Regeling van de Minister van Klimaat en Groene Groei van [PM datum], nr. WJZ/[PM nummer], 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 15, eerste lid, van het Besluit weerbaarheid kritieke entiteiten en de artikelen 19, 24, eerste lid, en 29 van het Cyberbeveiligingsbesluit;

Besluit:

Hoofdstuk 1. Wet weerbaarheid kritieke entiteiten: nadere criteria aanzienlijk verstorend effect

Paragraaf 1.1. Algemene bepalingen

Artikel 1. Begripsbepalingen

In dit hoofdstuk wordt verstaan onder:
gasopslagsysteem: gasopslagsysteem als bedoeld in artikel 1:1 van de Energiewet;
besluit: Besluit weerbaarheid kritieke entiteiten;
criteria: drempelwaarden als bedoeld in artikel 16, tweede lid, van het besluit, op basis waarvan wordt bepaald of een verstoring als gevolg van een incident aanzienlijk is;
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);
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;
injectie en productie: injectie van gas in en productie van gas uit een opslagsysteem;
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 ☐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;
wet: Wet weerbaarheid kritieke entiteiten;
wettelijke olievoorraden: wettelijke voorraad als bedoeld in artikel 1 van de Wet voorraadvorming aardolieproducten 2012.

Artikel 2. Reikwijdte

Dit hoofdstuk is van toepassing op kritieke entiteiten als bedoeld in artikel 6 van de wet die binnen de sector energie behoren tot de subsectoren:
a. elektriciteit;

b. gas;
c. olie.

Paragraaf 1.2. Nadere criteria meldplicht

Artikel 3. Nadere criteria aanzienlijk verstorend effect voor de subsector elektriciteit

Een verstoring is aanzienlijk als bedoeld in artikel 17, derde lid, van de wet en artikel 15, eerste lid, van het besluit, indien het incident gevolgen heeft of kan hebben voor:

a. de transmissie en distributie van elektriciteit van ten minste 100 megawatt afgenomen vermogen;
b. het beschikbaar vermogen van ten minste 100 megawatt bij een marktdeelnemer of elektriciteitsproducent;
c. het niet kunnen plaatsvinden van de day-ahead- of intradaykoppeling of aantasting van de integriteit daarvan, bij een elektriciteitsmarktbeheerder; of
d. de verkoop en wederverkoop van elektriciteit waarbij sprake is van een verstoring van de levering van elektriciteit aan ten minste 20.000 eindafnemers.

Artikel 4. Nadere criteria aanzienlijk verstorend effect voor de subsector gas

Een verstoring is aanzienlijk als bedoeld in artikel 17, derde lid, van de wet, en artikel 15, eerste lid, van het besluit, indien een incident gevolgen heeft of kan hebben voor:

a. de transmissie en distributie van gas voor ten minste 20.000 eindafnemers, of één of meer invoeders of gasopslagsystemen met als gevolg een aanzienlijke verstoring van de normale werking van het transmissie- of distributiesysteem voor gas;
b. de verkoop en wederverkoop van gas dat leidt tot een verstoring van de levering van gas aan ten tenminste 20.000 eindafnemers, ofwel één of meer invoerders of gasopslagsystemen met als gevolg een significante verstoring van de normale werking van het gasnet;
c. het LNG-systeem van ten minste 10 gigawattuur per dag; of
d. de injectie en productie, opslag, raffinage of behandeling van ten minste 100 gigawattuur gas per dag.

Artikel 5. Nadere criteria aanzienlijk verstorend effect voor de subsector aardolie

Een verstoring is aanzienlijk als bedoeld in artikel 17, derde lid, van de wet, en artikel 15, eerste lid, van het besluit, indien het incident gevolgen heeft of kan hebben voor:

a. het transport van olie of olieproducten via leidingen, dat voor ten minste 24 uur verstoord is;
b. de raffinage en behandeling van olie, dat voor ten minste 72 uur verstoord is en gevolgen heeft voor de levering van ten minste 50 kilo vaten per dag;
c. het beheer van de wettelijke olievoorraden;
d. de opslag van olie of olieproducten met gevolgen voor de levering van ten minste 100.000 m^3 olie of olieproducten.

Artikel 6. Geplande verstoringen

In afwijking van de artikelen 3, 4 en 5 is een verstoring niet aanzienlijk, indien de verstoring het gevolg is van een voorziene of geplande opschorting of beëindiging van een door de kritieke entiteit verleende essentiële dienst.

Hoofdstuk 2. Cyberbeveiligingswet: nadere criteria meldplicht, nadere regels zorgplicht en aanwijzing bevoegde autoriteiten

Paragraaf 2.1. Algemene bepalingen

Artikel 7. Begripsbepalingen

In dit hoofdstuk wordt verstaan onder:

gasopslagsysteem: gasopslagsysteem als bedoeld in artikel 1:1 van de Energiewet;

besluit: Cyberbeveiligingsbesluit;

criteria: de drempelwaarden die bepalen wanneer een incident significant is, binnen de parameters van artikel 25, tweede lid, van de wet;

day-aheadkoppeling: eenvormige day-aheadkoppeling als bedoeld in artikel 2, punt 26, van verordening (EU) 2015/1222 van de Commissie;

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);

exploitant van een laadpunt: exploitant van een laadpunt als bedoeld in artikel 2, punt 31, 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;

aardgas: gas als bedoeld in artikel 1.1 van de Energiewet;

injectie en productie: injectie van gas in en productie van gas uit een opslagsysteem;

intradaykoppeling: eenvormige intradaykoppeling als bedoeld in artikel 2, punt 27, van verordening (EU) 2015/1222 van de Commissie;

invoeders: invoeder 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;

transmissie- of distributiesysteem voor gas: transmissie- of distributiesysteem 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 8. 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 koeling;
c. aardolie;
d. aardgas;
e. waterstof.

Paragraaf 2.2. Nadere criteria meldplicht

Artikel 9. Nadere criteria ernstige operationele verstoring voor de subsector elektriciteit

Een operationele verstoring is ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, en artikel 24, eerste lid, van het besluit, indien het incident gevolgen heeft of kan hebben voor:

a. de transmissie en distributie van elektriciteit van ten minste 100 megawatt afgenomen vermogen;
b. het beschikbaar vermogen van ten minste 100 megawatt bij een marktdeelnemer, elektriciteitsproducent of een exploitant van een laadpunt;
c. het niet kunnen plaatsvinden van de day-ahead- of intradaykoppeling of aantasting van de integriteit daarvan, bij een elektriciteitsmarktbeheerder;
d. de verkoop en wederverkoop van elektriciteit waarbij sprake is van een verstoring van de levering van elektriciteit aan ten minste 20.000 eindafnemers.

