

Stand van zaken Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten

In deze mededeling wordt u geïnformeerd over de status van de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) en daarmee gerelateerde onderwerpen:

- wetsvoorstellen bij Raad van State;
- internetconsultatie Algemene Maatregelen van Bestuur (AMvB's);
- verwachte datum inwerkingtreding;
- opleiding voor bestuurders;
- afronding onderzoek beveiliging toeleveranciers;
- CERT-Water;
- themagroep fysieke en digitale veiligheid.

Wetsvoorstellen bij Raad van State

De wetsvoorstellen voor de Cbw en Wwke zijn op 2 december 2024 naar de Afdeling advisering van de Raad van State gestuurd. De wetsvoorstellen zijn beschikbaar op wetgevingskalender.overheid.nl.

In de wetsvoorstellen en de bijbehorende memories van toelichting zijn de consultatiereacties verwerkt.

Twee belangrijke punten uit onze consultatiereactie zijn in het wetsvoorstel Cbw overgenomen/verwerkt:

1. De eindverantwoordelijkheid voor de Cbw komt niet bij de ambtelijke leiding (secretaris-directeur) te liggen, maar bij het bestuur (dagelijks bestuur). Ieder lid van het bestuur moet over de benodigde kennis en vaardigheden beschikken om:
 - a. risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren;
 - b. risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen;
 - c. de gevolgen van de risico's en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.
2. Het ministerie van Infrastructuur en Waterstaat (IenW) (en dus niet het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)) wordt de bevoegde autoriteit voor de waterschappen als onderdeel van de sector overheid. Zodoende zal de Inspectie Leefomgeving en Transport (ILT) onze toezichthouder worden en niet de Rijksinspectie Digitale Infrastructuur (RDI).

De Raad van State is gevraagd om zo spoedig mogelijk advies uit te brengen.

Internetconsultatie AMvB's

Per AMvB zullen onderdelen uit de Cbw en Wwke nader uitgewerkt worden, zoals de zorgplicht en de meldplicht. Voor de Cbw is de verwachting dat de nieuwe versie van de Baseline Informatiebeveiliging Overheid (BIO2) in de AMvB zal worden aangewezen als kader voor de zorgplicht. Ook zullen in deze AMvB nadere eisen aan de opleiding voor bestuurders worden gesteld. Daarnaast was het aanvankelijk de bedoeling om in deze AMvB sectorale CSIRT's¹ zoals SURF-CERT (onderzoek en onderwijs) en de IBD (gemeenten) aan te wijzen, maar wordt er nu over gedacht om dit per ministeriële regeling te doen. De verwachting is dat de AMvB's op 5 maart 2025 in consultatie gaan. Vanwege de tijdsdruk is de planning dat de consultatie slechts 4 weken open staat. De koepels van de decentrale overheden hebben al aangegeven dit te kort te vinden en conform de Code Interbestuurlijke Verhoudingen minimaal 8 weken nodig te hebben om de achterban te consulteren en een gezamenlijke reactie op te stellen.

¹ Een Computer Emergency Response Team (CERT) of een Computer Security Incident Response Team (CSIRT) is een gespecialiseerd team van ICT-professionals dat in staat is snel te coördineren en escaleren in het geval van een beveiligingsincident met computers of netwerken dat de wettelijke drempelwaarde(n) overstijgt



Verwachte datum inwerkingtreding

De nieuwe Network and Information Security (NIS2) richtlijn en Critical Entities Resilience (CER) richtlijn zijn sinds 17 oktober 2024 geldig in de Europese Unie. In Nederland is het niet gelukt om deze EU-richtlijnen op tijd om te zetten in nationale wetgeving. De verwachting is dat de Cbw en Wwke in het 3e kwartaal van 2025 in werking treden. Tot de wetten in werking zijn getreden, hoeven organisaties zich niet aan de verplichtingen uit de richtlijn te houden. Wel hebben organisaties in bepaalde gevallen bepaalde rechten vanwege [rechtstreekse werking van sommige bepalingen in de NIS2-richtlijn](#).

