WHITEPAPER

NIS2

VOLDOE TIJDIG AAN DE VERPLICHTINGEN BINNEN DE NIS2-REGELGEVING

Medio 2025 is het zover: de NIS2 wetgeving gaat worden gehandhaafd. De Cyberbeveiligingswet vereist dat bedrijven en organisaties die actief zijn in kritieke sectoren hun digitale weerbaarheid versterken.

Wat zijn de stappen die u dient te nemen?

VOOR WIE?

De NIS2, en daarmee de Cyberbeveiligingswet, richt zich op kritieke organisaties en sectoren waarbij uitval van hun diensten kan zorgen voor maatschappelijk en economische ontwrichting. Zij dienen volgens de Europese Unie te werken aan een extra laag digitale bescherming.

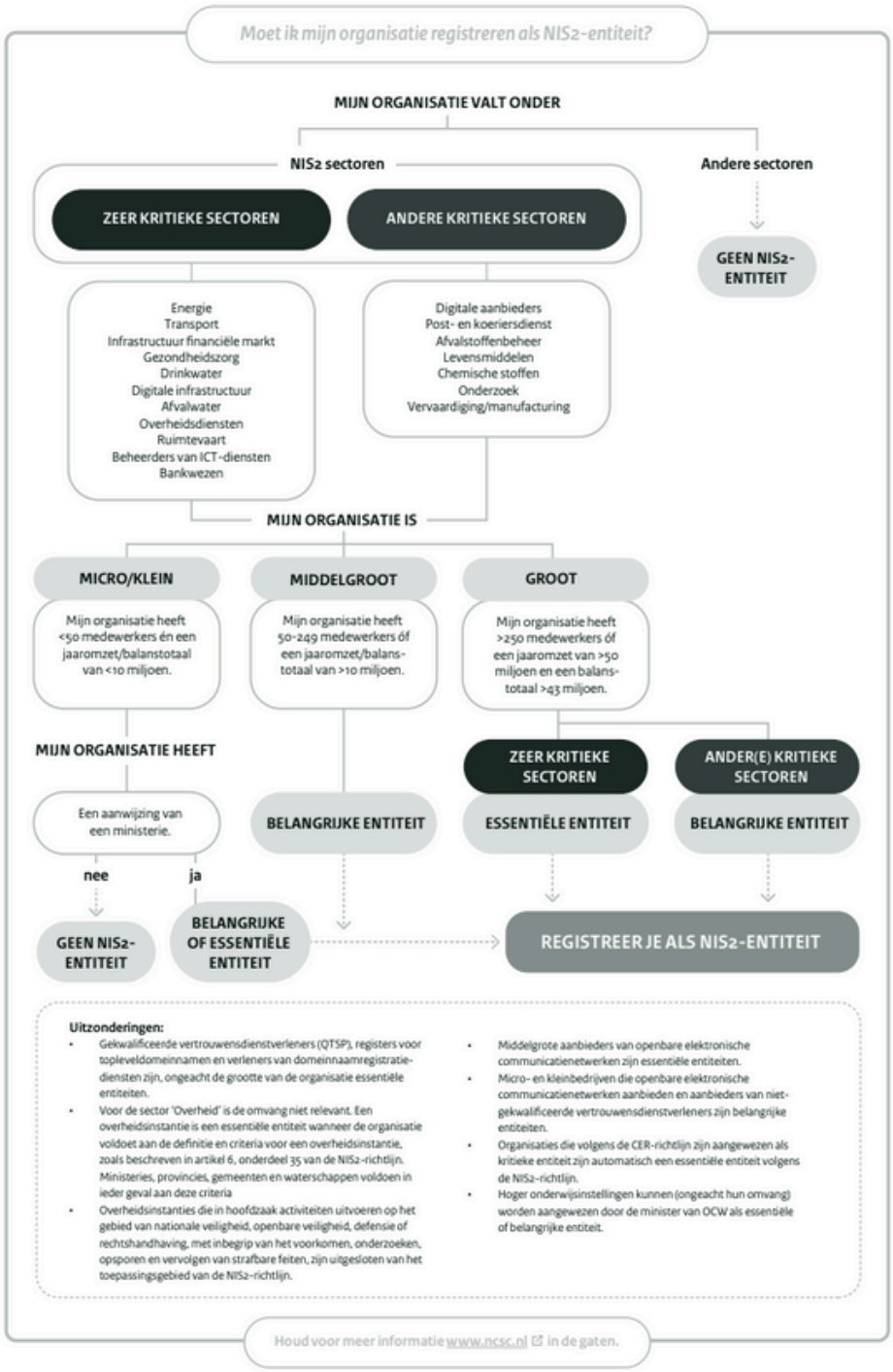
WANNEER?

