STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 22078
15 juli
2026

Regeling van de Minister van Klimaat en Groene Groei van 27 juni 2026, nr. WJZ/103641412, houdende nadere regels over cyberbeveiliging en de weerbaarheid van kritieke entiteiten in de energiesector (Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector) [KetenID WGK 28195]

De Minister van Klimaat en Groene Groei,

Gelet op artikel 7, eerste lid, van de Wet weerbaarheid kritieke entiteiten, artikel 15, tweede lid, van het Besluit weerbaarheid kritieke entiteiten en de artikelen 19, 23, eerste lid, en 28 van het Cyberbeveiligingsbesluit;

Gezien het overleg met de Minister van Justitie en Veiligheid;

Besluit:

HOOFDSTUK 1. WET WEERBAARHEID KRITIEKE ENTITEITEN: CRITERIA AANZIENLIJK VERSTOREND EFFECT

Paragraaf 1.1. Algemene bepalingen

Artikel 1. begripsbepalingen

In dit hoofdstuk wordt verstaan onder:
besluit: Besluit weerbaarheid kritieke entiteiten;
COVA: COVA als bedoeld in artikel 1 van de Wet voorraadvorming aardolieproducten 2012;
day-aheadkoppeling: eenvormige day-aheadkoppeling als bedoeld in artikel 2, punt 26, van verordening (EU) 2015/1222 van de Commissie van 24 juli 2015 tot vaststelling van richtsnoeren betreffende capaciteitstoewijzing en congestiebeheer (PbEU 2021, L 62);
distributiesysteembeheerder voor elektriciteit: distributiesysteembeheerder voor elektriciteit als bedoeld in artikel 1.1 van de Energiewet;
distributiesysteembeheerder voor gas: distributiesysteembeheerder voor gas als bedoeld in artikel 1.1 van de Energiewet;
eindafnemer: eindafnemer als bedoeld in artikel 1.1 van de Energiewet;
elektriciteitsmarktbeheerder: benoemde elektriciteitsmarktbeheerder als bedoeld in artikel 2, punt 8, van verordening (EU) 2019/943 van het Europees parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (herschikking) (PbEU 2019, L 158);
gas: gas als bedoeld in artikel 1.1 van de Energiewet;
gasopslagbeheerder: gasopslagbeheerder als bedoeld in artikel 1.1 van de Energiewet;
gasopslagsysteem: gasopslagsysteem als bedoeld in artikel 1.1 van de Energiewet;
gasproductienet: gasproductienet als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteembeheerder voor elektriciteit: interconnectorsysteembeheerder voor elektriciteit als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteembeheerder voor gas: interconnectorsysteembeheerder voor gas als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteem voor gas: interconnectorsysteem voor gas als bedoeld in artikel 1.1 van de Energiewet;
intradaykoppeling: eenvormige intradaykoppeling als bedoeld in artikel 2, punt 27, van verordening (EU) 2015/1222 van de Commissie van 24 juli 2015 tot vaststelling van richtsnoeren betreffende capaciteitstoewijzing en congestiebeheer (PbEU 2021, L 62);
invoeder: invoeder als bedoeld in artikel 1.1 van de Energiewet;
LNG-beheerder: LNG-beheerder als bedoeld in artikel 1.1 van de Energiewet;
LNG-systeem: LNG-systeem als bedoeld in artikel 1.1 van de Energiewet;
marktdeelnemer: marktdeelnemer als bedoeld in artikel 1.1 van de Energiewet;
opslag van olie en olieproducten: opslag van aardolie en oliehoudende producten in een daarvoor bestemde voorziening;
transmissiesysteem voor gas: transmissiesysteem voor gas als bedoeld in artikel 1.1 van de Energiewet;

transmissiesysteembeheerder voor gas: transmissiesysteembeheerder voor gas als bedoeld in artikel 1.1 van de Energiewet;
wet: Wet weerbaarheid kritieke entiteiten;
wettelijke olievoorraad: wettelijke voorraad als bedoeld in artikel 1 van de Wet voorraadvorming aardolieproducten 2012.

Artikel 2. aanwijzing categorieën van entiteiten

De volgende categorieën van entiteiten zijn aangewezen als bedoeld in artikel 7, eerste lid, van de wet:
a. interconnectorsysteembeheerder voor elektriciteit, behorende tot de subsector elektrictiteit en de sector energie;
b. interconnectorsysteembeheerder voor gas, behorende tot de subsector gas en de sector energie.

Artikel 3. reikwijdte

Dit hoofdstuk is van toepassing op:
a. kritieke entiteiten als bedoeld in artikel 6 van de wet die binnen de sector energie behoren tot de subsectoren:
   1°. elektriciteit;
   2°. gas;
   3°. olie;
b. kritieke entiteiten die onderdeel zijn van een aangewezen categorie als bedoeld in artikel 2.

Paragraaf 1.2. Criteria aanzienlijke verstoring voor de subsector elektriciteit

Artikel 4. transmissiesysteembeheerder, interconnectorsysteembeheerder en distributiesysteembeheerder voor elektriciteit

Voor een kritieke entiteit die transmissiesysteembeheerder voor elektriciteit, distributiesysteembeheerder voor elektriciteit of interconnectorsysteembeheerder voor elektriciteit is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de transmissie of distributie van elektriciteit van ten minste 100 MW geaggregeerd vermogen.

Artikel 5. elektriciteitsproducent en marktdeelnemer

Voor een kritieke entiteit die elektriciteitsproducent of marktdeelnemer is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor het beschikbaar geaggregeerd vermogen van ten minste 100 MW.

Artikel 6. elektriciteitsmarktbeheerder

Voor een kritieke entiteit die elektriciteitsmarktbeheerder is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor het tijdig kunnen plaatsvinden van de day-ahead- of intradaykoppeling of aantasting van de integriteit daarvan bij een elektriciteitsmarktbeheerder.

Paragraaf 1.3. Criteria aanzienlijke verstoring voor de subsector gas

Artikel 7. distributiesysteembeheerder voor gas

Voor een kritieke entiteit die distributiesysteembeheerder voor gas is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de distributie van gas voor ten minste 20.000 eindafnemers.

Artikel 8. transmissiesysteembeheerder voor gas

Voor een kritieke entiteit die transmissiesysteembeheerder voor gas is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de normale werking van het transmissiesysteem voor gas.

Artikel 9. interconnectorsysteembeheerder voor gas

Voor een kritieke entiteit die interconnectorsysteembeheerder voor gas is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de normale werking van het interconnectorsysteem voor gas.

Artikel 10. LNG-beheerder

Voor een kritieke entiteit die LNG-beheerder is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de invoeding van gas van ten minste 150 GWh per dag in het transmissiesysteem voor gas vanuit een LNG-systeem.

Artikel 11. gasopslagbeheerder

Voor een kritieke entiteit die gasopslagbeheerder is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de injectie, productie en opslag van gas, waaronder de onttrekking uit en invoeding in het transmissiesysteem voor gas, van ten minste 150 GWh per dag.

Artikel 12. gasopslagbeheerder van seizoensopslagen

Voor een kritieke entiteit die gasopslagbeheerder van seizoensopslagen is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de normale werking van het gasopslagsysteem, inclusief de injectie, productie en opslag van gas.

Artikel 13. aardgasbedrijf dat een gasproductienet beheert

Voor een kritieke entiteit die beheerder van een gasproductienet is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de normale werking van de productie, behandeling of invoeding van gas in het transmissiesysteem voor gas.

Paragraaf 1.4. Criteria aanzienlijke verstoring voor de subsector olie

Artikel 14. exploitant van oliepijpleidingen

Voor een kritieke entiteit die exploitant van oliepijpleidingen is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor het transport van olie of olieproducten via leidingen, dat voor ten minste 24 uur verstoord is.

Artikel 15. exploitant van de voorziening voor de raffinage en behandeling van olie

Voor een kritieke entiteit die exploitant is van de voorziening voor de raffinage en behandeling van olie, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de raffinage en behandeling van olie, die voor ten minste 72 uur verstoord is, met gevolgen voor de levering van ten minste 250.000 vaten per dag.

Artikel 16. exploitant van de voorziening voor de opslag van olie of olieproducten

Voor een kritieke entiteit die exploitant is van de voorziening voor de opslag van olie of olieproducten, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring gevolgen heeft of kan hebben voor de opslag van olie of olieproducten, die voor ten minste 72 uur verstoord is, met gevolgen voor de levering van ten minste 100.000 m^3 olie of olieproducten.

Artikel 17. exploitant van de voorziening voor de opslag van olie of olieproducten die voorraadplichtig is

Voor een kritieke entiteit die exploitant is van een voorziening voor de opslag van olie of olieproducten en voorraadplichtig is, is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien de verstoring leidt of kan leiden tot het niet beschikbaar

zijn van de wettelijke olievoorraad voor een periode van ten minste 72 uur.

Artikel 18. COVA

Voor COVA is een verstoring aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, tweede lid, van het besluit, indien:
a. de verstoring leidt of kan leiden tot het niet beschikbaar zijn van de wettelijke olievoorraden voor een periode van ten minste 72 uur; of
b. de verstoring andere gevolgen heeft of kan hebben voor het beheer van de wettelijke olievoorraden.

Paragraaf 1.5. Geplande onderbreking

Artikel 19. geplande onderbreking

In afwijking van de artikelen 3 tot en met 18 is een verstoring niet aanzienlijk, indien de verstoring het gevolg is van een voorziene of geplande onderbreking, opschorting of beëindiging van een door de kritieke entiteit verleende essentiële dienst.

HOOFDSTUK 2. CYBERBEVEILIGINGSWET: CRITERIA ERNSTIGE OPERATIONELE VERSTORING, NADERE REGELS ZORGPLICHT EN AANWIJZING AUTORITEITEN

Paragraaf 2.1. Algemene bepalingen

Artikel 20. begripsbepalingen

In dit hoofdstuk wordt verstaan onder:
besluit: Cyberbeveiligingsbesluit;
COVA: COVA als bedoeld in artikel 1 van de Wet voorraadvorming aardolieproducten 2012;
day-aheadkoppeling: eenvormige day-aheadkoppeling als bedoeld in artikel 2, punt 26, van verordening (EU) 2015/1222 van de Commissie van 24 juli 2015 tot vaststelling van richtsnoeren betreffende capaciteitstoewijzing en congestiebeheer (PbEU 2021, L 62);
distributiesysteem voor gas: distributiesysteem voor gas als bedoeld in artikel 1.1 van de Energiewet;
eindafnemer: eindafnemer als bedoeld in artikel 1.1 van de Energiewet;
elektriciteitsbedrijf: elektriciteitsbedrijf als bedoeld in artikel 2,onderdeel 57, van Richtlijn (EU) 2019/9441 van het Europees parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (herschikking) (PbEU 2019, L 158);
elektriciteitsmarktbeheerder: benoemde elektriciteitsmarktbeheerder als bedoeld in artikel 2, punt 8, van verordening (EU) 2019/943 van het Europees parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (herschikking) (PbEU 2019, L 158);
exploitant van een laadpunt: exploitant van een laadpunt als bedoeld in artikel 2, punt 39, van Verordening (EU) 2023/1804 van het Europees parlement en de Raad van 13 september 2023 betreffende de uitrol van infrastructuur voor alternatieve brandstoffen en tot intrekking van Richtlijn 2014/94/EU;
gas: gas als bedoeld in artikel 1.1 van de Energiewet;
gasopslagbeheerder: gasopslagbeheerder als bedoeld in artikel 1.1 van de Energiewet;
gasopslagsysteem: gasopslagsysteem als bedoeld in artikel 1.1 van de Energiewet;
gasproductienet: gasproductienet als bedoeld in artikel 1.1 van de Energiewet;
invoeder: invoeder als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteembeheerder voor elektriciteit: interconnectorsysteembeheerder voor elektriciteit als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteembeheerder voor gas: interconnectorsysteembeheerder voor gas als bedoeld in artikel 1.1 van de Energiewet;
interconnectorsysteem voor gas: interconnectorsysteem voor gas als bedoeld in artikel 1.1 van de Energiewet;
intradaykoppeling: eenvormige intradaykoppeling als bedoeld in artikel 2, punt 27, van verordening (EU) 2015/1222 van de Commissie van 24 juli 2015 tot vaststelling van richtsnoeren betreffende capaciteitstoewijzing en congestiebeheer (PbEU 2021, L 62);
leverancier: leverancier als bedoeld in artikel 1.1 van de Energiewet;LNG-beheerder: LNG-beheerder als bedoeld in artikel 1.1 van de Energiewet;
LNG-systeem: LNG-systeem als bedoeld in artikel 1.1 van de Energiewet;
marktdeelnemer: marktdeelnemer als bedoeld in artikel 1.1 van de Energiewet;
opslag van olie en olieproducten: opslag van aardolie en oliehoudende producten in een daarvoor bestemde voorziening;

transmissiesysteem voor gas: transmissiesysteem voor gas als bedoeld in artikel 1.1 van de Energiewet;
warmte: warmte als bedoeld in artikel 1, eerste lid, van de Warmtewet;
wet: Cyberbeveiligingswet;
wettelijke olievoorraden: wettelijke voorraad als bedoeld in artikel 1 van de Wet voorraadvorming aardolieproducten 2012.

Artikel 21. reikwijdte

Dit hoofdstuk is van toepassing op essentiële entiteiten en belangrijke entiteiten die binnen de sector energie behoren tot de subsectoren:
a. elektriciteit;
b. stadsverwarming en stadskoeling;
c. aardolie;
d. aardgas;
e. waterstof.

Paragraaf 2.2. Criteria ernstige operationele verstoring voor de subsector elektriciteit

Artikel 22. transmissiesysteembeheerder, interconnectorsysteembeheerder en distributiesysteembeheerder voor elektriciteit

Voor een essentiële entiteit en een belangrijke entiteit die transmissiesysteembeheerder voor elektriciteit, distributiesysteembeheerder voor elektriciteit of interconnectorsysteembeheerder voor elektriciteit is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet indien het incident gevolgen heeft of kan hebben voor de transmissie of distributie van elektriciteit van ten minste 100 MW geaggregeerd vermogen.

Artikel 23. elektriciteitsproducent en marktdeelnemer

Voor een essentiële entiteit en een belangrijke entiteit die elektriciteitsproducent of marktdeelnemer is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet indien het incident gevolgen heeft of kan hebben voor het beschikbaar geaggregeerd vermogen van ten minste 100 MW.

Artikel 24. exploitant van een laadpunt

Voor een essentiële entiteit en een belangrijke entiteit die een exploitant van een laadpunt is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet indien het incident gevolgen heeft of kan hebben voor het beschikbaar geaggregeerd vermogen van ten minste 100 MW.

Artikel 25. elektriciteitsmarktbeheerder

Voor een essentiële entiteit en een belangrijke entiteit die elektriciteitsmarktbeheerder is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet indien het incident gevolgen heeft of kan hebben voor het tijdig kunnen plaatsvinden van de day-ahead- of intradaykoppeling of aantasting van de integriteit daarvan bij een elektriciteitsmarktbeheerder.

Artikel 26. leverancier van elektriciteit

Voor een essentiële entiteit en een belangrijke entiteit die leverancier is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet indien het incident gevolgen heeft of kan hebben voor de uitvoering van de contractuele kernverplichtingen voor ten minste 20.000 eindafnemers van elektriciteit.

Paragraaf 2.3 Criteria ernstige operationele verstoring voor de subsector aardgas

Artikel 27. distributiesysteembeheerder voor gas

Voor een essentiële entiteit en belangrijke entiteit die distributiesysteembeheerder voor gas is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de distributie van gas voor ten minste 20.000 eindafnemers.

Artikel 28. transmissiesysteembeheerder voor gas

Voor een essentiële entiteit en een belangrijke entiteit die transmissiesysteembeheerder voor gas is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de normale werking van het transmissiesysteem voor gas.

Artikel 29. interconnectorsysteembeheerder voor gas

Voor een essentiële entiteit en een belangrijke entiteit die interconnectorsysteembeheerder voor gas is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de normale werking van het interconnectorsysteem voor gas.

Artikel 30. LNG-beheerder

Voor een essentiële entiteit en een belangrijke entiteit die LNG-beheerder is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan gevolgen hebben voor de invoeding van gas van ten minste 150 GWh per dag in het transmissiesysteem voor gas vanuit een LNG-systeem.

Artikel 31. gasopslagbeheerder

Voor een essentiële entiteit en een belangrijke entiteit die gasopslagbeheerder is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de injectie, productie en opslag van gas, waaronder de onttrekking uit en invoeding in het transmissiesysteem voor gas, van ten minste 150 GWh per dag.

Artikel 32. gasopslagbeheerder van seizoensopslagen

Voor een essentiële entiteit en een belangrijke entiteit die gasopslagbeheerder van seizoensopslagen is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de normale werking van het gasopslagsysteem, inclusief de injectie, productie en opslag van gas.

Artikel 33. aardgasbedrijf dat een gasproductienet beheert

Voor een essentiële entiteit en een belangrijke entiteit die beheerder van het gasproductienet is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de normale werking van de productie, behandeling of invoeding van gas in het transmissiesysteem voor gas.

Artikel 34. leverancier van gas

Voor een essentiële entiteit en een belangrijke entiteit die leverancier, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de uitvoering van de contractuele kernverplichtingen voor ten minste 20.000 eindafnemers van gas.

Paragraaf 2.4. Criteria ernstige operationele verstoring voor de subsector aardolie

Artikel 35. exploitant van oliepijpleidingen

Voor een essentiële entiteit en een belangrijke entiteit die exploitant van oliepijpleidingen is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor het transport van olie of olieproducten via leidingen, dat voor ten minste 24 uur verstoord is.

Artikel 36. exploitant van een voorziening voor de raffinage en behandeling van olie

Voor een essentiële entiteit en een belangrijke entiteit die exploitant is van een voorziening voor de raffinage en behandeling van olie, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de raffinage en behandeling van olie, dat voor ten minste 72 uur verstoord is, met gevolgen voor de levering van ten minste 250.000 vaten per dag.

Artikel 37. exploitant van een voorziening voor de opslag van olie of olieproducten

Voor een essentiële entiteit en een belangrijke entiteit die exploitant is van een voorziening voor de opslag van olie of olieproducten, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident gevolgen heeft of kan hebben voor de opslag van olie of olieproducten, dat voor ten minste 72 uur verstoord is, met gevolgen voor de levering van ten minste 100.000 m^3 olie of olieproducten.

Artikel 38. exploitant van de voorziening voor de opslag van olie of olieproducten die voorraadplichtig is

Voor een essentiële entiteit en een belangrijke entiteit die exploitant is van de voorziening voor de opslag van olie of olieproducten en voorraadplichtig, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het incident tot gevolg heeft of kan hebben dat wettelijke olievoorraden voor een periode van ten minste 72 uur niet beschikbaar zijn.

Artikel 39. COVA

Voor COVA is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien:
a. het incident tot gevolg heeft of kan hebben dat wettelijke olievoorraden voor een periode van ten minste 72 uur niet beschikbaar zijn;
b. het incident gevolgen heeft of kan hebben voor het beheer van de wettelijke olievoorraden.

Paragraaf 2.5. Criteria ernstige operationele verstoring voor de subsector stadsverwarming en stadskoeling

Artikel 40. exploitant van stadsverwarming of stadskoeling

Voor een essentiële entiteiten en een belangrijke entiteit die exploitant van stadsverwarming of stadskoeling is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien het voldoet aan één of meer van de volgende criteria:
a. het incident gevolgen heeft of kan hebben voor de productie van warmte of koude van ten minste 20 MW vermogen;
b. het incident gevolgen heeft of kan hebben voor de levering van warmte of koude voor ten minste 20.000 afnemers.

Paragraaf 2.6. Geplande onderbreking

Artikel 41. geplande onderbreking

In afwijking van de artikelen 22 tot en met 40 is een operationele verstoring niet ernstig, indien de verstoring het gevolg is van een voorziene of geplande onderbreking, opschorting of beëindiging van een door de verleende essentiële of belangrijke entiteit verleende essentiële of belangrijke dienst.

Paragraaf 2.7 Nadere regels zorgplicht

Artikel 42. beleid over beveiliging van netwerk- en informatiesystemen

Ter uitvoering van artikel 6 van het besluit legt de essentiële entiteit of de belangrijke entiteit als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het besluit, vast:
a. welke maatregelen voor het beheer van cyberbeveiligingsrisico's, met inbegrip van processen en controles, moeten worden gemonitord, gemeten, geanalyseerd en geëvalueerd;
b. de methoden voor het monitoren, meten, analyseren en evalueren om valide resultaten te waarborgen;
c. wanneer de monitoring en de meting moeten worden uitgevoerd;
d. wie is belast met het monitoren en meten van de doeltreffendheid van de maatregelen voor het beheer van cyberbeveiligingsrisico's;
e. wanneer de resultaten van de monitoring en meting moeten worden geanalyseerd en geëvalueerd;
f. wie is belast met het analyseren en evalueren van deze resultaten.

Artikel 43. bedrijfscontinuïteit

1. De processen en procedures voor het maken en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens, bedoeld in artikel 9, tweede lid, van het besluit, omschrijven

van welke software en gegevens een back-up wordt gemaakt en bevatten ten aanzien van die software en gegevens:
a. hersteltijden;
b. herstelpunten;
c. waarborgen voor de volledigheid en nauwkeurigheid van back-ups;
d. waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
e. waarborgen voor herstel van software en gegevens uit back-ups;
f. bewaartermijnen.

