Cyberbeveiligingswetgeving

De Network and Information Security 2 (NIS2) richtlijn is een Europese richtlijn die lidstaten verplicht om de digitale veiligheid te versterken. Deze richtlijn geeft een kader dat alle lidstaten in nationale wetgeving moeten omzetten. In Nederland gebeurt dat via de Cyberbeveiligingswet (Cbw), die de richtlijn praktisch toepast in de nationale context. De Cyberbeveiligingswet is recent aangeboden aan de Tweede Kamer. De regering streeft ernaar dat de Cyberbeveiligingswet in het 2e kwartaal van 2026 in werking treedt.

Wat is de Cyberbeveiligingswet?

De Cyberbeveiligingswet is opgesteld om de Nederlandse implementatie van de Europese NIS2-richtlijn te waarborgen. De richtlijn heeft als doel organisaties beter te beschermen tegen cyberaanvallen en hen te ondersteunen bij het verbeteren van hun informatiebeveiliging.

De NIS2-richtlijn volgt de oorspronkelijke NIS-richtlijn op, die in 2016 werd vastgesteld en in Nederland in 2018 werd geïmplementeerd via de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni was vooral van toepassing op aanbieders van essentiële diensten, zoals de water- en energievoorziening, banken, evenals op digitale dienstverleners.

Voor wie is de Cyberbeveiligingswet van toepassing?

De cyberbeveiligingswet zal de Wbni vervangen, maar belangrijker is dat met de komst van de NIS2-richtlijn de kring van organisaties waarop de vereisten van toepassing zijn, fors wordt uitgebreid. Ook nieuwe sectoren zoals gemeenten, onderwijsinstellingen, gezondheidszorg, chemische bedrijven, post- en koeriersdiensten en andere belangrijke maatschappelijke diensten moeten hun digitale beveiliging op orde brengen. Hierbij gelden overigens wel grootte-criteria, maar met meer dan 250 werknemers of een jaaromzet van meer dan € 50 miljoen wordt de organisatie al gezien als ‘groot’. De minister schat het aantal organisaties dat onder de Cbw gaat vallen op ca. 8.100 entiteiten.

Voor financiële instellingen geldt de DORA-Verordening als sectorspecifieke norm (‘lex specialis’). In de Memorie van Toelichting meldt de minister: “Dit betekent dat de bepalingen uit dit wetsvoorstel [Cbw] over de zorgplicht en de meldplicht en het toezicht en de handhaving daarop, niet van toepassing zijn op financiële entiteiten die onder de [DORA] verordening vallen.”

De Cbw zal met name grote impact hebben op de overheid. Binnen de overheid komen ook formele taken te liggen als de Cybercrisisbeheerautoriteit (Ministerie van Justitie) en het opstellen van een Cyberbeveiligingsstrategie.

Wat zijn de verplichtingen van de Cyberbeveiligingswet?

De cyberbeveiligingswet legt een aantal verplichtingen op aan organisaties. Dit zijn:

- Zorgplicht
- Meldplicht
- Registratieplicht

Zorgplicht

De zorgplicht vereist dat organisaties de juiste maatregelen nemen om cyberaanvallen te voorkomen en te beperken. Dit omvat het opstellen van interne beveiligingsregels en procedures, gebaseerd op risicoanalyses, het trainen van medewerkers en het goed regelen van de samenwerking met leveranciers. De leden van het bestuur van organisaties die onder de Cbw vallen dienen opleidingen te volgen teneinde toezicht te kunnen houden op de uitvoering.

Onder de zorgplicht vallen ten minste:

1. Een risicoanalyse en beveiliging van informatiesystemen;
2. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets;
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen;
4. Incidentenbehandeling;
5. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging;
6. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden;
7. Beveiliging van de toeleveranciersketen;
8. Beleid en procedures over het gebruik van cryptografie en encryptie;
9. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen;
10. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico’s te beoordelen.