Artikel 10. Nadere criteria ernstige operationele verstoring voor de subsector aardgas

Een operationele verstoring is ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, en artikel 24, eerste lid, van het besluit, indien een incident gevolgen heeft of kan hebben voor:

a. de transmissie en distributie van gas voor ten minste 20.000 eindafnemers of één of meer invoeders of gasopslagsystemen, met als gevolg een ernstige operationele verstoring van de normale werking van het transmissie- of distributiesysteem voor gas;
b. de verkoop en wederverkoop van gas dat leidt tot een verstoring van de levering van gas aan ten tenminste 20.000 eindafnemers;
c. één of meer invoerders of on gasopslagsystemen, met als gevolg een significante verstoring van de normale werking van het transmissie- of distributiesysteem voor gas;
d. het LNG-systeem van ten minste 10 gigawattuur per dag; of
e. de injectie en productie, opslag, , raffinage of behandeling van gas van ten minste 100 gigawattuur per dag gas.

Artikel 11. Nadere criteria ernstige operationele verstoring voor de subsector aardolie

Een operationele verstoring is ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, en artikel 24, eerste lid, van het besluit, indien het incident gevolgen heeft of kan hebben voor:

a. het transport van olie of olieproducten via leidingen, waarbij het transport voor ten minste 24 uur verstoord is;
b. de raffinage en behandeling van olie, waarbij dat voor ten minste 72 uur verstoord is en met een impact op de levering van ten minste 50 kilo vaten per dag;
c. het beheer van de wettelijke olievoorraden; of
d. de opslag van olie of olieproducten met gevolgen voor de levering van ten minste 100.000 m_3 olie of olieproducten.

Artikel 12. Nadere criteria ernstige operationele verstoring voor de subsector stadsverwarming en -koeling

Een operationele verstoring is ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, en artikel 24, eerste lid, van het besluit, indien het incident gevolgen heeft of kan hebben voor:

a. de productie van warmte of koude van ten minste 20 megawatt afgenomen vermogen;
b. de levering van warmte of koude voor ten minste 20.000 afnemers.

Artikel 13. Geplande verstoringen

In afwijking van de artikelen 9 tot en met 12, is een operationele verstoring niet ernstig indien de verstoring het gevolg is van een voorziene of geplande opschorting of beëindiging van een door de essentiële of belangrijke entiteit verleende essentiële dienst.

Paragraaf 2.3. Nadere regels zorgplicht

Artikel 14. Beleid over beveiliging van netwerk- en informatiesystemen

Als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het besluit, en ter uitvoering van artikel 19, van het besluit, bepaalt de essentiële entiteit of de belangrijke entiteit:

a. welke maatregelen voor het beheer van cyberbeveiligingsrisico's moeten worden gemonitord en gemeten, met inbegrip van processen en controles;
b. de methoden voor het monitoren, meten, analyseren en evalueren, al naargelang het geval, om te zorgen voor valide resultaten;
c. wanneer de monitoring en de meting moeten worden uitgevoerd;
d. wie verantwoordelijk is voor 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 deze resultaten moet analyseren en evalueren.

Artikel 15. Bedrijfscontinuïteit

1. Het bedrijfscontinuïteitplan, bedoeld in artikel 9, derde lid, van het besluit, houdt rekening met de uitgevoerde beoordeling en herbeoordeling 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 plan;
e. vereiste middelen, met inbegrip van back-ups en redundanties;
f. de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

2. De procedures, voor het maken, terugzetten en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens, bedoeld in artikel 9, tweede lid, van het besluit, omvatten in ieder geval:

a. hersteltijden;
b. herstelpunten;
c. waarborging van volledigheid en nauwkeurigheid van back-ups, ook configuratiegegevens en gegevens die zijn opgeslagen in cloudcomputingdiensten worden meegenomen;
d. passende waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
e. de wijze van herstel van software en gegevens uit back-ups;
f. bewaartermijnen.

Artikel 16. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

1. De procedures, bedoeld in artikel 11, derde lid, van het besluit, hebben betrekking op ten minste 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. De entiteiten legt de onderbouwing van een dergelijk besluit vast.

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 te detecteren en te voorkomen;
b. voert de essentiële entiteit of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit en legt zij de resultaten van deze scans vast;
c. evalueert de essentiële entiteit of belangrijke entiteit haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft, 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;
e. segmenteert de essentiële entiteit of belangrijke entiteit systemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het besluit bedoelde risicoanalyse.

4. De entiteit segmenteert, waar passend, haar systemen en netwerken van systemen en netwerken van derden.

Artikel 17. Beveiligingsaspecten ten aanzien van toegangsbeleid

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over bevoorrechte accounts en systeembeheeraccounts voor de logische en fysieke toegang tot netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, zorgt ervoor dat:

a. sterke identificatie-, authenticatie-, zoals multifactorauthenticatie, en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;
b. specifieke accounts worden opgezet die uitsluitend worden gebruikt voor systeembeheer, zoals installatie, configuratie, beheer of onderhoud;
c. voorrechten op het gebied van systeembeheer zoveel mogelijk worden geïndividualiseerd en beperkt;
d. systeembeheeraccounts alleen worden gebruikt om te verbinden met de systemen voor systeembeheer.

Paragraaf 2.4. Overige bepalingen

Artikel 18. Aanwijzing autoriteiten

De volgende autoriteiten zijn aangewezen als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet en artikel 29 van het besluit:

a. 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 19. Inwerkingtreding

[PM: Deze regeling treedt in werking met ingang van [DATUM] / de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.]

Artikel 20. Citeertitel

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

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

De Minister van Klimaat en Groene Groei,

Concept-toelichting

I. Algemeen

1. Inleiding

Deze regeling is van toepassing op entiteiten in de energiesector die onder de Wet weerbaarheid kritieke entiteiten (hierna ook: Wwke) of de Cyberbeveiligingswet (hierna ook: Cbw) vallen. Deze regeling is opgedeeld in twee hoofdstukken: een voor de Wwke en een voor de Cbw. Per paragraaf is vermeld op of de paragraaf bij de Wwke of de Cbw hoort.

