Regeling van de Minister van Economische Zaken van [PM datum], nr. WJZ/[PM nummer], houdende regels voor essentiële en belangrijke entiteiten in de EZ-sectoren (Regeling cyberbeveiliging EZ)

(KetenID WGK 28487)

De Minister van Economische Zaken ,

Gelet op de artikelen 20, 24, eerste lid, en 29 van het Cyberbeveiligingsbesluit;

Besluit:

Hoofdstuk 1. Algemene bepalingen

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:
alarmeringsdienst NL-Alert: alarmeringsdienst NL-Alert als bedoeld in artikel 1 van de Regeling alarmeringsdienst NL-Alert 2023;
alarmnummer: alarmnummer als bedoeld in artikel 7.7, tweede lid, van de Telecommunicatiewet;
besluit: Cyberbeveiligingsbesluit;
criteria: de drempelwaarden die bepalen wanneer een incident significant is, binnen de parameters van artikel 25, tweede lid, van de wet;
minister: Minister van Economische Zaken;
ruimtevoorwerp: ruimtevoorwerp als bedoeld in artikel 1 van de Wet ruimtevaartactiviteiten;
zone: een afgebakende groep van netwerk- en informatiesystemen.

Artikel 2. Reikwijdte

Deze regeling is van toepassing op essentiële entiteiten en belangrijke entiteiten die behoren tot een of meer van de volgende sectoren of subsectoren:

Sector	Subsector	Soorten entiteiten
Digitale infrastructuur		Aanbieders van internetknooppunten
		Aanbieders van openbare elektronische communicatienetwerken
		Aanbieders van openbare elektronische communicatiediensten
Onderzoek		Onderzoeksorganisaties, met als hoofddoel het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen, die op grond van artikel 15, vierde lid, van de wet

		onder de verantwoordelijkheid van de Minister vallen
Ruimtevaart		Operators van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatienetwerken
Post- en koeriersdiensten		Aanbieders van postdiensten als bedoeld in artikel 2, onderdeel 1 bis, van Richtlijn 97/67/EG1, met inbegrip van aanbieders van koeriersdiensten, voor zover zij ten minste een van de stappen in de postbestelketen verzorgen, met name het ophalen, sorteren, vervoeren en bestellen van postzendingen, met inbegrip van de ophaaldiensten, waarbij rekening moet worden gehouden met de mate waarin zij afhankelijk zijn van netwerk- en informatiesystemen. Uitgezonderd zijn vervoersdiensten die niet in samenhang met een van die stappen worden ondernomen
Vervaardiging	vervaardiging van informaticaproducten en van elektronische en optische producten	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 26, van NACE Rev. 2
	vervaardiging van elektrische apparatuur	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2
	vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	vervaardiging van motorvoertuigen, aanhangers en opleggers	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2

vervaardiging van andere transportmiddelen	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2

Hoofdstuk 2. Nadere regels zorgplicht

Artikel 3. 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;
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 4. Bedrijfscontinuïteit

1. Het bedrijfscontinuïteitsplan, 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. 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 van integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
e. de wijze van herstel van gegevens uit back-ups;
f. bewaartermijnen.

Artikel 5. 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 essentiële entiteit of belangrijke entiteit segmenteert, waar passend, haar systemen en netwerken van systemen en netwerken van derden.

Artikel 6. 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, als bedoeld 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.

Hoofdstuk 3. Nadere criteria meldplicht

Artikel 7. Algemene criteria significante incidenten

1. Voor de toepassing van artikel 25, tweede lid, van de wet, is een incident een significant incident indien het voldoet aan een of meer van de volgende criteria:
a. het heeft de dood van een of meer natuurlijke personen veroorzaakt of kan die veroorzaken;

b. het heeft aanzienlijke schade aan de gezondheid van een of meer natuurlijke personen veroorzaakt of kan die veroorzaken;
c. er is sprake van een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van een essentiële entiteit of een belangrijke entiteit;
d. het voldoet aan een of meer criteria, genoemd in de artikelen 8 tot en met 13.
2. In afwijking van het eerste lid is een geplande dienstonderbreking of een ander gevolg van onderhoudswerkzaamheden die door of namens een essentiële entiteit of een belangrijke entiteit worden uitgevoerd, geen significant incident.

