Netbeheer Nederland
Anna van Buerenplein 43
2595 DA Den Haag

Postbus 90608
2509 LP Den Haag
070 205 50 00
secretariaat@netbeheernederland.nl
netbeheernederland.nl

Ministerie van Justitie en Veiligheid
T.a.v. meneer D.M. van Weel
Postbus 20301
2500 EH Den Haag

Kenmerk
BR-2025-2153
Datum
28 maart 2025

Behandeld door
Jelle Dams
E-mail
jdams@netbeheernederland.nl

Doorkiesnummer
070 205 50 00

Onderwerp
Consultatiereactie Besluit weerbaarheid kritieke entiteiten

Geachte heer, mevrouw

Bijgaand treft u de reactie van Netbeheer Nederland (hierna: NBNL) aan op het concept Besluit weerbaarheid kritieke entiteiten (hierna: Bwke) ter implementatie van het voorstel voor de Wet weerbaarheid kritieke entiteiten (hierna: Wwke), zoals ter consultatie voorgelegd op 20 februari 2025. De Wwke strekt op haar beurt tot implementatie van de Critical Entities Resilience Directive (CER-richtlijn). Als vereniging van alle elektriciteits- en gasnetbeheerders in Nederland, heeft NBNL met veel interesse en belangstelling het concept besluit Bwke bestudeerd. NBNL waardeert de kans om te reageren op het Bwke en maakt hier middels dit schrijven graag gebruik van. In deze reactie geeft NBNL haar visie op het concept besluit en doen wij een aantal aanbevelingen voor verbetering.

NBNL staat positief tegenover de doelstellingen van de Europese CER-richtlijn, het wetsvoorstel Wwke en het voorliggende conceptbesluit Bwke. Tot op heden ontbrak er in Nederland een generiek wettelijk kader voor de fysieke weerbaarheid van vitale aanbieders. Gezien de huidige geopolitieke situatie, de toegenomen terroristische dreiging tegen Nederland en de impact van klimaatverandering op energie-infrastructuur, is versterking van de maatschappelijke weerbaarheid en veerkracht in Nederland van groot belang. Wij ondersteunen de algemene doelstellingen van het Bwke, maar signaleren enkele knelpunten en verbeterpunten die wij in deze reactie nader toelichten.

NBNL concentreert zich in haar consultatiereactie op de punten uit het Bwke welke aanpassing, verdere uitwerking of nadere toelichting behoeven. Daarnaast treft u in bijlage 1 een overzicht en nadere uitwerking van alle door NBNL gesignaleerde aandachtspunten. De belangrijkste punten zijn:

1. **Beperk regeldruk door aanwijzing van dezelfde toezichthouder als bij de Cyberbeveiligingswet (Cbw)**

De Wwke en Cbw maken deel uit van een breder wetgevingspakket dat gericht is op de (digitale) weerbaarheid van de maatschappij en de borging van vitale processen. Deze wetten overlappen elkaar deels en overlappen ook met bestaande en aankomende sectorale wetgeving. Dit leidt ertoe dat essentiële entiteiten met een lappendeken aan meldplichten en bevoegdheden van verschillende

toezichthouders worden geconfronteerd. Het is denkbaar dat één incident in de energiesector bij vijf of meer instanties gemeld moet worden, die allen onderzoek kunnen doen en aanvullende informatie kunnen vorderen.

NBNL pleit daarom voor:

- De aanstelling van dezelfde toezichthouder voor zowel Wwke als de Cbw. Dit minimaliseert de administratieve last en bevordert een efficiënte, consistente uitvoering en toezicht.
- Maximale coördinatie en samenwerking tussen toezichthouders, inclusief één centraal security-incident meldpunt, afstemming van informatieverzoeken en reactietermijnen en harmonisatie van drempelwaarden voor de meldplicht vanuit Wwke, Cbw en sectorale regelgeving zoals de Network Code on Cybersecurity .

2. De verplichting om beveiligingsmeldingen te beoordelen is te breed geformuleerd (Artikel 12 Bwke).

Artikel 12 van het Bwke vereist dat kritieke entiteiten alle beveiligingsadviezen en dreigingsinformatie beoordelen, ongeacht de bron. Dit onderscheidt niet tussen meldingen van bevoegde autoriteiten en meldingen van leveranciers en dienstverleners. Dit kan leiden tot een ongewenste toename van meldingen zonder directe relevantie en het risico op commerciële acquisitie door leveranciers.

NBNL adviseert daarom:

- De verplichting te beperken tot relevante dreigingsinformatie of adviezen voor producten of diensten die de essentiële entiteit reeds afneemt.
- Voorkomen dat leveranciers deze bepaling gebruiken voor commerciële upsell-strategieën, waarbij zij duurdere producten of diensten als ‘veiliger’ presenteren zonder objectieve noodzaak.
- De rol van leveranciers in beveiligingsmeldingen nader te definiëren, waarbij hun eigen verantwoordelijkheid en contractuele verplichtingen worden gewaarborgd.

