Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3968 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 oktober 2024

Op 31 januari 2024 heeft mijn voorganger uw Kamer geïnformeerd over de stand van zaken met betrekking tot de implementatie van twee Europese richtlijnen in nationale wetgeving, namelijk die van: de NIS2-richtlijn in de Cyberbeveiligingswet en die van de CER-richtlijn in de Wet weerbaarheid kritieke entiteiten. In deze brief is gemeld dat het omzetten van deze Europese richtlijnen in nationale wetgeving meer tijd vergt dan verwacht, en dat de implementatiedeadline van 17 oktober 2024 voor beide richtlijnen niet gehaald wordt.[1] Hetzelfde geldt op moment van schrijven ook voor andere lidstaten. Voor een actuele stand van zaken verwijs ik uw Kamer naar de website van de Europese Unie.[2]

Zoals eerder gecommuniceerd, komt de vertraging doordat de omzetting naar nationale wetgeving een omvangrijk en complex traject is. De impact voor Nederlandse organisaties is aanzienlijk en er zijn ten opzichte van bestaande wetgeving meer sectoren en meer organisaties die moeten voldoen aan de nieuwe wetgeving. Daarnaast hecht ik grote waarde aan het zorgvuldig verwerken van de circa 150 reacties die zijn binnengekomen tijdens de internetconsultatie en de interdepartementale afstemming hierover.

Beide wetten zullen een belangrijke basis vormen voor het cybersecuritystelsel en de weerbaarheid van de vitale infrastructuur en zijn daarom van grote waarde voor het verhogen van de weerbaarheid van ons land. Ondanks de vertraging in de omzetting van de richtlijnen worden organisaties, die onder de wetten komen te vallen, daarom door betrokken ministeries al benaderd en gewezen op de maatregelen die ze nu al kunnen treffen. Daarnaast zullen verschillende organisaties, in verband met de hieronder toegelichte rechtstreekse werking van enkele bepalingen uit de NIS2-richtlijn, al per 17 oktober 2024 bepaalde rechten

[1] Kamerstukken II 2023/24, 22 112, nr. 3868
[2] https://eur-lex.europa.eu/legal-content/en/NIM/?uri=CELEX%3A32022L2555

kst-22112-3968
ISSN 0921 - 7371
's-Gravenhage 2024

hebben, zoals het recht op bijstand van een Computer Incident Response Team (CSIRT) bij cyberincidenten. Zo tracht ik de gevolgen van de vertraging voor de weerbaarheid van Nederland zo beperkt mogelijk te houden.

Ik verwacht dat beide wetsvoorstellen in het vierde kwartaal van 2024 voor advies worden aangeboden aan de Afdeling advisering van de Raad van State. Afhankelijk van de tijd die nodig is voor het advies en de verwerking daarvan, zullen de voorstellen naar verwachting in het eerste kwartaal van 2025 naar uw Kamer worden gestuurd. Het streven is dat beide wetten in het derde kwartaal van 2025 in werking treden. Dit is uiteraard ook afhankelijk van de voortgang van de behandeling van de wetsvoorstellen in de Tweede en Eerste Kamer. In deze brief informeer ik u over de gevolgen van de niet-tijdige implementatie van beide richtlijnen.

Gevolgen van niet-tijdige implementatie van de CER-richtlijn

De CER-richtlijn wordt geïmplementeerd in de Wet weerbaarheid kritieke entiteiten. Organisaties zullen pas onder die wet vallen zodra ze op grond van die wet zijn aangewezen als «kritieke entiteit». Voor deze organisaties zullen de zorgplicht en de meldplicht uit deze wet pas van toepassing zijn vanaf tien maanden na hun aanwijzing als kritieke entiteit.

In de periode tussen 17 oktober 2024 en de datum van inwerkingtreding van de Wet weerbaarheid kritieke entiteiten gelden er *geen* verplichtingen voor organisaties vanuit de CER-richtlijn. Deze verplichtingen gelden pas voor organisaties wanneer de Wet weerbaarheid kritieke entiteiten in werking treedt én de organisatie wordt aangewezen als kritieke entiteit.