Artikel 8. Criteria significante incidenten bij aanbieders van elektronische communicatienetwerken of aanbieders van elektronische communicatiediensten

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten die aanbieder zijn van openbare elektronische communicatienetwerken of van openbare elektronische communicatiediensten, is een incident een significant incident indien het voldoet aan een of meer van de volgende criteria:
a. bij een onderbreking van de levering van een openbare elektronische communicatiedienst zijn ten minste 50.000 gebruikers getroffen;
b. de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening van het elektronische communicatienetwerk of de elektronische communicatiedienst worden opgeslagen, verzonden of verwerkt, is aangetast;
c. het alarmnummer is niet beschikbaar;
d. de alarmeringsdienst NL-Alert is niet beschikbaar.

Artikel 9. Criteria significante incidenten bij aanbieders van internetknooppunten

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten die aanbieder zijn van internetknooppunten, is een incident een significant incident indien:
a. ten minste 25% van het actuele totale verkeer dat door het internetknooppunt wordt verwerkt en behoort tot de eigen dienstverlening, gedurende 30 minuten of langer is uitgevallen; of
b. de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening van het internetknooppunt worden opgeslagen, verzonden of verwerkt, is aangetast.

Artikel 10. Criteria significante incidenten in de sector ruimtevaart

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten in de sector ruimtevaart, is een incident een significant incident indien het voldoet aan een of meer van de volgende criteria:
a. gedurende een bepaalde door de entiteit vastgestelde periode is geen communicatie met een ruimtevoorwerp mogelijk;
b. een verstoring of uitval treedt op van een netwerk- en informatiesysteem dat essentieel is voor economische of publieke activiteiten; of
c. manipulatie of corruptie van vlucht- of besturingsgegevens heeft plaatsgevonden waardoor een risico ontstaat voor de besturing of het behoud van een ruimtevoorwerp.

Artikel 11. Criteria significante incidenten in de sector post- en koerierdiensten

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten in de sector post- en koerierdiensten, is een incident een significant incident indien:
a. als gevolg van een verstoring in de beveiliging van netwerk- en informatiesystemen van de betrokken entiteit ten minste 30% van de gebruikers van de dienst hun poststukken als bedoeld in artikel 2, eerste lid, onderdeel b, van de Postwet 2009, ten minste twee bezorgdagen later ontvangt dan op grond van wettelijke of contractuele verplichtingen zou moeten; of
b. de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienstverlening van de post- en koeriersdienst worden opgeslagen, verzonden of verwerkt, is aangetast.

Artikel 12. Criteria significante incidenten in de sector vervaardiging

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten in de sector vervaardiging, is een incident een significant incident indien het voldoet aan één of meer van de volgende criteria:
a. verlies of degradatie van veiligheidsfuncties treedt op als gevolg van een niet-normaal functionerend industrie-specifiek netwerk- en informatiesysteem dat essentieel is voor de aansturing van de veiligheidsfuncties;
b. verlies van beschikbaarheid van essentiële besturings- of monitoringsfuncties treedt op door een niet-normaal functionerend industrie-specifiek netwerk- en informatiesysteem;
c. er is sprake van inbreuk op de integriteit van het industrie-specifieke netwerk- en informatiesysteem waardoor de kwaliteit van het product of het productieproces in gevaar is gekomen of kan komen;
d. als gevolg van een inbreuk op de beveiliging van netwerk- en informatiesystemen van de betrokken entiteit heeft milieuschade is opgetreden;
e. succesvolle ongeoorloofde toegang tot een industrie-specifiek netwerk- en informatiesysteem heeft plaatsgevonden waarbij de aanval het beveiligingsniveau overstijgt; of
f. er is sprake van succesvolle ongeoorloofde toegang tot een industrie-specifieke netwerk- en informatiesysteem die zich verspreidt naar meerdere zones of omgevingen.

Artikel 13. Criteria significante incidenten in de sector onderzoek

Voor zover het betreft essentiële entiteiten of belangrijke entiteiten in de sector onderzoek, als bedoeld in bijlage 2 bij de wet, die op grond van artikel 15, vierde lid, van de wet onder de verantwoordelijkheid van de Minister vallen, is een incident een significant incident indien de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast.