2. Het bedrijfscontinuïteitsplan, bedoeld in artikel 9, derde lid, van het besluit, houdt rekening met de uitgevoerde beoordeling van risico's, bedoeld in artikel 7 van het besluit, en omvat in ieder geval:
a. doel en reikwijdte;
b. taken en verantwoordelijkheden;
c. belangrijkste contacten en interne en externe communicatiekanalen;
d. voorwaarden voor activering en de-activering van het bedrijfscontinuïteitsplan;
e. vereiste middelen, met inbegrip van back-ups en redundanties;
f. voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

Artikel 44. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

1. De processen en procedures, bedoeld in artikel 11, derde lid, van het besluit, hebben tevens betrekking op de processen en procedures inzake:
a. beveiligingstesten;
b. beveiligingspatchbeheer.

2. De processen en procedures inzake beveiligingspatchbeheer zorgen ervoor dat:
a. waar passend, beveiligingspatches afkomstig zijn van betrouwbare bronnen en op integriteit worden gecontroleerd;
b. waar passend, beveiligingspatches worden getest voordat zij in productiesystemen worden toegepast;
c. beveiligingspatches worden toegepast binnen een redelijke termijn nadat zij beschikbaar zijn, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen, in welk geval de essentiële entiteit of belangrijke entiteit motiveert waarom de beveiligingspatches niet of op een later moment toegepast worden en dit documenteert.

3. Ter uitvoering van artikel 21, derde lid, onderdeel e, van de wet:
a. implementeert de essentiële entiteit of belangrijke entiteit maatregelen om het gebruik van kwaadaardige en ongeoorloofde software in haar netwerk- en informatiesystemen te detecteren en te voorkomen;
b. voert de essentiële entiteit of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit op haar netwerk- en informatiesystemen en legt zij de resultaten van deze scans vast;
c. evalueert de essentiële entiteit of belangrijke entiteit structureel haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft ten aanzien van haar netwerk- en informatiesystemen, voor zover artikel 17 van het besluit daar niet reeds toe verplicht;
d. verhelpt de essentiële entiteit of belangrijke entiteit onverwijld kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen, of motiveert waarom de kwetsbaarheid niet of op een later moment verholpen wordt en documenteert dit.

4. Ter uitvoering van artikel 21, derde lid, onderdeel g, van de wet segmenteert de essentiële entiteit of belangrijke entiteit:
a. haar netwerk- en informatiesystemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het besluit bedoelde risicoanalyse;
b. waar passend, haar netwerk- en informatiesystemen van de netwerk- en informatiesystemen van derden.

Artikel 45. beveiligingsaspecten ten aanzien van toegangsbeleid

1. Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, omvat het beleid over bevoorrechte accounts en systeembeheeraccounts.

2. Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, zorgt ervoor dat:
a. sterke identificatie-, authenticatie-, en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;

b. voorrechten op het gebied van systeembeheer zoveel mogelijk geïndividualiseerd en beperkt worden toegekend;
c. voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt.

Paragraaf 2.8. Aanwijzing autoriteiten

Artikel 46. aanwijzing autoriteiten

De volgende autoriteiten zijn aangewezen als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet en artikel 28 van het besluit:
a. de Autoriteit Nucleaire Veiligheid en Stralingsbescherming, genoemd in artikel 3, eerste lid, van de Kernenergiewet, voor de taken uit hoofde van die wet;
b. de Minister van Klimaat en Groene Groei, voor de taken uit hoofde van de Energiewet en de Mijnbouwwet;
c. de Autoriteit Consument en Markt, genoemd in artikel 2, eerste lid, van de Instellingswet Autoriteit Consument en Markt, voor de taken uit hoofde van de Energiewet en de Warmtewet.

HOOFDSTUK 3. SLOTBEPALINGEN

Artikel 47. inwerkingtreding

Indien het bij koninklijke boodschap van 2 juni 2025 ingediende voorstel van wet houdende regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten) (Kamerstukken 36 765) tot wet is of wordt verheven en die wet in werking treedt, treedt deze regeling op hetzelfde tijdstip in werking.

Artikel 48. citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

's-Gravenhage, 27 juni 2026

De Minister van Klimaat en Groene Groei,
S. van Veldhoven-van der Meer

TOELICHTING

I. Algemeen

1. Inleiding

Deze ministeriële regeling is van toepassing op entiteiten in de energiesector die binnen het toepassingsbereik vallen van de Wet weerbaarheid kritieke entiteiten (hierna ook: Wwke) of de Cyberbeveiligingswet. Deze regeling is opgedeeld in twee hoofdstukken: een voor de Wwke en een voor de Cyberbeveiligingswet. Ook deze toelichting bevat aparte hoofdstukken voor de regels onder de Wwke (hoofdstuk 3) en de regels onder de Cyberbeveiligingswet (hoofdstuk 4).

2. Hoofdlijnen van de ministeriële regeling

Deze ministeriële regeling heeft als doel om de digitale en fysieke weerbaarheid van kritieke, essentiële en belangrijke entiteiten binnen de energiesector te versterken en concretiseert onder andere de zorg- en meldplicht om duidelijkheid en rechtszekerheid te bieden aan deze entiteiten.
Deze regeling bevat criteria voor de meldplicht van significante incidenten als bedoeld in artikel 25, tweede lid van de Cyberbeveiligingswet en betreft de implementatie van artikel 23, derde lid, van richtlijn (EU) 2022/2555 over cyberbeveiliging (NIS2-richtlijn). Tevens bevat deze regeling criteria voor de meldplicht van incidenten die de essentiële dienst aanzienlijk verstoort of kan verstoren als bedoeld in artikel 17 van de Wwke en betreft de implementatie van artikel 15 van richtlijn (EU) 2022/2557 over de weerbaarheid van kritieke entiteiten (CER-richtlijn).
De terminologie en reikwijdte van de meldplicht verschillen tussen de Cyberbeveiligingswet en Wwke. Voor het overzicht is daarom voor een separate uitwerking en toelichting van de meldplicht gekozen. Daarbij geldt dat de criteria grotendeels gelijkluidend zijn vormgegeven. Dit bevordert de uitvoerbaarheid voor entiteiten die onder beide wetten vallen en de uitvoerbaarheid en handhaafbaarheid voor de toezichthouders.
Tevens bevat deze regeling nadere regels over de zorgplicht als bedoeld in artikel 19 van het Cyberbeveiligingsbesluit. De nadere invulling van de zorgplicht uit de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit concretiseert belangrijke onderdelen voor de beveiliging van netwerk- en informatiesystemen en versterkt daarmee de digitale weerbaarheid van entiteiten.
Daarnaast worden in deze regeling andere autoriteiten aangewezen waarmee samenwerking en informatie-uitwisseling gewenst is, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cyberbeveiligingswet en artikel 28 van het Cyberbeveiligingsbesluit. De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

3. Wet weerbaarheid kritieke entiteiten

3.1 Meldplicht

De meldplicht houdt in dat kritieke entiteiten incidenten die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren zo spoedig mogelijk (binnen 24 uur) moeten melden bij de bevoegde autoriteit. De criteria inzake de meldplicht beogen duidelijkheid te verschaffen over wanneer een kritieke entiteit een melding dient te maken bij het door de bevoegde autoriteit ingerichte meldpunt. Deze criteria zijn van toepassing op de subsectoren en categorieën van entiteiten binnen de energiesector waarvoor de Minister van Klimaat en Groene Groei beleidsverantwoordelijk is. Het gaat daarbij om de sectoren elektriciteit, gas, en aardolie. Voor de subsector waterstof en subsector stadsverwarming- en koeling wordt de meldplicht van de Wwke niet nader uitgewerkt, omdat vooralsnog geen kritieke entiteiten zijn voorzien in deze subsectoren.
De meldplicht heeft betrekking op elke gebeurtenis die het verlenen van een essentiële dienst aanzienlijk kan verstoren of verstoort, ook wanneer de gebeurtenis gevolgen heeft of kan hebben voor de nationale systemen die de rechtsstaat waarborgen. Onder de bewoording ‘kan verstoren of kan veroorzaken’ in de Wwke wordt interdepartementaal verstaan: ‘een reële kans dat het incident leidt tot een aanzienlijke verstoring in de (nabije) toekomst waarvan het gevaar op dat moment nog niet is geweken’. Het is aan de kritieke entiteit om in te schatten of een incident potentieel leidt tot een aanzienlijke verstoring van de essentiële dienst.

3.2 Meldtermijn en fasen van de melding

Een kritieke entiteit meldt op basis van artikel 17, eerste lid, van de Wwke, zonder onnodige vertraging een incident dat de verlening van haar essentiële dienst aanzienlijk verstoort of kan verstoren bij het door de bevoegde autoriteit ingerichte meldpunt. Hiertoe wordt één centraal meldloket onder regie van de Minister van Justitie en Veiligheid ingericht. De kritieke entiteit doet die melding binnen 24 uur nadat zij kennis heeft genomen van dat incident. De meldtermijn start zodra een kritieke entiteit kennis

heeft genomen van een incident waarvan op dat moment redelijkerwijs moet worden aangenomen dat deze heeft gezorgd of in potentie kan zorgen voor een aanzienlijke verstoring van de essentiële dienst. Indien melden binnen 24 uur operationeel niet mogelijk is, doet de kritieke entiteit de melding zo snel mogelijk nadat zij kennis heeft genomen van dat incident. De kritieke entiteit wordt geacht na het kennisnemen van een incident onderzoek te verrichten om vast te stellen of het incident de essentiële dienst aanzienlijk verstoort of kan verstoren. Daarnaast brengt de kritieke entiteit binnen een maand na de melding een gedetailleerd verslag uit. Deze regels volgen uit de Wwke en het Bwke, maar zijn voor de duidelijkheid alsnog op deze plek toegelicht.

3.3 Wettelijk kader versus praktische invulling meldplicht

De meldplicht geldt voor incidenten met een (mogelijke) aanzienlijke verstoring. Om te bepalen wat een 'aanzienlijke verstoring is', bevat de wet algemene parameters, met de mogelijkheid om bij of krachtens algemene maatregel van bestuur een of meerdere parameters nader uit te werken met criteria. De onderhavige ministeriële regeling werkt de meldplicht verder uit, door per sector en categorie van entiteit aan te geven wanneer er gemeld dient te worden. Deze criteria geven een uitwerking van de wettelijke norm en beogen entiteiten en toezichthouders duidelijkheid te bieden over wanneer in ieder geval sprake is van een meldplichtig incident.
Met het oog op de uitvoerbaarheid en regeldruk bij entiteiten is ervoor gekozen om niet alle parameters uit de wet per sector of categorie van entiteit uit te werken. Dit zou er immers toe leiden dat entiteiten voor al die criteria specifieke processen zouden moeten inrichten om tijdig te kunnen vaststellen of zij aan de precies geformuleerde criteria voldoen. Hierdoor is de meldplicht in deze regeling niet uitputtend geregeld en blijven de algemene criteria in de wet ook van toepassing. Echter zijn de in de regeling opgenomen criteria bedoeld als het primaire beoordelingskader voor entiteiten en voor het uitoefenen van toezicht en handhaving in de praktijk. Indien een situatie onder de in de regeling vastgelegde criteria valt, is er sprake is van een meldplichtig incident. Voor de parameter uit de wet die in deze regeling nader is ingevuld, is sprake van uitputtende criteria van de desbetreffende parameter, omdat de meldplichtcriteria daartoe werkelijk en zo compleet mogelijk strekken. Dit sluit niet uit dat ook in andere gevallen aan de andere parameters uit de wet kan zijn voldaan, met name in evidente gevallen waarin toepassing van uitsluitend de criteria van deze regeling zou leiden tot strijd met het doel en de strekking van de wet.

3.4 Totstandkoming criteria meldplicht

Bij het opstellen van de meldplichtcriteria in deze regeling is afstemming gezocht met diverse organisaties uit de energiesector, brancheverenigingen uit de desbetreffende sectoren en betrokken toezichthouders. Deze afstemming had als doel de regels goed te laten aansluiten op de praktijk en bestaande kaders, zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni) en sectorale regelgeving, om de uitvoerbaarheid en handhaafbaarheid te waarborgen en onnodige regeldruk te beperken.

Op grond van artikel 15, tweede lid, van het Besluit weerbaarheid kritieke entiteiten (hierna ook: Bwke) kan de Minister die het aangaat, na overleg met de Minister van Justitie en Veiligheid bij regeling criteria vaststellen voor het bepalen of sprake is van een aanzienlijke verstoring. Criteria zijn uitgewerkt die relevant zijn voorkritieke entiteiten in de energiesector en die in sommige gevallen al worden gehanteerd als melddrempel, zoals in de Wbni.
Uitgangspunt bij het uitwerken van de meldplichtcriteria is het waarborgen van de continuïteit van de levering van essentiële diensten en de leveringszekerheid van energie. Voor het uitwerken van 'aanzienlijke verstoring' is gekeken naar de gevolgen van een operationele verstoring van de eigen essentiële dienst van de betrokken kritieke entiteit en naar de gevolgen voor derden. Er is hierbij geen onderscheid gemaakt tussen een fysieke of digitale oorzaak, omdat dit niet altijd bekend is in de eerste fase van de melding (binnen 24 uur). Deze uitgangspunten hebben als gevolg dat de meldplichtcriteria voor de sectoren elektriciteit, olie en gas geharmoniseerd zijn met de meldplicht onder de Cyberbeveiligingswet. Dit komt de uitvoerbaarheid voor kritieke entiteiten ook ten goede, omdat kritieke entiteiten van rechtswege een essentiële entiteit onder de Cyberbeveiligingswet zijn.
Bij het opstellen van de meldplichtcriteria in deze regeling is onderscheid gemaakt tussen sectoren, subsectoren en categorieën van entiteiten, zoals bedoeld in artikel 17, vijfde lid van de Wwke. Generieke sectorale of subsectorale drempelwaarden doen onvoldoende recht aan de verschillende type bedrijfsprocessen van de diverse entiteiten. Daarnaast bestaan er verschillen in de mate waarin en manier waarop incidenten gevolgen hebben op de leveringszekerheid van energie evenals het kwantificeren van de melddrempels voor desbetreffende sectoren, subsectoren en categorieën van entiteiten.

Hoofdstuk 4. Cyberbeveiligingswet

4.1 Criteria meldplicht

4.1.1 Meldplicht

De meldplicht houdt in dat essentiële entiteiten en belangrijke entiteiten significante incidenten zo spoedig mogelijk melden. Dit zijn digitale beveiligingsincidenten die grote gevolgen hebben of kunnen hebben voor de (essentiële) dienstverlening van een organisatie. De meldplichtcriteria in deze regeling beogen duidelijk te verschaffen wanneer de essentiële entiteit en belangrijke entiteit een melding dient te maken van een significant incident. Deze regels zijn van toepassing op de energiesector en de daarbinnen genoemde subsectoren en soorten entiteiten waarvoor de Minister van Klimaat en Groene Groei als bevoegde autoriteit is aangewezen, bedoeld in artikel 15, eerste lid Cyberbeveiligingswet en genoemd in bijlage 2 van de Cyberbeveiligingswet. Het gaat daarbij om de volgende subsectoren: elektriciteit, aardgas, aardolie, stadsverwarming en -koeling en waterstof. Na toetsing bij entiteiten binnen de waterstofsector is ervoor gekozen om nog geen meldplichtcriteria uit te werken voor de waterstofsector. Gezien de beperktere rol van waterstof in het energiesysteem vormt het aanbod van waterstof geen strategisch risico voor de leveringszekerheid van energie. Het uitwerken van concretere meldplichtcriteria voor de waterstofsector is daarom op dit moment niet proportioneel. Aangezien deze subsector in ontwikkeling is, zal er periodiek worden geëvalueerd of uitwerking van deze criteria opportuun is. Daarnaast is er op dit moment gekozen om de algemene parameters in de Cyberbeveiligingswet voor het melden van een significant incident niet verder te concretiseren voor de sector onderzoek waarvoor de Minister van Klimaat en Groene Groei als bevoegde autoriteit is aangewezen. Dit gaat om entiteiten in de energiesector of bijbehorende subsectoren waarin de betrokken entiteit haar onderzoeksactiviteiten verricht, bedoeld in artikel 15, vierde lid van de Cyberbeveiligingswet en genoemd in bijlage 2 van de Cyberbeveiligingswet. Het is nog onvoldoende duidelijk om welke partijen het gaat, aangezien dit een nieuwe sector is die eerder niet onder de beleidsverantwoordelijkheid van de Minister van Klimaat en Groene Groei viel. Hierdoor is het op dit moment lastig in te schatten wat een concretisering zou betekenen voor de uitvoerbaarheid van deze onderzoeksorganisaties in de energiesector.

Tot slot zijn er ook geen aparte criteria uitgewerkt voor beheerders van gesloten distributiesystemen voor elektriciteit en gas. Zij vallen onder de definitie van distributiesysteembeheerder in bijlage 2 van de Cyberbeveiligingswet, maar de meldplichtcriteria voor distributiesysteembeheerders voor elektriciteit en gas in deze regeling zijn niet toepasbaar en uitvoerbaar voor beheerders van gesloten distributiesystemen. De verwachting is dat een aantal beheerders van gesloten distributiesystemen al vanwege hun andere vitale processen binnen andere sectoren onder de Cyberbeveiligingswet vallen, maar voor een deel is dit nog onbekend. Op dit moment is het daarom lastig in te schatten wie deze beheerders zijn, om hoeveel het gaat en wat de impact is op leveringszekerheid als er een incident plaatsvindt bij een beheerder van een gesloten distributiesysteem. Om deze redenen is ervoor gekozen om nog geen concretere meldplichtcriteria op te stellen voor deze beheerders. Mogelijke meldplichtcriteria kunnen eventueel op een later moment alsnog worden vastgesteld, bijvoorbeeld vanwege de invoeringstoets of de evaluatie van de Cyberbeveiligingswet. Vanwege de registratieplicht van de Cyberbeveiligingswet is dan duidelijker welke partijen in de sector onderzoek voor energie vallen en wat de identiteit en het aantal is van de beheerders van gesloten distributiesystemen die van rechtswege onder de Cyberbeveiligingswet vallen. In de tussentijd blijven de algemene parameters voor het melden van significante incidenten in artikel 25, tweede lid, leidend voor deze partijen.

De meldplicht geldt voor incidenten die als significant worden beschouwd. Een ‘incident’ is gedefinieerd in artikel 1 van de Cyberbeveiligingswet als: ‘een gebeurtenis die de beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit van netwerk- en informatiesystemen of diensten die worden aangeboden, in gevaar brengt.’ Een incident is volgens artikel 25, tweede lid, Cyberbeveiligingswet, een significant incident als het incident: 1) een ernstige operationele verstoring van de diensten voor de betrokken entiteit veroorzaakt of kan veroorzaken of 2) financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken of 3) andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. De bewoording ‘veroorzaakt of kan veroorzaken’ in de Cyberbeveiligingswet moet gelezen worden als ‘een reële kans op dat het incident leidt tot de genoemde gevolgen in de (nabije) toekomst waarvan het gevaar op dat moment nog niet is geweken’. Het is aan de essentiële entiteit en belangrijke entiteit om in te schatten of een incident potentieel leidt tot de genoemde significante gevolgen.

4.1.2 Fasen en wijze van melding

Een essentiële of belangrijke entiteit meldt een significant incident bij hun aangewezen sectorale Computer Security Incident Response Team (CSIRT) en de aangewezen toezichthoudende instantie. Hiertoe wordt één centraal meldloket onder regie van de Minister van Justitie en Veiligheid ingericht.

Op basis van artikel 26, eerste lid, van de Cyberbeveiligingswet doet de essentiële entiteit en belangrijke entiteit 'onverwijld een vroegtijdige waarschuwing, of indien dat niet mogelijk is, binnen 24 uur nadat zij kennis heeft gekregen van het significante incident.' Artikel 27, eerste lid, van de Cyberbeveiligingswet bepaalt voorts dat de entiteit onverwijld of, indien dit niet mogelijk is, binnen 72 uur nadat zij kennis heeft gekregen van het significante incident een melding daarvan doet bij het CSIRT en de bevoegde autoriteit. De meldtermijn begint dus te lopen zodra de entiteit kennis heeft gekregen van een incident waarvan op dat moment redelijkerwijs moet worden aangenomen dat dit significant is. Hierbij moet de nadruk liggen op actie om het incident te onderzoeken en om te bepalen of een incident significant is zoals bedoeld in artikel 25, tweede lid, Cyberbeveiligingswet. De regels over de verdere procedures van het melden van incidenten, zoals wanneer er moet worden gemeld en welke informatie de entiteit hierbij moet verstrekken zijn in de Cyberbeveiligingswetopgenomen (artikelen 26 tot en met 29).