De richtlijn is op 22 november 2022 vastgesteld door de Europese Raad. Op 16 januari 2023 startte de implementatietermijn van 21 maanden. De implementatie is Nederland helaas niet voor 17 oktober 2024 gelukt. Naar alle waarschijnlijkheid treedt de NIS2 in Nederland medio 2025 in werking.

DIENEN WIJ AAN DE NIS2 TE VOLDOEN?

De NIS2-richtlijn, of Network and Information Security 2-richtlijn, is een Europese wetgeving die is ontworpen om de cyberbeveiliging en weerbaarheid van essentiële diensten en digitale dienstverleners in de Europese Unie te verbeteren. Het introduceert strengere beveiligingsnormen en meldingsvereisten voor incidenten.

De flowchart van het Nationaal Cybersecurity Centrum vertelt u in één oogopslag of uw organisatie met deze richtlijn aan de slag dient te gaan. U kunt ook altijd de NIS2-zelfevaluatie van de Rijksoverheid doen.



Aanmelden

De registratiefunctionaliteit is per 17 oktober 2024 beschikbaar gemaakt, zodat organisaties zich kunnen voorbereiden en tijdig kunnen registreren.

START

ONZE ORGANISATIE KRIJGT MET DE NIS2 TE MAKEN. WAT NU?

De NIS2-richtlijn gaat in op de risico's die netwerk- en informatiesystemen bedreigen. Denk hierbij aan cyberbeveiligingsrisico's. Er worden 3 verplichtingen voorgeschreven:

1 REGISTRATIEPLICHT

Organisaties die volgens de flowchart en/of NIS2-zelfevaluatie een NIS2-entiteit zijn, dienen zich voor medio 2025 te registreren, zodat er een overzicht ontstaat van alle entiteiten die onder de NIS2-richtlijn vallen.

START DE NIS2-REGISTRATIE

2 ZORGPLICHT

NIS2-organisaties dienen een risicobeoordeling uit te voeren en op basis daarvan passende maatregelen te nemen om de beveiliging van hun netwerk- en informatiesystemen te waarborgen. Het volgende hoofdstuk neemt u mee in de te nemen stappen.

3 MELDPLICHT

Significante incidenten moeten binnen 24 uur worden gemeld aan de bevoegde autoriteiten en het Computer Security Indicent Response Team (CSIRT). Dit geldt voornamelijk voor incidenten die de diensteverlening aanzienlijk kunnen verstoren.

TOEZICHT

Organisaties die onder de NIS2-richtlijn vallen komen onder toezicht te staan, waarbij wordt gekeken naar de naleving van bovenstaande verplichtingen.

ZORGPLICHT

Organisaties dienen maatregelen te nemen om hun netwerk- en informatiesystemen te beschermen tegen incidenten. Dit geldt ook voor de fysieke omgeving waarin de systemen zich bevinden. Na een registratie in het NIS2-register, is het van belang aan de slag te gaan met de zorgplicht.

STAP 1 *Maak een risicoanalyse*

Bepaal in dit proces tenminste het volgende:

BEPAAL WAT U WILT BESCHERMEN

Identificeer wat waarde heeft voor uw bedrijf. Wat zijn de zogenaamde 'kroonjuwelen'? Dit kunnen bijvoorbeeld unieke ontwerpen, productiemethoden of klantgegevens zijn. Maar vergeet ook de financiële data en gegevens over medewerkers niet. Kortom: wat zijn de te beschermen belangen binnen mijn organisatie?

IDENTIFICEER RISICO'S

Zodra we weet wat er te beschermen is, kunnen we daar ook de waarde van bepalen. Wanneer iets een hogere waarde heeft, zal het vaak ook resulteren in een groter cyberrisico. In welke vorm dit risico komt, hangt af van uw organisatie. Zo kan men denken aan een hacker die een medewerker verleid om een bestand te openen, of juist in de vorm van brandgevaar of een kwetsbaarheid in het informatiesysteem. Hoe identificeert u risico's?

- **Historie:** welke risico's zijn al eerder voorgevallen?
- **Geldende wet- en regelgeving:** denk aan de AVG die risico's op datalekken concreet maken
- **Assessment:** organiseer een assessment met partijen die risico's in kaart brengen. Denk aan IT consultants, accountants en juridisch adviseurs.

