Notitie

Behandeld door Siebe Kok (skok@energie-nederland.nl)

Aan Ministerie van Justitie en Veiligheid

Datum 26-03-2025

Onderwerp Reactie op de internetconsultatie van het Cyberbeveiligingsbesluit en de ministeriele regeling

Reactie op de internetconsultatie van het Cyberbeveiligingsbesluit en de ministeriele regeling …

Met veel belangstelling heeft Vereniging Energie-Nederland* (hierna Energie-Nederland) kennisgenomen van het concept Cyberbeveiligingsbesluit (hierna: Cbb) en de onderliggende ministeriële regeling (hierna: MR) met de nadere uitwerking van de zorgplicht. Energie-Nederland maakt graag gebruik van de mogelijkheid op dit conceptbesluit en de concept regeling te reageren.

(* Zie pagina 11)

Algemeen

1. Energie-Nederland is over het algemeen positief over de verschenen conceptversie van het Cbb en de onderliggende MR met de nadere uitwerking van de zorgplicht, omdat er vergeleken met andere Europese implementaties van de NIS2 Richtlijn redelijk veel vrijheid wordt gegeven aan entiteiten om zelf risicogebaseerde afwegingen te maken. Ook staan we positief tegenover de doelen van de NIS2 en de Cyberbeveiligingswet. Het belang van het verhogen van de digitale veiligheid en weerbaarheid in Nederland is niet te onderschatten. Dat geldt in het bijzonder voor vitale sectoren zoals de energiesector. Wel zijn we kritisch op de uitwerking van een aantal punten in het Cbb. Deze worden hieronder verder toegelicht.
2. Energie-Nederland benadrukt graag dat de nadruk in de AMvB meer op praktische toepassing moet liggen dan op de schriftelijke vastlegging van bijvoorbeeld risico’s en maatregelen. Hierbij moet vooral rekening worden gehouden met het werkbaar houden van de maatregelen.

3. We steunen de keuze om de drempelwaarden voor significante incidenten voor de meldplicht in een sectorale ministeriële regeling vast te leggen. Wel vragen we om snelle duidelijkheid rond deze drempelwaarden aangezien bedrijven implementatietijd nodig hebben om deze correct te verwerken. Deze moeten dus ruim voor de inwerkingtreding van de wet bekend zijn. Wanneer dit niet mogelijk is, zou er net als in de Wwke een implementatietermijn van bijvoorbeeld 9 maanden kunnen worden vastgelegd.
4. Harmonisatie binnen de EU was een van de doelen van de NIS2. Echter toont het in januari 2025 verschenen ECSO rapport, met daarin een analyse van de implementatie binnen de verschillende lidstaten, aan dat de implementatie voorlopig tot minder harmonisatie leidt.[1] Energie-Nederland benadrukt dat harmonisatie op EU-niveau essentieel is voor een werkbare implementatie van de Cyberbeveiligingswet.
5. Een groot punt van zorg is de uitwerking van de gevolgen voor bedrijven met complexe bedrijfsmodellen. Dit is in december in een gesprek met o.a. het ministerie van J&V, de RDI en een aantal vertegenwoordigers van vitale sectoren besproken. Destijds is nadere uitwerking van de besproken scenario's beloofd. Tot op heden is deze niet ontvangen. Energie-Nederland behoudt zich graag het recht voor om op een later moment op deze uitwerking te reageren, ook wanneer de consultatiedeadline voor het Cyberbeveiligingsbesluit reeds gesloten is.
    a. Registratieplicht: Op dit moment moeten bedrijven elke juridische entiteit binnen hun groep apart met E-Herkenning gaan registreren, in sommige gevallen zelfs voor beide wetten (zowel Cbb als Bwke). Voor sommige bedrijven gaat dit om tientallen tot honderden entiteiten. De regeldruk wordt hiermee niet te overzien, zeker als er ook terugkerende kosten zijn indien elke wijziging in de bedrijfsstructuur moet worden doorgegeven.
    b. Bestuurders: wie wordt nu exact als bestuurder gezien? Gaat dit alleen over de bestuursleden die direct de entiteit besturen of ook om de bestuurslaag daarboven? Wij

[1] https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

vinden de direct betrokken bestuurders van belang. Andere bestuurders zijn optioneel.