Opleiding voor bestuurders

Conform artikel 20 van de NIS2-richtlijn en de implementatie daarvan in artikel 24 van de Cbw moeten de leden van het bestuur van een essentiële entiteit een opleiding volgen zodat zij 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. Nadere eisen aan deze opleiding voor bestuurders worden uitgewerkt in de AMvB. In afwachting van deze nadere eisen is CIO Rijk bezig met het opzetten van een opleiding voor overheidsbestuurders. De decentrale overheden mogen aan deze opleiding van CIO Rijk meedoen en kunnen daarbij hun eigen casuïstiek inbrengen. Het ministerie van IenW heeft aangegeven deze casuïstiek voor de watersector met de CIO Rijk af te gaan stemmen en heeft eind vorig jaar zelf Secura gecontracteerd om een eerste serie opleidingen voor de watersector te verzorgen. Het is nog niet bekend wanneer de centraal aangeboden opleidingen daadwerkelijk van start gaan, maar bestuurders hebben in ieder geval tot twee jaar na inwerkingtreding van de Cyberbeveiligingswet de tijd om aan de opleidingsvereisten te voldoen.

Afronding onderzoek beveiliging toeleveranciers

Met behulp van een subsidie van het ministerie van BZK heeft de Unie bureau Berenschot ingehuurd om nader onderzoek te verrichten naar de beveiliging van de toeleveringsketen waarvoor entiteiten in de NIS2 verantwoordelijk worden gehouden. Berenschot heeft de eindrapportage begin januari jl. opgeleverd en zal de resultaten aan de waterschappen presenteren in het overleg van de Coördinatoren Informatieveiligheid Waterschappen (CIW) d.d. 11 februari 2025 en het i-Platform d.d. 13 maart 2025. Het onderzoek zal in de volgende CBDF vergadering (6 juni 2025) worden gedeeld.

CERT-Water

In de Werkgroep Bedrijfsvoering, Digitalisering en Dienstverlening (WBDD) van 18 april 2024 en de CBCF van 31 mei 2024 is beeldvormend gesproken over het voornemen van het ministerie van IenW om een sectoraal CERT voor de watersector op te richten, waarin in eerste instantie de waterschappen samen met Rijkswaterstaat participeren. De waterschappen stonden hier destijds positief tegenover en hebben enkele randvoorwaarden aan het ministerie meegegeven waaronder ze met Rijkswaterstaat zouden willen samenwerken in een CERT-Water.

Wegens de politieke wisseling medio 2024 en het vertrek van enkele ambtenaren die bij de oprichting van een CERT-Water betrokken waren, is de verdere beeldvorming en besluitvorming daarna helaas stil komen te liggen. Pas nu het ministerie van IenW (in plaats van het ministerie van BZK) in het aangepaste wetsvoorstel als bevoegde autoriteit voor de waterschappen wordt aangewezen, gaat het ministerie de mogelijke besluitvorming over de oprichting van een CERT-Water langzaamaan weer oppakken. Er is op dit moment nog geen nieuwe planning bekend. De Unie heeft in gesprekken met het ministerie van IenW aangegeven dat spoedig duidelijkheid op dit dossier nodig is.

Themagroep fysieke en digitale veiligheid

Vanwege de komst van de Cbw en Wwke heeft de Unie eind vorig jaar de themagroep fysieke en digitale veiligheid opgericht. Doel van deze themagroep is om samen met de waterschappen vanuit verschillende



expertises te onderzoeken wat de impact van deze nieuwe wetten is en welke stappen de waterschappen nog moeten zetten om beide wetten tijdig te implementeren. Voor de Wwke wordt hierbij nadrukkelijk gekeken naar het al vitale proces Keren en beheren om daar voor het kritieke proces Afvalwater zoveel mogelijk van te leren. De themagroep is in dit kader nog op zoek naar een expert die de waterschappen op het gebied van Keren en beheren / vitaal wil vertegenwoordigen.