2. Hoofdlijnen van de ministeriële regeling

Deze ministeriële regeling bevat nadere criteria inzake de meldplicht van significante incidenten als bedoeld in artikel 25, tweede lid van de Cbw en betreft de implementatie van artikel 23, derde lid, van de richtlijn (EU) 2022/2555 over cyberbeveiliging (NIS 2-richtlijn). Tevens bevat deze regeling nadere criteria inzake 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 de richtlijn (EU) 2022/2557 over de weerbaarheid van kritieke entiteiten (CER-richtlijn).

De terminologie en reikwijdte van de meldplicht verschillen tussen de Cbw en Wwke. Ten behoeve van 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 alsmede de uitvoerbaarheid en handhaafbaarheid voor de toezichthouders.

Tevens bevat deze regeling nadere regels inzake de zorgplicht als bedoeld in artikel 20 van het Cyberbeveiligingsbesluit (hierna ook: Cbb) De nadere invulling van de zorgplicht uit de Cbw en Cbb 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 Cbw en artikel 29 van het Cbb. De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

3. Wet weerbaarheid kritieke entiteiten

3.1 Algemene toelichting nadere criteria meldplicht

Meldplicht
De nadere 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 nadere criteria zijn van toepassing op de subsectoren en categorieën van entiteiten binnen de energiesector waarvoor de Minister van Klimaat en Groene Groei beleidsverantwoordelijk voor is. Het gaat daarbij om de sectoren: elektriciteit, gas, en aardolie. Voor wat betreft de subsector waterstof en subsector stadsverwarming- en koeling wordt de meldplicht onder de Wwke niet nader ingevuld omdat vooralsnog geen kritieke entiteiten zijn voorzien in deze subsectoren.

De meldplicht, zoals bedoeld in artikel 17 van de Wwke, ziet 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. De bewoording 'kan verstoren of kan veroorzaken' in de Wwke moet gelezen worden als 'een reële kans op een incident dat 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.

Fasen van 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 meldplicht (binnen 24 uur melden) start als 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 dat operationeel niet mogelijk is, doet zij 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 verstoord of kan verstoren. Hierbij moet in ieder geval worden gekeken naar de criteria voor de meldplicht. Daarnaast brengt de kritieke entiteit binnen een maand na de melding een gedetailleerd verslag uit.

Totstandkoming nadere criteria
Bij het opstellen van de nadere criteria van de meldplicht is afstemming gezocht met diverse energiepartijen, 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 borgen en onnodige regeldruk te beperken.

Op grond van artikel 16, 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 aanvullende criteria vaststellen voor het bepalen of sprake is van een aanzienlijke verstoring. Niet alle parameters om te bepalen wanneer een verstoring aanzienlijk is als bedoeld in artikel 17, derde lid, Wwke, zijn toepasbaar dan wel uitvoerbaar voor de categorieën van entiteiten binnen de energiesector. Daarom zijn aanvullende criteria uitgewerkt die beter aansluiten bij de essentiële diensten van kritieke entiteiten in de energiesector en die in sommige gevallen reeds worden gehanteerd als melddrempel, zoals in de Wbni.

Uitgangspunt bij het uitwerken van de nadere criteria van de meldplicht is het waarborgen van de continuïteit van de levering van essentiële diensten en de leveringszekerheid van energie. Voor het nader uitwerken van de aanzienlijke verstoring is gekeken naar de gevolgen van een operationele verstoring van de eigen essentiële dienst van de betrokken kritieke entiteit en niet aan de hand van de gevolgen voor derden. Er wordt hierbij geen onderscheid gemaakt tussen een fysieke of digitale oorzaak, omdat dit vaak nog niet bekend is in de eerste fase van de melding (binnen 24 uur). Deze uitgangspunten hebben als gevolg dat de nadere criteria van de meldplicht voor de sectoren elektriciteit, olie en gas geharmoniseerd zijn met de nadere criteria van de meldplicht onder de Cbw. Dit komt de uitvoerbaarheid voor kritieke entiteiten ook ten goede, omdat kritieke entiteiten van rechtswege een essentiële entiteit onder de Cbw zijn.

Conform artikel 17, vijfde lid, van de Wwke, is bij het opstellen van de nadere criteria voor de meldplicht onderscheid gemaakt tussen sectoren, subsectoren en categorieën van entiteiten. Generieke sectorale of subsectorale drempelwaarden doen onvoldoende 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 categorieën van entiteiten.

Hoofdstuk 4. Cyberbeveiligingswet

4.1 Algemene toelichting nadere criteria meldplicht

Meldplicht
De nadere criteria meldplicht in deze regeling beogen duidelijk te verschaffen wanneer de essentiële entiteit en belangrijke entiteit een melding dient te maken van een significant incident. Deze nadere regels zijn van toepassing op de energiesector en de daarbinnen genoemde subsectoren en soorten entiteiten waarvoor de Minister van Klimaat en Groene Groei beleidsverantwoordelijkheid voor is. Het gaat daarbij om de subsectoren: elektriciteit, aardgas, aardolie, stadsverwarming en -koeling en waterstof. Na toetsing bij de sector, heeft de Minister ervoor gekozen om nog geen nadere criteria 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 nadere criteria meldplicht voor de waterstofsector is daarom op dit moment niet proportioneel. Aangezien deze subsector in ontwikkeling is, zal er periodiek worden geëvalueerd of de nadere uitwerking van deze criteria opportuun is.

De meldplicht heeft betrekking op incidenten die als significant worden beschouwd. Een 'incident' is gedefinieerd in artikel 1 van de Cbw als: "*een gebeurtenis die de beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit van netwerk- en informatiesystemen of diensten die worden aangeboden, in gevaar brengt*." Een incident wordt volgens de Cbw, artikel 25, tweede lid, gekenmerkt als 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 'kan verstoren of kan veroorzaken' in de Cbw moet gelezen worden als 'een reële kans op een incident dat leidt tot een ernstige operationele verstoring 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 een ernstige operationele verstoring van de essentiële dienst.

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 Cbw 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 Cbw 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 tijd 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 vast te stellen of de gestelde parameters om te bepalen wanneer een incident significant is zoals bedoeld in artikel 25, lid 2 Cbw. Deze parameters betreffen ernstige operationele verstoring, of financiële verliezen voor de betrokken entiteit, of aanzienlijke materiële of immateriële schade behaald worden of kunnen worden en te melden indien nodig. De regels omtrent 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 Cbw (artikelen 26 tot en met 29) opgenomen en krijgen daarom in deze ministeriële regeling geen verdere uitwerking.

