelde termijnen te melden;
- Toezichthouders moeten **toezicht** houden en hiervoor informatie verkrijgen van of bij de organisatie;
- (Bestuurders van) organisaties zijn **aansprakelijk**;
- Er kunnen **sancties** worden opgelegd.

Daarnaast benadrukt de NIS2-richtlijn de noodzaak van samenwerking en informatie-uitwisseling tussen organisaties en de overheid om bredere digitale veiligheid te bevorderen. Dit betekent dat je als bestuurder van een organisatie moet begrijpen hoe jouw activiteiten passen binnen het grotere geheel van de digitale veiligheid in jouw sector en in de samenleving als geheel.

Het niet naleven van de NIS2-richtlijn kan niet alleen leiden tot financiële consequenties, maar ook tot reputatieschade en verstoring van de activiteiten van jouw organisatie.

Het niet naleven van de NIS2-richtlijn kan niet alleen leiden tot financiële consequenties, maar ook tot reputatieschade en verstoring van de activiteiten van jouw organisatie. Als bestuurder is het dus van groot belang om de richtlijn serieus te nemen, de nodige maatregelen te implementeren en te zorgen voor een cultuur van digitale veiligheid binnen jouw organisatie. Dit draagt niet alleen bij aan de bescherming van jouw organisatie, maar ook aan die van het algehele, digitale ecosysteem.

Opleidingsplicht

In artikel 20 van de NIS2-richtlijn wordt gesteld dat *'leden van de bestuursorganen een opleiding moeten volgen en daarmee voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.'* Daarnaast wordt gesteld dat wordt aangemoedigd om een soortgelijke opleiding aan werknemers aan te bieden.

Voor deze opleidingsplicht is nog niet bekend of er meer specifieke vereisten aan de opleidingsvorm of -duur zullen worden gesteld. In de markt zijn er al verschillende vormen van opleidingen, van meerdaagse trainingen tot enkele sessies van een paar uur, in-house trainingen tot groepstrainingen op externe locaties en met of zonder opleidingscertificaat. Ook is nog niet expliciet gedefinieerd wat er met 'bestuursorgaan' wordt bedoeld, aangezien dit niet als definitie is opgenomen in de NIS2. Dit kunnen dus de directe bestuurders zijn, de directie en het management, maar ook toezichthoudende functionarissen zoals een raad van commissarissen.

Naar onze mening staat de lengte en inhoud van een dergelijke training dan ook niet voorop, maar het te bereiken resultaat. Daarmee zal de vorm en inhoud dan ook aangepast dienen te worden aan de organisatie en onder meer het kennisniveau van de betreffende bestuursorganen en bestuurders.

Zorgplicht

In artikel 21 van de NIS2-richtlijn wordt de zorgplicht nader gedefinieerd. In dit artikel wordt gesteld dat een organisatie maatregelen moet nemen om zich te beschermen tegen incidenten. Deze maatregelen zijn zeer algemeen gedefinieerd en moeten omvatten:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van

kwetsbaarheden;
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Om invulling te geven aan deze maatregelen kan heel goed worden gekeken naar bestaande certificeringen, best-practices en normenkaders, zoals de ISO27001:2022, NIST CSF en diverse sectorspecifieke, afgeleide of gerelateerde kaders. Deze kaders omvatten reeds maatregelen, hierboven benoemd, en kunnen daarmee prima voorzien in 'passende' beveiliging.

Opvallend, in deze maatregelen en relatief nieuw, zijn de vereisten rond beveiliging van de toeleveringsketen en beveiliging bij het verwerven van netwerk- en informatiesystemen. Deze zien expliciet toe op beveiliging in de keten en bij het inkopen van diensten of digitale oplossingen. Aangezien organisaties steeds meer gebruik maken van 'de cloud' is het dus ook belangrijk om toe te zien op veiligheid van deze ingekochte diensten en/of cloudsoftware. Deze normen vragen dus ook om goede kennis en kunde om risico's ten aanzien van toeleveranciers en cloudleveranciers te kunnen beoordelen en vragen om aantoonbare beheersing door deze leveranciers.

Meldplicht

In artikel 23 van de NIS2-richtlijn zijn tijdslijnen gespecificeerd waarbinnen een organisatie incidenten met betrekking tot informatie- en cyberbeveiliging moet melden bij een CSIRT. De Nederlandse overheid heeft vanuit de NIS2-richtlijn de verplichting om een gedegen meldstructuur en een CSIRT op te zetten. Voor een organisatie betekent dit dat binnen 24 uur een vroegtijdige waarschuwing, binnen 72 uur een incidentmelding, een tussentijds verslag en binnen een maand een eindverslag moet worden afgegeven. Deze meldingen zullen door het CSIRT op Europees niveau (geaggregeerd) worden gerapporteerd om zo zicht te houden op de algemene staat van informatie- en cyberbeveiliging en ontwikkelingen (per lidstaat).

Deze meldingsplicht lijkt sterk op de meldingsplicht voor datalekken onder de AVG. Door de daar reeds gebruikte werkwijze te kopiëren, kunnen al de nodige eerste stappen zijn gezet voor het verder invullen van deze vereiste.