6. De Cbw en het onderliggende Cbb leveren veel regeldruk op, in het bijzonder voor MKB bedrijven. Naar verwachting zal hiervoor gerichte overheidsondersteuning komen. Energie-Nederland raadt hierbij aan zoveel mogelijk aan te sluiten bij bestaande programma's vanuit bijvoorbeeld het DTC. Er is al voldoende versnippering als het aankomt op het vinden van de juiste informatie.
7. Energie-Nederland pleit voor een gedeeltelijke overgangsregeling van tenminste negen maanden, in lijn met de Wwke. Energie-Nederland gaat graag met u in gesprek om tot een redelijke, al dan niet gefaseerde, implementatietermijn voor de verschillende onderdelen van de Cbw en het Cbb te komen. Er is daarnaast tijd nodig voor bedrijven om de Cbw en het Cbb, maar ook andere wetgeving goed te implementeren alvorens nieuwe wetgeving wordt ontwikkeld.
8. In haar advies op de Cyberbeveiligingswet adviseert de Raad van State om nader te motiveren waarom een afwijking van de Wet open overheid noodzakelijk is.[2] Bij deze wil Energie-Nederland graag benadrukken dat de informatie die in het kader van de Cbw gedeeld wordt strikt vertrouwelijk en zeer gevoelig is voor bedrijven. Zonder uitzondering op de Woo zullen bedrijven zeer terughoudend zijn meldingen te doen of informatie te delen. Dit zal de weerbaarheid van Nederland niet ten goede komen. We verzoeken daarom dan ook dringend om de door de Raad van State gevraagde motivatie aan te leveren.

Samenhang met Bwke

9. Energie-Nederland heeft veel leden die zowel onder de Wwke en de Cbw gaan vallen. Dit betekent dat er voor beide wetten registraties, meldingen en audits zullen komen. We pleiten dan ook voor één toezichthouder voor de energiesector die verantwoordelijk wordt voor beide wetten. Deze toezichthouder is dan in staat om een integrale audit kan doen, in lijn met de huidige praktijk bij veel bedrijven.

[2] https://www.raadvanstate.nl/adviezen/@147382/w16-24-00336-ii/

10. De samenhang van het pakket Cbw en Cbb met de Wet weerbaarheid kritieke entiteiten (Wwke) en het Besluit weerbaarheid kritieke entiteiten (Bwke) is van groot belang. Bedrijven doen hun risicoanalyse volgens een all-hazards approach. Om de regeldruk niet onnodig te verhogen is het van groot belang dat de samenhang tussen beide trajecten wordt bewaakt. Dit betekent specifiek dat we graag één kanaal voor meldingen onder zowel de Cbw als de Wwke zouden zien.
11. Hoewel we begrijpen dat dit door de woordkeuze in Europese richtlijnen niet altijd mogelijk is, willen we er toch op wijzen dat de terminologie in beide wetten zoveel mogelijk geharmoniseerd moet worden. In de Wwke/Bwke gaat het over kritieke entiteiten en aanzienlijke verstoringen, in de Cbw/Cbb over essentiele en belangrijke entiteiten en significante incidenten. In hoeverre is het mogelijk om de Bwke en Cbb te harmoniseren in proces en terminologie - om de regeldruk (compliance) *en* de benodigde effort voor toezichthouder(s) & CSIRTS - te minimaliseren?

Zorgplicht

1. De formulering " … *periodiek …"* wordt in het Cbb een aantal keer genoemd (bijvoorbeeld in artikel 9 lid 1, 2 en 3, artikel 14 lid 2 en artikel 15 lid 3. Energie-Nederland stelt voor om in de Nota van Toelichting toe te voegen dat hiermee bedoeld wordt dat er op basis van de risicoanalyse door de entiteit zelf kan bepalen hoe frequent dit dan daadwerkelijk is.
2. Strikte logging en monitoring eisen kunnen conflicteren met privacywetgeving: Artikel 8 verplicht bedrijven om alle security-gerelateerde activiteiten te loggen, zonder expliciete uitzondering voor gevoelige persoonsgegevens. Harmoniseer logging-eisen met de AVG en zorg voor richtlijnen over data-minimalisatie en bewaartermijnen.
3. Artikel 9 verplicht een uniform bedrijfscontinuïteits- en crisisbeheerplan, terwijl OT-systemen in de energiebranche andere herstelmechanismen vereisen dan IT-systemen. Voeg een (sectorale) uitzonderingsmogelijkheid toe voor OT-systemen en implementeer alternatieve continuïteitsstrategieën.
4. Artikel 10 Cbb verplicht bedrijven om contractuele afspraken te maken met leveranciers over cybersecurity, terwijl internationale

leveranciers (zoals Microsoft, AWS) vaak hun eigen securitystandaarden hanteren. Het opleggen van afspraken aan dit soort leveranciers is vaak niet uitvoerbaar. In dit geval zijn de meeste bedrijven overgeleverd aan de voorwaarden die deze grote bedrijven hanteren. Hierin is geen maatwerk mogelijk.