Hoofdstuk 4. Overige en slotbepalingen

Artikel 14. Aanwijzing autoriteiten

De volgende autoriteiten zijn aangewezen als autoriteiten als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet:
a. de Minister van Economische Zaken, uit hoofde van de Wet ruimtevaartactiviteiten;
b. de Minister van Economische Zaken, uit hoofde van Verordening (EU) 2019/881;
c. de Minister van Economische Zaken, uit hoofde van Verordening (EU) 2024/2847;

d. de Minister van Economische Zaken, uit hoofde van de Telecommunicatiewet.

Artikel 15. Intrekking Regeling aanwijzing aanbieders essentiële diensten EZK

De Regeling aanwijzing aanbieders essentiële diensten EZK wordt ingetrokken.

Artikel 16. Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 17. Citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging EZ.

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

's-Gravenhage,

De Minister van Economische Zaken,

TOELICHTING

I. Algemeen

1. Inleiding

De Cyberbeveiligingswet implementeert de NIS2-richtlijn[1] en beoogt een hoger niveau van cyberweerbaarheid voor de onder haar werkingssfeer vallende essentiële en belangrijke entiteiten te bewerkstelligen. De Cyberbeveiligingswet verplicht deze entiteiten tot het treffen van passende technische en organisatorische maatregelen ter bevordering van de cyberweerbaarheid van hun netwerk- en informatiesystemen, alsmede tot het melden van significante incidenten die verband houden met de beveiliging daarvan.

In deze ministeriële regeling worden de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) nader uitgewerkt voor de sectoren die onder de verantwoordelijkheid van de Minister van Economische Zaken vallen, namelijk de sectoren ruimtevaart, post- en koeriersdiensten, vervaardiging, onderzoek voor zover het binnen het EZ-domein valt, en binnen de sector digitale infrastructuur voor de soorten entiteiten aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten en aanbieders van internetknooppunten. Voor de overige soorten entiteiten binnen de sector digitale infrastructuur, zoals aanbieders van cloudcomputingdiensten of datacenterdiensten geldt rechtstreeks de Uitvoeringsverordening (EU) 2024/2690[2].

Bij de sector vervaardiging gaat het om de volgende subsectoren a) vervaardiging van informaticaproducten en van elektronische en optische producten b) vervaardiging van elektrische apparatuur c) vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd d) vervaardiging van motorvoertuigen, aanhangers en opleggers e) vervaardiging van andere transportmiddelen.
Bij het opstellen van deze regeling is waar mogelijk afstemming gezocht met en om input gevraagd van bedrijven en/of brancheverenigingen uit desbetreffende sectoren, om de maatregelen zo goed mogelijk te laten aansluiten bij de bestaande praktijk, dat deze uitvoerbaar zijn en om te waarborgen dat de voorgeschreven maatregelen niet onnodige regeldruk creëren bij essentiële en belangrijke entiteiten.

2. Hoofdlijnen van de regeling

---

[1] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

[2] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (PbEU L 2024/2690).

2.1 Algemeen
In deze regeling worden verschillende verplichtingen ter bevordering van de beveiliging van de netwerk- en informatiesystemen, die zijn uitgewerkt in het Cyberbeveiligingsbesluit, nader ingevuld. Verder omvat deze regeling een nadere invulling van de criteria die bepalen of een incident significant is of niet. Ook voorziet zij in de mogelijkheid voor toezichthouders tot het uitwisselen van informatie die voor de toezichtspraktijk van belang is.

2.2 Zorgplicht
In deze regeling worden voor de in artikel 2 genoemde sectoren 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 de 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 deze uitvoeringsverordening vallen op basis van artikel 4 van het Cyberbeveiligingsbesluit.