Toezicht

In artikel 32 van de NIS2-richtlijn staat beschreven welke instrumenten de toezichthouders mogen toepassen bij toezicht op essentiële, respectievelijk belangrijke entiteiten. Deze variëren van audit en opvragen van informatie door de toezichthouder tot het aantonen van de gehanteerde instrumenten vanuit een onafhankelijke audit. Daarbij wordt beperkt onderscheid gemaakt tussen toezicht op een essentiële of een belangrijke entiteit, maar verwacht kan worden dat de mate van toezicht en de inzet van instrumenten in eerste instantie zal afhangen van de capaciteit van de toezichthouder. Vergelijkbaar aan toezicht op de Algemene Verordening Gegevensbescherming, waarbij de Autoriteit Persoonsgegevens als toezichthouder zich in eerste instantie richtte op 'de grote jongens' en overduidelijke 'overtredingen', mede omwille van beschikbare capaciteit om alle meldingen op te volgen.

In welke mate gesteund kan worden op het aantoonbaar voldoen aan certificeringen, best-practices of normenkaders, zoals de ISO27001:2022, is nog niet bekend. Of het bijvoorbeeld voldoende is om op basis van een self assessment aan te tonen dat passend invulling wordt gegeven aan de zorgplicht of dat een onafhankelijk oordeel nodig is? En of dan een certificering of een assuranceverklaring wordt gevraagd?

Hoe dan ook is duidelijk dat passend invulling moet worden gegeven aan de vereisten uit de NIS2 en dat toezicht om aantoonbaarheid hiervan zal vragen.

Cyberaanvallen wachten niet op nieuwe wetgeving en kunnen in elke fase toeslaan.

Aansprakelijkheid en sancties

In de NIS2-richtlijn worden expliciet de verantwoordelijkheden van bestuursorganen benoemd. Zij moeten maatregelen voor het beheer van cyberrisico's goedkeuren en zijn aansprakelijk voor het niet voldoen aan de zorgplicht. Hierbij wordt gedoeld op persoonlijke aansprakelijkheid. Dit is ook om te voorkomen dat slechts één bestuurder invloed uitoefent op de securitystrategie. Bij bestuurders is er vaak een verdeling van taken en is het nogal eens het geval dat de bestuurder die de informatiebeveiliging en cybersecurity niet in het takenpakket heeft, hier ook niets meedoet en of affiniteit mee heeft, terwijl dit zo langzamerhand (de data in en van een organisatie) welhaast een van de meest essentiële onderdelen is van een organisatie.

Als mogelijke sancties voor het niet voldoen aan de NIS2-richtlijn is een maximale sanctie van tien miljoen euro of twee procent van de wereldwijde jaaromzet voor een essentiële entiteit en een maximale sanctie van zeven miljoen euro of 1,4 procent van de wereldwijde jaaromzet voor een belangrijke entiteit genoemd. Onze verwachting is dat het toekennen van sancties op soortgelijke wijze als bij de AVG zal plaatsvinden en gelijke tred zal houden met de vormgeving van toezicht. Er hoeft niet direct tot boetes als sanctie te worden overgegaan door de toezichthouder. Deze kan ook waarschuwingen of de verplichting tot het oplossen van waargenomen tekortkomingen opleggen aan de organisatie.

Perspectief

Gezien de Network and Information Security Directive 2 (NIS2) wordt het duidelijk dat het versterken van de digitale veerkracht een dringende en voortdurende inspanning vereist. Hoewel de volledige uitwerking van NIS2 in nationale wetgeving nog enige tijd kan vergen, is het van cruciaal belang voor organisaties om nu al proactieve maatregelen te nemen. Het wachten op formele richtlijnen zou een riskante strategie zijn, gezien de voortdurende en steeds geavanceerdere cyberdreigingen.

Organisaties die vooruit willen kijken, dienen niet alleen te voldoen aan de wettelijke vereisten van NIS2, maar ook te investeren in de algehele weerbaarheid van hun digitale systemen. Door zich te concentreren op het implementeren van best-practices zoals ISO27001, het helder definiëren van verantwoordelijkheden en aansprakelijkheden, het uitvoeren van uitgebreide beoordelingen en het opzetten van effectieve monitoring en incidentrespons, kunnen zij een solide basis leggen voor een duurzame en adaptieve digitale beveiligingsinfrastructuur.

De realiteit is dat informatie- en cyberbeveiliging niet kan wachten. Cyberaanvallen wachten niet op nieuwe wetgeving en kunnen in elke fase toeslaan. Door nu al te investeren in beveiligingsmaatregelen, kunnen organisaties veerkracht opbouwen, zich voorbereiden op mogelijke dreigingen en de continuïteit van hun activiteiten waarborgen. NIS2 vormt niet alleen een verplichting, maar ook een kans voor organisaties om zichzelf te versterken in een digitaal landschap dat voortdurend evolueert. Het is tijd om niet langer af te wachten, maar proactief de leiding te nemen in het waarborgen van digitale veiligheid en veerkracht.

Daarnaast is het essentieel om te beseffen dat de impact van NIS2 zich niet beperkt tot alleen de aangewezen organisaties. De gehele keten zal worden getroffen, aangezien cybersecurity een onderling verbonden en gedeeld aspect is binnen moderne bedrijfsvoering. Verplichtingen en verantwoordelijkheden zullen naar verwachting verder doorsijpelen, waardoor het nemen van proactieve maatregelen niet alleen wettelijk vereist is, maar ook nodig om de integriteit en veiligheid van de bredere digitale ecosystemen te waarborgen.