5. Artikel 10, lid 2 schrijft voor dat de entiteit waar mogelijk schriftelijke afspraken maakt met haar rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten en borgt dat deze afspraken worden nagekomen. In laatste zin wordt toegevoegd: “De entiteit houdt de afspraken actueel”. De laatste zin is irrelevant, want afspraken zijn geldig gedurende looptijd van een contract.
6. Artikel 12, 13, 14 bevatten de formulering ‘…binnen de entiteit werkzame personen ….’ Of ‘…binnen de entiteit verantwoordelijk zijn…’. Deze formulering maakt het in organisaties met een internationale groepsstructuur ingewikkeld en inefficiënt, indien voor deze rollen/werkzaamheden gebruik wordt gemaakt van personen binnen de groep, maar buiten de specifieke entiteit. Suggestie: pas aan naar ‘binnen of namens de entiteit…’
7. In artikel 12 gaat het woord “opleiding” te ver. Dit suggereert een langdurig traject bij een gecertificeerde instelling. We stellen voor hier in plaats van “opleiding”, “cursus” of “training” te gebruiken.
8. Bij artikel 14 wordt in de memorie van toelichting gesproken over een screening voor personeel. Hoe ver deze screening gaat hangt zou af moeten hangen van het risicobeleid dat een bedrijf hanteert. Zolang duidelijk vastgelegd is waarom bepaalde keuzes gemaakt worden moet dit voldoende zijn. Kan dat in de Nota van Toelichting worden verduidelijkt?
9. Artikel 16 beveiligingsaspecten tav beheer van assets: bevat de formulering ‘…beheer en de werking van netwerk- en informatiesystemen…’. Met name ‘de werking’ voegt hierin, omdat we het hebben over beleid, een onnodige vaagheid toe en lijkt niet echt relevant. Wat wordt hiermee bedoeld? Suggestie:ver wijder ‘werking’ in deze zin of vervang door bijvoorbeeld ‘gebruik’, ‘operationeel houden’ al naar gelang wat hier bedoeld wordt?

10. In artikel 8.2 van de Cyberbeveiligingswet wordt gesproken over bijna-incidenten. Kan de definitie van bijna-incidenten in het Cbb of de sectorale MR met de nadere uitwerking van de drempelwaarden worden opgenomen?

Opleidingsplicht

11. In artikel 21 wordt het doel van de training voor bestuurders beschreven. Er zijn veel bedrijven die een heel aantal activiteiten hebben die, in verschillende entiteiten, onder zowel Cbe als Bwke vallen. Leden van het bestuur van deze entiteiten kunnen ver van de dagelijkse operatie afstaan. De opleidingsplicht moet niet het doel voorbij schieten. Bestuurders hoeven niet tot in detail uit te kunnen leggen hoe een informatiesysteem werkt of welke gevolgen bepaalde risico's hierop kunnen hebben. Ze moeten zich vooral bewust zijn op welke manier risico's binnen hun bedrijf beoordeeld en gemanaged worden. Energie-Nederland stelt voor om dit te verhelderen in de wetstekst.
    a. Voorbeeld: Artikel 21 eisen aan de training: lid 2 is te uitgebreid en omvat technische onderwerpen die niet nodig zijn voor de doelgroep (raad van bestuur niveau), zoals beheer van informatiesystemen, cryptografie en multi-factor authenticatie. Suggestie: voeg de niet-technische onderwerpen toe aan lid 1 en laat lid 2 achterwege.
12. Het Cbb stelt training door een 'onafhankelijke' trainer verplicht. Daarmee wordt de indruk gewekt dat deze afkomstig moet zijn van buiten het bedrijf, of intern onafhankelijk moet zijn van de security-afdeling, de afdeling die het cybersecuritybeleid uitvoert (de CISO). Dit is problematisch om de volgende redenen:
    a. CISO's hebben specifieke kennis van het bedrijf die onmisbaar is tijdens een training. Externe partijen kunnen slechts algemene kennis delen. Daarmee biedt een externe trainer alleen de schijn van meer veiligheid. Buiten de CISO's hebben andere delen van de organisatie de benodigde kennis doorgaans niet.
    b. Tegelijk moeten wel kosten gemaakt worden voor inhuur van deze externe trainers. Dat kan gaan om duizenden euro's per bedrijf, afhankelijk van de grootte van het

bedrijf. Dat zijn vermijdbare kosten als de kennis al in huis is.

c. Daarbij komen nog op overheidsniveau de kosten van het inrichten van een controle van de kwaliteit van de externe trainers. Dit kan prima vervangen worden door een controle door de RDI of de kwaliteit van de training door de CISO's van voldoende niveau was.