2.3 Meldplicht
De Cyberbeveiligingswet heeft tot doel om de cyberweerbaarheid van essentiële en belangrijke entiteiten te verhogen. De meldplicht is één van de instrumenten om de daadwerkelijke cyberweerbaarheid van essentiële en belangrijke entiteiten inzichtelijk te maken.
Naast de nadere invulling van de zorgplicht bevat deze regeling criteria op grond waarvan wordt bepaald of een incident significant is voor de sectoren, subsectoren en soorten entiteiten waarvoor de Minister van Economische Zaken verantwoordelijk is. Voor een incident dat als significant wordt aangemerkt, geldt een meldplicht op grond van artikel 25, eerste lid, van de Cbw.
Door meldingen van significante incidenten kunnen toezichthouders patronen en kwetsbaarheden signaleren en entiteiten gerichte aanwijzingen geven voor verdere verbetering van hun cyberweerbaarheid.
In artikel 1 van de Cyberbeveiligingswet is het begrip "incident" als volgt gedefinieerd: "*een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt*." In artikel 25, tweede lid, van de wet is bepaald dat er sprake is van een significant incident als een incident een ernstige operationele verstoring voor de betrokken entiteit veroorzaakt of kan veroorzaken, of andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Dit betekent dat in sommige situaties ook incidenten als significant kunnen worden aangemerkt waarbij de externe gevolgen beperkt zijn. Het kan dan bijvoorbeeld gaan om verstoringen in interne bedrijfsprocessen die de entiteit zelf raken, maar die weinig of geen externe gevolgen hebben.
In artikel 24, 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 er sprake is van een significant incident. Hierbij kan er onderscheid worden gemaakt tussen sectoren, subsectoren en soorten entiteiten. Met deze regeling wordt gebruik gemaakt van deze bevoegdheid. Zodra een incident bij een essentiële of

belangrijke entiteit aan één of meerdere criteria voldoet zoals in deze regeling is opgenomen dan is er sprake van een significant incident. In dat geval dient de essentiële of belangrijke entiteit een melding te maken. De uitwerking van de meldcriteria omvat zowel algemene criteria, die gelden voor alle sectoren en subsectoren waarop deze regeling van toepassing is, als specifieke criteria, die uitsluitend gelden voor de betrokken sectoren, subsectoren of soorten entiteiten. Een essentiële of belangrijke entiteit meldt een significant incident bij het eigen CSIRT en de toezichthoudende instantie. Hiervoor is één centraal meldloket ingericht onder regie van de Minister van Justitie en Veiligheid. De regels omtrent de verdere procedures van het melden van significante incidenten, zoals het tijdstip van meldingen en de te verstrekken informatie, zijn opgenomen in de artikelen 26 tot en met 29 van de Cyberbeveiligingswet en worden in deze regeling niet verder uitgewerkt.

2.4 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 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.
In het Cyberbeveiligingsbesluit is ervoor gekozen om het mogelijk te maken dat Onze Minister die het aangaat deze autoriteiten als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet bij regeling kan aanwijzen. De reden hiervoor is dat naar verwachting vooral bevoegde autoriteiten zullen worden aangewezen die uit hoofde van sectorale regelgeving een rol hebben in het toezicht op entiteiten die ook onder toepassing van de wet vallen. Door dit bij regeling te regelen kan door de vakminister vanuit diens verantwoordelijkheid voor sectoren hier een passende invulling aan gegeven worden en waar nodig worden bijgesteld. De aanwijzing maakt het in het bijzonder voor bevoegde autoriteiten mogelijk om in het geval van overlappend toezicht nauwer samen te werken, informatie uit te wisselen en op die wijze doelmatig en doeltreffend toezicht te bevorderen en daarmee ook onnodige toezichtslasten voor entiteiten te beperken.

3. Toezicht en handhaving

Met het toezicht op de naleving van deze regeling worden ambtenaren van de Rijksinspectie Digitale Infrastructuur belast. Op grond van artikel 68 van de Cbw kan de minister hiervoor ambtenaren bij besluit aanwijzen. De betreffende ambtenaren oefenen hun bevoegdheden uit met inachtneming van artikel 69 van de Cbw.

4. Notificatie

[PM]

5. Regeldruk

Deze regeling veroorzaakt geen nieuwe regeldruk ten opzichte van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. Voor de meldplicht is de regeldruk voor alle relevante sectoren verantwoord in de memorie van toelichting bij het wetsvoorstel. Voor de zorgplicht is de regeldruk toegelicht in het besluit. Zowel de meldplicht als de zorgplicht krijgen een nadere invulling in deze regeling, maar deze leveren geen additionele regeldruk op.

6. Advies en consultatie

6.1 Internetconsultatie

[PM]

6.2 Advies Adviescollege Toetsing Regeldruk

[PM]

6.3 Uitvoering en handhavingstoets

[PM]

7. Evaluatie

Deze regeling wordt periodiek geëvalueerd en waar nodig aangepast, zo volgt uit artikel 24, tweede lid, van het Cbb. Op grond van die bepaling evalueert de Minister van Economische Zaken ten minste elke vier jaar de doeltreffendheid van de nadere regels over de meldplicht en de effecten daarvan in de praktijk, en past deze zo nodig aan.