ANALYSEER DE GEVONDEN RISICO'S

Nu u weet wat u wilt beschermen en welke risico's er zijn, kunnen we ook verder inzoomen op het risico zelf. Wat is de kans dat dit gebeurt? En wat is de schade als het dan zou gebeuren? Hoe verhoudt de huidige weerbaarheid van de te beschermen belangen zich tot de dreigingen?

BESLUIT DE VERVOLGAANPAK

Iedere keuze kan geld kosten in dit proces. Daarom is het belangrijk om te besluiten in welke cyberrisico's en de daarbij behorende oplossingen u investeert. Dit doet u aan de hand van uw *risicobereidheid* - een in te nemen standpunt over de geïdentificeerde risico's. Er zijn 4 mogelijke acties in dit geval:

1. Accepteren:
u bent zich bewust van het risico en accepteert het.
2. Oplossen (of mitigeren):
u gaat maatregelen nemen om het risico te verkleinen en desnoods uit te sluiten.
3. Overdragen:
u verschuift het risico naar een ander. Denk hierbij aan verzekeringen.
4. Stoppen:
de activiteiten waarop uw organisatie een risico loopt worden niet meer uitgevoerd.

ZORGPLICHT (VERVOLG)

STAP 2 *Neem passende maatregelen*

Met de risico's in kaart ontstaat ook zicht op passende maatregelen. Dit is uiteraard een maatwerk aanpak en afhankelijk van de risicobeoordeling. Interessante maatregelen zijn:

ORGANISEER IDENTITEIT EN TOEGANG

Krijg effectief grip op de gebruikers en de autorisaties die zij hebben. Dit gebruikersbeheer en het monitoren daarvan geeft een voorsprong in de cyberbeveiliging en het terugdringen van risico's.

VEILIG GEDRAG BINNEN DE ORGANISATIE

De zwakke schakel in het IT-landschap is veelal de mens. Training en kennisdeling in teams is een cruciale bijdrage aan de digitale weerbaarheid van uw organisatie. Er zijn diverse cybersecurity awareness trainingen beschikbaar.

EIGENAARSCHAP VAN INFORMATIE

Nu de mensen bekend zijn en getraind zijn in cyberveiligheid, is het van belang te kijken naar de waarde van de bedrijfsinformatie. Welke delen van uw organisatie zijn cruciaal en hoe zijn deze beveiligd?

5 BASISPRINCIPES VAN DIGITALE WEERBAARHEID

Het Nationaal Cyber Security Centrum (NCSC) heeft in het kader van passende maatregelen vijf basisprincipes ontworpen om organisaties te helpen hun cyberbeveiliging te verbeteren.

1. Breng risico's in kaart
2. Bevorder veilig gedrag
3. Bescherm systemen, applicaties en apparaten
4. Beheer toegang tot data en diensten
5. Bereid u voor op incidenten

Cruciale onderdelen als we kijken naar het Cybersecuritybeeld Nederland 2024 dat onlangs is uitgebracht door de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Niet alleen criminele, maar (dankzij de turbulente geopolitieke tijden) ook statelijke actoren verbreden hun capaciteiten, waarbij ze gebruik maken van een bredere gereedschapskist.

ZORGPLICHT (VERVOLG)

STAP 3 *Ontwikkel procedures ten aanzien van incidenten*

Al spannen we ons tot het uiterste in om ze te voorkomen - er is altijd een kans op incidenten. Daarom is het van belang om procedures te ontwikkelen voor het detecteren, monitoren, oplossen en melden van incidenten. Dit alles voor een adequate respons wanneer uw organisatie wordt getroffen.

DETECTEREN EN MONITOREN

Een aanval is niet altijd op klaarlichte dag en in het zicht van u als gebruiker. Daarom is het raadzaam om systemen en processen te implementeren om vroegtijdige detectie mogelijk te maken. Denk hierbij aan Intrusion Detection Systems (IDS) en Security Information and Event Management (SIEM) systemen.

OPLOSSEN: INCIDENT RESPONSE PLAN

Is er een incident gedetecteerd is het cruciaal dat de te nemen stappen en verantwoordelijkheden bij eenieder bekend zijn. Dit is vast te leggen in een Incident Response Plan, welke beschrijft hoe te handelen bij welk type incident, inclusief communicatieprotocollen en herstelmaatregelen.