Wel kent de CER-richtlijn ook voor lidstaten een aantal verplichtingen na 17 oktober 2024. Voor de Rijksoverheid betreft dit het vaststellen van een nationale strategie (artikel 4 CER), het uitvoeren van een risicobeoordeling (artikel 5 CER) en het identificeren van kritieke entiteiten (artikel 6 CER). De uiterlijke termijn voor het voldoen aan deze verplichtingen uit artikelen 4 en 5 is 17 januari 2026 en voor artikel 6 is dit 17 juli 2026. Door alle betrokken ministeries worden voorbereidingen getroffen, al dat niet in het kader van staand beleid uit de Aanpak vitaal,[3] om tijdig aan deze verplichtingen te voldoen.

Gevolgen van niet-tijdige implementatie van de NIS2-richtlijn

De NIS2-richtlijn wordt geïmplementeerd in de Cyberbeveiligingswet. Deze wet zal van toepassing zijn op essentiële en belangrijke entiteiten. Daarbij zal het, anders dan bij de CER-richtlijn, ten eerste gaan om entiteiten die van rechtswege onder de richtlijn vallen en dus zonder aanwijzing door een lidstaat essentiële of belangrijke entiteit zullen zijn. Daarnaast gaat het om entiteiten die pas na aanwijzing door de overheid als essentiële of belangrijke entiteit onder de Cyberbeveiligingswet zullen komen te vallen.

In de periode tussen 17 oktober 2024 en de datum van inwerkingtreding van de Cyberbeveiligingswet gelden er voor organisaties geen verplichtingen vanuit de NIS2-richtlijn. Voor alle essentiële en belangrijke entiteiten gaan die verplichtingen in de NIS2-richtlijn pas gelden zodra de Cyberbeveiligingswet in werking treedt. Er kan dus ook niet op de naleving hiervan toezicht worden gehouden door de Nederlandse toezichthouder. Dit geldt eveneens voor verplichtingen die voortvloeien uit de Europese uitvoeringsverordening die nadere invulling geeft aan de

[3] Kamerstukken II 2022/23, 30 821, nr. 182.

plichten uit de NIS2-richtlijn.[4] Voor organisaties die nu onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen, blijven in deze periode de uit die wet voortvloeiende rechten en plichten, alsook het toezicht op de naleving van die plichten, gelden. De Wbni blijft, ook voor zover het taken en bevoegdheden van overheidsinstanties zoals het NCSC betreft, van kracht totdat de Cyberbeveiligingswet in werking treedt. Sommige bepalingen uit de NIS2-richtlijn hebben in deze periode zogenoemde rechtstreekse werking. Dat betekent dat organisaties die van rechtswege onder de richtlijn vallen, vanaf 17 oktober 2024 bepaalde rechten zullen hebben, zoals het ontvangen van bijstand bij een cyberincident van een CSIRT.

Uitgangspunt zal gelet hierop zijn dat in de periode van 17 oktober 2024 tot de datum van inwerkingtreding van de Cyberbeveiligingswet uitvoering wordt gegeven aan bovenbedoelde rechtstreekse werking en het interpreteren van de Wbni conform de NIS2-richtlijn (richtlijnconforme interpretatie). Daarbij zal het beleid hierover nadrukkelijk rekening houden met de systematiek en uitgangspunten van de Cyberbeveiligingswet.

Beantwoording vragen en factsheet

Om organisaties helderheid te geven over de gevolgen van de niet-tijdige implementatie van de NIS2-richtlijn in de periode van 17 oktober 2024 tot de datum van inwerkingtreding van de Cyberbeveiligingswet, is een aantal antwoorden op vragen, die leven onder organisaties, gepubliceerd. Een kopie is bijgevoegd als bijlage bij deze Kamerbrief.

Daarnaast is een factsheet opgesteld over de gevolgen van de niet-tijdige implementatie van de NIS2-richtlijn, waarin wordt ingegaan op de gevolgen voor organisaties die van rechtswege onder de NIS2-richtlijn vallen én de daarmee samenhangende uitvoeringspraktijk.