8. Inwerkingtreding

[PM Vanwege de samenhang tussen deze ministeriële regeling, het Cbb en de Cbw, dienen deze op hetzelfde moment in werking te treden.]

II. Artikelsgewijze toelichting

Hoofdstuk 1. Algemene bepalingen

Artikel 1 – Begripsbepalingen
Dit artikel bevat de begripsbepalingen die in deze regeling worden gebruikt. Voor zover begrippen reeds zijn gedefinieerd in de Cyberbeveiligingswet of het Cyberbeveiligingsbesluit, sluiten de definities in deze regeling daarbij aan. Een aantal definities zijn uitgewerkt in andere wet- en regelgeving. Voor de uitleg van die begrippen wordt verwezen naar de desbetreffende wet- en regelgeving.

Artikel 2 – Reikwijdte
Dit artikel bepaalt welke entiteiten onder deze regeling vallen. Het betreft aanbieders van internetknooppunten, aanbieders van openbare elektronische communicatienetwerken en aanbieders van elektronische communicatiediensten, alsmede entiteiten in de sectoren ruimtevaart, post- en koerierdiensten en vervaardiging. De sector onderzoek valt onder deze regeling voor zover de betrokken entiteit onderzoeksactiviteiten verricht binnen een sector of subsector die onder de verantwoordelijkheid van de Minister van Economische Zaken valt.

Hoofdstuk 2. Nadere regels zorgplicht

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen
Dit artikel werkt artikel 6 van het Cyberbeveiligingsbesluit (Cbb) 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 de essentiële en belangrijke entiteiten, als onderdeel van hun 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 gemonitord, 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 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 4 - Bedrijfscontinuïteit
Dit artikel beschrijft de nadere maatregelen die de belangrijke entiteit of essentiële entiteit moet nemen op het gebied van bedrijfscontinuïteitsplan, bedoeld in artikel 9 van het Cyberbeveiligingsbesluit.

Bedrijfscontinuïteitsplan
De essentiële entiteit en de belangrijke entiteit dienen 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. Zo worden de duur en gevolgen van dergelijke incidenten beperkt. Bij het opstellen daarvan moet de entiteit rekening 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 eerste lid omschrijven de elementen 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 bedrijfsvoeringscontext van de betreffende belangrijke entiteit of essentiële entiteit. In de praktijk kan het bedrijfscontinuïteitsplan zoals hier bedoeld deel uitmaken van een algemeen bedrijfs- en continuïteitsplan van de belangrijke of 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 of belangrijke entiteit ervoor dat er voldoende middelen beschikbaar zijn om de primaire processen doorgang te laten vinden. Bij redundantie worden systemen, veelal kritieke systemen, dubbel uitgevoerd om hiermee de beschikbaarheid te verhogen en hierdoor wordt het netwerk kwetsbaar.

Back-upplannen
Op basis van de risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit en het bedrijfscontinuïteitsplan dient de belangrijke entiteit of essentiële entiteit back-upplannen vast te stellen. De onderdelen van artikel 4, tweede lid, omschrijven welke aspecten in de back-upplannen terug dienen te komen. Het bepalen van hersteltijden, in het Engels bekend als *recovery time objective (RTO),* heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. Herstelpunten, in het Engels 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 maar ook 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 back-ups nauwkeurig te zijn. Dit houdt in dat de gemaakte back-ups een juiste en consistente weergave vormen van de gebruikte software en gegevens, zodat deze bij herstel zonder afwijkingen kunnen worden teruggezet en opnieuw inzetbaar zijn.
Voorts moeten de beschikbaarheid en integriteit van back-ups zijn gewaarborgd, zodat deze in geval van een incident daadwerkelijk kunnen worden gebruikt. In het bijzonder is het van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet als gevolg van kwaadwillende handelingen, zoals ransomware-aanvallen, onbruikbaar kunnen worden. Tevens moet de vertrouwelijkheid van back-ups zijn gewaarborgd, om ongeautoriseerde toegang tot de daarin opgenomen gegevens te voorkomen.
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 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 back-upplan 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. Anderzijds biedt het testen meer zekerheid dat er geen technische belemmeringen zijn om de back-ups daadwerkelijk terug te zetten.

