Vooruitblik op de Cyberbeveiligingswet: waar staan we nu en wat kan je nu al doen?

30 juni 2025

In juni 2025 bevinden we ons op een belangrijk kruispunt in de implementatie van de Europese NIS2-richtlijn in Nederland. Met de recente indiening van de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) bij de Tweede Kamer, is de volgende fase van het wetgevingsproces in gang gezet. Hoewel de formele inwerkingtreding van deze wetten pas wordt verwacht in het tweede kwartaal van 2026, is duidelijk dat organisaties nu al stappen moeten zetten richting hun digitale weerbaarheid.

Cyberveilig Nederland (CVNL) biedt via dit artikel een overzicht van de actuele stand van zaken, de kernverplichtingen uit de Cbw, het toekomstige toezicht en wat organisaties nu al kunnen doen ter voorbereiding.

1. De Europese achtergrond: NIS2 en CER-richtlijnen

De Cyberbeveiligingswet (Cbw) is de Nederlandse implementatie van de Europese NIS2-richtlijn. Deze richtlijn beoogt de digitale weerbaarheid van essentiële en belangrijke sectoren in de Europese Unie te vergroten. Elk lidstaat heeft de verantwoordelijkheid om de NIS2-richtlijn te vertalen naar nationale wetgeving. De NIS2 is de opvolging van de NIS, die in Nederland bekend is onder de naam Wet bescherming netwerk infrastructuur (Wbni).

Tegelijk met het wetgevingstraject van de Cbw wordt de Wet weerbaarheid kritieke entiteiten (Wwke) vertaald naar nationale wetgeving. De Wwke is de implementatie van de CER-richtlijn (Critical Entities Resilience).

Beide wetten zorgen voor kaders voor versterking van de infrastructuur en samenwerking tussen lidstaten op het gebied van veiligheid en continuïteit van dienstverlening. Beide wetten zijn minder vrijblijvend en ze omvatten meer sectoren dan de huidige NIS/Wbni.

2. Status van wetgeving en implementatie

Beide wetsvoorstellen zijn op 4 juni 2025 ingediend bij de Tweede Kamer. De verwachting is dat deze *pas* in het tweede kwartaal van 2026 in werking zullen treden[1]. Tot die tijd gelden er formeel nog geen verplichtingen voor organisaties die nieuw onder de NIS2/Wwke komen te vallen, maar de overheid roept op om niet af te wachten en al in actie te komen. Overigens gelden er wel rechten voor de organisaties die onder deze wet komen te vallen (zie rechten en plichten). Tevens blijft de Wbni voor sectoren die daar nu al onder vallen onverminderd van kracht.

Ondertussen worden ook de bijbehorende algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen verder uitgewerkt door de verschillende departementen, waarbij onder meer de zorgplicht en sectorspecifieke drempelwaarden voor meldplichtige incidenten worden gespecificeerd.

Tijdens de commissievergadering van de Tweede Kamer commissie Digitale Zaken is besloten dit wetsvoorstel niet-controversieel te verklaren. Dit besluit dient begin juli bekrachtigd te worden door de Tweede Kamer.

3. Wie valt onder de Cyberbeveiligingswet?

De wet is van toepassing op zogenoemde essentiële en belangrijke entiteiten. Dit kunnen organisaties zijn in sectoren als energie, transport, water, digitale infrastructuur, zorg, financiële dienstverlening en voedsel. Het zelfevaluatie-instrumenten, de NIS2-Zelfevaluatie kan helpen bij het bepalen of jouw organisatie onder de wet valt.

Deze zelfevaluatie geeft geen antwoord op de vraag onder welke jurisprudentie organisaties vallen die in meerdere landen (binnen en/of buiten Europa) gevestigd zijn. Ook geeft dit geen antwoord situaties waarbij organisaties bijvoorbeeld holding of coöperatie structuren hebben waarbij de één wel en de ander niet onder de Cbw valt. Oftewel, het geeft voor organisaties gevestigd in meerdere landen of vallend onder complexe juridische structuren geen antwoord op de vraag óf én onder welke nationale wetgeving de organisatie valt, aan welke zorgplicht voldaan moet worden en in welk land gemeld moet worden. Momenteel wordt er vanuit de overheid gewerkt aan een handreiking om antwoord te geven op deze vraag. Zodra CVNL deze informatie heeft zal dat gedeeld worden.

[1] Wetsvoorstel Cbw ingediend bij Tweede Kamer | Nieuwsbericht | Nationaal Cyber Security Centrum

4. Verplichtingen en rechten voor organisaties

De wet introduceert drie centrale verplichtingen:

- Zorgplicht: het nemen van passende technische en organisatorische maatregelen, waaronder risicoanalyses, beleid voor evaluatie, bedrijfscontinuïteitsplannen en ketenbeveiliging.
- Meldplicht: ernstige ICT-incidenten moeten worden gemeld bij het desbetreffende CSIRT en de relevante toezichthouder. Dit zal via het portaal verlopen waar organisaties zich ook moeten registreren.
- Registratieplicht: entiteiten moeten zich registreren in een centraal register.