4.1.3 Wettelijk kader versus praktische invulling meldplicht

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden. De wet bevat daartoe algemene parameters, met de mogelijkheid om bij of krachtens algemene maatregel van bestuur één of meerdere parameters uit te werken met criteria. De onderhavige ministeriële regeling werkt de meldplicht verder uit, door per sector, subsector en soort entiteit aan te geven wanneer er gemeld dient te worden. Deze criteria geven een uitwerking van de wettelijke norm en beogen entiteiten en toezichthouders duidelijkheid te bieden over wanneer in ieder geval sprake is van een meldplichtig incident.
Met het oog op de uitvoerbaarheid en regeldruk bij entiteiten is ervoor gekozen om niet alle parameters uit de wet per sector, subsector of soort entiteit nader uit te werken. Dit zou er immers toe leiden dat entiteiten voor al die criteria specifieke processen zouden moeten inrichten om tijdig te kunnen vaststellen of zij aan de precies geformuleerde criteria voldoen. Hierdoor is de meldplicht in deze regeling niet uitputtend geregeld en blijven de algemene parameters in de wet ook meldplichtig. Echter zijn de in deze regeling opgenomen criteria bedoeld als het primaire beoordelingskader voor belangrijke en essentiële entiteiten en voor het uitoefenen van toezicht en handhaving in de praktijk. Indien een situatie onder de in deze regeling vastgelegde criteria valt, is er sprake is van een meldplichtig incident. Voor de parameter uit de wet die in deze regeling is uitgewerkt (ernstige operationele verstoring), is sprake van uitputtende criteria, omdat de meldplichtcriteria in deze regeling daartoe werkelijk en zo compleet mogelijk strekken. Dit sluit niet uit dat ook in andere gevallen aan de parameters uit de wet kan zijn voldaan, met name in evidente gevallen waarin toepassing van uitsluitend de criteria van de regeling zou leiden tot strijd met het doel en de strekking van de wet.

4.1.4 Totstandkoming criteria

In artikel 23, eerste lid van het Cyberbeveiligingsbesluit is bepaald dat de Minister die het aangaat, na overleg met de Minister van Justitie en Veiligheid bij regeling de criteria kan vaststellen op basis waarvan wordt bepaald of sprake is van een significant incident, als bedoeld in artikel 25, tweede lid, van de Cyberbeveiligingswet. Bij het opstellen van de meldplichtcriteria in deze regeling is afstemming gezocht met organisaties uit de energiesector, branchevereniging uit de desbetreffende sectoren en betrokken toezichthouders. Deze afstemming had als doel de regels goed te laten aansluiten op de praktijk en bestaande kaders, zoals de Wbni en sectorale regelgeving, om de uitvoerbaarheid en handhaafbaarheid te waarborgen en onnodige regeldruk te beperken.
Uitgangspunt bij het uitwerken van de meldplichtcriteria is het waarborgen van de continuïteit van de levering van essentiële diensten en de leveringszekerheid van energie. Voor het uitwerken van de ernst van operationele verstoring is gekeken naar de gevolgen van een operationele verstoring van de eigen essentiële dienst van de betrokken essentiële entiteit en belangrijke entiteit en niet aan de hand van de gevolgen voor derden. Er wordt hierbij geen onderscheid gemaakt tussen een fysieke of digitale oorzaak, omdat die vaak nog niet bekend is in de eerste fase van de melding (binnen 24 uur). Deze uitgangspunten hebben als gevolg dat de meldplichtcriteria voor de sectoren elektriciteit, olie en gas geharmoniseerd zijn met de meldplichtcriteria onder de Wwke. Dit komt de uitvoerbaarheid voor kritieke entiteiten ook ten goede, omdat kritieke entiteiten van rechtswege een essentiële entiteit onder de Cyberbeveiligingswet zijn.
Op basis van deze gesprekken en uitgangspunten, is ervoor gekozen om alleen de parameter met betrekking tot de ernstige operationele verstoring uit te werken (artikel 25, tweede lid, onderdeel a van de Cyberbeveiligingswet). De andere twee parameters van artikel 25, tweede lid, van de Cyberbeveiligingswet zijn namelijk niet voor alle subsectoren en soorten entiteiten toepasbaar dan wel uitvoerbaar. Daarom zijn er criteria uitgewerkt die beter aansluiten bij de (essentiële) diensten van essentiële entiteiten en belangrijke entiteiten in de energiesector en die in sommige gevallen reeds worden gehanteerd als melddrempel in andere wet- en regelgeving, zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Overeenkomstig artikel 25, derde lid, van de Cyberbeveiligingswet, is in deze regeling onderscheid

gemaakt tussen sectoren, subsectoren en soorten entiteiten bij het uitwerken van meldplichtcriteria. Algemene sectorale of subsectorale criteria doen namelijk geen recht aan de verschillende type bedrijfsprocessen waar de diverse entiteiten een verantwoordelijkheid voor hebben. Daarnaast bestaan er verschillen in de mate waarin en manier waarop incidenten gevolgen hebben op de leveringszekerheid van energie evenals het kwantificeren van de melddrempels voor desbetreffende sectoren, subsectoren en soorten van entiteiten.

4.2 Nadere regels zorgplicht

In deze ministeriële regeling zijn voor de in artikel 21 genoemde subsectoren nadere regels gesteld ten aanzien van de zorgplicht uit de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. Het doel van deze nadere invulling is om de algemene normen uit de wet en het besluit verder te concretiseren op onderdelen die worden gezien als van groot belang voor de beveiliging van netwerk- en informatiesystemen. Dit biedt duidelijkheid aan essentiële en belangrijke entiteiten en zorgt voor een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen. Bij het opstellen van deze nadere regels is getracht aan te sluiten bij de systematiek uit de wet, het Cyberbeveiligingsbesluit en Uitvoeringsverordening (EU) 2024/2690. Daarmee zou de regeling goed toepasbaar moeten zijn voor entiteiten die tevens binnen het bereik van de uitvoeringsverordening vallen op basis van artikel 4 van het Cyberbeveiligingsbesluit. Net zoals voor de uitwerking van de zorgplicht in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit zijn voor het nader uitwerken van de zorgplicht in deze regeling bestaande normenkaders gehanteerd als uitgangspunt, zoals de ISO27001 en NEN7510. Hierbij is gecontroleerd of de zorgplicht in deze regeling deze normenkaders niet doorkruist. In de artikelsgewijze toelichting, wordt waar van toepassing, naar bestaande normenkaders verwezen. Dit is in lijn met de aanpak in de memorie van toelichting bij de Cyberbeveiligingswet en de nota van toelichting bij het Cyberbeveiligingsbesluit. Entiteiten behouden hiermee de ruimte om hun bestaande normenkader te blijven hanteren, waarbij ze wel moeten zorgen dat de regels in de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en deze regeling alsnog worden nageleefd. Ook staat het doel van specifieke eisen in het artikelsgewijze deel van deze toelichting verder uitgewerkt. Deze regeling hanteert, net zoals de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit een risicogebaseerde aanpak en schrijft daarom niet overal voor hoe invulling gegeven moet worden aan de maatregelen. Essentiële en belangrijke entiteiten dienen conform de zorgplicht van artikel 21 van de Cyberbeveiligingswet deze maatregelen op passende en evenredige wijze in te vullen. Hiermee worden de risico's beheerst die samenhangen met de beveiliging van de netwerk- en informatiesystemen die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken. Ook kunnen hiermee incidenten worden voorkomen of de gevolgen worden beperkt.

4.3 Aanwijzing autoriteiten

Voor een aantal wetten geldt dat deze nauwe raakvlakken hebben met de Cyberbeveiligingswet. Het is daarom gewenst dat de bevoegde autoriteiten, CSIRT's en het centrale contactpunt onder de Cyberbeveiligingswet (hierna: Cbw-instanties) voor de doeltreffende en doelmatige uitvoering van hun taken samenwerken en informatie uitwisselen met de autoriteiten die toezicht houden op de naleving van deze andere wetgeving, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cyberbeveiligingswet en artikel 28 van het Cyberbeveiligingsbesluit.

Het betreft hierbij allereerst de samenwerking met de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS). Deze autoriteit houdt op grond van de Kernenergiewet onder andere toezicht op kerncentrales voor elektriciteitsproductie. Aangezien elektriciteitsproducenten ook onder het bereik van de Cyberbeveiligingswet vallen is het gewenst dat deze samenwerking tussen de Cbw-instanties en de ANVS een grondslag krijgt.

Ten tweede betreft het de samenwerking met de Minister van Klimaat en Groene Groei uit hoofde van de Energiewet en de Mijnbouwwet. Het Staatstoezicht op de Mijnen (SodM) houdt namens de Minister van Klimaat en Groene Groei toezicht op de naleving van regels over veiligheid in de gassector, oliesector en bij windparken op zee. Op grond van de Energiewet hebben onder andere transmissie- en distributiesysteembeheerders verplichtingen voor gegevensbeveiliging, evenals voor geheimhouding van aangewezen materialen, hulpmiddelen en gegevens. Het betreft daarbij entiteiten die (deels) tevens onder de reikwijdte van de Cyberbeveiligingswet vallen en daar met samenhangende verplichtingen te maken hebben, waardoor samenwerking van de Energiewet-toezichthouders met de genoemde Cbw-instanties wenselijk is in het kader van een doeltreffende en doelmatige taakuitvoering.

Ten slotte betreft het de samenwerking met de Autoriteit Consument en Markt (ACM), die een toezichthoudende taak heeft ten aanzien van de elektriciteits-, gas- en warmtesector, waaronder ten aanzien van de betrouwbaarheid van de transmissie- en distributiesystemen voor elektriciteit en gas,

waarvoor dezelfde redenen voor aanwijzing onder artikel 51, tweede lid, onderdeel i, Cyberbeveiligingswet gelden.

5. Regeldruk

5.1 Regeldruk Wwke

Deze regeling veroorzaakt geen nieuwe regeldruk ten opzichte van de Wet weerbaarheid kritieke entiteiten en het Besluit weerbaarheid kritieke entiteiten. De regeldruk voor kritieke entiteiten is verantwoord in de bijbehorende toelichtingen van het wetsvoorstel en het besluit. De aanwijzing van aanvullende categorieën van entiteiten (artikel 2) zou gevolgen kunnen hebben voor de regeldruk. Echter, deze gevolgen zijn niet significant omdat het aantal entiteiten die door deze aanvullende aanwijzing onder de Wwke vallen zeer beperkt is.

5.2 Regeldruk Cyberbeveiligingswet

Deze regeling veroorzaakt ook geen incidentele of structurele aanvullende regeldruk ten opzichte van de reeds berekende regeldruk voor essentiële en belangrijke entiteiten onder de Cyberbeveiligingswet (Cyberbeveiligingswet) en het Cyberbeveiligingsbesluit (Cyberbeveiligingsbesluit). De meld- en zorgplicht in deze regeling betreft een uitwerking van de Cyberbeveiligingswet en Cyberbeveiligingsbesluit en kan niet los worden gezien van het gehele pakket aan regels in de zorg- en meldplicht uit de NIS2-richtlijn, Cyberbeveiligingswet en Cyberbeveiligingsbesluit. Alle artikelen die de zorgplicht concretiseren betreffen aspecten die een entiteit reeds op grond van de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en een richtlijnconforme interpretatie daarvan, bij de beleidsvorming moet betrekken.
Die artikelen betreffen een verduidelijking en zijn reeds verdisconteert in de omvang van de lasten die zijn beschreven in de memorie van toelichting op de Cyberbeveiligingswet en de nota van toelichting op het Cyberbeveiligingsbesluit. De zorgplicht in deze regeling is daarbij onlosmakelijk verbonden met de verplichte risicoanalyse die essentiële en belangrijke entiteiten moeten uitvoeren. Om deze redenen worden de regels over de zorgplicht in deze regeling niet beschouwd als aanvullende verplichtingen ten aanzien van de Cyberbeveiligingswet en Cyberbeveiligingsbesluit.

De hoogte van de drempelwaarde voor het doen van een melding onder de Cyberbeveiligingswet, brengt ook geen aanvullende uitvoeringslasten met zich mee voor essentiële en belangrijke entiteiten. De drempelwaarde is zo gekozen dat het aantal meldingen dat gedaan moet worden, niet hoger zal liggen dan waar al rekening mee is gehouden bij de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. De last van deze meldingen is reeds becijferd in de memorie van toelichting bij de Cyberbeveiligingswet en de nota van toelichting bij het Cyberbeveiligingsbesluit.

De regeldruk voor essentiële en belangrijke entiteiten in alle sectoren, zoals vermeld in bijlage 2 bij de Cyberbeveiligingswet, is becijferd en verantwoord in de bijbehorende toelichtingen van de wetsvoorstellen en besluiten. Daarbij is reeds rekening gehouden met de kosten die entiteiten moeten maken om maatregelen te treffen (de zorgplicht) en om meldingen van meldplichtige incidenten te doen (meldplicht). Voor de Cyberbeveiligingswet, Cyberbeveiligingsbesluit en deze regeling gaat dit naar schatting om 480 bedrijven voor de energiesector.

6. Uitvoerings- en handhaafbaarheidstoetsen

6.1 Inleiding

Een versie van deze regeling is voorgelegd aan de Rijksinspectie Digitale Infrastructuur (RDI), het Staatstoezicht op de Mijnen (SodM) en de Autoriteit Consument en Markt (ACM). Door deze organisaties wordt de consultatieversie van deze Regeling uitvoerbaar, handhaafbaar, en fraudebestendig geacht, indien rekening wordt gehouden met een aantal aangedragen hoofd- en aandachtspunten. Gezien de nadere uitwerking van de zorgplicht voor de Cyberbeveiligingswet gezamenlijk is opgesteld door de Ministers van Klimaat en Groene Groei, Economische Zaken, Landbouw, Visserij, Voedselzekerheid Natuur en Infrastructuur en Waterstaat, zijn alle binnengekomen uitvoerings- en handhaafbaarheidstoetsen (UHT's) gezamenlijk geanalyseerd en verwerkt. Om deze reden zal voor het zorgplichtdeel ook worden ingegaan op punten uit UHT's van andere toezichthouders dan hierboven genoemd.

6.2 Rijksinspectie Digitale Infrastructuur

In de toets heeft de RDI aandacht gevraagd voor duidelijkheid in hoeverre de open norm van artikel 17 van de Wwke en artikel 25 van de Cyberbeveiligingswet met deze regeling uitputtend wordt ingevuld. Ook vraagt de RDI om explicieter in de bepalingen te benoemen op welke subsector of categorieën of

soorten van entiteiten de nadere meldplicht criteria van toepassing zijn. Tevens vraagt de RDI aandacht om in de nadere criteria meldplicht voor de transmissie- en distributiesysteembeheerder binnen de subsector elektriciteit rekening te houden met de andere twee kerntaken (balanshandhaving en marktfacilitering) van de transmissiesysteembeheerder of toe te lichten waarom de meldplicht in relatie tot deze taken niet van toepassing is. Daarnaast heeft de RDI aandacht gevraagd om verduidelijking van het criterium dat de verkoop en wederverkoop van gas en elektriciteit betreft. Tot slot vraagt de RDI aandacht voor de integraliteit van de onderhavige regeling en de Regeling cyberbeveiliging EZ van de Minister van Economische Zaken en Klimaat.

De RDI heeft in hun UHT gevraagd om in de toelichting op de zorgplicht te verduidelijken op welke wijze de verplichtingen in deze regeling en de opener geformuleerde zorgplicht uit de Cyberbeveiligingswet betekent voor de invullingen van de verplichtingen in de praktijk. Hier wordt artikel 43 ten aanzien van bedrijfscontinuïteit als voorbeeld genoemd. De RDI benoemt daarbij het belang dat de terminologie van de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit, de onderhavige regeling en bijbehorende toelichtingen op dezelfde wijze terugkomt.

6.3 Staatstoezicht op de Mijnen

In de toets geeft het SodM een drietal hoofdpunten mee. De eerste betreft het ontbreken van de sectorale risicobeoordeling. SodM geeft daarbij aan dat deze risicobeoordeling concrete handvatten biedt op basis waarvan een toezichthouder kan handhaven. Ten tweede geeft het SodM aan geen toegang tot het NCSC-portaal te hebben waar de meldingen onder de Wwke door kritieke entiteiten worden ingediend. Als laatste hoofdpunt geeft SodM mee dat implicaties voor handhaafbaarheid niet duidelijk zijn omdat de kritieke entiteiten nog niet zijn aangewezen.

6.4 Autoriteit Consument en Markt

De ACM heeft in de toets aandacht gevraagd voor het borgen van goede samenwerking tussen betrokken toezichthouders, het wederzijds uitwisselen van informatie en expertise en hier een verplichtend artikel in de regeling op te nemen voor het afsluiten van een samenwerkingsprotocol. Tevens vraagt de ACM aandacht voor het juridisch inregelen van informatie-uitwisseling met de inlichtingen- en veiligheidsdiensten en de NCTV.

6.5 Verwerking van de reacties

Als gevolg van de door hen uitgevoerde uitvoeringstoetsen zijn een aantal aanscherpingen gedaan in deze regeling, die met name zijn gericht op het verduidelijken van de meldplichtcriteria in algemene zin evenals de nadere criteria die gelden voor specifieke sectoren. Ten aanzien van de nadere regels zorgplicht voor de Cyberbeveiligingswet is de algemene toelichting aangevuld, waarbij is aangegeven waarom deze nadere uitwerking van de zorgplicht in de regeling is uitgewerkt en hoe dit zich verhoudt tot de zorgplicht in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. Tevens is de toelichting op artikel 43 ten aanzien van bedrijfscontinuïteit verduidelijkt waarbij de verhouding met het bedrijfscontinuïteitsplan in artikel 9, derde lid, van het Cyberbeveiligingsbesluit en de risicobeoordelingen in artikel 7 van het Cyberbeveiligingsbesluit wordt benoemd. Daarnaast zijn de onderdelen van artikel 43, eerste lid, die geadresseerd dienen te worden in het bedrijfscontinuïteitsplan nader toegelicht. Ook is de terminologie zoveel mogelijk gelijkgetrokken.

Een aantal aangedragen punten worden niet in deze regeling geregeld, zoals de sectorale risicobeoordeling, het al dan niet toegang verlenen tot het NCSC-portaal en de aanwijzing van kritieke entiteiten, en zijn daarom niet verwerkt in deze regeling. Voor wat betreft het informatie uitwisselen bieden artikel 28 uit de Wwke en artikel 51 uit de Cyberbeveiligingswet hiervoor een grondslag. Bij de Wwke is dit open geregeld en bij de Cyberbeveiligingswet via een delegatiegrondslag, wat verder is uitgewerkt in artikel 46 van deze regeling.

7. Advies Adviescollege Toetsing Regeldruk

7.1 Inleiding

Een concept van deze regeling is voor advies voorgelegd aan het Adviescollege Toetsing Regeldruk (ATR). Hieronder volgt een globale bespreking van het advies.

7.2 Nut en noodzaak

Het ATR ziet geen aanleiding voor opmerkingen over nut en noodzaak.

7.3 Minder belastende alternatieven

Het ATR adviseert te onderbouwen hoe de drempelwaarden en de uitwerking van de zorgplicht tot stand zijn gekomen, in welke mate bij de drempelwaarden de samenleving wordt ontwricht, welke mogelijk minder belastende alternatieven zijn overwogen en waarom die alternatieven niet zijn gekozen. De reactie op dit advies is als volgt. Deze regeling is in nauwe afstemming met diverse energiepartijen, brancheverenigingen en betrokken toezichthouders de nadere criteria van de meldplicht opgesteld. Bij het opstellen van de criteria stond een aantal uitgangspunten centraal, zoals het borgen van de leveringszekerheid, de uitvoerbaarheid en een balans in het aantal meldingen. Voor het bepalen van de hoogte van de drempelwaarden is gekeken naar de potentiële effecten van een incident. Deze effecten zijn nog niet zo ernstig dat de samenleving daardoor ontwricht raakt. In het overgrote deel van de gevallen gaat het om een ernstige aanzienlijke of operationele verstoring van een essentiële dienst. Beoogd is een drempelwaarde vast te stellen dat uitsluitend de meest ernstige verstoring gemeld worden, ook om onnodige regeldruk te voorkomen. Naar aanleiding van dit advies van het ATR is in de toelichting van deze regeling extra toegelicht hoe de drempelwaarden tot stand zijn gekomen en welke alternatieven zijn overwogen.

Voor wat betreft de zorgplicht, worden in deze regeling enkele bepalingen uit de Cyberbeveiligingswet en Cyberbeveiligingsbesluit verder geconcretiseerd en verduidelijkt. Voor die verduidelijking zijn de uitvoeringslasten reeds bij de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit becijferd. De artikelen 42 tot en met 45, waarin de zorgplicht op onderdelen nader geconcretiseerd wordt is met de volgende facetten nadrukkelijk rekening gehouden om de regeldruk zo laag mogelijk te houden. De regeling onderkent dat een entiteit onder verschillende sectoren kan vallen. Om die reden is een uniform luidende zorgplicht opgenomen voor de entiteiten voor sectoren van de Minister van Economische Zaken en Klimaat, de Minister van Klimaat en Groene Groei, de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur en de Minister van Infrastructuur en Waterstaat.

Er is aansluiting gezocht bij internationaal gebruikelijke standaarden (zoals ISO 2700X). Daarbij zij opgemerkt dat deze standaard voor bedrijven niet is voorgeschreven. Voorts is aansluiting gezocht bij de Uitvoeringsverordening 2024/2690. Beide standaarden bevatten veel meer normen dan in deze regeling opgenomen. De opgenomen regels betreffen een scherpe selectie. De overwogen alternatieven zijn: niet reguleren en reguleren op welke wijze uitvoering moet worden gegeven aan de zorgplicht (hoe).