Artikel 5 - 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 hun netwerk- en informatiesystemen. In het eerste lid van dit artikel 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.

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 het 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. Het is aan de entiteit om te bepalen hoe dit wordt gedocumenteerd.

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 omvatten het gebruik van firewalls en *intrusion prevention systems* om de interne

netwerken van de relevante entiteiten te beschermen en om het gebruik van antivirussoftware om potentiële kwaadaardige software op te kunnen sporen.

Onderdeel b
Op grond van dit onderdeel voeren essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uit en leggen zij de resultaten daarvan vast. Het is aan de entiteit hoe de resultaten worden vastgelegd. Deze scans maken het mogelijk om inzicht te krijgen in 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.

Onderdeel c
Op grond van dit onderdeel 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.

Onderdeel d
Op grond van dit onderdeel 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. Het is aan de entiteit hoe de resultaten worden vastgelegd. Evenals bij het niet toepassen van een beveiligingspatch wordt voor de toezichthouder dan duidelijk waarom er wordt afgeweken en kan de toezichthouder oordelen of deze beslissing terecht is genomen.

Onderdeel e
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 hun 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. Daarbij wordt rekening gehouden met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen. Een essentiële entiteit of 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 is daarnaast best practice 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
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. Bij netwerksegmentatie gaat het om het onderverdelen van een fysiek netwerk in verschillende logische onderdelen die van elkaar afgeschermd kunnen worden. Op elk netwerksegment kunnen verschillende beveiligingsmaatregelen worden toegepast. Zo krijgt een kwaadwillende die in een bepaald netwerksegment is gekomen, niet automatisch ook toegang tot andere delen van het netwerk. 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 6 - Beveiligingsaspecten ten aanzien van toegangsbeleid
Essentiële entiteiten en belangrijke entiteiten dienen 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 authorisatie 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. Ook voorkomt het dat accounts voor meerdere doeleinden worden gebruikt en dat acties niet herleidbaar zijn tot specifieke personen. Daardoor wordt het risico op fouten of misbruik verminderd. Tevens wordt 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 geborgd is.

Hoofdstuk 3. Nadere criteria meldplicht

Artikel 7 – Algemene criteria significante incidenten
Dit artikel bevat algemene criteria op grond waarvan wordt bepaald of een incident significant is. Deze criteria gelden voor alle entiteiten waarop deze regeling van toepassing is.

Eerste lid

Voor essentiële en belangrijke entiteiten is sprake van een significant incident indien het incident heeft geleid, of kan leiden, tot de dood van een persoon of tot aanzienlijke schade aan de gezondheid van een persoon. Deze criteria zijn uitgewerkt in onderdelen a en b.
Bij de beoordeling of sprake is van aanzienlijke gezondheidsschade, houden entiteiten rekening met de vraag of het incident aanzienlijke gezondheidsproblemen, zoals ernstige verwondingen, heeft veroorzaakt of kan veroorzaken. Van entiteiten wordt daarbij niet verlangd dat zij aanvullende informatie verzamelen waartoe zij redelijkerwijs geen toegang hebben.
Er is tevens sprake van een significant incident indien een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van een entiteit heeft plaatsgevonden. Dit is uitgewerkt in onderdeel c.
Bij dergelijke incidenten hoeft nog geen sprake te zijn van feitelijke schade of directe gevolgen. De enkele vaststelling dat een kwaadwillende actor zich ongeoorloofd toegang heeft verschaft tot de netwerk- en informatiesystemen van de entiteit, brengt reeds een aanzienlijk risico met zich mee voor de betrokken entiteit en mogelijk ook voor andere partijen, zoals de afnemers van een product of dienst waarin een kwetsbaarheid aanwezig is die door een actor kan worden misbruikt.
Een actor kan zich bovendien in de netwerk- en informatiesystemen van een essentiële of belangrijke entiteit nestelen met de bedoeling om op een later moment een verstoring van de dienstverlening te veroorzaken of anderszins schade toe te brengen.
Voor het CSIRT en de toezichthoudende instantie is het van belang dat dergelijke incidenten worden gemeld, omdat zij ook een risico kunnen vormen voor andere partijen.

