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-2025-2154
Datum
28 maart 2025

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

Doorkiesnummer
070 205 50 00

Onderwerp
Consultatiereactie Cyberbeveiligingsbesluit

Geachte heer, mevrouw,

Bijgaand treft u de reactie van Netbeheer Nederland (hierna: NBNL) aan op het concept Cyberbeveiligingsbesluit (hierna: Cbb), zoals ter consultatie voorgelegd op 20 februari 2025. De Cbw strekt op haar beurt tot implementatie van de Europese Network and Information Security Directive (NIS2-richtlijn). Als vereniging van alle elektriciteits- en gasnetbeheerders in Nederland, heeft NBNL met veel interesse en belangstelling het conceptbesluit Cbb bestudeerd. NBNL waardeert de kans om te reageren op de Cbb en maakt hier middels dit schrijven graag gebruik van. In deze reactie geeft NBNL haar visie op het conceptbesluit en de bijhorende Ministeriële Regeling en doen wij een aantal aanbevelingen voor verbetering.

NBNL staat positief tegenover de doelstellingen van de Europese NIS2-richtlijn, het wetsvoorstel Cbw en het voorliggende conceptbesluit Cbb. Het verhogen van digitale veiligheid en weerbaarheid is cruciaal voor de continuïteit van onze werkzaamheden en het waarborgen van een van de meest betrouwbare energiesystemen ter wereld. Dit is vooral van belang in een tijd waarin digitale dreigingen onverminderd groot zijn. Wij ondersteunen de algemene doelstellingen van het Cbb, maar signaleren enkele knelpunten en verbeterpunten die wij in deze reactie nader toelichten.

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

1. Beperk regeldruk door coördinatie tussen toezichthouders en harmonisatie van verplichtingen

De Cbw en Wwke vormen onderdeel van een breed pakket aan huidige en toekomstige wetgeving die beoogt de (digitale) weerbaarheid van de maatschappij en de continuïteit van vitale processen te borgen. De beide wetten overlappen daarbij (deels) zowel elkaar als met bestaande en aankomende sectorale wetgeving. Hierdoor krijgen essentiële entiteiten nog meer te maken met een lappendeken aan meldplichten en bevoegdheden van verschillende toezichthouders.

NBNL pleit daarom voor:

- Een centraal meldstructuur, waarbij één centraal incidentmeldpunt wordt ingevoerd, informatieverzoeken en reactietermijnen worden geharmoniseerd en drempelwaarden voor meldplichten worden afgestemd tussen de Cbw, Wwke en sectorale regelgeving zoals de Network Code on Cybersecurity (NCCS)

2. De verplichtingen om beveiligingsmeldingen te beoordelen is te breed geformuleerd

Artikel 17 Cbb maakt geen onderscheid tussen meldingen van bevoegde autoriteiten en meldingen van commerciële leveranciers. Dit kan leiden tot ongewenste acquisitiepraktijken en onnodige regeldruk.

NBNL adviseert voor:

- De verplichting zou beperkt moeten worden tot meldingen van bevoegde autoriteiten, CSIRT en relevante overheidsinstanties, en relevante adviezen en dreigingsinformatie over producten of diensten die reeds worden afgenomen.

3. Het Nationaal Register kan de zwakke plek van de vitale infrastructuur worden

Het NCSC zal een nationaal register van essentiële en belangrijke entiteiten beheren. In artikel 28 Cbb is onduidelijk of het registratieplicht zich beperkt tot publieke domeinen of ook interne informatie omvat.

NBNL adviseert daarom voor:

- De registratieplicht beperken tot de publieke domeinen.
- Registratie van genomen maatregelen bij security-incidenten niet verplicht stellen.
- Overwegen af te zien van een centraal register en eventueel in plaats daarvan een federatief stelsel te hanteren, waarbij gevoelige informatie binnen de systemen van de essentiële entiteit blijft.
- Het NCSC zou naar de essentiële en belangrijke entiteiten transparant moeten maken welke beveiligingsmaatregelen het zelf treft (bijvoorbeeld via ISO-27001-certificering of SOC2 type 2 verklaring).

4. Zorgplicht: aantoonbaarheid van het toepassen van beleid

Het Cbb vereist dat organisaties hun cyberbeleid schriftelijk vastleggen en aantoonbaar toepassen, maar artikel 6 lid 4 geeft onvoldoende duidelijkheid over hoe dit moet worden aangetoond.

NBNL adviseert voor:

- Expliciet maken dat aantoonbaarheid via een ISMS (zoals ISO-27001) voldoet.

5. Zorgplicht: Differentie binnen het beleidshuis

Het Cbb beschouwt procedures als onderdeel van beleid, wat onnodig inflexibel is.