Tegelijkertijd kunnen organisaties in bepaalde gevallen ook al rechten ontlenen aan de wet, ondanks dat deze nog niet formeel in werking is getreden. Op basis van de NIS2-richtlijn geldt in sommige gevallen een rechtstreekse werking. Dit betekent bijvoorbeeld dat organisaties nu al aanspraak kunnen maken op ondersteuning bij incidentafhandeling door hun sectorale CSIRT[2]. Organisaties die geen sectorale CSIRT hebben krijgen te maken met het Nationaal Cyber Security Centrum (NCSC) die als nationale CSIRT zal fungeren.

Dit betekent overigens niet dat het NCSC de rol van een Incident Respons dienstverlener gaat overnemen. Zoals het NCSC zelf schrijft: “Ondersteuning van de CSIRT is … geen vervanging van reguliere cyberbeveiligingsdiensten”.

Mocht een organisatie zich niet registreren, maar blijken wel onder de Cbw te vallen, dan blijven de verplichtingen zoals hierboven genoemd onverminderd van kracht. Mocht een organisatie zich wel registreren maar blijken niet onder de Cbw te vallen dan wordt de registratie gezien als een vrijwillige registratie. De rechten en plichten zoals hierboven genoemd zijn dan niet van toepassing op de betreffende organisatie. Omdat het NCSC mogelijk wel kan adviseren in het incident is het doen van een vrijwillige melding altijd van meerwaarde.

[2] IBD voor gemeentes, WaterCERT voor waterschappen, SURF-CERT voor onderwijsinstellingen en Z-CERT voor de zorg-sector.

5. Toezicht en handhaving

Toezichthouders zoals de Rijksinspectie Digitale Infrastructuur (RDI), de Inspectie Leefomgeving en Transport (ILT), en andere sectorale toezichthouders werken samen aan het toezicht. Er wordt gewerkt met een open norm-toetsingskader waarin ook internationale standaarden als ISO 27001, NIST of IEC 62443 een rol kunnen spelen. Toch zijn deze niet verplichtend; toezichthouders vormen altijd een eigen oordeel. Het toezicht is risico- en systeemgericht en kan bestaan uit inspecties, audits, aanwijzingen en bestuurlijke boetes. De bewijslast voor naleving van de zorgplicht ligt ten allen tijden bij de organisatie zelf, en dus niet bij de toezichthouder.

In de wet wordt ook gesproken over het doen van een beveiligingsscan om naleving te toetsen. Deze scan kan door de toezichthouder worden ingezet om te beoordelen in hoeverre een organisatie voldoet aan de zorgplicht. Voor belangrijke entiteiten wordt de beveiligingsscan uitgevoerd of gefaciliteerd door de bevoegde autoriteit. De kosten hiervan komen doorgaans voor rekening van de autoriteit zelf. De scan kan bestaan uit een technische beoordeling van systemen, kwetsbaarhedenscans, en/of interviews met verantwoordelijken binnen de organisatie. De uitkomsten geven input voor verdere interventies of handhaving. De beveiligingsscan komt voor rekening van de bevoegde autoriteit.

Een audit en/of controlefunctionaris daarentegen komen voor rekening van de organisaties zelf.

Er zijn kortweg gezegd twee soorten inspecties, te weten de incident inspectie (bij incident of in geval van reactief toezicht) en reguliere inspecties. Reguliere inspecties vinden plaats bij essentiële entiteiten (pro-actief). Daarbij kan de gehele zorgplicht getoetst worden of een deel daarvan. Toezichthouders zijn van plan om inzichten (geanonimiseerd) breder te delen zodat meerdere organisaties hier lering uit kunnen trekken.

Samenwerking tussen toezichthouders kan bestaan uit het doen van gezamenlijke inspecties, het gezamenlijk ontwikkelen van tools, het delen van ervaringen en inzichten tussen toezichthouders, e.d. Hierbij wordt vanzelfsprekend rekening gehouden met de geldende regels omtrent het onderling delen van informatie.

6. Wat kun je nu al doen?

Hoewel de wet pas in 2026 in werking treedt, is het raadzaam om nu al te starten met de voorbereidingen. Organisaties kunnen:

- een zelfevaluatie uitvoeren om te bepalen of zij onder de wet vallen;
- een quickscan uitvoeren om hun huidige weerbaarheidsniveau te bepalen;
- maatregelen nemen om te voldoen aan de zorgplicht;
- het bestuur betrekken bij de voorbereidingen en bewustwording vergroten, mede ook vanwege de bestuurdersaansprakelijkheid.

Praktische tools zijn te vinden via digitaltrustcenter.nl/nis2/startpunt.

7. Vragen of hulp nodig?

Voor algemene vragen over dit artikel of de Cyberbeveiligingswet kun je terecht bij Cyberveilig Nederland via **info@cyberveilignederland.nl**.

Heeft u inhoudelijke vragen over de implementatie van de wet? Neem dan contact op met **info@ncsc.nl**, met het verzoek om Cyberveilig Nederland in de cc op te nemen. Zo houdt CVNL ook zicht op de vragen die er spelen binnen het veld.