Uitvoeren van taken door een CSIRT in de overgangsperiode

Zoals hierboven vermeld zullen organisaties, die als essentiële of belangrijke entiteit van rechtswege onder de NIS2-richtlijn vallen, in de periode van 17 oktober 2024 tot de inwerkingtreding van de Cyberbeveiligingswet rechten kunnen ontlenen aan enkele, in het factsheet opgesomde, bepalingen in de richtlijn over taken van een CSIRT. Dat laatste geldt overigens ook in sommige, daarin eveneens genoemde, gevallen voor andere relevante partijen. In Nederland zullen deze CSIRT-taken in deze periode worden uitgevoerd door het onder de Wbni aangewezen Nationaal Cyber Security Centrum (NCSC) en het CSIRT voor digitale diensten (CSIRT-DSP)[5]. Voor de zorg zal het expertisecentrum voor cybersecurity in de zorg Z-CERT[6] deze taak op zich nemen. Hiermee anticipeert de Minister van VWS op de Cyberbeveiligingswet dat het voornemen bevat Z-CERT aan te wijzen[7] als CSIRT onder deze wet. Daarbij bedient Z-CERT de sector al sinds 2015 en is mede gezien het huidige dreigingsbeeld het voor entiteiten van belang dat er continuïteit van de dienstverlening is. Z-CERT heeft de beste kennispositie om de entiteiten te ondersteunen in het op peil houden en verhogen van de weerbaarheid.

---

[4] Dit betreft de uitvoeringshandelingen op basis van de NIS2-richtlijn over zorg- en meldplicht (artikel 21, lid 5 en artikel 23, lid 11).

[5] In het geval van digitale dienstverleners, zijnde online marktplaatsen, online zoekmachines en cloudcomputerdiensten.

[6] In het geval van zorginstellingen, vervaardigers van farmaceutische basisproducten en vervaardigers van medische hulpmiddelen.

[7] Overheid.nl | Consultatie Cyberbeveiligingswet (internetconsultatie.nl) pagina 28 memorie van toelichting

Voor de samenleving levert dit een zo hoog mogelijk niveau van dienstverlening op.

Het CSIRT kan indien nodig, op basis van een risicogebaseerde benadering, prioriteit geven aan bepaalde taken.

Registratie in de periode tot inwerkingtreding van de wet

Essentiele entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, kunnen zich vanaf 17 oktober 2024 op vrijwillige basis registreren bij het NCSC. Deze registratie is pas na inwerkingtreding van de Cyberbeveiligingsdienst verplicht. Om ervoor te zorgen dat entiteiten de informatie voor de registratie laagdrempelig kunnen aanleveren en beheren, heeft het kabinet ervoor gekozen om een centrale registratiefunctionaliteit in te richten bij het NCSC. In dit registratieportaal is het ook mogelijk incidenten vrijwillig te melden.

Communicatie

Bij het informeren van entiteiten die van rechtswege onder de NIS2-richtlijn vallen, staat het informeren en activeren van de doelgroepen centraal.

Voor een optimaal bereik van alle doelgroepen is er een interdepartementale communicatiewerkgroep actief. Hierin zitten communicatie- en beleidsadviseurs van alle betrokken departementen en de uitvoeringsorganisaties Nationaal Cybersecurity Centrum (NCSC), CSIRT-DSP, het Digital Trust Center (DTC) en de Rijksinspectie Digitale Infrastructuur (RDI). Verder is er een publiek-privaat NIS2-overleg actief met vertegenwoordigers uit de overheid en diverse brancheorganisaties. Ieder vakdepartement en uitvoeringsorganisatie is verantwoordelijk voor het informeren en activeren van hun eigen sector en achterban.

Specifiek voor de periode van 17 oktober 2024 tot de inwerkingtreding van de Cyberbeveiligingswet heeft de communicatie als centrale boodschap: organisaties die van rechtswege onder de NIS2-richtlijn vallen hebben vanaf 17 oktober 2024 wel al bepaalde rechten, maar niet de plichten vanuit de NIS2-richtlijn. Doelgroepen worden opgeroepen om niet te wachten en zich nu al te beveiligen tegen de bestaande risico's. Hiertoe worden diverse communicatiemiddelen en -kanalen ingezet.

Door al zoveel als mogelijk in de geest van de Cyberbeveiligingswet te handelen, staan we organisaties bij om zich te beveiligen en ondersteunen we hen bij incidenten. Hiermee verhogen we de digitale weerbaarheid van Nederland, ook in deze periode.

De Minister van Justitie en Veiligheid,
D.M. van Weel