3. Centraal opslaan van incident-gerelateerde informatie kan risico’s opleveren.

De registratie van meldplichtige security-incidenten zou geen gedetailleerde informatie over genomen maatregelen mogen bevatten. Dit om te voorkomen dat uiterst gevoelige informatie van alle essentiële entiteiten op één centrale locatie wordt bewaard, wat een zwakke plek voor de vitale infrastructuur kan vormen.

NBNL adviseert daarom:

- Geen centraal register met gevoelige details, eventueel een federatief stelsel waarbij de meest gevoelige informatie binnen de systemen van de essentiële entiteit blijft.
- Duidelijkheid over welke beveiligingsmaatregelen de bevoegde overheidsinstantie treft om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te garanderen (conform artikel 11 NIS2).
- Bevoegde overheidsinstanties zouden moeten aantonen dat hun beveiliging minstens op het niveau is dat op grond van de Cbw van een essentiële dienstverlener wordt verwacht. Dit kan via een ISO-27001-certificering of een SOC2 type 2-verklaring.

Wij danken u voor de gelegenheid om onze appreciatie uit te spreken en onze aandachtspunten kenbaar te maken. Wij hopen van harte dat onze input bijdraagt aan de verbetering van het onderliggende conceptbesluit. NBNL is graag bereid om haar reactie nader (mondeling) toe te lichten, mocht dit gewenst zijn. Verder denkt NBNL uiteraard graag mee bij de verder te nemen vervolgstappen en de uitwerking van het Bwke.

Met vriendelijke groet,

Jinny Moe Soe Let
Directeur Beleid & Communicatie

Bijlage 1: artikelsgewijze reactie op de Bwke

Artikel	Opmerking
Art. 2 Bwke	Er wordt ingezet op een sectorale invulling van de ondersteuning aan kritieke entiteiten. Hier moet onderstreept blijven dat aan kritieke en belangrijke entiteiten wordt gevraagd wat de behoeftes zijn (vraaggericht) en geen aannames (top-down) worden gedaan waarop ondersteuning vervolgens wordt gebaseerd.
Art. 4 (uitvoering van artikel 15 van de wet) Bwke	De Wwke beschrijft een all-hazard benadering voor weerbaarheid. Hoofdstuk 4 van de Bwke lijkt vooral in te gaan op fysieke security. Hier lijkt de all-hazard benadering los te zijn gelaten, waarbij bijvoorbeeld klimaat gerelateerde risico's weinig tot niet worden benoemd. Hoe moet de all-hazard benadering worden ingevuld, daarbij lettend op andere (sectorale) wetgeving m.b.t. weerbaarheid?
Art. 6 Bwke	Artikel 6 doet vermoeden dat het gaat over het onderhoud van assets en assetbeheer. Security komt hier niet in terug. Het advies is om het begrip security alsnog in te voegen in dit artikel, om verwarring te voorkomen. Daarnaast is verduidelijking nodig op welke manier dit artikel zich verhoudt tot andere wetgeving op het gebied van security en veiligheid van kritieke infrastructuur (b.v. artikel 5.20 van de Energiewet, lid 2 onderdeel b of specificaties van pijpleidingen).
Art. 8, 1 Bwke	Graag verduidelijking voor de term "nutsvoorziening" of deze vervangen door de term "noodvoorziening". Graag ook verduidelijking voor de term "veilige locatie".
Art. 9, 3 Bwke	Hoe verhoudt dit artikel zich tot bestaand eisen en toezicht op continuïteitsplannen van de netbeheerders door ACM en SODM?
Art. 11, 2 Bwke	Aan netbeheerders wordt via andere wetgeving -zoals artikel 3.18 Energiewet- verplichtingen tot rubricering van gevoelige informatie opgelegd. Op dit moment is er vanuit het perspectief van deze verschillende wetgeving nog geen sprake van een uniforme zienswijze op de door de kritieke entiteiten uit te voeren rubriceringswijze. Welke verwachting heeft de Minister omtrent de door kritieke entiteiten toe te passen rubriceringscategorieën, en welke beveiligingsmaatregelen worden door de Minister per rubriceringscategorie als voldoende verondersteld? Voorstel is om de term rubriceren (voor de overheid) te vervangen door de term classificeren (gangbaar bij entiteiten).
Art. 18, 1 Bwke	In artikel 18 wordt gesproken over het bewaren van persoonsgegevens. Daarbij wordt niet gesproken over bewaartermijnen voor overige (incidenten)informatie die wordt gedeeld met een bevoegd gezag onder de meldplicht. Ook hier moeten richtlijnen voor worden opgesteld zodat kwetsbare informatie vertrouwelijk kan worden uitgewisseld. Daarnaast moet in de Bwke onderstreept en gemotiveerd worden waarom de WOO niet van toepassing wordt (en kan worden) verklaard op gegevens die in het kader van de Wwke met de overheid worden gedeeld.
Art. 19 Bwke	Gelet op de verschillende verplichtingen binnen de Bwke onderschrijven de netbeheerders een gefaseerde inwerkingtreding van bepaalde onderdelen