Niet-reguleren had als nadeel dat onduidelijkheid over de norm leidt tot hogere transactiekosten, voordat (rechts)zekerheid van compliance wordt verkregen. Het reguleren van het ‘hoe’ betekent dat de entiteiten minder ruimte of vrijheid hebben om invulling te geven aan de verplichtingen, en daarmee tegen hogere lasten compliant worden. Daarbij geldt voor regulering van het ‘hoe’, dat daarbij onvoldoende rekening kan worden gehouden met de verschillen tussen sectoren en entiteiten. Hiermee wordt ook de mogelijkheid behouden voor essentiële en belangrijke entiteiten om hun eigen normenkaders te hanteren voor het beheersen van hun risico’s ten aanzien van de beveiliging van netwerk- en informatiesystemen, zoals de ISO/IEC of sectorale normen. Het voldoen aan een eigen normenkader betekent op zichzelf niet dat een entiteit aan de zorgplicht van de Cyberbeveiligingswet, Cyberbeveiligingsbesluit en deze regeling voldoet. De entiteit dient te waarborgen dat de maatregelen die zij moet nemen op grond van de Cyberbeveiligingswet in ieder geval onderdeel zijn van het maatregelenpakket.

7.4 Werkbaarheid

Het ATR adviseert om de werkbaarheid van de regeling nader toe te lichten en dit per sectoronderdeel uit te splitsen, en daarbij na te gaan of gekozen kan worden voor het meest regelluwe alternatief van melden. Ook gaat het ATR in op de werkbaarheid van de zorgplicht voor kleine en middelgrote entiteiten. Daarnaast licht het ATR hierbij toe dat voor de meldplicht onder de Cyberbeveiligingswet en Wwke verschillende termijnen gelden. De reactie hierop is als volgt. In de toelichting van deze regeling zijn de werkbaarheid en de minder belastende alternatieven nader uitgewerkt per categorie of soort entiteit binnen de verschillende subsectoren van de sector energie. Hierbij is zoveel mogelijk aansluiting gezocht bij bestaande (wettelijke) meldcriteria of beargumenteerd van afgeweken om de werkbaarheid ten goede te komen, na overleg met de desbetreffende sectorpartijen. De fases van melden onder de Cyberbeveiligingswet en Wwke volgen rechtstreeks uit de Europese richtlijnen en daarmee biedt deze regeling niet de mogelijkheid om hiervan af te wijken. Om de werkbaarheid van de zorgplicht onder de Cyberbeveiligingswet ten goede te komen is er gekozen voor een uniform geformuleerde zorgplicht met de Minister van Economische Zaken en Klimaat, de Minister van Klimaat en Groene Groei, de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur en de Minister van Infrastructuur en Waterstaat. Dit is de beste garantie om stapelingen of knelpunten in verplichtingen en daarmee in toezicht zoveel mogelijk te voorkomen. Voor het opstellen van de zorgplichtregels is gebruik gemaakt van bestaande internationale en sectorale standaarden. Voor de meldplichtcriteria is

juist voor de werkbaarheid een sectorspecifieke benadering gekozen om zo goed aan te kunnen sluiten bij de essentiële of belangrijke bedrijfsprocessen van de entiteiten. In 7.2.2 is de werkbaarheid nader toegelicht.

7.5 Invoeringstoets

Het ATR adviseert om een jaar na de inwerkingtreding van deze regeling een invoeringstoets uit te voeren. Naar aanleiding van een amendement op het wetsvoorstel van de Cyberbeveiligingswet, is geregeld dat er een invoeringstoets plaatsvindt 18 maanden na inwerkingtreding van de Cyberbeveiligingswet. Voor de Wwke geldt geen invoeringstoets. De invoeringstoets kan aanleiding geven tot aanpassing van deze regeling, bijvoorbeeld wanneer de zorg- en meldplicht in de Cyberbeveiligingswet zou worden aangepast vanwege de invoeringstoets.

7.6 Gevolgen regeldruk

Het ATR adviseert meer inzicht te geven in de regeldrukeffecten voor de ondernemers die onder deze regeling vallen. In hoofdstuk 5 is de regeldruk nader toegelicht. De conclusie is dat deze regeling voor zowel de kritieke entiteiten onder de Wwke als de essentiële en belangrijke entiteiten onder de Cyberbeveiligingswet niet leidt tot aanvullende regeldruk ten opzichte van de reeds berekende regeldruk voor de zorg- en meldplicht onder de Wwke, het Bwke, de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit.

8. Internetconsultatie

8.1 Inleiding

Een concept van deze regeling is opengesteld voor consultatie op www.internetconsultatie.nl. Hieronder volgt een globale bespreking van de adviezen en reacties.

8.2 Toepassingsbereik

8.2.1 Toepassingsbereik Cyberbeveiligingswet en aanwijzingsprocedure Wwke

In de consultatie hebben meerdere organisaties gevraagd voor een verduidelijking van het toepassingsbereik voor een aantal entiteiten in de energiesector onder de Cyberbeveiligingswet en de aanwijzingsprocedure van kritieke entiteiten onder de Wwke. De reactie hierop is als volgt. Deze regeling regelt niet het toepassingsbereik van de Cyberbeveiligingswet noch regelt deze regeling de aanwijzing van kritieke entiteiten.

8.2.2 Reikwijdte ‘exploitant van een laadpunt’ (Cyberbeveiligingswet)

Onder meer de Raad Nederlandse Detailhandel, ElaadNL en IKEA hebben in hun reactie gevraagd om verduidelijking van de reikwijdte van ‘exploitant van een laadpunt’, oftewel *Charge Point Operators* (CPO’s). Daarbij stelt E-laad voor om het toepassingsbereik voor CPO’s te baseren op beheerd vermogen, bijvoorbeeld 100 MW, in plaats van op de grootte van de organisatie. De reactie hierop is als volgt. De NIS2-richtlijn is alleen van toepassing op de sectoren en type entiteiten uit de bijlagen van de NIS2-richtlijn, voor zover zij voldoen aan de omvangscriteria die uit de NIS2-richtlijn voortvloeien. Er is op dit moment daarom geen mogelijkheid om de reikwijdte ten aanzien van CPO’s alleen te baseren op het beheerd vermogen. De Minister van Klimaat en Groene Groei is eveneens van mening dat toepassingsbereik ten aanzien van exploitanten van laadpunten verduidelijkt dient te worden. Het kabinet heeft de Europese Commissie daarom gevraagd om aanpassing van de NIS2-richtlijn op dit punt.

8.2.3 Definitie marktdeelnemers (Cyberbeveiligingswet en Wwke)

Holland Solar, Energy Storage NL en NedZero vragen om de definitie van marktdeelnemers te verduidelijken. Daarnaast geven deze organisaties en NBNL aan dat ook fabrikanten van producten en diensten, zoals omvormers en HEMS, en andere aansturende partijen die toegang hebben tot geaggregeerde assets van een bepaald vermogen, bijvoorbeeld 100 MW, onder het toepassingsbereik van de Cyberbeveiligingswet en Wwke zouden moeten vallen. De reactie hierop is als volgt. Fabrikanten van producten en diensten zoals omvormers en HEMS vallen niet onder de reikwijdte van de Wwke en Cyberbeveiligingswet. Echter, de Wwke en Cyberbeveiligingswet verplichen entiteiten zorg te dragen voor de beveiliging van hun toeleveringsketen waaronder cruciale (digitale) componenten, zoals omvormers. Hierbij wordt de entiteit geacht te kijken naar de afhankelijkheden van producten en diensten van leveranciers, en zorgdragen voor maatregelen om risico’s te beheersen die samenhangen met het gebruik van software, hardware of diensten.

8.2.4 Aanwijzen kritieke entiteiten (Wwke)

Energie Nederland vraagt in haar reactie om duidelijkheid over de aanwijzingsprocedure van kritieke entiteiten. De Minister van Klimaat en Groene Groei heeft de bevoegdheid kritieke entiteiten in de energiesector aan te wijzen bij besluit of regeling. Er is gekozen om organisaties bij besluit (beschikking) aan te wijzen als kritieke entiteit vanwege de vertrouwelijkheid. De Minister van Klimaat en Groene Groei is verplicht om de kritieke entiteiten aan te wijzen binnen één maand na inwerkingtreding van de Wwke.

8.3 Meldplicht

8.3.1 Algemeen

Meerdere organisaties, zoals RWE en Vemobin, vragen om verduidelijking met betrekking tot het meldportaal, toegang tot meldingsinformatie, en dit te harmoniseren voor Cyberbeveiligingswet en Wwke. De reactie hierop is als volgt. Deze regeling regelt enkel de nadere meldplicht criteria voor de energiesector. Het meldportaal, proces en toegang worden geregeld bij wet en besluit. Voor kritieke entiteiten onder de Wwke, alsmede belangrijke dan wel essentiële entiteiten onder de Cyberbeveiligingswet, is er eenzelfde meldportaal. Dit meldportaal wordt technisch en functioneel beheert door het Nationaal Cyber Security Centrum (NCSC). De toelichting op het meldproces en de toegang staat beschreven in paragraaf 8.3.1 van de memorie van toelichting op de Wwke en paragraaf 8.1.4 van de memorie van toelichting bij de Cyberbeveiligingswet.

Norea vraagt daarnaast aandacht voor de koppeling van de melddrempels aan de risico-gebaseerde aanpak waarbij organisaties prioriteit geven aan kroonjuwelen. De toelichting hierop is dat er geen nadrukkelijke link wordt gemaakt met de risico-gebaseerde aanpak, maar dat de meldplichtcriteria al betrekking hebben op belangrijke of essentiële diensten ten opzichte van leveringszekerheid van energie.

8.3.2 Incident veroorzaakt door kwaadwillend handelen

Vemobin vraagt om verduidelijking van de samenhang van de meldplicht en de continuïteit in productie. Zij geven daarbij als voorbeeld of een cyberaanval gemeld worden als dit niet leidt tot verstoring van de productie. De Wwke en Cyberbeveiligingswet bieden op dit moment geen grondslag om een meldplicht vast te stellen voor incidenten die veroorzaakt zijn door kwaadwillend handelen, maar bijvoorbeeld niet tot een aanzienlijke of ernstige operationele verstoring van de essentiële dienst leiden. Echter, het staat een kritieke, essentiële of belangrijke entiteit vrij om vrijwillig een melding te doen bij situaties waarbij het vermoeden bestaat, dan wel bevestigd is, dat incidenten zijn veroorzaakt door kwaadwillend handelen.

8.3.3 Uitzondering meldplicht/geplande onderbreking

Zowel Vemobin als RWE vragen om uitzonderingen op de meldplicht. RWE stelt dat er naast een geplande onderbreking, ook andere uitzonderingen denkbaar zijn. Vemobin vraagt om een uitzondering voor situaties waar een geplande onderbreking ongepland uitloopt, zolang deze niet wordt veroorzaakt door externe factoren zoals een hack. Naar aanleiding van deze reactie is extra tekst opgenomen bij de artikelsgewijze toelichting bij de artikelen over de geplande onderbrekingen (19 en 41). In aanvulling op onderhoudswerkzaamheden, is nu ook toegelicht dat er niet gemeld hoeft te worden als een bepaalde essentiële dienst niet beschikbaar is op basis van een vooraf bepaalde contractuele overeenkomst.

8.3.4 Meldplichtcriteria voor de subsector elektriciteit

Door Netbeheer Nederland, Holland Solar, Energy Storage NL, NedZero, en Energie Nederland is gevraagd om in het artikel voor de elektriciteitsproducenten en marktdeelnemers toe te voegen dat het gaat om geaggregeerd vermogen van 100 MW. Netbeheer Nederland geeft daarnaast ook aan dat in het artikel voor de transmissie- en distributiesysteembeheerders expliciet gemaakt moet worden dat het om geaggregeerd vermogen gaat. Naar aanleiding van deze reactie is dit in de regeling aangepast.

Energie Nederland pleit voor het verwijderen van het artikel over de verkoop en wederverkoop van elektriciteit, omdat incidenten die impact hebben op de verkoop en wederverkoop in geen geval leiden tot een verstoring in de levering van elektriciteit. Naar aanleiding van deze reactie is het artikel en de toelichting voor leveranciers van elektriciteit aangepast in overleg met Energie Nederland. Voor leveranciers geldt de meldplicht voor incidenten die gevolgen hebben of kunnen hebben voor de uitvoering van de contractuele kernverplichtingen.

8.3.5 Meldplichtcriteria voor de subsector (aard)gas

Energie Nederland pleit voor het verwijderen van het artikel over de verkoop en wederverkoop van gas, omdat incidenten die impact hebben op de verkoop en wederverkoop in geen geval leiden tot een verstoring in de levering van gas. Naar aanleiding van deze reactie is het artikel en de toelichting voor leveringsbedrijven voor gas aangepast in overleg met Energie Nederland. Voor leveringsbedrijven voor gas ziet de meldplicht op incidenten die gevolgen hebben of kunnen hebben voor de uitvoering van de contractuele kernverplichtingen.

Netbeheer Nederland pleit voor het herformuleren van de artikelen die betrekking hebben op de nadere criteria voor de meldplicht voor de subsector (aard)gas. Na overleg met Netbeheer Nederland, waaronder Gasunie, en andere betrokken gaspartijen zijn de nadere criteria voor de subsector (aard)gas gewijzigd. De wijzigingen hebben betrekking op het opsplitsen van transmissie en distributie van gas, het toevoegen van een drempel voor de interconnector-systeembeheerder, het opsplitsen van de criteria voor gasopslagbeheerders, en het aanpassen van de kwantitatieve drempelwaarden voor productie, opslag en LNG-systeembeheerders.

8.3.6 Meldplichtcriteria voor de subsector aardolie

Uit de reactie van VEMOBIN is naar voren gekomen dat met betrekking tot de artikelen voor de oliesector, het onvoldoende duidelijk is welke olieproducten binnen de reikwijdte van de regeling vallen. Naar aanleiding van deze reactie is in de toelichting van deze regeling expliciet beschreven wat er wordt verstaan onder olieproducten.

Tevens vraagt VEMOBIN de drempelwaarde te verhogen van het artikel voor raffinage en behandeling van olie naar 250.000 vaten per dag. Naar aanleiding van deze reactie en in overleg met betrokken organisatie is de drempelwaarde aangepast. In de artikelsgewijze toelichting wordt dit nader uitgelegd.

Daarnaast vraagt VEMOBIN te specificeren wat er wordt verstaan onder wettelijke voorraden. Naar aanleiding van deze reactie en overleg met betrokken organisaties zijn een aantal wijzigingen aangebracht. Naast een artikel voor de exploitanten voor de voorziening van opslag van ruwe olie en olieproducten is ook een artikel opgenomen voor de exploitanten voor de voorziening van opslag van ruwe olie en olieproducten die tevens voorraadplichtig zijn. In de artikelsgewijze toelichting wordt dit uitgebreid toegelicht. Daarnaast geldt voor de centrale entiteit voor de voorraadvorming een meldplicht die betrekking heeft op het bredere beheer van de wettelijke olievoorraden.

8.3.7 Meldplichtcriteria voor de subsector stadsverwarming en -koeling

Energie Nederland vraagt in haar reactie om te verduidelijken wat er wordt bedoeld met afgenomen vermogen en stelt voor om het aan te passen naar beschikbaar vermogen. Naar aanleiding van deze reactie is het artikel aangepast. Het artikel ziet op het wegvallen van beschikbare vermogen. De artikelsgewijze toelichting bij het artikel gaat hier nader op in.

8.4 Zorgplicht

8.4.1 Inleiding

Aangezien de nadere uitwerking van de zorgplicht gezamenlijk is opgesteld door de Minister van Economische Zaken en Klimaat, de Minister van Klimaat en Groene Groei, de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur en de Minister van Infrastructuur en Waterstaat, zijn de voor deze Ministers binnengekomen consultatiereacties gezamenlijk geanalyseerd en verwerkt. Om deze reden zal in deze consultatieparagraaf op de binnengekomen reacties vanuit verschillende sectoren worden ingegaan.

8.4.2 Algemeen

Meerdere partijen, zoals BTG en ElaadNL, hebben in hun reactie aangegeven graag de verwijzing naar bestaande normen, zoals ISO/NEN en sectorspecifieke normen, in de regeling te willen zien. Naar aanleiding van deze reacties, is de toelichting op de algemene inleiding zorgplicht aangepast in lijn met de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit.

NOREA stelt in haarreactie voor om netwerk segmentatie uit te breiden naar leveranciersscreening en ketenaudits. Dit voorstel is niet in de zorgplicht in de regeling opgenomen, gezien deze verplichting voor een verhoogde regeldruk bij essentiële en belangrijke entiteiten zorgt, aanzienlijk verhoogde kosten en in sommige gevallen moeilijk uitvoerbaar is. Daarbij werkt deze regeling het artikel over

beveiliging van de toeleveringsketen uit het Cyberbeveiligingsbesluit bewust niet verder uit, omdat dit een nieuwe verplichting is ui de Richtlijn en de regels uit het Cyberbeveiligingsbesluit voor nu als voldoende worden geacht. Daarnaast vraagt NOREA in haar reactie om een verplichting aan entiteiten op te leggen om op basis van de Internationale Digitale Rapportage Standaard (IDRS) een cyberjaarverslag op te stellen. Dit wordt niet geregeld bij deze regeling, aangezien deze regeling een implementatie is van de Europese NIS2-richtlijn waarbij aan entiteiten geen aanvullende verplichtingen worden opgelegd. Momenteel verkennen de ministeries van Binnenlandse Zaken en Economische Zaken en Klimaat, naar aanleiding van een motie van Kamerlid Kathmann (Tweede Kamer, 27 mei 2025, 26 643, nr. 1342), hoe het cyberjaarverslag, op basis van de IDRS, ingevoerd kan worden als brede standaard op een wijze die leidt tot lastenverlichting en het verbeteren van de veiligheid.

8.4.3 Duidelijker onderscheid tussen IT en OT-systemen

Meerdere partijen, zoals Holland Solar en Energie Nederland, vragen om een duidelijker onderscheid aan te brengen tussen IT en OT, waaronder voor patchmanagement. Dit onderscheid is doorgevoerd in meerdere onderdelen van de toelichting op het artikel over de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen. Wat betreft patchmanagement, is bijvoorbeeld nader toegelicht in artikel 44, tweede lid, onderdeel c, dat bij het toepassen van beveiligingspatches op OT-systemen de noodzaak van continuïteit van dienstverlening en de verouderde aard van veel industriële componenten meegewogen kan worden om te bepalen of de nadelen van deze toepassing zwaarder wegen dan de voordelen voor cyberbeveiliging.

8.4.4 Beveiligingsaspecten ten aanzien van toegangsbeleid

RWE onderschrijft het belang van sterke identificatie- en authenticatieprocedures, en een zorgvuldig gereguleerde autorisatie. Zij benadrukken in hun reactie dat niet alle OT-systemen technisch in staat zijn om deze functionaliteit te ondersteunen en adviseren om een clausule op te nemen, zoals ‘waar mogelijk’ of verplichting om ‘alternatieve maatregelen te definiëren’ voor systemen die deze functionaliteit niet kunnen implementeren. Als reactie hierop, is het artikel hierover aangepast waarbij er ruimte wordt geboden om dit mee te nemen in het beleid over bevoorrechte accounts en systeembeheeraccounts. Bovendien geldt voor alle zorgplicht maatregelen dat deze passend en evenredig worden ingevuld. Het artikel in deze regeling over toegangsbeleid is ook aangepast naar aanleiding van de feedback van Centraal Bureau Levensmiddelenhandel en de Nederlandse Zuivel Organisatie. Hierin wordt nu erkend dat het tijdelijk verhogen van bevoegdheden een volwaardig alternatief is voor vaste admin-accounts.

8.4.5 Evaluatie regeling

Netbeheer Nederland heeft in de consultatiereactie aangegeven het wenselijk te vinden als deze regeling en specifiek de meldplicht, na twee jaar geëvalueerd zou worden. In de Cyberbeveiligingswet is geregeld dat er twee jaar na inwerkingtreding een evaluatie plaatsvindt; de evaluatie van de Wwke vindt plaats na vier jaar. De meldplicht in beide wetten wordt meegenomen in deze evaluatie. Specifiek voor deze regeling zal een invoeringstoets, 18 aantal maanden na inwerkingtreding worden uitgevoerd.

8.5 Aangewezen autoriteiten

RWE vraagt in haar reactie ten behoeve van het voorkomen van interpretatieverschillen bij de uitvoering om verduidelijking van de taken, verantwoordelijkheden en bevoegdheden van onder meer de Minister van KGG en de ACM als aangewezen autoriteiten. Onze reactie is als volgt. Deze regeling regelt enkel de grondslag voor informatie-uitwisseling voor de Cyberbeveiligingswet. Bij de Wwke volgt deze grondslag uit de wet.

9. Notificatie

Ter voldoening aan de Notificatierichtlijn[1] is beoordeeld of voorschriften in deze regeling als technisch voorschrift genotificeerd moeten worden bij de Europese Commissie. Ook is ter voldoening aan de Dienstenrichtlijn[2] beoordeeld of voorschriften in deze regeling als eis kwalificeren in de zin van genoemde richtlijn, welke eveneens genotificeerd moeten worden bij de Europese Commissie. De

[1] Richtlijn 2015/1535 van het Europees parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (codificatie) (*PbEU* 2015, L 241).