Totstandkoming nadere criteria
In artikel 24, eerste lid van het Cbb 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 Cbw. Bij het opstellen van de nadere criteria van de meldplicht is afstemming gezocht met diverse energiepartijen, 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 Wbni en sectorale regelgeving, om de uitvoerbaarheid en handhaafbaarheid te borgen en onnodige regeldruk te beperken.

Uitgangspunt bij het uitwerken van de nadere criteria van de meldplicht is het waarborgen van de continuïteit van de levering van essentiële diensten en de leveringszekerheid van energie. Voor het nader 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 nadere criteria van de meldplicht voor de sectoren elektriciteit, olie en gas geharmoniseerd zijn met de nadere criteria van de meldplicht onder de Wwke. Dit komt de uitvoerbaarheid voor kritieke entiteiten ook ten goede, omdat kritieke entiteiten van rechtswege een essentiële entiteit onder de Cbw zijn.

Op basis van deze gesprekken en uitgangspunten, is ervoor gekozen om alleen de parameter met betrekking tot de ernstige operationele verstoring, om te bepalen of er sprake is van een significant incident, nader uit te werken. De andere twee parameters als bedoeld in artikel 25, tweede lid, van de Cbw zijn namelijk niet voor alle subsectoren en soorten entiteiten toepasbaar dan wel uitvoerbaar. Daarom zijn er nadere 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 Wbni.

Conform artikel 25, derde lid, van de Cbw, is in deze regeling onderscheid gemaakt tussen sectoren, subsectoren en soorten entiteiten bij het nader 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.

De essentiële entiteit en belangrijke entiteit zijn verplicht significante incidenten te melden zodra de Cbw, het Cbb en deze regeling van kracht zijn.

4.2 Nadere regels zorgplicht

Algemene inleiding nadere regels zorgplicht

In deze ministeriële regeling worden voor de in artikel 2 genoemde sectoren nadere regels gesteld over de zorgplicht uit de Cbw en het Cbb. Het doel van deze nadere invulling is om de algemene normen uit de wet en het besluit verder te concretiseren op onderdelen die van groot belang zijn voor de beveiliging van netwerk- en informatiesystemen en die daarom als zodanig worden voorgeschreven. 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 Cbb 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 Cbb.

4.3 Aanwijzing autoriteiten

Voor een aantal wetten geldt dat deze nauwe raakvlakken hebben met de Cbw. Het is daarom gewenst dat de bevoegde autoriteiten, CSIRT's en het centrale contactpunt onder de Cbw (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 Cbw en artikel 29 van het Cbb.

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 Cbw 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 Cbw 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, Cbw gelden.

5. Regeldruk

Deze regeling veroorzaakt geen nieuwe regeldruk ten opzichte van de Wwke en het Besluit weerbaarheid kritieke entiteiten. De regeldruk voor kritieke entiteiten is verantwoord in de bijbehorende toelichtingen van het wetsvoorstel en het besluit. [PM resultaten indienen aanvraag ATR na consultatie en UHT]

De regeling veroorzaak geen nieuwe regeldruk ten opzichte van de Cbw en het Cbb. De regeldruk voor essentiële entiteiten en belangrijke entiteiten is verantwoord in de bijbehorende toelichtingen van het wetsvoorstel en het besluit. [PM resultaten indienen aanvraag ATR na consultatie en UHT]

6. Uitvoering

Voor deze regeling hebben de Rijksinspectie Digitale Infrastructuur (RDI) en het Staatstoezicht op de Mijnen (SodM) uitvoerings- en handhaafbaarheidstoets (UHT) uitgebracht. Als gevolg van deze toets [PM resultaten toets en beschrijving aanpassingen].

7. Consultaties

[PM internetconsultatie]

8. Evaluatie

Deze regeling zal periodiek worden geëvalueerd en waar nodig aangepast of aangevuld. Conform artikel 16, derde lid van het Bwke en artikel 24, tweede lid van het Cbb, evalueert de Minister van Klimaat en Groene Groei ten minste elke vier jaar de doeltreffendheid van de nadere regels van de meldplicht en de effecten daarvan in de praktijk en zal indien nodig aanpassingen doorvoeren.

II. Artikelsgewijs

Paragraaf 1.2 Nadere criteria meldplicht (Wwke)

Artikel 3 - nadere criteria aanzienlijk verstorend effect voor de subsector elektriciteit
Artikel 3 bevat een nadere uitwerking van artikel 17 van de Wwke en artikel 15 van het Bwke. Voor de categorieën van entiteiten binnen de elektriciteitssector is met oog op de leveringszekerheid, de operationele balans van het elektriciteitsnet als uitgangspunt genomen voor het ontwikkelen van melddrempels.

Artikel 3, onderdeel a, regelt dat transmissie- en distributiesysteembeheerders voor elektriciteit een melding moeten doen indien een incident leidt of kan leiden tot 100MW niet geleverde energie. De drempelwaarde is uitgedrukt in weggevallen vermogen (megawatt) en betreft gepland maar niet geleverd vermogen. Omdat de factor tijd in deze berekening is verdisconteerd, is gekozen voor een uniforme drempelwaarde. De melddrempel van 100MW is in lijn met het N-1-criterium en houdt rekening met de redundantie die in het elektriciteitssysteem is ingebouwd. Het N-1-criterium 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 Wbni.

Artikel 3, onderdeel b, regelt dat marktdeelnemers en elektriciteitsproducenten een melding moeten doen indien een incident leidt of kan leiden tot een niet beschikbaar vermogen van 100MW. Dit niet beschikbare vermogen heeft betrekking op het netto vermogen van de kritieke entiteit (capaciteit van de assets) omdat een verstoring met betrekking tot het beschikbare vermogen kan leiden tot onbalans van het elektriciteitsnet. Deze drempelwaarde heeft betrekking op zowel het gebruik als invoer (geleverde energie) op het elektriciteitsnet.

Artikel 3, onderdeel c, regelt dat elektriciteitsmarktbeheerders moeten melden indien een incident leidt of kan leiden tot het niet kunnen plaatsvinden van de day-ahead of intraday-koppeling ongeacht het verhandelde vermogen wat ermee gemoeid is. 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.