Tweede lid
Er is geen sprake van een significant incident indien de dienstverlening op een vooraf gepland moment wordt onderbroken als gevolg van geplande onderhoudswerkzaamheden die door of namens de essentiële of belangrijke entiteit worden uitgevoerd. Onderhoudswerkzaamheden zijn noodzakelijk voor het correct functioneren van de netwerk- en informatiesystemen.
Ook geplande onderbrekingen van de dienstverlening als gevolg van vooraf vastgestelde contractuele afspraken tussen partijen worden niet als een significant incident beschouwd.
Deze bepaling geldt uitsluitend ten aanzien van de geplande gevolgen van de onderhoudswerkzaamheden. Indien tijdens of als gevolg van de geplande onderhoudswerkzaamheden ongeplande gevolgen ontstaan geldt deze bepaling niet. Zo kan bijvoorbeeld een incorrecte systeemupdate leiden tot een niet-voorziene uitval van netwerk- en informatiesystemen, met gevolgen voor de dienstverlening van de essentiële of belangrijke entiteit. In dat geval is sprake van een significant incident, indien tevens aan één of meer criteria van deze regeling wordt voldaan.

Artikel 8 - Criteria significante incidenten bij aanbieders van elektronische communicatienetwerken of aanbieders van elektronische communicatiediensten
Elektronische communicatiediensten- en netwerken zijn essentieel voor de communicatie tussen natuurlijke personen, bedrijven, overheidsorganisaties en andere instituties. Voor de goede functionering en continuering van deze diensten is het essentieel dat de desbetreffende essentiële en belangrijke entiteiten significante incidenten melden bij de toezichthouder en het CSIRT.

Onderdeel a
Er is sprake van een incident met betrekking tot beschikbaarheid als de openbare elektronische communicatiedienst niet meer wordt geleverd. Het kan hier bijvoorbeeld gaan om een storing waarbij gebruikers niet meer kunnen bellen of waarbij gebruikers geen toegang meer hebben tot het internet. Ten aanzien van openbare elektronische communicatiediensten geldt dat een incident als significant wordt beschouwd als ten minste 50.000 gebruikers zijn getroffen. Indien de dienst niet beschikbaar is voor een dusdanig aantal gebruikers, kan er vanuit gegaan worden dat er sprake is van een significante impact op de maatschappij.
De niet beschikbaarheid van een dienst moet worden gemeten vanaf het moment waarop de dienst niet beschikbaar is voor gebruikers tot het moment waarop de reguliere werking van diensten of activiteiten zijn hersteld tot het serviceniveau dat vóór het incident werd verleend. Wanneer een relevante entiteit niet in staat is te bepalen wanneer de niet-beschikbaarheid van een dienst begon, moet de niet-beschikbaarheid worden gemeten vanaf het moment dat dit door de entiteit werd gedetecteerd.
Om vast te stellen of een incident significant is, moeten entiteiten in voorkomend geval het aantal door het incident getroffen gebruikers bepalen. Het gaat bij gebruikers om natuurlijke personen of rechtspersonen die van een openbare elektronische communicatiedienst gebruik maken voor particuliere of zakelijke doeleinden. Daarbij hoeven zij niet r noodzakelijkerwijze op die dienst te zijn geabonneerd.
Immers, bij bepaalde elektronische communicatiediensten, zoals nummeronafhankelijke elektronische communicatiediensten, zal de gebruiker niet altijd een overeenkomst hebben gesloten met de entiteit. Ook gebruikers van deze diensten moeten als gebruikers worden gezien. Bij een zakelijke gebruiker zal er veelal sprake zijn van meerdere natuurlijke personen die toegang hebben tot en gebruik maken van de verleende dienst van de entiteit, maar zelf geen overeenkomst hebben gesloten met die entiteit. Het kan hierbij gaan over de eigen werknemers van een zakelijke gebruiker. Deze werknemers kunnen in de context van deze regeling als afzonderlijke gebruikers worden beschouwd.
Wanneer een essentiële of belangrijke entiteit niet in staat is om precies het aantal getroffen gebruikers te bepalen, moet bij het bepalen van het totale aantal door het incident getroffen gebruikers rekening worden gehouden met de schatting van de relevante entiteit van het mogelijke maximale aantal getroffen gebruikers. Het gaat hierbij om diensten die in Nederland worden aangeboden, waaronder internettoegangsdiensten (vast en mobiel) en telefonie (vast en mobiel).