[2] Richtlijn 2006/123/EG van het Europees parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (*PbEU* 2006, L 376).

uitkomst van die beoordeling is dat deze regeling geen technische voorschriften of eisen in de zin van de Dienstenrichtlijn bevat, waardoor notificatie niet aan de orde is.

II. Artikelsgewijs (Wwke)

Artikel 1. begripsbepalingen

Deze regeling gebruikt veelal begrippen die ook in de Energiewet worden gehanteerd. Dit sluit aan bij het principe dat in wetgeving eenheid in terminologie wordt nagestreefd. Als de Energiewet een begrip niet bevat, is aangesloten bij andere Nederlandse wetgeving of een EU-verordening. Dit betekent dat er soms verschillen zijn met de omschrijving van 'soorten entiteiten' die zijn vermeld in bijlage 1, sector energie, bij de Wwke. Daar wordt bij verschillende soorten entiteiten immers verwezen naar begrippen in EU-richtlijnen en die begrippen zijn vervolgens in de Nederlandse wetgeving geïmplementeerd, met name in de Energiewet.

Artikel 1 bevat begripsbepalingen die van toepassing zijn op hoofdstuk 1: het Wwke-hoofdstuk van deze regeling. De begripsbepalingen *besluit* en *wet* zijn opgenomen, zodat duidelijk is dat deze begrippen in hoofdstuk 1 verwijzen naar het Besluit weerbaarheid kritieke entiteiten en de Wet weerbaarheid kritieke entiteiten, en niet naar het Cyberbeveiligingsbesluit en de Cyberbeveiligingswet.

Artikel 2. aanwijzing categorieën van entiteiten

Artikel 2 regelt dat de interconnectorsysteembeheerder voor elektriciteit en de interconnectorsysteembeheerder voor gas onder het toepassingsbereik van de Wet weerbaarheid kritieke entiteiten komen. Dit is noodzakelijk omdat de Minister van Klimaat en Groene Groei anders niet in de gelegenheid is partijen die onder deze definitie vallen aan te wijzen als kritieke entiteit.

Paragraaf 1.2. Criteria aanzienlijke verstoring voor de subsector elektriciteit

Paragraaf 1.2 bevat de nadere uitwerking van artikel 17 van de Wwke en artikel 14 van het Bwke. Voor de categorieën van entiteiten binnen de elektriciteitssector is de leveringszekerheid, waaronder zekerheid van netbeschikbaarheid, transport en netbalans, als uitgangspunt genomen voor de totstandkoming van de meldplichtcriteria.

Artikel 4. transmissiesysteembeheerder, interconnectorsysteembeheerder en distributiesysteembeheerder voor elektriciteit

Algemeen

Artikel 4 regelt dat transmissie-, interconnector-, en distributiesysteembeheerders voor elektriciteit een melding moeten doen indien een incident leidt of kan leiden tot 100 MW geaggregeerd vermogen van niet getransporteerde elektriciteit. Omdat de factor tijd in deze berekening is verdisconteerd, is gekozen voor een uniforme drempelwaarde. Bij de toepassing van de melddrempel van 100 MW dient rekening te worden gehouden met de redundantie die in het elektriciteitssysteem is ingebouwd. Er is daarom gekozen om met deze drempelwaarde aan te sluiten op het zogenoemde N-1-criterium dat wordt toegepast op het ontwerp van elektriciteitsnetten en dat garandeert dat de stroomvoorziening ook blijft werken als één component van het systeem uitvalt. Tevens sluit de kwantificering van dit criterium aan bij bestaande meldplichten in andere wet- en regelgeving, zoals in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

De drempelwaarde is weergegeven in weggevallen vermogen uitgedrukt in MW. Het betreft zowel weggevallen momentaan vermogen als het vermogen dat gepland was om te worden getransporteerd, maar door het incident niet kon worden getransporteerd. Voor het berekenen van het vermogen wordt uitgegaan van het momentane of geplande gebruik, niet van de maximale transmissie- of distributiecapaciteit. Dit omdat het gaat om de daadwerkelijke impact van een incident en niet om de theoretische capaciteit die getransporteerd had kunnen worden.

Een incident waarbij een component van het systeem uitvalt, maar er door N-1-maatregelen geen impact is van 100 MW of meer op het momentane of geplande vermogen op het transmissie- of distributiesysteem, raakt daarmee derhalve niet de drempelwaarde en hoeft niet te worden gemeld. Het kan dus zijn dat er een incident plaatsvindt, maar dat dit via N-1-maatregelen niet tot gevolgen leidt of had kunnen leiden zoals het direct omleiden van elektriciteit via andere elektriciteitslijnen en -stations. Hierdoor blijft uitval van 100 MW vermogen uit waardoor dit incident niet gemeld dient te worden. In gevallen waar er alsnog sprake is van een (tijdelijke) onderbreking van 100 MW of meer

aan momentaan of gepland vermogen ondanks inzet van N-1-maatregelen, dient alsnog gemeld te worden.

Verschillende scenario's

Er moet aldus in verschillende scenario's gemeld worden. Bij momentaan gebruik is er in de regel sprake van gelijktijdigheid van het incident en de uitval van 100 MW getransporteerde elektriciteit. De transmissie- en distributiesysteembeheerders dienen dus te melden zodra er kennis is genomen van een incident dat leidt of kan leiden tot 100 MW uitval van momentaan vermogen. Er dient ook gemeld te worden in een situatie wanneer ten tijde van het incident niet 100 MW getransporteerd werd, maar dat voor een later moment bijvoorbeeld 200 MW ingepland (gepland vermogen) dat geen doorgang kon vinden door het incident. De maximale transportcapaciteit speelt geen rol bij het bepalen van het momentane of geplande vermogen. In beide gevallen gaat het dus om wegvallen van ten minste 100 MW vermogen wat niet direct opgelost kan worden en leidt tot te weinig transmissie- of distributiecapaciteit.

Een door een incident veroorzaakt tekort aan transmissienetcapaciteit van 100 MW of meer momentaan of gepland vermogen kan door de transmissienetbeheerder opgevangen worden door *redispatch* of andere (toekomstige) maatregelen, zoals *gridboosters* of *storage-as-transmission*. Op deze wijze kunnen congestie- of onbalansproblemen opgelost worden. In een dergelijk geval dient echter wel gemeld te worden, omdat de beschikbare momentane of geplande systeemcapaciteit door het incident niet meer beschikbaar is. Dit gaat ook op voor incidenten waarbij interconnectoren betrokken zijn. Indien ten minste 100 MW niet via een andere interconnector getransporteerd kon worden en er daarom redispatching of andere balansinstrumenten moesten worden ingezet, wordt de melddrempel gehaald.

Balanshandhaving en marktfacilitering

Transmissiesysteembeheerders hebben naast transport van elektriciteit, ook de wettelijke taken voor balanshandhaving en marktfacilitering. Deze taken zijn nauw verbonden met de transmissie taak en het N-1-criterium. Het N-1-criterium zorgt ervoor dat een incident waarbij er sprake is van een enkelvoudige storing niet direct leidt tot congestie of onbalans op het systeem waardoor het systeem de tijd heeft om congestie te voorkomen of de balans te herstellen door inzet van verschillende (balans)instrumenten, zoals inzet van regel- of noodvermogen en redispatching. Een incident is ook meldingsplichtig als de oorzaak van het afgenomen vermogen van ten minste 100 MW niet het gevolg is van verminderde transmissiecapaciteit, maar veroorzaakt wordt door een verstoring van de balanshandhaving bij de transmissiesysteembeheerder, bijvoorbeeld het niet kunnen activeren van regel- of noodvermogen. Ondanks het belang van de marktfaciliteringstaak van transmissiesysteembeheerders, is er op dit moment gekozen om deze voor nu buiten de reikwijdte van de meldplicht te laten. Dit is in lijn met de aanpak voor de Gedelegeerde Verordening (EU) 2024/1366 van de Commissie van 11 maart 2024 tot aanvulling van Verordening (EU) 2019/943 van het Europees parlement en de Raad door middel van de vaststelling van een netcode inzake sectorspecifieke regels voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen. In die verordening worden eerst de resultaten van de Europese risicobeoordelingen afgewacht om te kunnen bepalen bij welke drempels deze taak en daarmee leveringszekerheid in het geding komt.

Artikel 5. elektriciteitsproducent en marktdeelnemer

Artikel 5 regelt dat marktdeelnemers en elektriciteitsproducenten een melding moeten doen indien een incident leidt of kan leiden tot het niet beschikbaar zijn van 100 MW geaggregeerd vermogen. Dit niet beschikbare vermogen heeft betrekking op het netto vermogen van de kritieke entiteit. Het gaat daarom over de gevolgen van het incident voor de totale capaciteit van de assets die ingezet kunnen worden. Een aanzienlijke verstoring met betrekking tot het beschikbare vermogen kan leiden tot onbalans van het elektriciteitssysteem tenzij de desbetreffende asset niet in gebruik is of was uitgeschakeld. Deze drempelwaarde heeft betrekking op zowel afname als invoer op het transmissie- of distributiesysteem voor elektriciteit. Er wordt hier, in tegenstelling tot de drempelwaarde voor transmissie- en distributiesysteembeheerders, gerekend met het totale beschikbare vermogen van assets. Hiervoor is gekozen omdat voor de stabiliteit van het elektriciteitssysteem, de mate waarin capaciteit op korte termijn inzetbaar moet zijn om bijvoorbeeld fluctuaties op te vangen relevant is. Het wegvallen van het beschikbare vermogen beperkt deze flexibiliteit, ook als het vermogen op het moment van het incident niet daadwerkelijk werd benut. Door te rekenen met het beschikbare vermogen wordt beter inzicht verkregen in de potentiële impact van een incident op de leveringszekerheid en systeemstabiliteit.

Artikel 6. elektriciteitsmarktbeheerder

Artikel 6 regelt dat elektriciteitsmarktbeheerders moeten melden indien een incident leidt of kan leiden tot het niet tijdig kunnen plaatsvinden van de day-ahead- of intraday-koppeling, ongeacht het verhandelde vermogen. Ook dient een incident gemeld te worden dat leidt of kan leiden tot een aantasting van de integriteit van de marktkoppeling waardoor mogelijk verkeerde prijzen ontstaan op de elektriciteitsmarkt. Indien de desbetreffende elektriciteitsmarktbeheerder terugvalprocedures inzet waardoor de day-ahead- en intraday-koppeling alsnog tijdig kan plaatsvinden ondanks een incident, hoeft er niet gemeld te worden.

Paragraaf 1.3. Nadere criteria aanzienlijke verstoring voor de subsector gas

Paragraaf 1.3 bevat een nadere uitwerking van artikel 17 van de Wwke en artikel 14 van het Bwke. Voor de categorieën van entiteiten binnen de gassector is voor het opstellen van meldcriteria gekeken naar het waarborgen van de leveringszekerheid van gas. Daarnaast sluit de kwantificering van het meldcriterium deels aan bij de al bestaande melddrempel onder huidige wet- en regelgeving, zoals in de Wbni. Voor sommige criteria, zoals voor LNG-systeembeheerders, is er bewust afgeweken van bestaande melddrempels gezien de veranderende rol in het systeem. Dit wordt verder per lid toegelicht. Binnen de melddrempels voor de subsector gas wordt geen onderscheid gemaakt tussen incidenten die betrekking hebben op hoogcalorisch en laagcalorisch gas; de vastgestelde drempels zijn op beide gastypen van toepassing.

Artikel 7. distributiesysteembeheerder voor gas

Op grond van artikel 7 geldt voor de distributiesysteembeheerders voor gas een melddrempel indien een incident gevolgen heeft of kan hebben op 20.000 eindafnemers die geen gas meer ontvangen. Voor het begrip eindafnemer geldt de begripsbepaling in artikel 1.1 van de Energiewet: een aangeslotene die gas koopt of wil kopen voor eigen gebruik. In tegenstelling tot het meldcriterium voor transmissiesysteembeheerders voor gas, is er voor distributiesysteembeheerders gekozen om te kijken naar de gevolgen voor het aantal eindafnemers omdat distributiesysteembeheerders vanuit hun rol en verantwoordelijkheid meer zicht hebben op het aantal eindafnemers. De gekwantificeerde drempel van 20.000 eindafnemers sluit aan bij de drempel voor de meldplicht onder de Wbni.

Artikel 8. transmissiesysteembeheerder voor gas

Voor transmissiesysteembeheerder geldt, op grond van artikel 8, een meldplicht indien een incident gevolgen heeft of kan hebben voor de normale werking van het transmissiesysteem voor gas. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering. De werking van het transmissiesysteem voor gas wordt continu gemonitord door de transmissiesysteembeheerder. De verantwoordelijkheid voor de inschatting wanneer het transmissiesysteem voor gas normaal of abnormaal functioneert ligt bij de transmissiesysteembeheerder. Hierbij wordt gekeken naar het functioneren van kritieke exit- of entrypunten van het gassysteem. Deze melddrempel betekent niet dat er altijd gemeld dient te worden door de transmissiesysteembeheerder als een exitpunt uitvalt. Het verschilt per casus en moment of een dergelijk exitpunt kritiek is voor de leveringszekerheid van gas, omdat er ook via andere wegen belevering kan plaatsvinden. Voor andere scenario's kan het wel van belang zijn om te melden, zoals bijvoorbeeld het uitvallen van een compressorsysteem of het niet kunnen voldoen aan de kwaliteitscriteria. Bovendien kan de normale werking van het transmissiesysteem voor gas per seizoen verschillen, afhankelijk van de vraag naar gas. Het beoordelen van de gevolgen voor de normale werking van het transmissiesysteem voor gas vergt daarom een beoordeling per geval. Hierom is gekozen om geen kwantitatieve melddrempel op te nemen voor een transmissiesysteembeheerder voor gas.

Artikel 9. interconnectorsysteembeheerder voor gas

Artikel 9 regelt dat een interconnectorsysteembeheerder voor gas moet melden zodra een incident gevolgen heeft of kan hebben voor de normale werking van het interconnectorsysteem voor gas. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering. Interconnectoren voor gas zijn van groot belang voor de gasleveringszekerheid, omdat het grensoverschrijdende handel mogelijk maakt. Dit vergroot de stabiliteit en verbetert de werking van de gasmarkt. De werking van het interconnectorsysteem werkt bij wijze van spreken als een 'aan- en uitknop'. Een aanzienlijke verstoring van het interconnectorsysteem kan daarom al snel leiden tot een volledige uitval van dit systeem waardoor gas bijvoorbeeld niet naar Nederland kan stromen of naar het land waarmee de interconnector verbonden is. Om deze reden is hier dus gekozen om geen kwantitatieve drempelwaarde op te nemen, maar een vergelijkbaar generiek criterium op te nemen als die voor de transmissiesysteembeheerder voor gas.

Artikel 10. LNG-beheerder

Artikel 10 regelt dat beheerders van een systeem voor LNG (vloeibaar gas) dienen te melden indien een incident gevolgen heeft of kan hebben voor het LNG-systeem van ten minste 150 GWh per dag. LNG is belangrijk voor de gasleveringszekerheid in Nederland en Europa doordat het fungeert als een flexibele en gediversifieerde importbron via terminals. Het toenemende belang van LNG maakt dat er gekozen is voor 150 GWh per dag in plaats van het aanhouden van de 10 GWh per dag die gehanteerd werd in de Wbni. 10 GWh per dag als melddrempel is te laag in vergelijking tot de hoeveelheden LNG die gebruikt worden in het gassysteem. Dit kan bijvoorbeeld bij een terminal gaan om 500 GWh per dag. Als een klein deel van deze capaciteit wegvalt, bijvoorbeeld 10 GWh per dag, zal dat weinig tot geen impact hebben op de gaslevering. Bij een hogere capaciteitsuitval, zoals bij 150 GWh per dag, kan dit wel het geval zijn. 150 GWh per dag komt ongeveer overeen met halvering van de capaciteit voor een halve dag per LNG-systeembeheerder. Verstoringen van 150 GWh per dag of meer zouden daarmee relevant kunnen zijn voor de leveringszekerheid op nationaal niveau.

Artikel 11. gasopslagbeheerder

Artikel 11 regelt dat een gasopslagbeheerder dient te melden indien een incident gevolgen heeft of kan hebben voor de injectie, productie en opslag van ten minste 150 GWh gas per dag. Dit criterium heeft geen betrekking op gasopslagbeheerders van seizoensopslagen, aangezien hier een apart criterium in artikel 12 voor is opgenomen. Het waarborgen van de continuïteit van deze essentiële diensten is essentieel voor de balanshandhaving van het gassysteem, ook tijdens piekperiodes, en om de leveringszekerheid van gas te waarborgen. Met injectie en productie wordt bedoeld het injecteren van gas in een gasopslagsysteem en het produceren van gas uit een gasopslagsysteem. Er is voor 150 GWh per dag gekozen, in tegenstelling tot 100 GWh per dag die gehanteerd werd in de Wbni, omdat dit passender is bij de werking van het gasopslagsystemen en de bedrijfsvoering van gasopslagbeheerders. Er zijn bepaalde reserves en daarmee redundantie ingebouwd waardoor uitval van minder dan 150 GWh per dag geringe impact heeft op de leveringszekerheid van gas. Daarbij is deze drempelwaarde geharmoniseerd met die voor LNG-systeembeheerders.

Artikel 12. gasopslagbeheerder van seizoensopslagen

Voor een gasopslagbeheerder van seizoensopslagen geldt een ander meldcriterium dan de criteria voor gasopslagbeheerders in artikel 11, aangezien de drempelwaarde van 150 GWh per dag niet toepasbaar en uitvoerbaar is. Voor een gasopslagbeheerder van seizoensopslagen geldt, op grond van artikel 12 een meldplicht indien een incident gevolgen heeft of kan hebben voor de normale werking van het gasopslagsysteem van seizoensopslagen, met inbegrip van injectie, productie en opslag. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de werking van het gasopslagsysteem. De verantwoordelijkheid voor de inschatting wanneer het gasopslagsysteem van seizoenopslagen normaal of abnormaal functioneert ligt bij de gasopslagbeheerder. Er is hier voor een generiek criterium gekozen, aangezien de seizoensopslagen zowel technisch als in capaciteit verschillend van aard zijn. Er kan daarbij gekeken worden naar de afwijking ten opzichte van de nominatie voor de asset. Het betreft weggevallen commerciële injectie-, productie- of opslagcapaciteit, wat kan leiden tot een directe onbalans tussen vraag en aanbod van gas, wat bij technische beschikbaarheid niet het geval is. Ondanks dat er verschil zit in impact bij gereduceerde injectie- of productiecapaciteit, is ervoor gekozen hier geen onderscheid in te maken, aangezien de impact van geval tot geval kan verschillen, waarbij de timing van het incident een cruciale factor is.

Artikel 13. aardgasbedrijf dat een gasproductienet beheert

Gasproductienetten zijn van groot belang voor de gasleveringszekerheid, omdat het transport van offshore gas naar een verwerkingsinstallatie, terminal of aanlandingsterminal mogelijk maakt en verwerking van dit gas faciliteert. Artikel 13 regelt dat een aardgasbedrijf dat een gasproductienet beheert moet melden zodra een incident gevolgen heeft of kan hebben voor de normale werking van productie, behandeling of invoeding van gas in het transmissiesysteem voor gas. Er is voor een generiek criterium gekozen in plaats van een specifieke drempelwaarde, omdat de ernst van de verstoring van de normale werking van een gasproductienet per moment kan verschillen.

Onder de normale werking van een gasproductienet wordt verstaan: het beschikbaar hebben van de productie-, behandelings- en invoedingscapaciteit, rekening houdend met geplande werkzaamheden en ongeplande verstoringen die gangbaar zijn binnen de industrie. Tevens omvat de normale werking het gehele productieproces om gas afkomstig van offshore gasproducenten binnen de Nederlandse Exclusieve Economische Zone (EEZ) via het gaspijpleidingstelsel te behandelen in een verwerkingsinstallatie, zodat het gas geschikt wordt voor het invoeden in het gastransportnet van de transmissiesysteembeheerder voor gas.

Van een aanzienlijke verstoring van de normale werking van het gasproductienet is sprake wanneer deze processen ongepland en gedurende langere tijd geheel of gedeeltelijk worden onderbroken, waardoor het transport van gas van offshore productieplatformen binnen de Nederlandse EEZ naar een verwerkingsinstallatie, terminal of aanlandingsterminal niet of in significant mindere mate mogelijk is. Verstoringen die binnen de ontwerpmarges van het gasproductienet kunnen worden opgevangen en geen gevolgen hebben voor de continuïteit van de gaslevering, worden niet aangemerkt als een aanzienlijke verstoring van de normale werking van het gasproductienet. De verantwoordelijkheid voor de inschatting wanneer de normale werking van een gasproductienet verstoord is, ligt bij het aardgasbedrijf dat een gasproductienet beheert.

Paragraaf 1.4. Criteria aanzienlijke verstoring voor de subsector olie

In deze regeling is geen drempelwaarde opgenomen voor de exploitanten van de voorziening voor de productie van olie, gezien er in Nederland relatief weinig aardolie wordt geproduceerd en er geen kritieke entiteiten zijn voorzien in deze categorie.