MELDEN

Onderdeel van dit Incident Response Plan is het maken van een melding aan de Computer Security Incident Response team en de toezichthouder. Meer hierover in het volgende hoofdstuk.

MELDPLICHT

NIS2-organisaties dienen significante incidenten te melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Binnen 24 uur na waarneming van het incident wordt er een eerste melding verwacht, zodat details over het incident ook andere organisaties kan helpen om zich beter te wapenen. Na melding begint ook direct de bijstand van het sectorale CSIRT.

WAAR MELDEN?

Vanaf 17 oktober 2024 is het mogelijk om een vrijwillige melding te maken van een incident via de website van het NCSC. Deze meldplicht wordt vanaf medio 2025 daadwerkelijk gehandhaafd, met aanzienlijke boetes voor essentiële en belangrijke organisaties die nalatig blijken in het doen van een melding.

WELKE INCIDENTEN MELDEN?

Alleen incidenten die een ernstige operationele verstoring van de diensten of financiële verliezen voor een organisatie (kunnen) veroorzaken, dienen gemeld te worden. Kortom; incidenten die (kunnen) leiden tot significante materiële of immateriële schade. De exacte drempelwaarden voor deze meldingen worden later gecommuniceerd.

BELANGRIJKE ONDERDELEN MELDING INCIDENT

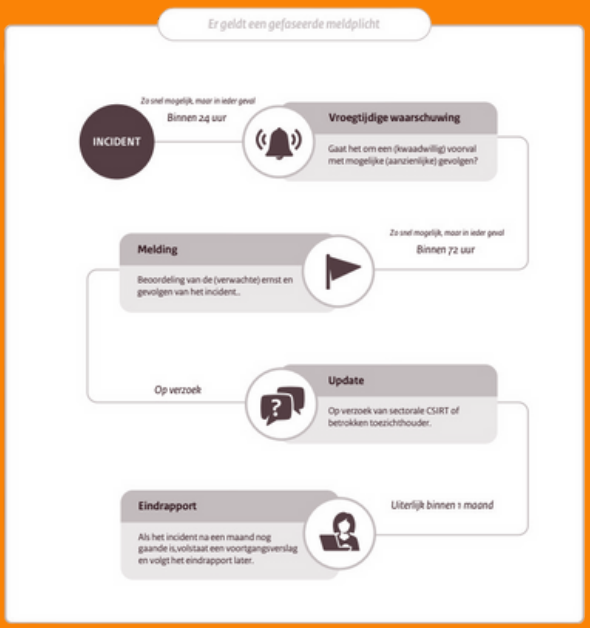
Vindt er een incident plaats, is het van belang om zo snel mogelijk melding te maken en hiervoor minimaal het volgende te verzamelen:

- Datum en tijd incident
- Type incident
- Oorzaak incident
- Impact incident
- Gegevens contactpersoon

Zodra het CSIRT de melding ontvangt, wordt er vanuit het sectorale CSIRT ondersteuning verleend. De specifieke bijstand verschilt uiteraard per situatie en is afhankelijk van de (potentiële) impact.

GEFASEERDE MELDPLICHT

*Er geldt een bijzondere meldplicht voor partijen die ook onder de Digital Operational Resilience Act (DORA) of Netwerkcode cybersecurity voor grensoverschrijdend elektriciteitsstromen vallen. Deze entiteiten moeten binnen **vier uur** een vroegtijdige waarschuwing geven.*



KEEP IT SIMPLE

Ook voor dit IT onderwerp geldt: houd het overzicht. Het uitstel van de wetgeving gaat niet tot afstel leiden, maar geeft organisaties wel de kans zich tijdig voor te bereiden. Hopelijk gaat deze whitepaper u daarbij helpen.

U STAAT ER NIET ALLEEN VOOR

Binnen Agerion IT zijn onze cybersecurity experts dagelijks met deze materie bezig. Heeft u vragen, schroom dan ook niet om ons even te bellen of te mailen. We staan u graag te woord.

Zoekt u naar een projectmanager om deze NIS2-transitie te begeleiden?
Wij hebben een team vol ervaring en motivatie om cybersecurityrisico's te analyseren en passende maatregelen te vinden en uiteindelijk ook te treffen. Hands-on Cybersecurity specialisten.

AGERION
keep IT simple

U BENT VAN HARTE WELKOM

Scheepmakershaven 2
3261 KN Oud-Beijerland

T. +31 (0) 186 - 20 10 10
E. info@agerion.nl
www.agerion.nl