Meldplicht

Zodra er zich toch een incident voordoet, moeten organisaties dit tijdig melden. Binnen 24 uur moet een eerste melding worden gedaan bij de toezichthouder, deze toezichthouder verschilt per sector maar voor de meeste organisaties zal dit de Rijksinspectie Digitale Infrastructuur (RDI) worden. Vervolgens is het verplicht om binnen 72 uur aanvullende informatie aan te leveren en uiteindelijk een volledig verslag op te stellen.

Registratieplicht

Organisaties die onder de Cbw vallen, moeten zich in Nederland registreren bij de aangewezen bevoegde autoriteit. Voor deze organisaties is dat het Nationaal Cyber Security Centrum (NCSC). Deze registratieplicht geeft de NCSC een overzicht van de vitale diensten en bedrijven die beschermd moeten worden en maakt gerichte handhaving mogelijk.

Toezicht

Bijzonder aan de Cbw is dat de Nederlandse wetgever ervoor heeft gekozen om de ‘vakministers’ aan te wijzen als de bevoegde autoriteit, maar in de praktijk kan het toezicht namens de minister ook worden uitgevoerd door een ander overheidsorgaan. Per sector (voor zover vallend onder een ander ministerie) kan er dus sprake zijn van een andere toezichthouder. Het handhavingsinstrumentarium van de toezichthouder kan uiteenlopen van het verplichten tot een beveiligingsaudit, openbaarmaking van de overtreding tot het opleggen van een last onder dwangsom of een bestuurlijke boete.

Wat zijn de gevolgen?

Vanuit ons perspectief (en onze bekendheid met zowel ISO27001 als DORA implementaties) is de Cyberbeveiligingswet geen volkomen nieuw raamwerk met nieuwe eisen. Wel worden er andere accenten gelegd die kunnen bijdragen aan een nog grotere betrokkenheid van de leiding bij een adequate implementatie, zoals bijvoorbeeld toezicht en handhaving.

Tegelijk zullen de verschillende ministeries een flinke kluif hebben aan het verzamelen van de capaciteit om de toezichthoudende rol ook effectief te kunnen invullen. De schaarste aan goed opgeleide professionals zal daarom zeker niet afnemen.
Verschillen ten opzichte van de DORA zijn bijvoorbeeld de registratieplicht. Die kent de DORA niet. Maar de procedures rondom het melden van ernstige incidenten zijn in opzet bijvoorbeeld redelijk vergelijkbaar, al is de DORA veel gedetailleerder uitgewerkt. Hetzelfde geldt voor het toezicht op de beveiliging van de leveranciersketen.

Binnen de overheid is gewerkt aan de update van de Baseline Informatiebeveiliging (“BIO 2.0”). Deze is in lijn gebracht met de ISO27001:2022 standaard en zal dienen als normenkader voor de zorgplicht die de overheid heeft op het gebied van informatiebeveiliging.

Verantwoordelijkheid ligt bij het bestuur

De verantwoordelijkheid voor cybersecurity ligt nadrukkelijk bij het bestuur en de directie. De Cbw legt deze plicht expliciet bij bestuurders en directieleden. Zij moeten cybersecurity structureel op de bestuurlijke agenda plaatsen, toezien op de uitvoering van de benodigde beveiligingsmaatregelen en verantwoording afleggen aan de toezichthouder. Daarmee wordt cybersecurity niet langer gezien als een technische kwestie, maar als een onderwerp voor de gehele organisatie.

Hoe kunnen we u helpen?

Binnen InAudit is veel kennis en ervaring aanwezig op het gebied van implementatie van raamwerken voor informatiebeveiliging. Daarnaast zijn we ook specialist in het uitvoeren van audits of tussentijdse reviews. Voor veel bestuurders biedt de uitkomsten van een dergelijk onderzoek vaak veel inzichten in waar de organisatie staat en waar de prioriteiten liggen.

Wat er ook gedaan moet worden, we hebben de kennis en ervaring en we helpen u graag !