Voor kritieke entiteiten binnen de oliesector geldt over het algemeen dat een verstoring van een essentiële dienst in de regel minder snel directe en acute gevolgen heeft voor de leveringszekerheid van energie dan in de gas- of elektriciteitssector. Dit hangt onder andere samen met het karakter van de oliesector als niet-gereguleerde, internationale markt. Er bestaat echter verschil tussen diverse categorieën van entiteiten binnen de oliesector en de mate waarin een verstoring doorwerkt naar de continuïteit van de energievoorziening.

Paragraaf 1.4 vermeldt op diverse plekken olieproducten. Dat zijn geraffineerde vloeibare brandstoffen en gasvormige LPG. Omdat raffinaderijen een veelheid aan producten importeren, raffineren, behandelen, verladen en (tijdelijk) opslaan, is de productstroom gespecificeerd en beperkt tot die producten, waarvan een onvoorziene productiestop als gevolg van een verstoring kan leiden tot een aanzienlijke impact op de leveringszekerheid van energie.

Artikel 14. exploitant van oliepijpleidingen

Op grond van artikel 14 geldt voor de exploitanten van oliepijpleidingen dat er gemeld dient te worden indien het incident gevolgen heeft of kan hebben op het transport van olie of olieproducten via leidingen dat voor ten minste 24 uur verstoord is. Dit betekent dat er geen transport van olie of olieproducten mogelijk is. Gezien de mate van redundantie van leidingen voor transport van olie of olieproducten en met het oog op eventuele cascade-effecten voor (importafhankelijke) buurlanden, is de melddrempel op deze wijze vastgesteld. Het opnemen van deze melddrempel draagt er ook toe bij dat risico's tijdig kunnen worden onderkend, zowel op nationaal als op internationaal niveau.

Artikel 15. exploitant van de voorziening voor de raffinage en behandeling van olie

Artikel 15 regelt dat gemeld dient te worden indien de raffinage en behandeling van voor ten minste 72 uur verstoord is of kan worden, met een impact op de levering van ten minste 250.000 vaten per dag (250 kb/d). De gecombineerde drempel doet recht aan het specifieke karakter van raffinage en behandeling, waarbij de gevolgen van verstoring sterk afhankelijk zijn van de marktsituatie en de beschikbaarheid van alternatieven. Met de gekozen drempel wordt aangesloten bij het gegeven datkortdurende of kleinschalige uitval in de praktijk veelal kan worden opgevangen zonder merkbare effecten voor afnemers, mede door de hoge liquiditeit van de markt en de sterke internationale verwevenheid van de Nederlandse raffinagesector. Wanneer een verstoring gedurende meerdere dagen aanhoudt én een substantieel deel van de totale capaciteit raakt, is het aannemelijk dat de levering van deze essentiële dienst beïnvloed wordt. Een voorbeeld hiervan is dat merkbare effecten optreden, zoals op de levering of de tijdigheid van de levering. Door de drempel te stellen op 72 uur met een impact op de levering van ten minste 250.000 vaten per dag, is de meldplicht gericht op situaties die daadwerkelijk als aanzienlijk verstorend kunnen worden aangemerkt, terwijl tegelijkertijd wordt voorkomen dat tijdelijke, beheersbare of lokaal op te vangen incidenten leiden tot onnodige meldingen en extra regeldruk.

Artikel 16. exploitant van de voorziening voor de opslag van olie of olieproducten

Op grond van artikel 16 geldt voor de opslag van olie of olieproducten dat er gemeld dient te worden indien het incident gevolgen heeft of kan hebben voor de opslag van olie of olieproducten, dat voor tenminste 72 uur verstoord is en gevolgen heeft voor de levering van ten minste 100.000m3 olie(producten). Ook bij de opslag van olie(producten) kunnen de gevolgen afhankelijk zijn van de marktsituatie en de beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld waarbij rekening is gehouden met de cumulatieve effecten van uitval van kritieke entiteiten, omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de

leveringszekerheid. Om dit te ondervangen is gekozen voor het volume van 100.000m3. Gecombineerd met de minimumduur van 72 uur, is de meldplicht gericht op situaties die daadwerkelijk als aanzienlijk verstorend kunnen worden aangemerkt, terwijl tegelijkertijd wordt voorkomen dat tijdelijke, beheersbare of lokaal op te vangen incidenten leiden tot onnodige meldingen en extra regeldruk.

Artikel 17. exploitant van de opslag van olie of olieproducten die voorraadplichtig is

Op grond van artikel 17 dient er gemeld te worden indien een incident gevolgen heeft of kan hebben voor het niet beschikbaar hebben van de wettelijke olievoorraad voor meer dan 72 uur. *Wettelijke olievoorraad* is als begripsbepaling opgenomen in artikel 1. Deze begripsbepaling verwijst naar de begripsbepaling *wettelijke voorraad* in de Wet voorraadvorming aardolieproducten 2012 (Wva) en betreft de voorraad aardolieproducten waarmee wordt beoogd aan de voor Nederland geldende internationale verplichtingen te voldoen. Voor een tijdsduur van 72 uur is gekozen omdat in deze tijdspanne de centrale entiteit voor de voorraadvorming van aardolie de mogelijkheid heeft om naar andere opslaglocaties uit te wijken voor een eventuele inzet van de strategische voorraad. Met het niet beschikbaar hebben van de wettelijke olievoorraad wordt impliciet een drempel van 0 m^3 bedoeld. Dit houdt in dat elke vermindering van de feitelijke beschikbaarheid van de strategische voorraad, ongeacht de omvang, gemeld moet worden indien dit langer dan 72 uur voortduurt. Hier is voor gekozen omdat strategische voorraden altijd beschikbaar moeten zijn. Nederland is wettelijk gehouden een minimale hoeveelheid strategische olievoorraden aan te houden op grond van de Wva. Een incident dat ertoe leidt of kan leiden dat (een deel van) deze voorraad niet beschikbaar is, raakt direct aan deze wettelijke verplichting en dient daarom onverwijld te worden gemeld. De keuze voor de drempel houdt verband met het feit dat Nederland zich reeds op de ondergrens van de minimale wettelijke verplichting bevindt. Indien een voorraadplichtige entiteit een deel van de aan haar toevertrouwde strategische voorraad niet beschikbaar heeft, betekent dit dat Nederland niet langer voldoet aan de verplichtingen uit hoofde van de Wva.

Artikel 17 geldt voor kritieke entiteiten die op grond van een overeenkomst met Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA) voorraadplichtig zijn belast met het beheer van (een deel van) de wettelijke olievoorraden. Voor een voorraadplichtige kritieke entiteit beperkt de meldplicht zich derhalve tot incidenten die betrekking hebben op de daadwerkelijke fysieke opslag van strategische voorraden, aangezien zij uitsluitend voor dit onderdeel verantwoordelijk zijn en niet voor de overige beheertaken met betrekking tot de wettelijke olievoorraden. In de praktijk zal doorgaans eerst de betrokken voorraadplichtige kritieke entiteit melding doen, aangezien zij in de regel als eerste kennisneemt van een incident. Vervolgens zal op grond van artikel 18, ook COVA, vanuit haar systeemverantwoordelijkheid, een melding verrichten.

Ten slotte kan het voorkomen dat een opslagterminal tevens strategische voorraden beheert voor andere lidstaten. De als kritiek aangewezen voorraadplichtige entiteiten zijn uitsluitend meldplichtig onder het regime van de Wet weerbaarheid kritieke entiteiten en de daarop gebaseerde regelgeving, voor zover het incident betrekking heeft op de beschikbaarheid van de Nederlandse strategische voorraden. Incidenten bij voorraden van andere lidstaten vallen buiten de reikwijdte van deze meldplicht.

Artikel 18. COVA

Op grond van artikel 18 dient COVA te melden indien een incident gevolgen heeft of kan hebben voor het beheer van wettelijke olievoorraden. Met wettelijke voorraad wordt zoals bedoeld in de Wet voorraadvorming aardolieproducten 2012, de voorraad aardolieproducten waarmee wordt beoogd aan de voor Nederland geldende internationale verplichtingen te voldoen. Deze strategische voorraden worden aangehouden om Nederland weerbaar te maken bij verstoringen van de olietoevoer. Het beheer omvat het selecteren van opslaglocaties, het inkopen en verkopen van voorraden, en het bewaken van de productkwaliteit. De strategische olievoorraden zijn van essentieel belang voor het waarborgen van de leveringszekerheid van olie. Om die reden dienen incidenten te worden gemeld die (mogelijk) aanzienlijke gevolgen hebben op het beheer van deze wettelijke olievoorraden.

Paragraaf 1.5. Geplande onderbreking

Artikel 19. Geplande onderbreking

Op grond van artikel 19 hoeft een geplande onderbreking of opschorting, door bijvoorbeeld onderhoudswerkzaamheden en de daarbij behorende gevolgen, niet te worden gemeld. Onderhoudswerkzaamheden die leiden tot beperkte beschikbaarheid of niet-beschikbaarheid van de essentiële dienst worden niet als aanzienlijke verstoringen worden beschouwd indien de beperkte beschikbaarheid of niet-beschikbaarheid van de essentiële dienst plaatsvindt volgens een geplande onderhoudsactiviteit. Wanneer een essentiële dienst niet beschikbaar is als gevolg van geplande onderbrekingen, zoals

onderbrekingen, of niet-beschikbaarheid van diensten op basis van een vooraf bepaalde contractuele overeenkomst, wordt dit ook niet als een aanzienlijke verstoring beschouwd.

III. Artikelsgewijs (Cyberbeveiligingswet)

Artikel 20. begripsbepalingen

Deze regeling gebruikt veelal begrippen die ook in de Energiewet worden gehanteerd. Dit sluit aan bij het principe dat in wetgeving eenheid in terminologie wordt nagestreefd. Als de Energiewet een begrip niet bevat, is aangesloten bij andere Nederlandse wetgeving of een EU-verordening. Dit betekent dat er soms verschillen zijn met de omschrijving van 'soorten entiteiten' die zijn vermeld in bijlage 1, sector energie, bij de Cyberbeveiligingswet. Daar wordt bij verschillende soorten entiteiten immers verwezen naar begrippen in EU-richtlijnen en die begrippen zijn vervolgens in de Nederlandse wetgeving geïmplementeerd, met name in de Energiewet.

Artikel 20 bevat begripsbepalingen die van toepassing zijn op hoofdstuk 2: het Cyberbeveiligingswet-hoofdstuk van deze regeling. De begripsbepalingen *besluit* en *wet* zijn opgenomen, zodat duidelijk is dat deze begrippen in hoofdstuk 2 verwijzen naar het Cyberbeveiligingsbesluit en de Cyberbeveiligingswet, en niet naar het Besluit weerbaarheid kritieke entiteiten en de Wet weerbaarheid kritieke entiteiten.

Paragraaf 2.2 Criteria ernstige operationele verstoring voor de subsector elektriciteit

Paragraaf 2.1 bevat een uitwerking van artikel 25, tweede lid, onderdeel a, van de Cyberbeveiligingswet. Voor de soorten entiteiten binnen de elektriciteitssector is de leveringszekerheid waaronder zekerheid van netbeschikbaarheid, transport en netbalans, als uitgangspunt genomen voor de totstandkoming van de meldcriteria.

Artikel 22. Transmissiesysteembeheerder, interconnectorsysteembeheerder en distributiesysteembeheerder voor elektriciteit

Algemeen

Artikel 22 regelt dat transmissie-, interconnector, en distributiesysteembeheerders voor elektriciteit een melding moeten doen indien een incident leidt of kan leiden tot 100 MW geaggregeerd niet getransporteerde elektriciteit. Omdat de factor tijd in deze berekening is verdisconteerd, is gekozen voor een uniforme drempelwaarde. Bij de toepassing van de melddrempel van 100 MW dient rekening te worden gehouden met de redundantie die in het elektriciteitssysteem is ingebouwd. Er is daarom gekozen om met deze drempelwaarde aan te sluiten op het N-1-criterium dat wordt toegepast op het ontwerp van elektriciteitsnetten dat garandeert dat de stroomvoorziening blijft werken ook als één component van het net uitvalt. Tevens sluit de kwantificering van dit criterium aan bij bestaande meldplichten in andere wet- en regelgeving, zoals in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

De drempelwaarde is weergegeven in weggevallen vermogen uitgedrukt in MW. Het betreft zowel weggevallen momentaan vermogen als het vermogen dat gepland was om te worden getransporteerd, maar door het incident niet kon worden getransporteerd. Voor het berekenen van het vermogen wordt uitgegaan van het momentane of geplande gebruik, niet van de maximale transmissie- of distributiecapaciteit. Dit omdat het gaat om de daadwerkelijke impact van een incident en niet om de theoretische capaciteit die getransporteerd had kunnen worden.

Een incident waarbij een component van het systeem uitvalt, maar er door N-1-maatregelen geen impact is van 100 MW of meer op het momentane of geplande vermogen op het transmissie- of distributienet, raakt daarmee derhalve niet de drempelwaarde en hoeft niet te worden gemeld. Het kan dus zijn dat er een incident plaatsvindt, maar dat dit via N-1-maatregelen niet tot gevolgen leidt of had kunnen leiden zoals het direct omleiden van elektriciteit via andere elektriciteitslijnen en -stations. Hierdoor blijft uitval van 100 MW vermogen uit waardoor dit incident niet gemeld dient te worden. In gevallen waar er alsnog sprake is van een (tijdelijke) onderbreking van 100 MW of meer aan momentaan of gepland vermogen ondanks inzet van N-1-maatregelen, dient alsnog gemeld te worden.

Verschillende scenario's

Er moet aldus in verschillende scenario's gemeld dient worden. Bij momentaan gebruik is er in de regel sprake van gelijktijdigheid van het incident en de uitval van 100 MW getransporteerde elektriciteit. De transmissie- en distributiesysteembeheerders dienen dus te melden zodra er kennis is genomen van een incident wat leidt of kan leiden tot 100 MW uitval van momentaan vermogen. Er

dient ook gemeld te worden in een situatie wanneer ten tijde van het incident niet 100 MW getransporteerd werd, maar dat voor een later moment bijvoorbeeld 200 MW ingepland (gepland vermogen) dat geen doorgang kon vinden door het incident. De maximale transportcapaciteit speelt geen rol bij het bepalen van het momentane of geplande vermogen. In beide gevallen gaat het dus om wegvallen van ten minste 100 MW vermogen wat niet direct opgelost kan worden en leidt tot te weinig transmissie- of distributiecapaciteit.

Een door een incident veroorzaakt tekort aan transmissienetcapaciteit van 100 MW of meer momentaan of gepland vermogen kan door de transmissienetbeheerder opgevangen worden door *redispatch* of andere (toekomstige) maatregelen, zoals *gridboosters* of *storage-as-transmission*. Op deze wijze kunnen congestie- of onbalansproblemen opgelost worden. In een dergelijk geval dient echter wel gemeld te worden, omdat de beschikbare momentane of geplande netcapaciteit door het incident onbeschikbaar is geworden. Dit gaat ook op voor incidenten waarbij interconnectoren betrokken zijn. Indien ten minste 100 MW niet via een andere interconnector getransporteerd kon worden en er derhalve redispatching of andere balansinstrumenten moesten worden ingezet, wordt de melddrempel gehaald.

Balanshandhaving en marktfacilitering

Transmissiesysteembeheerders hebben naast transport van elektriciteit, ook de wettelijke taken voor balanshandhaving en marktfacilitering. Deze taken zijn nauw verbonden met de transmissie taak en het N-1-criterium. Het N-1-criterium zorgt ervoor dat een incident waarbij er sprake is van een enkelvoudige storing niet direct leidt tot congestie of onbalans op het net waardoor het systeem de tijd heeft om congestie te voorkomen of de balans te herstellen door inzet van verschillende (balans-)instrumenten, zoals inzet van regel- of noodvermogen en redispatching. Een incident is ook meldplichtig als de oorzaak van het afgenomen vermogen van ten minste 100 MW niet het gevolg is van verminderde transmissiecapaciteit, maar veroorzaakt wordt door een verstoring van de balanshandhaving aan de zijde van de transmissiesysteembeheerder, bijvoorbeeld het niet kunnen activeren van regel- of noodvermogen. Ondanks het belang van de marktfaciliteringstaak van transmissiesysteembeheerders, is er op dit moment gekozen om deze voor nu buiten scope van de meldplicht te laten. Dit is in lijn met de aanpak voor de Gedelegeerde Verordening (EU) 2024/1366 van de Commissie van 11 maart 2024 tot aanvulling van Verordening (EU) 2019/943 van het Europees parlement en de Raad door middel van de vaststelling van een netcode inzake sectorspecifieke regels voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen. In die verordening worden eerst de resultaten van de Europese risicobeoordelingen afgewacht om te kunnen bepalen bij welke drempels deze taak en daarmee leveringszekerheid in het geding komt.

Artikel 23. elektriciteitsproducent en marktdeelnemer

Artikel 23 regelt dat marktdeelnemers en elektriciteitsproducenten een melding moeten doen indien een incident leidt of kan leiden tot het niet beschikbaar zijn van 100 MW geaggregeerd vermogen. Dit niet beschikbare vermogen heeft betrekking op het netto vermogen van de essentiële of belangrijke entiteit. Het gaat derhalve over de gevolgen van het incident voor de totale capaciteit van de assets die ingezet kunnen worden. Een ernstige operationele verstoring met betrekking tot het beschikbare vermogen kan leiden tot onbalans van het elektriciteitssysteem tenzij de desbetreffende asset niet in gebruik is of was uitgeschakeld. Deze drempelwaarde heeft betrekking op zowel afname als invoer op het transmissie- of distributiesysteem voor elektriciteit. Er wordt hier, in tegenstelling tot de drempelwaarde voor transmissie- en distributiesysteembeheerders, gerekend met het totale beschikbare vermogen van assets. Hiervoor is gekozen omdat voor de stabiliteit van het elektriciteitssysteem, de mate waarin capaciteit op korte termijn inzetbaar moet zijn om bijvoorbeeld fluctuaties op te vangen relevant is. Het wegvallen van het beschikbare vermogen beperkt deze flexibiliteit, ook als het vermogen op het moment van het incident niet daadwerkelijk werd benut. Door te rekenen met het beschikbare vermogen wordt beter inzicht verkregen in de potentiële impact van een incident op de leveringszekerheid en systeemstabiliteit.

Artikel 24. exploitant van laadpunten

Artikel 24 regelt dat exploitanten van laadpunten een melding moeten doen indien een incident leidt of kan leiden tot het niet beschikbaar zijn van 100 MW geaggregeerd vermogen. Deze drempelwaarde is gelijkgetrokken met die van elektriciteitsproducenten en marktdeelnemers, aangezien het uitgangspunt hetzelfde is. Het gaat hierbij om de impact die een mogelijk een incident heeft of kan hebben op de stabiliteit van het elektriciteitssysteem.

Artikel 25. elektriciteitsmarktbeheerder

Artikel 25 regelt dat elektriciteitsmarktbeheerders moeten melden indien een incident leidt of kan

leiden tot het niet tijdig kunnen plaatsvinden van de day-ahead- of intraday-koppeling ongeacht het verhandelde vermogen. Ook dient een incident gemeld te worden dat leidt of kan leiden tot een aantasting van de integriteit van de marktkoppeling waardoor mogelijk verkeerde prijzen ontstaan op de elektriciteitsmarkt. Indien de desbetreffende elektriciteitsmarktbeheerder terugvalprocedures inzet waardoor de day-ahead en intraday-koppeling alsnog tijdig kan plaatsvinden ondanks een incident, hoeft er niet gemeld te worden.

Artikel 26. leverancier van elektriciteit

Artikel 26 regelt dat leveranciers van elektriciteit moeten melden indien een incident gevolgen heeft of kan hebben voor de uitvoering van de contractuele kernverplichtingen van de leverancier voor ten minste 20.000 eindafnemers van elektriciteit. Het gaat hierbij om lopende leveringsovereenkomsten met eindafnemers. De drempelwaarde is in lijn met de overige drempelwaarden in deze regeling, zoals die voor distributiesysteembeheerders en leveranciers van gas. Een ernstige operationele verstoring bij een leverancier van elektriciteit leidt er niet toe dat eindafnemers geen elektriciteit meer geleverd krijgen. Een dergelijke verstoring heeft daarmee geen directe impact op de leveringszekerheid van energie, maar kan wel een marktverstorende werking hebben, waardoor de leveringszekerheid indirect wordt geraakt. Om deze reden is in dit criterium verwezen naar de kernverplichtingen van een leverancier die geraakt worden, namelijk de (wettelijke) verplichtingen waaraan leveranciers richting hun klanten moeten voldoen. Hierbij kan met name gedacht worden aan de kerntaken: 1) zorgdragen voor de inkoop, balancering en contractuitvoering, 2) juiste en tijdige facturatie van afgenomen energie en 3) correcte en tijdige verwerking van meetdata.
De Cbw hanteert het begrip ‘elektriciteitsbedrijf dat de functie van levering verricht’, dat voorkomt in EU-wetgeving. Dit begrip is inhoudelijk gelijk aan het hier gehanteerde begrip ‘leverancier’.