Op grond van artikel 3, onderdeel d, moeten energieleveranciers een melding doen indien een incident gevolgen heeft of kan hebben voor de verkoop of wederverkoop van elektriciteit dat leidt tot een verstoring van de levering van elektriciteit aan ten minste 20.000 eindafnemers. Met een eindafnemer wordt overeenkomstig artikel 1.1 van de Energiewet bedoeld: "een aangeslotene die elektriciteit of gas koopt of wil kopen voor eigen gebruik". Hiermee wordt geen onderscheid gemaakt tussen kleine of grote aansluitingen, omdat het niet duidelijk is wie er achter de aansluiting zit.

Artikel 4. Nadere criteria aanzienlijk verstorend effect voor de subsector gas
Artikel 4 bevat een nadere uitwerking van artikel 17 van de Wwke en artikel 15 van het Bwke. Voor de categorieën van entiteiten binnen de gassector is voor het opstellen van melddrempels gekeken naar het waarborgen van de leveringszekerheid. Daarnaast sluit de kwantificering van het meldcriterium aan bij de al bestaande melddrempel onder huidige wet- en regelgeving, zoals in de Wbni. 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.

Op grond van artikel 4, onderdeel a, geldt voor de transmissie- en distributiesysteembeheerders voor gas een tweeledige melddrempel. De ene melddrempel wordt bereikt indien een incident gevolgen heeft of kan hebben op 20.000 eindafnemers die geen gas meer ontvangen. Met een eindafnemer wordt zoals bedoeld in artikel 1.1 van de Energiewet, een aangeslotene die elektriciteit of gas koopt of wil kopen voor eigen gebruik. De andere melddrempel wordt bereikt

indien een incident gevolgen heeft of kan hebben voor invoeders en/of gasopslagsystemen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering, waardoor de normale werking van het gasnet aanzienlijk wordt verstoord.

Artikel 4, onderdeel b, regelt dat energieleveranciers een melding moeten doen indien een incident gevolgen heeft of kan hebben voor de verkoop of wederverkoop van gas dat leidt tot een verstoring van de levering van gas aan ten minste 20.000 eindafnemers. Met een eindafnemer wordt zoals bedoeld in artikel 1.1 van de Energiewet, een aangeslotene dat elektriciteit of gas koopt of wil kopen voor eigen gebruik. Hiermee wordt geen onderscheid gemaakt tussen kleine – of grote aansluitingen, omdat het niet duidelijk is wie er achter de aansluiting zit.

Artikel 4, onderdeel c, regelt voor *liquefied natural gas* (LNG)-systeembeheerders dat er gemeld dient te worden indien een incident gevolgen heeft of kan hebben voor het LNG-systeem van ten minste 10 GWh per dag. Hierbij gaat het om het systeem, als bedoeld in artikel 1.1. van de Energiewet, "dat gebruikt wordt voor het vloeibaar maken van gas, voor de invoer of de verlading, en voor de hervergassing van vloeibaar gas, met inbegrip van ondersteunende diensten en tijdelijke opslag die nodig zijn voor het proces van hervergassing en de daaropvolgende invoeding op het systeem, en met uitzondering van een LNG-systeem dat uitsluitend ten dienste staat van een transmissiesysteembeheerder voor gas bij de uitvoering van zijn wettelijke taken of verplichtingen."

Artikel 4, onderdeel d, regelt dat er gemeld dient te worden indien een incident gevolgen heeft of kan hebben voor de injectie en productie, opslag, raffinage of behandeling van ten minste 100GWh gas per dag. 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 opslagsysteem. Met opslag van gas wordt bedoeld het opslaan van gas in daarvoor bestemde gasopslagsystemen om daar op een later moment gebruik van te kunnen maken. Dit kunnen ondergronds gasopslagsystemen zijn, te weten voormalig gasvelden en voormalig zoutcavernes, en bovengrondse gasopslagsystemen, zoals bijvoorbeeld een peakshaverinstallatie. Bij raffinage en behandeling van gas gaat het om het bewerken/aanpassen van de samenstelling van het gas aan de geldende kwaliteitseisen of het geschikt maken voor transport, opslag en levering van gas.

Artikel 5. Nadere criteria aanzienlijk verstorend effect voor de subsector aardolie
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.

Op grond van artikel 5, onderdeel a, geldt voor de exploitanten van transmissieleidingen 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. 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 5, onderdeel b, 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 50 kilo vaten per dag (50kb/d). Bij raffinage en behandeling kunnen de gevolgen afhankelijk zijn van de marktsituatie en beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld met een langere tijdsduur alvorens een incident moet worden gemeld en is rekening gehouden met de cumulatieve effecten van uitval van kleinere kritieke entiteiten

omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de leveringszekerheid. Om dit te ondervangen is voor raffinage en behandeling een drempelwaarde van 72 uur met impact op de levering van tenminste 50 kilo vaten per dag.

Op grond van artikel 5, onderdeel c, dient er gemeld te worden 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 die (mogelijk) aanzienlijke gevolgen hebben op het beheer van deze wettelijke olievoorraden te worden gemeld.

Op grond van artikel 5, onderdeel d, geldt voor de opslag van olie of olieproducten dat er gemeld dient te worden indien het incident gevolgen heeft of kan hebben op de levering van ten minste 100.000m^3 olie en/of olieproducten. Ook bij de opslag van olie en/of olieproducten kunnen de gevolgen afhankelijk zijn van de marktsituatie en beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld waarbij rekening is gehouden met de cumulatieve effecten van uitval van kleinere kritieke entiteiten omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de leveringszekerheid. Om dit te ondervangen is voor op opslag van olie en/of olieproducten een drempelwaarde van 100.000m^3 vastgesteld.

Artikel 6 - Geplande verstoringen
Op grond van artikel 6 hoeft een geplande verstoring, door bijvoorbeeld onderhoudswerkzaamheden en de daarbij behorende gevolgen, niet te worden gemeld. Als onderhoud leidt tot een (mogelijke) aanzienlijke verstoring die op voorhand niet voorzien was, geldt de meldplicht wel.

<u>Paragraaf 2.2 Nadere criteria meldplicht (Cbw)</u>

Artikel 9. Nadere criteria ernstige operationele verstoring voor de subsector elektriciteit

Artikel 9 bevat een nadere uitwerking van artikel 25, tweede lid, onderdeel a, van de Cbw en artikel 24, eerste lid, van het Cbb. Voor de soorten entiteiten binnen de elektriciteitssector is met oog op de leveringszekerheid, de operationele balans van het elektriciteitsnet als uitgangspunt genomen voor het ontwikkelen van de melddrempels.