De beste oplossing zou zijn om ook training door een gekwalificeerde interne CISO toe te staan als trainer. De huidige opzet is te beperkend.

Meldplicht

13. In artikel 24, lid 2, wordt gesproken over een evaluatie van de doeltreffendheid van de in artikel 24 eerste lid vastgestelde criteria. Energie-Nederland wordt graag betrokken bij de evaluatie van de criteria. Dit heeft binnen de NIS1/Wbni ook al de nodige discussie opgeleverd die voorkomen kan worden door de sectoren in een vroeg stadium aan te haken.
14. Energie-Nederland heeft een sterke voorkeur voor één gemeenschappelijk meldpunt waar zowel meldingen onder de Cbw als de Wwke kunnen worden gedaan.
15. Onduidelijk is wie er een melding doet van een significant incident wanneer dit plaatsvindt bij/door een rechtstreekse leverancier of dienstverlener die zelf ook essentiële entiteit of belangrijke entiteit is. Dit kan strikter worden geformuleerd (zie ook ministeriele regeling zorgplicht, artikel 6): *“Alle betrokken essentiële entiteiten in de directe keten doen een melding van een significant incident bij CSIRT / Toezichthouder”*. Dit levert wel het risico van dubbele meldingen op, maar voorkomt dat meldingen niet gedaan worden door onduidelijkheden of miscommunicatie.
16. Art 25 lid 2(b) van de Cbw - Betreft het hier het aanrichten van schade aan onze dienstverlenging waar andere entiteiten verderop in de keten last van hebben, of directe schade aan

andere identiteiten? Voor een bedrijf is de schade verderop in de keten lastig of niet te bepalen. Hiervoor moeten realistische drempelwaarden gehanteerd worden op basis van informatie waar bedrijven ook daadwerkelijk over kunnen beschikken. Dit moet in de MR waarin de drempelwaarden voor de meldplicht worden besproken verduidelijkt worden. Energie-Nederland denkt hierover graag mee bij het opstellen van deze MR.

17. Art 26 lid 2b - Wat wordt hier bedoelt met 'grensoverschrijdend'? Energie-Nederland stelt voor hier ‘landsgrensoverschrijdend’ te gebruiken.
18. Artikel 28 verstrekking overige informatie: Lid 3 onderdeel b geeft aan dat de entiteit moet registreren ‘haar domeinnamen’. Worden hier de hoofddomeinnamen (zoals ook gebruikt voor email verkeer) bedoeld, of alle domeinnamen waarvan de entiteit eigenaar is? In het laatste geval ontstaat een enorme schaduw administratie van domeinnamen en dit is zeer inefficiënt. In de DNS gegevens zijn domein namen al te herleiden tot juridische entiteiten indien nodig in geval van serieuze incidenten.
19. Art 30 lid 1&2 – Nog onduidelijk is of de entiteit zelf mag bepalen *hoe* ontvangers van diensten worden geïnformeerd in geval van een significant incident. Energie-Nederland heeft een sterke voorkeur om bedrijven zelf de communicatie met directe afnemers te laten verzorgen. Dit om onnodige paniek te voorkomen.
20. Artikel 30 lid 2 - Moeten we ook afnemers van diensten onverwijld inlichten die mogelijkerwijs zijn geraakt? Of last krijgen? Hoe wordt dit bepaald? Ook hierover gaan we graag in gesprek voor het opstellen van een MR waarin de drempelwaarden voor de meldplicht worden besproken verduidelijkt worden.

Ministeriële Regeling (nadere uitwerking van de zorgplichtmaatregelen)

Algemene opmerkingen

1. In meerdere artikelen van de Ministeriële Regeling wordt voorgeschreven dat bepaalde activiteiten in procedures moeten worden vastgelegd. De essentie is dat de activiteiten worden gedocumenteerd en aantoonbaar worden toegepast. Het soort document (proces, instructie, procedure, etc.) waarin dit wordt vastgelegd is niet relevant.
2. Energie-Nederland benadrukt graag dat de nadruk in de MR meer op praktische toepassing moet liggen dan op de schriftelijke vastlegging van bijvoorbeeld risico's en maatregelen. Hierbij moet vooral rekening worden gehouden met het werkbaar houden van de maatregelen. Het is in het kader van de zorgplicht vooral belangrijk dat bedrijven hun eigen risicomodellen kunnen hanteren die op basis van de bedrijfsspecifieke kenmerken het meest geschikt zijn.
3. In de MR staat het begrip 'kritieke entiteiten' genoemd.[3] Dit begrip komt niet voor in de Cbw of het Cbb. Kan er een definitie worden opgenomen waaruit blijkt wat bedoeld wordt met het begrip kritieke entiteit?