Paragraaf 2.2 Criteria ernstige operationele verstoring voor de subsector aardgas

Paragraaf 2.2 bevat een uitwerking van artikel 25, tweede lid, onderdeel a, van de Cyberbeveiligingswet. Voor de soorten van entiteiten binnen de gassector is voor het opstellen van meldcriteria gekeken naar het waarborgen van de leveringszekerheid van gas. Daarnaast sluit de kwantificering van de meldcriteria deels aan bij de al bestaande melddrempels onder huidige wet- en regelgeving, zoals in de Wbni. Voor sommige criteria, zoals voor LNG-systeembeheerders, is bewust afgeweken van bestaande melddrempels, gezien hun veranderende rol in het systeem. Dit wordt verder per artikel toegelicht. In de artikelen voor de subsector aardgas is geen onderscheid gemaakt tussen incidenten die betrekking hebben op hoogcalorisch en laagcalorisch gas; de vastgestelde drempels zijn op beide gastypen van toepassing.

Artikel 27. distributiesysteembeheerder voor gas

Op grond van artikel 27 geldt voor de distributiesysteembeheerders voor gas een meldplicht indien een incident gevolgen heeft of kan hebben voor de distributie van gas voor ten minste 20.000 eindafnemers. In tegenstelling tot het meldcriterium voor transmissiesysteembeheerders, is er voor distributiesysteembeheerders gekozen om te kijken naar de gevolgen voor het aantal eindafnemers omdat distributiesysteembeheerders vanuit hun rol en verantwoordelijkheid meer zicht hebben op het aantal eindafnemers. De gekwantificeerde drempel van 20.000 eindafnemers sluit aan bij de drempel voor de meldplicht onder de Wbni.

Artikel 28. transmissiesysteembeheerder voor gas

Voor transmissiesysteembeheerder geldt, op grond van artikel 28, een meldplicht indien een incident gevolgen heeft of kan hebben voor de normale werking van het transmissiesysteem van gas. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering. De werking van het transmissiesysteem voor gas wordt door het transmissiesysteem continu gemonitord door de transmissiesysteembeheerder. De transmissiesysteembeheerder is zelf verantwoordelijk voor de inschatting of het transmissiesysteem normaal functioneert. Hierbij wordt gekeken naar het functioneren van kritieke exit- of entrypunten van het gassysteem. Deze melddrempel betekent niet dat er altijd gemeld dient te worden door de transmissiesysteembeheerder als een exitpunt uitvalt. Het verschilt per geval en moment of een dergelijk exitpunt kritiek is voor de leveringszekerheid van gas, omdat er ook via andere wegen levering kan plaatsvinden. Voor andere scenario’s kan het wel van belang zijn om te melden, zoals bijvoorbeeld bij het uitvallen van een compressorsysteem of het niet kunnen voldoen aan de kwaliteitscriteria. Bovendien kan de normale werking van het gassysteem per seizoen verschillen, afhankelijk van de vraag naar gas. Het inschatten van gevolgen voor de normale werking van het transmissiesysteem vergt daarom een specifieke beoordeling per geval. Om deze redenen is afgezien van het vaststellen van een kwantitatieve melddrempel.

Artikel 29. interconnectorsysteembeheerder voor gas

Artikel 29 regelt dat een interconnectorsysteembeheerder voor gas moet melden zodra een incident gevolgen heeft of kan hebben voor de normale werking van het interconnectorsysteem voor gas. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering. Interconnectoren voor gas zijn van groot belang voor de gasleveringszekerheid, omdat het grensoverschrijdende handel mogelijk maakt. Dit vergroot de stabiliteit en verbetert de werking van de gasmarkt. De werking van het interconnectorsysteem werkt bij wijze als een 'aan- en uitknop'. Een aanzienlijke verstoring van het interconnectorsysteem kan daarom al snel leiden tot een volledige uitval van dit systeem waardoor gas bijvoorbeeld niet naar Nederland kan stromen of naar het land waarmee de interconnector verbonden is. Om deze reden is hier dus gekozen om geen kwantitatieve drempelwaarde op te nemen, maar een vergelijkbaar generiek criterium op te nemen als die voor de transmissiesysteembeheerder voor gas.

Artikel 30. LNG-beheerder

Artikel 30 regelt dat beheerders van een systeem voor LNG (vloeibaar gas) dienen te meldenindien een incident gevolgen heeft of kan hebben voor het LNG-systeem van ten minste 150 GWh per dag. LNG is belangrijk voor de gasleveringszekerheid in Nederland en Europa doordat het fungeert als een flexibele en gediversifieerde importbron via terminals. Het toenemende belang van LNG maakt dat er gekozen is voor 150 GWh per dag in plaats van het aanhouden van de 10 GWh per dag die gehanteerd werd in de Wbni. 10 GWh per dag als melddrempel is te laag in vergelijking tot de hoeveelheden LNG die gebruikt worden in het gassysteem. Dit kan bijvoorbeeld bij een terminal gaan om 500 GWh per dag. Als een klein deel van deze capaciteit wegvalt, bijvoorbeeld 10 GWh per dag, zal dat weinig tot geen impact hebben op de gaslevering. Bij een hogere capaciteitsuitval, zoals bij 150 GWh per dag, kan dit wel het geval zijn. 150 GWh per dag komt ongeveer overeen met halvering van de capaciteit voor een halve dag per LNG-systeembeheerder. Verstoringen van 150 GWh per dag of meer zouden daarmee relevant kunnen zijn voor de leveringszekerheid op nationaal niveau.

Artikel 31. gasopslagbeheerder

Artikel 31 regelt dat een gasopslagbeheerder dient te melden indien een incident gevolgen heeft of kan hebben voor de injectie, productie en opslag van ten minste 150 GWh gas per dag. Dit criterium heeft geen betrekking op gasopslagbeheerders van seizoensopslagen, aangezien hier een apart criterium in artikel 12 voor is opgenomen. Het waarborgen van de continuïteit van deze essentiële diensten is essentieel voor de balanshandhaving van het gassysteem, ook tijdens piekperiodes, en om de leveringszekerheid van gas te waarborgen. Met injectie en productie wordt bedoeld het injecteren van gas in een gasopslagsysteem en het produceren van gas uit een gasopslagsysteem. Er is voor 150 GWh per dag gekozen, in tegenstelling tot 100 GWh per dag die gehanteerd werd in de Wbni, omdat dit passender is bij de werking van het gasopslagsystemen en de bedrijfsvoering van gasopslagbeheerders. Er zijn bepaalde reserves en daarmee redundantie ingebouwd waardoor uitval van minder dan 150 GWh per dag geringe impact heeft op de leveringszekerheid van gas. Daarbij is deze drempelwaarde geharmoniseerd met die voor LNG-systeembeheerders.

Artikel 32. gasopslagbeheerder van seizoensopslagen

Voor een gasopslagbeheerder van seizoensopslagen geldt een ander meldcriterium dan de criteria voor gasopslagbeheerders in artikel 31, aangezien de drempelwaarde van 150 GWh per dag niet toepasbaar en uitvoerbaar is. Voor een gasopslagbeheerder van seizoensopslagen geldt, op grond van artikel 32 een meldplicht indien een incident gevolgen heeft of kan hebben voor de normale werking van het gasopslagsysteem van seizoensopslagen, met inbegrip van injectie, productie en opslag. Dit gaat om aanzienlijke verstoringen met als gevolg een tijdelijke of volledige onderbreking van de werking van het gasopslagsysteem. De verantwoordelijkheid voor de inschatting wanneer het gasopslagsysteem van seizoenopslagen normaal of abnormaal functioneert ligt bij de gasopslagbeheerder. Er is hier voor een generiek criterium gekozen, aangezien de seizoensopslagen zowel technisch als in capaciteit verschillend van aard zijn. Er kan daarbij gekeken worden naar de afwijking ten opzichte van de nominatie voor de asset. Het betreft weggevallen commerciële injectie-, productie- of opslagcapaciteit, wat kan leiden tot een directe onbalans tussen vraag en aanbod van gas, wat bij technische beschikbaarheid niet het geval is. Ondanks dat er verschil zit in impact bij gereduceerde injectie- of productiecapaciteit, is ervoor gekozen hier geen onderscheid in te maken, aangezien de impact van geval tot geval kan verschillen, waarbij de timing van het incident een cruciale factor is.

Artikel 33. aardgasbedrijf dat een gasproductienet beheert

Gasproductienetten zijn van groot belang voor de gasleveringszekerheid, omdat het transport van offshore gas naar een verwerkingsinstallatie, terminal of aanlandingsterminal mogelijk maakt en

verwerking van dit gas faciliteert. Artikel 33 regelt dat een aardgasbedrijf dat een gasproductienet beheert moet melden zodra een incident gevolgen heeft of kan hebben voor de normale werking van productie, behandeling of invoeding van gas in het transmissiesysteem voor gas. Er is voor een generiek criterium gekozen in plaats van een specifieke drempelwaarde, omdat de ernst van de verstoring van de normale werking van een gasproductienet per moment kan verschillen.

Onder de normale werking van een gasproductienet wordt verstaan: het beschikbaar hebben van de productie-, behandelings- en invoedingscapaciteit, rekening houdend met geplande werkzaamheden en ongeplande verstoringen die gangbaar zijn binnen de industrie. Tevens omvat de normale werking het gehele productieproces om gas afkomstig van offshore gasproducenten binnen de Nederlandse Exclusieve Economische Zone (EEZ) via het gaspijpleidingstelsel te behandelen in een verwerkingsinstallatie, zodat het gas geschikt wordt voor het invoeden in het gastransportnet van de transmissiesysteembeheerder voor gas.

Van een aanzienlijke verstoring van de normale werking van het gasproductienet is sprake wanneer deze processen ongepland en gedurende langere tijd geheel of gedeeltelijk worden onderbroken, waardoor het transport van gas van offshore productieplatformen binnen de Nederlandse EEZ naar een verwerkingsinstallatie, terminal of aanlandingsterminal niet of in significant mindere mate mogelijk is. Verstoringen die binnen de ontwerpmarges van het gasproductienet kunnen worden opgevangen en geen gevolgen hebben voor de continuïteit van de gaslevering, worden niet aangemerkt als een aanzienlijke verstoring van de normale werking van het gasproductienet. De verantwoordelijkheid voor de inschatting wanneer de normale werking van een gasproductienet verstoord is, ligt bij het aardgasbedrijf dat een gasproductienet beheert.

Artikel 34. leverancier van gas

Artikel 34 regelt dat leveranciers van gas, moeten melden indien een incident gevolgen heeft of kan hebben voor de uitvoering van de contractuele kernverplichtingen van de leverancier voor ten minste 20.000 eindafnemers van gas. Het gaat hierbij om lopende leveringsovereenkomsten met eindafnemers. De drempelwaarde is in lijn met de overige drempelwaarden in deze regeling, zoals die voor distributiesysteembeheerders en leveranciers van gas. Een ernstige operationele verstoring bij een leverancier van gas leidt er niet toe dat eindafnemers geen gas meer geleverd krijgen. Een dergelijke verstoring heeft daarmee geen directe impact op de leveringszekerheid van energie, maar kan wel een marktverstorende werking hebben, waardoor de leveringszekerheid indirect wordt geraakt. Om deze reden is in dit criteirum verwezen naar de kernverplichtingen van een leverancier die geraakt worden, namelijk de (wettelijke) verplichtingen waaraan leveranciers richting hun klanten moeten voldoen. Hierbij kan met name gedacht worden aan de kerntaken: 1) zorgdragen voor de inkoop, balancering en contractuitvoering, 2) juiste en tijdige facturatie van afgenomen energie en 3) correcte en tijdige verwerking van meetdata.

De Cbw hanteert het begrip ‘leveringsbedrijf voor gas’, dat voorkomt in EU-wetgeving. Dit begrip is inhoudelijk gelijk aan het hier gehanteerde begrip ‘leverancier’.

Paragraaf 2.4. Criteria ernstige operationele verstoringvoor de subsector aard olie

Paragraaf 2.4 bevat een uitwerking van artikel 25, tweede lid, onderdeel a, van de Cyberbeveiligingswet. Voor de soorten van entiteiten binnen de aardoliesector is voor het opstellen van de meldcriteria gekeken naar het waarborgen van de leveringszekerheid van aardolie. Voor essentiële en belangrijke entiteiten binnen de oliesector geldt over het algemeen dat een verstoring van een essentiële of belangrijke dienst in de regel minder snel directe en acute gevolgen heeft voor de leveringszekerheid van energie dan in de gas- of elektriciteitssector. Dit hangt onder andere samen met het karakter van de oliesector als niet-gereguleerde, internationale markt. Er bestaat echter verschil tussen diverse categorieën van entiteiten binnen de oliesector en de mate waarin een verstoring doorwerkt naar de continuïteit van de energievoorziening.

In deze regeling is geen nader criterium opgenomen voor de exploitanten van de voorziening voor de productie van olie, gezien er in Nederland relatief weinig aardolie wordt geproduceerd waardoor dit proces minder kritiek vanuit het oogpunt van leveringszekerheid.

Paragraaf 2.4 vermeldt op diverse plekken olieproducten. Dat zijn geraffineerde vloeibare brandstoffen en gasvormige LPG. Omdat raffinaderijen een veelheid aan producten importeren, raffineren, behandelen, verladen en (tijdelijk) opslaan is de productstroom gespecificeerd en beperkt tot die producten, waarvan een onvoorziene productiestop als gevolg van een verstoring kan leiden tot een aanzienlijke impact op de leveringszekerheid van energie.

Artikel 35. exploitant van oliepijpleidingen

Op grond van artikel 34 geldt voor de exploitanten van oliepijpleidingen, dat er gemeld dient te worden indien gevolgen heeft of kan hebben op het transport van olie of olieproducten via leidingen dat voor ten minste 24 uur verstoord is. Dit betekent dat er geen transport van olie of olieproducten mogelijk is. Gezien de mate van redundantie van leidingen voor transport van olie en/of olieproducten en met het oog op eventuele cascade-effecten voor (importafhankelijke) buurlanden, is er een melddrempel van 24 uur verstoring vastgesteld. Het opnemen van deze melddrempel draagt er ook toe bij dat risico's tijdig kunnen worden onderkend, zowel op nationaal als op internationaal niveau.

Artikel 36. exploitant van de voorziening voor de raffinage en behandeling van olie

Artikel 36 regelt dat gemeld dient te worden indien de raffinage en behandeling van voor ten minste 72 uur verstoord is of kan worden, met een impact op de levering van ten minste 250.000 vaten per dag (250 kb/d). De gecombineerde drempel doet recht aan het specifieke karakter van raffinage en behandeling, waarbij de gevolgen van verstoring sterk afhankelijk zijn van de marktsituatie en de beschikbaarheid van alternatieven. Met de gekozen drempel wordt aangesloten bij het gegeven dat kortdurende of kleinschalige uitval kan in de praktijk veelal worden opgevangen zonder merkbare effecten voor afnemers, mede door de hoge liquiditeit van de markt en de sterke internationale verwevenheid van de Nederlandse raffinagesector. Wanneer een verstoring gedurende meerdere dagen aanhoudt én een substantieel deel van de totale capaciteit raakt, is het aannemelijk dat de levering van deze essentiële of belangrijke dienst beïnvloed wordt. Een voorbeeld hiervan is dat merkbare effecten optreden zoals op de levering of de tijdigheid van de levering. Door de drempel te stellen op 72 uur met een impact op de levering van ten minste 250.000 vaten per dag, is de meldplicht gericht op situaties die daadwerkelijk als aanzienlijk verstorend kunnen worden aangemerkt, terwijl tegelijkertijd wordt voorkomen dat tijdelijke, beheersbare of lokaal op te vangen incidenten leiden tot onnodige meldingen en extra regeldruk.

Artikel 37. exploitant van de voorziening voor de opslag van olie of olieproducten

Op grond van artikel 37 geldt voor de opslag van olie of olieproducten dat er gemeld dient te worden indien het incident gevolgen heeft of kan hebben voor de opslag van olie of olieproducten, dat voor tenminste 72 uur verstoord is en gevolgen heeft voor de levering van ten minste 100.000m3 olie(producten). Ook bij de opslag van olie(producten) kunnen de gevolgen afhankelijk zijn van de marktsituatie en de beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld waarbij rekening is gehouden met de cumulatieve effecten van uitval van kritieke entiteiten, omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de leveringszekerheid. Om dit te ondervangen is gekozen voor het volume van 100.000m3. Gecombineerd met de minimumduur van 72 uur, is de meldplicht gericht op situaties die daadwerkelijk als aanzienlijk verstorend kunnen worden aangemerkt, terwijl tegelijkertijd wordt voorkomen dat tijdelijke, beheersbare of lokaal op te vangen incidenten leiden tot onnodige meldingen en extra regeldruk.

Artikel 38. exploitant van de opslag van olie of olieproducten die voorraadplichtigis

Op grond van artikel 38 dient er gemeld te worden indien een incident gevolgen heeft of kan hebben voor het niet beschikbaar hebben van de wettelijke olievoorraad voor meer dan 72 uur. *Wettelijke olievoorraad* is als begripsbepaling opgenomen in artikel 1. Deze begripsbepaling verwijst naar de begripsbepaling *wettelijke voorraad* in de Wet voorraadvorming aardolieproducten 2012 (Wva) en betreft de voorraad aardolieproducten waarmee wordt beoogd aan de voor Nederland geldende internationale verplichtingen te voldoen. Voor een tijdsduur van 72 uur is gekozen omdat in deze tijdspanne de centrale entiteit voor de voorraadvorming van aardolie de mogelijkheid heeft om naar andere opslaglocaties uit te wijken voor een eventuele inzet van de strategische voorraad. Met het niet beschikbaar hebben van de wettelijke olievoorraad wordt impliciet een drempel van 0m3 bedoeld. Dit houdt in dat elke vermindering van de feitelijke beschikbaarheid van de strategische voorraad, ongeacht de omvang, gemeld moet worden indien dit langer dan 72 uur voortduurt. Hier is voor gekozen omdat strategische voorraden altijd beschikbaar moeten zijn. Nederland is wettelijk gehouden een minimale hoeveelheid strategische olievoorraden aan te houden op grond van de Wva. Een incident dat ertoe leidt of kan leiden dat (een deel van) deze voorraad niet beschikbaar is, raakt direct aan deze wettelijke verplichting en dient daarom onverwijld te worden gemeld. De keuze voor de drempel houdt verband met het feit dat Nederland zich reeds op de ondergrens van de minimale wettelijke verplichting bevindt. Indien een voorraadplichtige entiteit een deel van de aan haar toevertrouwde strategische voorraad niet beschikbaar heeft, betekent dit dat Nederland niet langer voldoet aan de verplichtingen uit hoofde van de Wva.

Artikel 38 voorziet in een meldplicht voor essentiële en belangrijke entiteiten die op grond van een overeenkomst met Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA) voorraad-

plichtig zijn belast met het beheer van (een deel van) de wettelijke olievoorraden. Voor een voorraadplichtige essentiële of belangrijke entiteiten beperkt de meldplicht zich derhalve tot incidenten die betrekking hebben op de daadwerkelijke fysieke opslag van strategische voorraden, aangezien zij uitsluitend voor dit onderdeel verantwoordelijk zijn en niet voor de overige beheertaken met betrekking tot de wettelijke olievoorraden. In de praktijk zal doorgaans eerst de betrokken voorraadplichtige essentiële en belangrijke entiteit melding doen, aangezien zij in de regel als eerste kennisneemt van een incident. Vervolgens zal op grond van artikel 39, ook COVA, vanuit haar systeemverantwoordelijkheid, een melding verrichten.

Ten slotte kan het voorkomen dat een opslagterminal tevens strategische voorraden beheert voor andere lidstaten. De essentiële en belangrijke entiteiten met een voorraadplicht zijn uitsluitend meldplichtig onder het regime van de Cyberbeveiligingswet en de daarop gebaseerde regelgeving, voor zover het incident betrekking heeft op de beschikbaarheid van de Nederlandse strategische voorraden. Incidenten bij voorraden van andere lidstaten vallen buiten de reikwijdte van deze meldplicht.

Artikel 39. COVA

Op grond van artikel 39 dient COVA te melden indien een incident gevolgen heeft of kan hebben voor het beheer van wettelijke olievoorraden. Met wettelijke voorraad wordt zoals bedoeld in de Wet voorraadvorming aardolieproducten 2012, de voorraad aardolieproducten waarmee wordt beoogd aan de voor Nederland geldende internationale verplichtingen te voldoen. Deze strategische voorraden worden aangehouden om Nederland weerbaar te maken bij verstoringen van de olietoevoer. Het beheer omvat het selecteren van opslaglocaties, het inkopen en verkopen van voorraden, en het bewaken van de productkwaliteit. De strategische olievoorraden zijn van essentieel belang voor het waarborgen van de leveringszekerheid van olie. Om die reden dienen incidenten te worden gemeld die (mogelijk) ernstige operationele gevolgen hebben op het beheer van deze wettelijke olievoorraden.

Paragraaf 2.5. Criteria ernstige operationele verstoringvoor de subsectorstadsverwarming en stadskoeling

Artikel 40. Exploitant van stadsverwarming of stadskoeling

Artikel 40 bevat een nadere uitwerking van artikel 25, tweede lid, onderdeel a, van de Cyberbeveiligingswet. Voor dit criterium is gekeken naar de gehanteerde criteria binnen de sectoren elektriciteit en aardgas, aangezien aardgas en elektriciteit een belangrijke rol spelen in het produceren en leveren van warmte.