Artikel 9, onderdeel a, regelt dat transmissie- en distributiesysteembeheerders voor elektriciteit een melding moeten doen indien een incident leidt of kan leiden tot 100MW niet geleverde energie. De drempelwaarde is uitgedrukt in afgenomen (weggevallen) vermogen (megawatt) en betreft gepland maar niet geleverd vermogen. Omdat de factor tijd in deze berekening is verdisconteerd, is gekozen voor een uniforme drempelwaarde. De melddrempel van 100MW is in lijn met het N-1 criterium en houdt rekening met de redundantie die in het elektriciteitssysteem is ingebouwd. Het N-1 criterium 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 Wbni.

Artikel 9, onderdeel b, regelt dat marktdeelnemers, elektriciteitsproducenten en exploitanten van laadpunten een melding moeten doen indien een incident leidt kan leiden tot een niet-beschikbaar vermogen van 100MW. Dit niet beschikbare vermogen heeft betrekking op het netto vermogen van de essentiële entiteit en belangrijke entiteit (capaciteit van de assets), omdat een verstoring met betrekking tot het beschikbare vermogen kan leiden tot onbalans van het elektriciteitsnet. Deze drempelwaarde heeft betrekking op zowel het gebruik als invoer (geleverde energie) op het elektriciteitsnet.

Artikel 9, onderdeel c, regelt dat elektriciteitsmarktbeheerders moeten melden indien een incident leidt of kan leiden tot het niet kunnen plaatsvinden van de day-ahead- of intraday-koppeling ongeacht het verhandelde vermogen wat ermee gemoeid is. 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.

Op grond van artikel 9, onderdeel d, moeten energieleveranciers een melding doen indien een incident gevolgen heeft of kan hebben voor de verkoop of wederverkoop van elektriciteit dat leidt tot een verstoring van de levering van elektriciteit aan ten minste 20.000 eindafnemers. Met een eindafnemer wordt zoals bedoeld in artikel 1.1 van de Energiewet, "een aangeslotene dat elektriciteit of gas koopt of wil kopen voor eigen gebruik". Hiermee wordt geen onderscheid gemaakt tussen kleine- of grote aansluitingen, omdat op dit moment het niet duidelijk is wie er achter de aansluiting zit.

Artikel 10. Nadere criteria ernstige operationele verstoring voor de subsector aardgas

Artikel 10 bevat een nadere uitwerking van artikel 25, tweede lid, onderdeel a, van de Cbw en artikel 24, eerste lid, van het Cbb. Voor de soorten entiteiten binnen de gassector is voor het opstellen van melddrempels gekeken naar het borgen van de leveringszekerheid. Daarnaast sluit de kwantificering van het meldcriterium aan bij de al bestaande melddrempel onder huidige wet- en regelgeving, zoals in de Wbni. Binnen de melddrempels voor de subsector aardgas wordt geen onderscheid gemaakt of het incident betrekking heeft op hoogcalorisch dan wel laagcalorisch gas; de vastgestelde drempels zijn op beide gastypen van toepassing.

Op grond van artikel 10, onderdeel a, geldt voor de transmissie- en distributiesysteembeheerders van gas een tweeledige melddrempel. De ene melddrempel wordt bereikt indien een incident gevolgen heeft of kan hebben op 20.000 eindafnemers die geen gas meer ontvangen. Met een eindafnemer wordt zoals bedoeld in artikel 1.1. van de Energiewet, "een aangeslotene die elektriciteit of gas koopt of wil kopen voor eigen gebruik". De andere melddrempel wordt bereikt indien een incident gevolgen heeft of kan hebben voor invoerders en/of gasopslagsystemen met als gevolg een tijdelijke of volledige onderbreking van de gaslevering, waardoor de normale werking van het gasnet ernstig wordt verstoord.

Artikel 10, onderdeel b, regelt dat energieleveranciers een melding moeten indien een incident gevolgen heeft of kan hebben voor de verkoop of wederverkoop van gas dat leidt tot een verstoring van de levering van gas aan ten minste 20.000 eindafnemers. Met een eindafnemer wordt zoals bedoeld in artikel 1.1 van de Energiewet, "een aangeslotene dat elektriciteit of gas koopt of wil kopen voor eigen gebruik". Hiermee wordt geen onderscheid gemaakt tussen kleine- of grote aansluitingen, omdat op dit moment het niet duidelijk is wie er achter de aansluiting zit.

Artikel 10, onderdeel c, regelt voor *liquefied natural gas* (LNG)-systeembeheerders dat er gemeld dient te worden indien een incident gevolgen heeft of kan hebben voor het LNG-systeem van ten minste 10 GWh per dag. Hierbij gaat het om het systeem, als bedoeld in artikel 1.1. van de Energiewet, "dat gebruikt wordt voor het vloeibaar maken van gas, voor de invoer of de verlading, en voor de hervergassing van vloeibaar gas, met inbegrip van ondersteunende diensten en tijdelijke opslag die nodig zijn voor het proces van hervergassing en de daaropvolgende invoeding op het systeem, en met uitzondering van een LNG-systeem dat uitsluitend ten dienste staat van een transmissiesysteembeheerder voor gas bij de uitvoering van zijn wettelijke taken of verplichtingen."

Artikel 10, onderdeel d, regelt dat er gemeld dient te worden indien een incident gevolgen heeft of kan hebben voor de injectie en productie, opslag, raffinage of behandeling van ten minste 100GWh gas per dag. 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 opslagsysteem. Met opslag van gas wordt bedoeld het opslaan van gas in daarvoor bestemde gasopslagsystemen om daar op een later moment gebruik van te kunnen maken. Dit kunnen ondergronds gasopslagsystemen zijn, te weten voormalig gasvelden en voormalig zoutcavernes, en bovengrondse gasopslagsystemen, zoals bijvoorbeeld een peakshaverinstallatie. Bij raffinage en behandeling van gas gaat het om het bewerken/aanpassen van de samenstelling van het gas aan de geldende kwaliteitseisen of het geschikt maken voor transport, opslag en levering van gas.

Artikel 11. Nadere regels ernstige operationele verstoring voor de subsector aardolie

Artikel 11 bevat een nadere uitwerking van artikel 25, tweede lid, onderdeel a, van de Cbw en artikel 24, eerste lid, van het Cbb. Voor essentiële entiteiten en belangrijke entiteiten binnen de aardoliesector 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 aardgas- of elektriciteitssector. Dit hangt onder andere samen met het karakter van de oliesector als niet-gereguleerde internationale markt. Er bestaat echter verschil tussen de soorten entiteiten binnen de oliesector en de mate waarin een verstoring doorwerkt naar de continuïteit van de energievoorziening.

