

NIS 2 voor Humankind

Richard Kranendonk, 22 oktober 2024

Inhoud

Inhoud.....	1
Inleiding.....	2
Verplichtingen voor organisaties onder de NIS 2	2
Zorgplicht	2
Risicoanalyse.....	3
Maatregelen	3
Incidentrespons.....	3
Toeleveringsketen.....	3
Meldplicht.....	4
Verantwoordelijkheid bestuur	4
Verhouding van deze verplichtingen tot het Project Informatiebeveiliging.....	5

Inleiding

Wat is de NIS 2?

De NIS 2 (Network and Information Security directive) is een Europese richtlijn met als doel in voor de samenleving essentiële en belangrijke sectoren de continuïteit van dienstverlening en bescherming van informatie te waarborgen.

Tijdslijn

De richtlijn is op Europees niveau op 16 januari 2023 in werking getreden, met een deadline voor nationale omzettingswetten in de lidstaten van 17 oktober 2024. Alleen België en Kroatië hebben dat gehaald – Nederland verwacht dat de wet pas in het tweede of derde kwartaal van 2025 in werking kan treden, omdat 'de omzetting naar nationale wetgeving een omvangrijk en complex traject is'.

Toepassingsgebied

De richtlijn heeft 'essentiële' en 'belangrijke' sectoren gedefinieerd waarvoor de NIS 2 gaat gelden vanaf een bepaalde organisatiegrootte. De Gezondheidszorg valt hier onder, onderwijs en kinderopvang vooralsnog niet. Er is voor Humankind dus vooralsnog geen verplichting aan de NIS 2 te voldoen.

Verplichtingen voor organisaties onder de NIS 2

De NIS 2 kent aan organisaties een Zorgplicht, Meldplicht en Registratieplicht toe. De Registratieplicht houdt in dat organisaties waarop de richtlijn van toepassing is, zich moeten registreren in het 'entiteitenregister'. De website van het Nationaal Cyber Security Centrum (NCSC, Min. van Justitie en Veiligheid) geeft hierover [meer informatie](#). Op de Zorgplicht en Meldplicht ga ik hieronder verder in.

Zorgplicht

Hoewel de nationale omzettingswet dus nog niet gepubliceerd is, en nadere, sectorspecifieke regels nog gesteld kunnen worden, weten we al wel dat de zorgplicht in lijn zal zijn met bestaande kaders als de BIO ([Baseline Informatiebeveiliging Overheid](#)) en de ISO 27002¹.

Verschillende websites van de overheid geven ook informatie over wat we kunnen verwachten. De website van het NCSC is m.i. de meest complete en gestructureerde hiervan.

Vanuit de richtlijn wordt in ieder geval verwacht dat de organisatie 'robuuste' risicomanagement processen inricht. De richtlijn benadrukt daarbij het cyclische karakter van risicomanagement, dus het steeds opnieuw doorlopen van de cyclus risico-identificatie, -analyse, treffen van maatregelen, beoordeling van de effectiviteit, aanbrengen van verbetering (een PDCA cyclus).

¹ De ISO 27002 is een nadere uitwerking van de maatregelen die in de Annex A van de ISO 27001 benoemd worden. Voor ons project Informatiebeveiliging gebruiken we de ISO 27001/27002 als kapstok. De BIO is ook gebaseerd op de ISO 27001 / 27002.

Passend informatiebeveiligingsbeleid, en controle op en rapportage over de naleving daarvan, is ook een vereiste.

De website van het NCSC vult dit verder in met een stappenplan waarvan de hoofdstappen zijn: 1) Risicoanalyse, 2) Maatregelen en 3) Incidentrespons.

Risicoanalyse

- Identificeer de processen en systemen die noodzakelijk zijn om de doelen van de organisatie te vervullen
- Identificeer dreigingen voor de Beschikbaarheid, Vertrouwelijkheid en Integriteit
- Beoordeel of huidige maatregelen (technisch en organisatorisch) voldoende bescherming bieden
- Prioriteer de risico's mbv een Risicomatrix (kans x impact)
- Wijs risico-eigenaren aan en bepaal hun mandaat en verantwoordelijkheden

Maatregelen

Maatregelen moeten 'passend' en 'adequaat' zijn, op basis van de voorgaande risicoanalyse.

De website van de NCSC noemt als voorbeelden van maatregelen:

- Beleg het eigenaarschap van informatie en risico's
- Bevorder veilig gedrag en een cultuur waarin incidenten veilig gemeld en verwerkt kunnen worden
- Veranker de risicomanagementcyclus in de organisatie door het juist beleggen van verantwoordelijkheden
- Organiseer identiteits- en toegangsbeheer.