NBNL adviseert voor:

- Procedures en technische standaarden moeten als zelfstandige producten worden beschouwd die invulling geven aan beleid. Dit maakt organisaties flexibeler en sluit beter aan bij een correct ingeregelde governance-structuur.

6. Beveiliging van de toeleveringsketen

Artikel 10 Cbb vereist dat essentiële entiteiten afspraken maken met leveranciers over cyberbeveiliging. In de praktijk is invloed op grote, internationale leveranciers beperkt. De huidige opzet legt een zware last op de essentiële entiteiten om compliance van duizenden leveranciers te borgen.

NBNL pleit voor:

- Zet eisen en verplichtingen door naar analogie van de AVG naar sub-leveranciers, zodat directe leveranciers verantwoordelijk blijven voor de naleving in de keten.

7. MR: Risico-gebaseerde aanpak

De MR moet de zorgplicht verder uitwerken, maar wijkt in de huidige vorm af van de risico-gebaseerde aanpak van de Cbw. Dit leidt tot verhoogde regeldruk en onduidelijkheid over de prioritering van maatregelen.

NBNL pleit voor:

- Duidelijk maken dat entiteiten een risico-gebaseerde invulling mogen hanteren bij de naleving.
- Specifiek voor OT-systemen (Operationele Technologie) ruimte bieden voor alternatieve beveiligingsmaatregelen zoals meerlaagse beveiligingsstrategieën, in plaats van een generieke verplichting tot software-updates.
- Artikel 7 lid 3, dat updates zonder onderscheid tussen IT- en OT-systemen verplicht stelt, moet worden beperkt tot hoog-risico kwetsbaarheden en alternatieve maatregelen.

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 denken wij uiteraard graag mee bij de verder te nemen vervolgstappen en de uitwerking van het Cbb.

Met vriendelijke groet,

Jinny Moe Soe Let
Directeur Beleid & Communicatie

Bijlage 1: artikelsgewijze reactie op de Cbw

Artikel	Opmerking
Art. 4 Cbb	Artikel 4 Cbbbeschrijft een uitzondering van artikel 6 tot en met 16 en 24 voor een aantal entiteiten. Een groot deel van deze entiteiten is onderdeel van onze bedrijfsvoering. Weerbare ketenpartners zijn van belang om kwetsbaarheden te voorkomen (ketenafhankelijkheid). Waarom is er gekozen voor het uitzonderen van deze entiteiten?
Art. 5 Cbb	Het principe security by design wordt niet specifiek genoemd in de AMvB van de Cbw. Op verschillende plekken in de AMvB komen wel onderdelen van het security by design principe terug. Toevoeging van het security by design principe geeft de entiteit een praktisch handvat en urgentiebesef om vanaf de beginfase te zorgen voor weerbaarheidsmaatregelen. Daarnaast schept het consistentie met de Bwke waar dit wel wordt genoemd.
Art. 9, 1 Cbb	In de AMvB Wwke wordt ook gesproken over een bedrijfscontinuïteitsplan (artikel 9). Waarom wordt in de Cbb en Bwke geen koppeling gemaakt tussen de twee wetgevingen op dit punt? Dit geldt ook voor artikel 10 Cbb en artikel 7 Bwke. Dit voorkomt verwarring.
Art. 12, 2 Cbb	Wordt hier bedoeld dat naast een generieke basisopleiding specifieke opleidingen worden verwacht voor medewerkers met een specifieke rol of verantwoordelijkheid in de beveiliging van netwerk- en informatiesystemen? Zo ja, kan meer duidelijkheid gegeven worden over wat hier geëist wordt?
Art. 16, 3 Cbb	Geldt deze inventarisatie voor de gehele inventaris, of alleen datgene dat nodig is voor het leveren van de kritieke dienst-? Welke "informatie" anders dan informatie over "gerelateerde netwerk- en informatiesystemen" wordt hier bedoeld ?
Art. 20 Cbb	Hoe verhoudt dit artikel tot artikel 10 lid 2 en lid 3 van de Wwke ? Het advies is om de trainingseisen voor beide wetten identiek te maken.
Art. 22, 1 Cbb	Het is onduidelijk wat er precies wordt verstaan onder een onafhankelijke trainer. De ervaring leert dat externe trainers niet altijd in staat zijn om een training te geven die past bij de rollen van de bestuurders van een essentiële of belangrijke entiteit. Het zou mogelijk moeten zijn om tailor-made trainingen te laten geven door eigen experts.
Art. 36 Cbb	Gelet op de verschillende verplichtingen binnen de Cbb en MR onderschrijven de netbeheerders een gefaseerde inwerkingtreding van bepaalde onderdelen