Op grond van artikel 11, onderdeel a, geldt voor de exploitanten van transmissieleidingen 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. 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 internationaal niveau.

Artikel 11, onderdeel b, regelt dat er gemeld dient te worden indien de raffinage en behandeling van olie voor ten minste 72 uur verstoord is of kan worden, met een impact op de levering van ten minste 50 kilo vaten per dag (50kb/d). Bij raffinage en behandeling kunnen de gevolgen afhankelijk zijn van de marktsituatie en beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld met een langere tijdsduur alvorens een incident moet worden gemeld en is rekening gehouden met de cumulatieve effecten van uitval van kleinere essentiële en belangrijke entiteiten omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de leveringszekerheid. Om dit te ondervangen is voor raffinage en behandeling een drempelwaarde van 72 uur met impact op de levering van tenminste 50kb/d.

Op grond van artikel 11, onderdeel c, dient er gemeld te worden 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 die (mogelijk) ernstige operationele gevolgen hebben op het beheer van deze wettelijke olievoorraden te worden gemeld.

Op grond van artikel 11, onderdeel d, geldt voor de opslag van olie of olieproducten dat er gemeld dient te worden indien het incident gevolgen heeft of kan hebben op de levering van ten minste 100.000 m3 olie en/of olieproducten. Ook bij de opslag van olie en/of olieproducten kunnen de

gevolgen afhankelijk zijn van de marktsituatie en beschikbaarheid van alternatieven. Om hier recht aan te doen zijn melddrempels vastgesteld waarbij rekening is gehouden met de cumulatieve effecten van uitval van kleinere essentiële en belangrijke entiteiten omdat een opeenstapeling van dergelijke uitvallen wel degelijk risico's kan opleveren voor de leveringszekerheid. Om dit te ondervangen is voor op opslag van olie en/of olieproducten een drempelwaarde van 100.000m3 vastgesteld.

Artikel 12. Nadere regels ernstige operationele verstoring voor de subsector stadsverwarming en – koeling

Artikel 12 bevat een nadere uitwerking van artikel 25, tweede lid, onderdeel a, van de Cbw en artikel 24, eerste lid, van het Cbb. Om tot het vaststellen van nadere criteria voor essentiële en belangrijke entiteiten in de sector stadsverwarming- en koeling te komen, is er gekeken naar de gehanteerde criteria binnen de sector elektriciteit en aardgas, aangezien aardgas en elektriciteit een belangrijke rol spelen in het produceren en leveren van warmte. Bij het opstellen van nadere criteria is er een onderscheid gemaakt tussen productie van warmte en/of koeling enerzijds en levering anderzijds.

Artikel 12, 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 en/of koeling van ten minste 20 MW afgenomen vermogen. Voor de productie is aansluiting gevonden bij de criteria van elektriciteit door te kijken naar de gevolgen die een incident heeft of kan hebben op het afgenomen vermogen (MW). De drempelwaarde is uitgedrukt in afgenomen (weggevallen) vermogen (megawatt) en betreft gepland, maar niet geleverd vermogen. Hier is een drempelwaarde van 20 MW aangekoppeld om het significant genoeg te maken. Dit sluit aan bij artikel 6.10 van het bij koninklijke boodschap van 18 juni 2024 ingediende voorstel van wet houdende regels omtrent productie, transport en levering van warmte (Wet collectieve warmte) (Kamerstukken 36576). Hierin is opgenomen dat het bij een installatie van tenminste 20MW significant genoeg is om wijziging van zeggenschap aan de Minister te moeten melden.

Op grond van artikel 12, onderdeel b, geldt dat er gemeld dient te worden indien een incident gevolgen heeft of kan hebben voor de levering van warmte en koeling aan 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 en/of koeling meer ontvangen. Voor de levering van warmte en koeling is aangesloten bij de criteria voor 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.

Artikel 13. Geplande verstoringen

Op grond van artikel 13 hoeft een geplande verstoring, door bijvoorbeeld onderhoudswerkzaamheden en de daarbij behorende gevolgen, niet te worden gemeld. Als onderhoud leidt tot een (mogelijke) ernstige operationele verstoring die op voorhand niet voorzien was, geldt de meldplicht wel.

<u>Paragraaf 2.3 Nadere regels zorgplicht (Cbw)</u>

Artikel 14 - Beleid over beveiliging van netwerk- en informatiesystemen

Artikel 14 bevat een nadere uitwerking van artikel 6 van het Cbb, ten aanzien van het beleid over de beveiliging van netwerk- en informatiesystemen en ten aanzien van de managementsystematiek.

Artikel 14 regelt dat de essentiële en de belangrijke entiteit, als onderdeel van de managementsystematiek, moeten bepalen welke maatregelen voor het beheer van cyberbeveiligingsrisico's worden gemonitord en gemeten, hoe dit gebeurt, wanneer dit plaatsvindt en wie daarvoor verantwoordelijk is. 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 gevolgd, met welke methoden, met welke frequentie en door wie de beoordeling wordt uitgevoerd, ontstaat een sluitende cyclus van plannen, uitvoeren, toetsen en bijsturen. Daarmee wordt geborgd dat het inzicht in de effectiviteit van de maatregelen actueel is en dat resultaten 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 15 - Bedrijfscontinuïteit

Artikel 15 beschrijft de nadere maatregelen die de belangrijke entiteit of essentiële entiteit moet nemen op het vlak van bedrijfscontinuïteitplan, bedoeld in artikel 9 van het Cyberbeveiligingsbesluit.

Bedrijfscontinuïteitsplan

De essentiële entiteit en belangrijke entiteit dient een bedrijfscontinuïteitsplan 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. Bij het opstellen daarvan moet de entiteit rekening houden met de risicobeoordelingen op grond van artikel 7 van het Cbb, zodat zij alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen. De onderdelen van het eerste lid omschrijven de onderdelen die normaliter geadresseerd zouden moeten worden in het plan. Met de zinssnede "waar passend" wordt tot uitdrukking gebracht dat de invulling van het bedrijfscontinuïteitsplan dient aan te sluiten bij de bedrijfsvoering context van de betreffende belangrijke entiteit en essentiële entiteit. In de praktijk kan het bedrijfscontinuïteitsplan zoals hier bedoeld deel uitmaken van een algemeen bedrijfs- en continuïteitsplan van de belangrijke en essentiële entiteit.