Opmerkingen per artikel

4. Artikel 3 en 4: de MR geeft een zeer gedetailleerde uitwerking van de zorgplicht, maar mist flexibiliteit, vooral voor energiebedrijven waar al cybersecurity frameworks gehanteerd worden. Dit zorgt mogelijk voor onnodige overlap en extra administratieve lasten. Artikel 3 en 4 leggen strikte eisen op voor het beleid en risicomanagement, maar er staat niet expliciet dat bestaande frameworks als basis kunnen dienen. Dit kan dubbel werk veroorzaken. Geef ruimte om compliant te zijn door aan te geven dat er ook gebruikt kan worden gemaakt van internationale standaarden.

[3] Pagina 1 concept MR: "Dit concept geldt voor essentiële, belangrijke en kritieke entiteiten in de volgende sectoren en subsectoren."

5. Artikel 5: Dit artikel kan worden geïnterpreteerd alsof er een uniform back-up beleid, inclusief tests, vereist wordt. OT-systemen in de energiesector werken met real-time data en hebben andere herstelmechanismen dan IT-systemen. Om dit op te lossen zou er een uitzondering toegevoegd moeten worden voor OT-systemen, waarbij alternatieve continuïteitsmaatregelen volstaan.
6. Artikel 7: Verplichting tot segmentatie en patching kan conflicteren met operationele realiteit: Artikel 7 verplicht segmentatie en snelle toepassing van patches, maar in een productieomgeving is real-time patching niet altijd mogelijk vanwege operationele risico's. Geef bedrijven de ruimte om de invulling van maatregelen als patching, MFA (multi-factor authenticatie) en back-ups te baseren op risico en impact in plaats van een strikte verplichting.
7. Artikel 9: Dit artikel benoemt het gebruik van MFA en strikte toegangscontrole, maar veel OT- en ook IT-systemen ondersteunen dit niet of kunnen hierdoor uitvallen. Naast dat dit in verhouding moet staan tot de risico's (zie lid 2) moet ook rekening gehouden worden met de mogelijkheden bij legacy systemen.

Over Vereniging Energie-Nederland

Vereniging Energie-Nederland (hierna Energie-Nederland) is de brancheverenigingvoor alle partijen die betrokken zijn bij het produceren, leveren en verhandelen van stroom, gas en warmte. Wij vertegenwoordigen vrijwel de volledige energiemarkt in Nederland. Onze ruim 80 leden – waaronder vele nieuwkomers – zijn actief in hernieuwbare en niet-hernieuwbare energie. Zij bieden diverse diensten aan en komen voortdurend met innovatieve en duurzame initiatieven.

Wij maken ons in Den Haag en Brussel sterk voor de belangen van onze leden op elk gebied van energievoorziening. Van het opwekken en verhandelen van energie tot aan de levering ervan aan consumenten en bedrijven. Daarnaast ondersteunen we de ontwikkeling van nieuwe dienstverlening van onze leden. Denk bijvoorbeeld aan hulp bij het verduurzamen van gebouwen.
Als brancheverenigingdragen wij bij aan een duurzame toekomst. Wij blijven ons inzetten voor een energiemarkt waarin duurzaamheid, betrouwbaarheid, leveringszekerheid en betaalbaarheid centraal staan.

Het is onze ambitie om een halvering van de CO2-uitstoot te bereiken in 2030. In 2050 moet de energievoorziening 100% CO2-neutraal zijn. Met het oog op de geplande uitrol van hernieuwbare energiebronnen, is Nederland op weg om koploper te worden in Europa.

Wij streven naar een optimale markt met laagdrempelige toe- en uittreding. Met ruimte voor nieuwe en innovatieve spelers en bedrijven. Energiebedrijven moeten voldoende prikkels krijgen om te investeren. Omdat onze energiemarkt Europees is, streven wij naar oplossingen en beleid op Europees niveau. Dit zorgt voor een gelijk speelveld om collectief en efficiënt te kunnen verduurzamen.