Incidentrespons

- Organisaties moeten een incident respons plan (IRP) opstellen over hoe te reageren in het geval van ernstige verstoringen, en daarvan te herstellen en terug te keren naar 'business as usual'.
- Organisaties moeten procedures ontwikkelen voor het detecteren, monitoren, oplossen en melden van incidenten.

Toeleveringsketen

Omdat grote delen van de informatiehuishouding uitbesteed worden aan leveranciers (IT dienstverleners, Software-as-a-Service, etc.), is de organisatie ook verantwoordelijk voor het bewaken van de veiligheid van de toeleveringsketen.

De richtlijn verwacht dat de volgende activiteiten aantoonbaar worden uitgevoerd:

- evalueren van de beveiligingsmaatregelen van leveranciers en de kwaliteit van hun producten en diensten
- opnemen van risicomanagement-maatregelen in de contracten met leveranciers
- de leveranciers contractueel verplichten dat zij op hun beurt de veiligheid van hun leveranciers waarborgen
- beleid en basiseisen opstellen voor de selectie van leveranciers.

Meldplicht

De richtlijn schrijft voor dat NIS2-organisaties significante incidenten moeten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder (NSCS). Significante zijn incidenten die een ernstige operationele verstoring van de diensten of financiële verliezen voor de organisatie (kunnen) veroorzaken, of (kunnen) leiden tot aanzienlijke materiële of immateriële schade bij andere organisaties. De exacte drempelwaarden worden nog uitgewerkt.

Verantwoordelijkheid bestuur

De NIS 2 benadrukt de verantwoordelijkheid en aansprakelijkheid van het bestuur van de organisatie in het borgen van informatiebeveiliging. Hieronder vallen:

- het goedkeuren van maatregelen
- zorgdragen voor de effectieve implementatie van maatregelen
- het bewaken van de uitvoering van deze maatregelen
- leiderschap tonen t.a.v. initiatieven op het gebied van informatiebeveiliging

Het bestuur kan wel de verantwoordelijkheden op dit vlak delegeren, maar niet de aansprakelijkheid – in uiterste gevallen kunnen bestuurders persoonlijk aansprakelijk worden gesteld voor het verzaken van hun plichten.

Het management van een organisatie is verplicht zich te laten trainen op het gebied van risicomanagement en de impact van cybersecurity risico's op dienstverlening en bescherming van informatie.

Daarnaast moet het management zorgen voor regelmatige training van de werknemers op dit gebied. Hiermee erkent de richtlijn dat informatieveiligheid collectieve inzet vergt van alle werknemers.

Verhouding van deze verplichtingen tot het Project Informatiebeveiliging

Omdat ISO 27001 / 27002 binnen ons project als richtlijn wordt gebruikt, komen vrijwel alle verplichten uit de NIS 2 aan de orde. De kwaliteit van de uitvoering hiervan binnen de organisatie is natuurlijk bepalend.

In onderstaande tabel worden de verplichtingen uit de richtlijn afgezet tegen de producten uit de aanbidding voor dit project.

Verplichting NIS 2	Product uit de Aanbidding van dit project
Cyclisch risicomanagement	III. Risicomanagement IV. Implementatie PDCA cyclus met de Canvas Methode
Informatiebeveiligingsbeleid	I. Leidende principes en doelen vaststellen II. Beleid op hoofdlijnen
Risicoanalyse	
Identificeren van kritieke processen en systemen	I. Calamiteitenplan (onderdeel van ...)
Identificeren dreigingen voor de Beschikbaarheid, Vertrouwelijkheid en Integriteit	I. Calamiteitenplan (onderdeel van ...)
Beoordelen adequaatheid van maatregelen	II. Risico analyse II. Fit/gap analyse t.o.v. framework
Prioritering risico's	II. Risico analyse
Bepalen risico-eigenaren	II. Besturingsmodel
Maatregelen	
Bepalen informatie-eigenaren	Onderdeel van OrgFit programma
Bevorder veilig gedrag en een cultuur	<i>Management moet voorwaarden scheppen;</i> IV. Implementatie PDCA cyclus met de Canvas Methode
Beleggen van verantwoordelijkheden	III. Capaciteiten ontwikkelen (onderdeel van ...)
Identiteits- en toegangsbeheer	II. Implementatieplan maatregelen (onderdeel van ...)
Incidentrespons	I. Calamiteitenplan (onderdeel van ...)
Toeleveringsketen	III. Leveranciersmanagement
Meldplicht	
Bestuursverantwoordelijkheid	
Goedkeuren, implementeren en bewaking van maatregelen	III. Sturing op informatieveiligheid
Leiderschap	<i>Managementverantwoordelijkheid</i>
Training management	I. Workshop Sturen op Risico's
Training van werknemers	II. Implementatieplan maatregelen (onderdeel van ...)