Door te zorgen voor ten minste gedeeltelijke redundantie van netwerk- en informatiesystemen, assets (met inbegrip van faciliteiten, uitrusting en benodigdheden), personeel met de nodige verantwoordelijkheid, bevoegdheid en bekwaamheid en passende communicatiekanalen zorgen de essentiële entiteit en belangrijke entiteit ervoor dat er voldoende middelen beschikbaar zijn om de primaire processen doorgang te laten vinden.

Back-upplannen

Op basis van de risicobeoordelingen op grond van artikel 7 van het Cbb en het bedrijfscontinuïteitsplan dient de belangrijke entiteit of essentiële entiteit back-upplannen vast te stellen. De onderdelen van artikel 15, tweede lid, omschrijven welke aspecten in de back-upplannen 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 back-ups volledig zijn, ziet erop 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 back-ups

nauwkeurig te zijn, wat inhoudt dat er een integere backup van de software en gegevens dient te worden gemaakt die in het geval van herstel succesvol kan worden teruggeplaatst en weer kan worden gebruikt. Daarnaast dient de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups gewaarborgd te worden, zodat de back-ups ook daadwerkelijk ingezet kunnen worden. In het bijzonder is hierbij van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door acties van kwaadwillende, zoals ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups dient gewaarborgd te worden, om zo ongeautoriseerde toegang tot gegevens te voorkomen. De risicobeoordelingen op grond van artikel 7 van het Cbb zijn derhalve zowel relevant voor het bepalen van welke software en gegevens in back-ups dienen te worden opgenomen, als het bepalen van de eerdergenoemde waarborgen. Het is tevens van belang dat de vertrouwelijkheid, integriteit en beschikbaarheid van de back-ups doorlopend gemonitord wordt, zodat de essentiële en belangrijke entiteit tijdig wordt geïnformeerd over tekortkomingen. Het plan dient tevens te omschrijven op welke wijze de gegevens hersteld kunnen worden. Ook dienen de back-upplannen te omschrijven hoe lang de betreffende back-ups bewaard moeten worden. Ten slotte dient de essentiële entiteit en belangrijke entiteit, waar mogelijk, periodiek het terugzetten van back-ups te testen, om zo de werking van back-ups in de praktijk te testen. Belangrijke entiteiten en essentiële entiteiten oefenen op deze wijze het terugzetten van back-ups, zodat zij bij incidenten over de kennis en vaardigheden beschikken om dit uit te voeren. Daarnaast biedt het periodiek testen meer zekerheid dat er geen technische belemmeringen zijn om de back-ups daadwerkelijk terug te zetten.

Artikel 16 - Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Artikel 16, derde lid, van het Cbb stelt essentiële en belangrijke entiteiten verplicht om processen en procedures te hebben voor het onderhoud en beheer van haar netwerk- en informatiesystemen. In artikel 16, eerste lid, van deze ministeriele regeling is gespecificeerd dat deze procedures 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.

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 16, 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. Het vereiste geldt waar passend, omdat bij patches zoals reguliere systeemupdates van besturingssystemen doorgaans geen afzonderlijke controle door de essentiële en belangrijke entiteit op herkomst en integriteit nodig is vanwege reeds ingebouwde technische controles. 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. 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.

Ter bescherming van diens netwerk- en informatiesystemen dienen essentiële entiteiten en belangrijke entiteiten op grond van artikel 16, derde lid, onderdeel a, 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.

Op grond van artikel 16, derde lid, onderdeel b, voeren essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uit 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. Door de resultaten te documenteren, kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.

Op grond van artikel 16, derde lid, onderdeel c, evalueren essentiële en belangrijke entiteiten hun blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van hebben. 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.

Op grond van artikel 16, derde lid, onderdeel d, nemen essentiële entiteiten en belangrijke entiteiten maatregelen om kwetsbaarheden te adresseren. 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.

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 derde lid, onderdeel e, dienen essentiële entiteiten en belangrijke entiteiten diens netwerken te segmenteren overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het Cbb bedoelde risicobeoordeling. Hierbij kunnen entiteiten zelf in acht nemen op welke wijze de netwerksegmentatie wordt toegepast, waarbij 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 Informatie Technologie (IT)- en Operationele Technologie (OT)-systemen en deze waar mogelijk van elkaar te scheiden. Het zijn daarnaast goede praktijken om toegang te verlenen tot een netwerk of zone op basis van een beoordeling van de beveiligingsvoorschriften, systemen die van cruciaal belang zijn voor de werking van de entiteit of voor de veiligheid in beveiligde zones te houden, en 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.

Op grond van het vierde lid dienen essentiële en belangrijke entiteiten, waar passend, hun systemen en netwerken 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 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 17 - Beveiligingsaspecten ten aanzien van toegangsbeleid

De essentiële entiteit of belangrijke entiteit dient vastgesteld beleid te hebben voor het gebruik van bevoorrechte accounts en systeembeheeraccounts voor de logische en fysieke toegang tot netwerk- en informatiesystemen. 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. Het beleid legt vast hoe deze accounts worden toegewezen, gebruikt en beheerd, en wordt schriftelijk vastgelegd zodat de toepassing aantoonbaar is.

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 sterke identificatie- en authenticatieprocedures, zoals multifactorauthenticatie, worden toegepast en dat autorisatie zorgvuldig wordt geregeld. Zo wordt de dreiging van phishing en andere misbruik van dergelijke accounts zoveel mogelijk tegengegaan. Daarnaast schrijft het lid voor dat specifieke accounts uitsluitend worden gebruikt voor systeembeheer en dat de voorrechten van deze accounts zoveel mogelijk worden geïndividualiseerd en beperkt tot het strikt noodzakelijke. Dit draagt bij aan een duidelijke scheiding van functies, en het voorkomt dat accounts voor meerdere doeleinden worden gebruikt en dat acties niet herleidbaar zijn tot specifieke personen, waardoor het risico op fouten of misbruik wordt verminderd. Tevens is vastgelegd dat systeembeheeraccounts alleen verbinding maken met de systemen waarvoor zij zijn bedoeld, zodat activiteiten traceerbaar en controleerbaar blijven en de veiligheid van de netwerk- en informatiesystemen gewaarborgd is.

De Minister van Klimaat en Groene Groei,