Artikel 40 onderdeel a, regelt dat exploitanten van stadsverwarming of stadskoeling als bedoeld in artikel 2, onderdeel 19, van Richtlijn (EU) 2018/2001, een melding moeten doen indien een incident gevolgen heeft of kan hebben voor de productie van warmte of koude van ten minste 20 MW vermogen. Voor de productie is aangesloten bij de criteria voor elektriciteit door te kijken naar de gevolgen die een incident heeft of kan hebben op het vermogen, uitgedrukt in MW. De drempelwaarde is uitgedrukt in het wegvallen van beschikbaar vermogen in MW en betreft gepland, maar niet geleverd vermogen. De drempelwaarde van 20 MW sluit aan bij artikel 6.14, eerste lid, van de Wet collectieve warmte. Die bepaling regelt dat een wijziging van zeggenschap bij een installatie van tenminste 20 MW aan de Minister van Klimaat en Groene Groei moet worden gemeld.

Op grond van artikel 40, onderdeel b, moeten exploitanten van stadsverwarming of stadskoeling een incident melden indien het incident gevolgen heeft of kan hebben voor de levering van warmte of koude voor ten minste 20.000 afnemers. Met andere woorden, deze melddrempel wordt bereikt indien een incident gevolgen heeft of kan hebben op ten minste 20.000 afnemers die geen warmte of koude meer ontvangen. Voor de levering van warmte en koude is aangesloten bij het criterium voor distributiesysteembeheerders van aardgas, namelijk het aantal afnemers dat getroffen is of kan worden. De functie van aardgas en warmte zijn in de kern namelijk hetzelfde: het verwarmen van huizen en gebouwen en gebruik in industriële processen.

Paragraaf 2.6. Geplande onderbreking

Artikel 41. geplande onderbreking

Op grond van artikel 41 hoeft een geplande onderbreking of opschorting, door bijvoorbeeld onderhoudswerkzaamheden en de daarbij behorende gevolgen, niet te worden gemeld. Onderhoudswerkzaamheden die leiden tot beperkte beschikbaarheid of niet-beschikbaarheid van de essentiële dienst worden niet als aanzienlijke verstoringen worden beschouwd indien de beperkte beschikbaarheid of

niet-beschikbaarheid van de essentiële dienst plaatsvindt volgens een geplande onderhoudsactiviteit. Wanneer een essentiële dienst niet beschikbaar is als gevolg van geplande onderbrekingen, zoals onderbrekingen of niet-beschikbaarheid van diensten op basis van een vooraf bepaalde contractuele overeenkomst, wordt dit ook niet als een aanzienlijke verstoring beschouwd.

Paragraaf 2.7 Nadere regels zorgplicht

Artikel 42. beleid over beveiliging van netwerk- en informatiesystemen

Dit artikel werkt artikel 6 van het Cyberbeveiligingsbesluit nader uit voor wat betreft het beleid ten aanzien van de beveiliging van netwerk- en informatiesystemen en ten aanzien van de managementsystematiek. Dit artikel regelt dat essentiële en de belangrijke entiteiten, als onderdeel van de managementsystematiek, de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's dienen te toetsen door te bepalen welke maatregelen worden gemonitord, gemeten, geanalyseerd en geëvalueerd, hoe dit gebeurt, wanneer dit plaatsvindt en wie is belast met deze verantwoordelijkheid. Dit is een doorlopend proces. Het doel van de managementsystematiek is ervoor te zorgen dat de netwerk- en informatiebeveiligingsrisico's van de organisatie inzichtelijk zijn, dat passende en evenredige maatregelen worden genomen om de risico's te beheersen en dat deze maatregelen structureel worden beoordeeld en waar nodig bijgesteld. Door in de systematiek vast te leggen welke maatregelen worden gemonitord, met welke methoden, met welke frequentie en door wie de beoordeling wordt uitgevoerd, ontstaat een sluitende cyclus van plannen, uitvoeren, toetsen en bijsturen. Opvolging van deze evaluatie en beoordeling dient plaats te vinden. Deze verplichting is niet in dit artikel opgenomen, aangezien dit al volgt uit artikel 6, vierde lid, en artikel 19 van het Cyberbeveiligingsbesluit. Daarmee wordt gewaarborgd dat het inzicht in de effectiviteit van de maatregelen actueel is en dat resultaten van deze cyclus tot verdere verbetering van de beveiliging leiden. Deze elementen sluiten aan bij de werkwijze die in de praktijk gebruikelijk is in managementsystemen voor informatiebeveiliging, en sluit aan bij internationale normen, zoals de ISO-normen.

Artikel 43. bedrijfscontinuïteit

Dit artikel werkt artikel 9, derde lid, van het Cyberbeveiligingsbesluit nader uit ten aanzien van het bedrijfscontinuïteitsplan.

Processen en procedures voor back-ups van software en gegevens

Op basis van artikel 9, tweede lid, van het Cyberbeveiligingsbesluit dient de belangrijke entiteit of essentiële entiteit processen en procedures voor back-ups van software en gegevens vast te stellen en toe te passen. De risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit zijn derhalve zowel relevant voor het bepalen van welke software en gegevens in back-ups dienen te worden opgenomen, als het bepalen van de hierna genoemde waarborgen.

De onderdelen van 42, eerste lid, omschrijven welke aspecten in de processen en procedures voor back-ups van software en gegevens terug dienen te komen. Het bepalen van hersteltijden, in het Engels ook wel bekend als *recovery time objective (RTO),* heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. Herstelpunten, in het Engels ook wel bekend als *recovery point objective (RPO),* heeft betrekking op de frequentie van de back-ups. Het voorschrift dat de processen en procedures dienen te waarborgen dat back-ups volledig zijn, ziet erop dat de processen en procedures dienen te waarborgen dat alle gegevens die nodig zijn voor het herstellen van de betreffende netwerk- en informatiesystemen zijn opgenomen, waaronder configuratiegegevens en gegevens die in cloudcomputingdiensten zijn opgeslagen. Dit is noodzakelijk om te waarborgen dat systemen en processen bij een herstel weer volledig functioneren. Daarnaast dienen de processen en procedures te waarborgen dat de back-ups nauwkeurig zijn. Hiermee wordt bedoeld dat de informatie in geval van herstel succesvol kan worden gebruikt, bijvoorbeeld door ervoor te zorgen dat de gegevens in de back-up zich in een staat bevinden die een succesvol herstel mogelijk maken

Daarnaast dienen de processen en procedures ervoor te zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups gewaarborgd worden, zodat de back-ups ook daadwerkelijk ingezet kunnen worden. Met integriteit wordt bedoeld dat de entiteit borgt dat de back-ups niet gemanipuleerd of beschadigd zijn door bijvoorbeeld derden. Dit voorkomt dat dat de geback-upte data is gewijzigd, beschadigd of aangetast tijdens het backupproces, de opslag of het herstel. Voor de beschikbaarheid is het in het van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door acties van kwaadwillenden, zoals ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups dient gewaarborgd te worden, om zo ongeautoriseerde toegang tot gegevens te voorkomen. Ook dienen de processen en procedures waarborgen te bevatten voor het herstellen van software en gegevens. Dit omvat zowel de wijze

waarop back-ups herstelt kunnen worden als het waarborgen dat back-ups wanneer noodzakelijk daadwerkelijk teruggezet kunnen worden. Een gangbare praktijk hierbij is periodiek testen van het terugzetten van back-ups, om zo de werking van back-ups in de praktijk te verifiëren en testen. Ten slotte dienen de processen en procedures te omschrijven hoe lang de betreffende back-ups bewaard moeten worden.

Bedrijfscontinuïteitsplan

De essentiële entiteit en belangrijke entiteit dient op grond van artikel 9, derde lid, Cyberbeveiligingsbesluit een bedrijfscontinuïteitsplan (hierna ook: plan) op te stellen, om zo voorbereid te zijn op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen en om op dergelijke incidenten goed en tijdig te kunnen reageren, om zo de duur en gevolgen van dergelijke incidenten te beperken. Op grond van artikel 42 dient de entiteit bij het opstellen van het plan rekening te houden met de risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit, zodat zij alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen.

De onderdelen van het tweede lid omschrijven de onderdelen die geadresseerd dienen te worden in het plan. Allereerst dient het plan het doel en de reikwijdte van het plan te bevatten, zodat de context van het bedrijfscontinuïteitsplan en het toepassingsbereik ervan op voorhand duidelijk is. Het ligt hierbij voor de hand dat de entiteit zich met name richt op de voor de entiteit kritieke processen van het bedrijf. Het vastleggen van de belangrijkste contacten en interne en externe communicatiekanalen in een bedrijfscontinuïteitsplan is van belang voor snelle, gecoördineerde actie en communicatie tijdens incidenten of crises. Hierbij kan gedacht worden aan contacten voor directe actie, zoals noodnummers van hulpdiensten, sleutelpersoneel in de organisatie zoals crisisteams, IT/OT-specialisten, directie, evenals externe partners als leveranciers, klanten of overheidsorganisaties. Wat betreft overheidsorganisaties kan in ieder geval gedacht worden aan de bevoegde autoriteit en het CSIRT waar significante incidenten gemeld dienen te worden. De voorwaarden voor activering en de-activering beschrijven in welke gevallen of onder welke omstandigheden het bedrijfscontinuïteitsplan of onderdelen geactiveerd dan wel gedeactiveerd wordt. De vereiste middelen, met inbegrip van back-ups en redundanties, beschrijven welke middelen nodig zijn om een goede uitvoering aan het bedrijfscontinuïteitsplan te geven. Ten slotte dient het bedrijfscontinuïteitsplan de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen te bevatten, om zo de overgang naar een normale bedrijfsvoering te waarborgen.

In de praktijk kan het bedrijfscontinuïteitsplan zoals hier bedoeld deel uitmaken van een algemeen bedrijfs- en continuïteitsplan van de belangrijke en essentiële entiteit. Het bedrijfscontinuïteitsplan kan bovendien uit verschillende deelplannen bestaan, zolang de integraliteit wordt gewaarborgd en gezamenlijk aan de onderdelen als bedoeld in het eerste lid wordt voldaan.

Artikel 44. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Eerste lid

Artikel 11, derde lid, van het Cyberbeveiligingsbesluit verplicht essentiële en belangrijke entiteiten om processen en procedures te hebben voor het onderhoud en beheer van haar netwerk- en informatiesystemen. Deze processen en procedures hebben ten minste betrekking op het configuratiebeheer en het wijzigingsbeheer van de netwerk- en informatiesystemen van de entiteit. In het eerste lid van onderhavig artikel uit de regeling is gespecificeerd dat deze procedures daarnaast ook ten minste betrekking dienen te hebben op beveiligingstesten en beveiligingspatchbeheer. Beveiligingstesten zijn noodzakelijk om vast te stellen of de getroffen maatregelen in de praktijk doeltreffend functioneren en of kwetsbaarheden tijdig aan het licht komen. Door structureel processen en procedures voor beveiligingstesten vast te leggen, wordt geborgd dat testen systematisch, herhaalbaar en volgens vooraf bepaalde criteria plaatsvinden. Dit voorkomt dat testen ad hoc of onvolledig worden uitgevoerd en draagt eraan bij dat tekortkomingen tijdig kunnen worden verholpen voordat deze tot incidenten leiden.

Tweede lid

Om potentiële risico's voor de beveiliging van netwerk- en informatiesystemen weg te nemen dienen essentiële en belangrijke entiteiten processen en procedures in te richten voor het toepassen van beveiligingspatches. Beveiligingspatchbeheer is van belang om bekende kwetsbaarheden in software en systemen tijdig te verhelpen en misbruik daarvan te voorkomen. Op grond van artikel 44, tweede lid, onderdeel a, geldt dat waar passend gecontroleerd moet worden of beveiligingspatches afkomstig zijn van betrouwbare bronnen en of de integriteit van deze patches gewaarborgd is. Dit vergt niet in alle gevallen handmatige actie van de essentiële entiteit of belangrijke entiteit. Zo is er bij reguliere

systeemupdates van besturingssystemen doorgaans al sprake van ingebouwde technische controles op herkomst en integriteit van beveiligingspatches. De essentiële en belangrijke entiteit dient zich hiervan dan wel te vergewissen. Op grond van onderdeel b geldt dat beveiligingspatches, waar passend, getest moeten worden voordat zij in de productieomgeving worden toegepast. De noodzaak van een dergelijke test is afhankelijk van de risico's die het installeren van de patch met zich meebrengt. Voornoemde stappen dragen ertoe bij dat de toepassing van patches geen nieuwe kwetsbaarheden of verstoringen veroorzaakt. Vervolgens bepaalt onderdeel c dat beveiligingspatches binnen een redelijke termijn nadat zij beschikbaar zijn moeten worden toegepast, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen op het gebied van cyberbeveiliging. Dit kan bijvoorbeeld het geval zijn voor het toepassen van beveiligingspatches op OT-systemen waarbij het belang van continuïteit van dienstverlening en de verouderde aard van veel industriële componenten een rol speelt. 'OT' verwijst naar 'Operationele Technologie'. Hierbij kan gedacht worden aan het ongepland stilzetten van kritieke bedrijfsprocessen van een entiteit ter uitvoering van de patch, terwijl de patch ook uitgevoerd kan worden op een al ingepland moment van breder onderhoud aan de netwerk- en informatiesystemen. Indien een essentiële of belangrijke entiteit hiervoor kiest, dient de motivatie voor het niet of niet direct toepassen van de beveiligingspatch gedocumenteerd te worden.

Derde lid, onderdeel a

Ter bescherming van hun netwerk- en informatiesystemen dienen essentiële entiteiten en belangrijke entiteiten op grond van dit onderdeel maatregelen te nemen tegen kwaadaardige en ongeoorloofde software. Typische oplossingen voor netwerkbeveiliging omvatten het gebruik van firewalls en *intrusion prevention systems* om de interne netwerken van de relevante entiteiten te beschermen, alsmede het gebruik van antivirussoftware om potentiële kwaadaardige software op te kunnen sporen.

Derde lid, onderdeel b

Op grond van dit onderdeel voeren essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uit op hun netwerk- en informatiesystemen en leggen zij de resultaten daarvan vast. Deze scans maken het mogelijk om inzicht te krijgen in bekende kwetsbaarheden in systemen en applicaties en vormen daarmee een belangrijk hulpmiddel om risico's tijdig te onderkennen. De entiteit voert de scans waar passend toe door rekening te houden met de blootstelling van systemen aan dreigingen en hun netwerktoegankelijkheid, alsmede met de kritikaliteit van die systemen voor de continuïteit van de dienstverlening en de potentiële impact van uitval of misbruik. Kwetsbaarheidsscans in OT-systemen vereisen vaak een andere aanpak dan IT-systemen vanwege het belang van de continuïteit van de operationele diensten of door verouderde apparatuur. Het is daarom aan de essentiële en belangrijke entiteiten om een passende vorm van kwetsbaarheidsscan in te zetten gegeven hun omgeving van netwerk- en informatiesystemen en de mogelijke risico's die zich daarvoor kunnen doen. Zo kan het in OT-omgevingen noodzakelijk zijn om dit op een passieve wijze vorm te geven om zo verstoring van processen te voorkomen. Door de resultaten te documenteren, kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.

Derde lid, onderdeel c

Op grond van dit onderdeel evalueren essentiële en belangrijke entiteiten hun blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van hebben ten aanzien van hun netwerk- en informatiesystemen. Dit is voor zover artikel 17 van het besluit daar niet reeds toe verplicht. Artikel 43, derde lid, onderdeel c, regelt daarmee aanvullend dat kwetsbaarheden uit de uitgevoerde kwetsbaarheidsscans van de essentiële of belangrijke entiteit of meldingen van interne werknemers ook geëvalueerd en verholpen dienen te worden. Door deze evaluatie structureel uit te voeren, ontstaat een actueel beeld van het risicolandschap en kan tijdig worden bepaald welke aanvullende maatregelen nodig zijn om de weerbaarheid te vergroten.

Derde lid, onderdeel d

Op grond van dit onderdeel nemen essentiële entiteiten en belangrijke entiteiten onverwijld maatregelen om kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen te verhelpen. Indien een kwetsbaarheid niet of op een later moment verholpen wordt dient de essentiële entiteit en belangrijke entiteit dit te motiveren en te documenteren. Evenals bij het niet toepassen van een beveiligingspatch wordt voor de toezichtspraktijk dan duidelijk waarom er wordt afgeweken en kan de toezichthouder oordelen of deze beslissing terecht is genomen.

Vierde lid, onderdeel a

Essentiële entiteiten en belangrijke entiteiten dienen ook te waarborgen dat bij incidenten met betrekking tot de beveiliging van een netwerk- en informatiesysteem de gevolgen voor andere netwerk- en informatiesystemen worden beperkt. Op grond van het vierde lid, onderdeel a, dienen essentiële entiteiten en belangrijke entiteiten diens netwerken te segmenteren overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het Cyberbeveiligingsbesluit bedoelde risicobeoordeling. Hierbij kunnen entiteiten zelf in acht nemen op welke wijze ze de netwerksegmentatie toepassen. Netwerksegmentatie gaat om het onderverdelen van systemen en netwerken in verschillende, van elkaar gescheiden segmenten, waardoor er geen automatische toegang is tussen systemen en netwerken. Daarbij wordt rekening gehouden wordt met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen. Een essentiële entiteit en een belangrijke entiteit doet er verstandig aan bij de netwerksegmentatie nadrukkelijk te betrekken of er sprake is van IT- en OT-systemen en deze waar mogelijk van elkaar te scheiden. Het zijn daarnaast goede praktijken om toegang tot een netwerk of zone te verlenen op basis van een beoordeling van de beveiligingsvoorschriften, om systemen die van cruciaal belang zijn voor de werking van de entiteit of voor de veiligheid in beveiligde zones te houden, en om een gedemilitariseerde zone in communicatiekanalen uit te rollen om te waarborgen dat communicatie die afkomstig is van of bestemd is voor haar netwerken beveiligd is. Andere goede praktijken zijn het specifieke netwerk voor het beheer van netwerk- en informatiesystemen te scheiden van het operationele netwerk van de entiteit, de kanalen voor netwerkbeheer te scheiden van ander netwerkverkeer, en de productiesystemen voor de diensten van de entiteit te scheiden van de systemen die worden gebruikt voor de ontwikkeling en tests, met inbegrip van back-ups.

Vierde lid, onderdeel b

Op grond van het vierde lid, onderdeel b, dienen essentiële en belangrijke entiteiten, waar passend, hun netwerk- en informatie te segmenteren van de systemen en netwerken van derden. Deze verplichting beoogt te voorkomen dat de beveiliging van de eigen netwerk- en informatiesystemen wordt ondermijnd door kwetsbaarheden of incidenten bij externe partijen waarmee wordt samengewerkt, zoals leveranciers, onderhoudspartners of dienstverleners. Door een duidelijke scheiding aan te brengen tussen interne en externe netwerken kan worden beperkt dat een beveiligingsincident of een kwetsbaarheid bij een derde partij zich verspreidt naar de systemen van de entiteit zelf. De mate waarin segmentatie noodzakelijk is, hangt af van de aard van de samenwerking en de gevoeligheid van de uitgewisselde gegevens. In de praktijk kan dit bijvoorbeeld worden vormgegeven door het toepassen van strikte toegangscontroles, het gebruik van beveiligde communicatiekanalen en het beperken van directe netwerkverbindingen met derden tot het strikt noodzakelijke.

Artikel 45. beveiligingsaspecten ten aanzien van toegangsbeleid

Het beleid, bedoeld in artikel 15, eerste lid, van het Cyberbeveiligingsbesluit, dient ook beleid te omvatten over bevoorrechte accounts en systeembeheeraccounts. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Systeembeheeraccounts zijn een specifieke categorie bevoorrechte accounts die worden gebruikt voor het beheer van systemen, zoals het uitvoeren van updates, het wijzigen van configuraties of het beheren van gebruikersrechten. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

Het tweede lid geeft nadere invulling aan het beleid voor bevoorrechte accounts en systeembeheeraccounts door te specificeren welke maatregelen en procedures moeten worden toegepast. Het beleid moet ervoor zorgen dat bij bevoorrechte en systeembeheeraccounts sterke identificatie- en authenticatieprocedures worden toegepast en dat autorisatie zorgvuldig wordt geregeld. Bij sterke authenticatie kan gedacht worden aan phishing-bestendige multifactorauthenticatie. Zo wordt de dreiging van phishing en ander misbruik van dergelijke accounts zoveel mogelijk tegengegaan. Daarnaast schrijft het lid voor dat de voorrechten van deze accounts zoveel mogelijk geïndividualiseerd en beperkt worden toegekend. Dit zorgt er voor dat misbruik beter te herleiden is tot specifieke accounts. Tevens is vastgelegd dat voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt. Dit verkleint tezamen het risico op misbruik of onbedoelde gevolgen van het inzetten van deze voorrechten.

Artikel 47. inwerkingtreding

De Wwke en de Cyberbeveiligingswet treden op hetzelfde moment in werking. Artikel 47 regelt dat deze regeling eveneens op dat moment in werking treedt. Hiermee wordt een uitzondering toegepast op de vaste verandermomenten voor regelgeving en de minimuminvoeringstermijn. Voor de

motivering bij het toepassen van deze uitzondering wordt verwezen naar het inwerkingtredingsbesluit bij de Wwke en de Cyberbeveiligingswet.

De Minister van Klimaat en Groene Groei,
S. van Veldhoven-van der Meer