Onderdeel b
In dit onderdeel is een criterium opgenomen die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten verplicht stelt om een incident te melden indien de integriteit, de vertrouwelijkheid of de authenticiteit van opgeslagen, verzonden of verwerkte gegevens in verband met de dienstverlening is aangetast. Bij elektronische communicatie kan het bijvoorbeeld gaan over verkeersgegevens. Deze gegevens zijn vertrouwelijk van aard, waardoor deze ook blootgesteld kunnen worden aan het risico van onbedoelde openbaarmaking of verlies. De vertrouwelijkheid van gegevens kan bijvoorbeeld worden gecompromitteerd indien de encryptie van een dienst niet heeft gewerkt of er sprake is geweest van ongeoorloofde toegang waarbij kwaadwillenden gegevens van de entiteit hebben ontvreemd. Ook kan er sprake zijn van de aantasting van de integriteit van de dienstverlening. Bij kwaadwillende toegang kunnen gegevens worden gecorrumpeerd die noodzakelijk zijn voor het correct functioneren van de

netwerk- en informatiesystemen van aanbieders van elektronische communicatienetwerken of aanbieders van elektronische communicatiediensten. Dergelijke aantastingen kunnen niet alleen de systemen zelf verstoren, maar ook de dienstverlening aan derden. Ook authenticiteit wordt meegenomen in het meldcriterium, omdat dit kan samenhangen met integriteit en vertrouwelijkheid. De plicht om incidenten te melden is echter niet gelimiteerd tot kwaadwillende toegang want ook onbedoelde menselijke fouten vallen onder dit criterium. Hierbij kan gedacht worden aan onbedoelde openbaarmaking van vertrouwelijke gegevens of het foutief uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Onderdelen c en d
Aangezien een verstoring van het alarmnummer 112 significante maatschappelijke gevolgen teweeg kan brengen, met in het uiterste geval doden of gewonden, is elke niet-beschikbaarheid van deze dienst meldingsplichtig, ongeacht de aard en omvang van de verstoring. Dit is opgenomen in onderdeel c.
Ditzelfde geldt voor verstoringen in de dienstverlening van de alarmdienst NL-alert. Dit is verwerkt in onderdeel d.

Artikel 9 - Criteria significante incidenten bij aanbieders van internetknooppunten
Het goed functioneren van internetknooppunten is essentieel voor het functioneren van het internet als geheel. Het is daarom van belang dat significante incidenten die gevolgen hebben voor de beschikbaarheid van de dienstverlening van internetknooppunten gemeld worden bij het desbetreffende CSIRT en de toezichthoudende instantie.

Onderdeel a
In dit onderdeel is geregeld dat een incident significant is wanneer ten minste 25% van het actuele totale verkeer door het internetknooppunt gedurende 30 minuten of langer is uitgevallen. Bij de tijdsberekening dient het Border Gateway Protocol (BGP) als standaard genomen te worden. Hiermee wordt bedoeld de "BGP hold time" instelling van de meeste internet routers. Deze waarde specificeert hoe lang het duurt tot een router veronderstelt dat zijn connectie met een andere router verbroken is bij het uitblijven van BGP-berichten van die andere router. Bij het bereken van het verlies van het actuele totale verkeer wordt uitsluitend rekening gehouden met het daadwerkelijk verloren verkeer dat is weggevallen als gevolg van het uitvallen van de dienstverlening zelf. Het kan namelijk ook voorkomen dat, bij constatering van problemen bij de dienstverlening van het internetknooppunt, diens gebruikers ervoor kiezen om het verkeer middels een ander internetknooppunt door te laten geleiden. Omdat hier van buiten het internetknooppunt het internetverkeer wordt hergerouteerd (bijvoorbeeld door een klant zelf), hoeft er geen rekening gehouden te worden met deze gebruikers bij het bepalen of de uitval van de dienstverlening bij een internetknooppunt voldoet aan het criterium van onderdeel a.

Onderdeel b
In dit onderdeel is een criterium opgenomen die internetknooppunten verplicht om een incident te melden indien de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast. Evenals bij aanbieders van elektronische communicatienetwerken en aanbieders van elektronische communicatiediensten is dit een belangrijk criterium, aangezien incidenten op dit vlak niet alleen gevolgen kunnen hebben voor het internetknooppunt zelf, maar ook voor derden. De vertrouwelijkheid van gegevens kan bijvoorbeeld worden

aangetast wanneer de encryptie van een dienst niet correct heeft gewerkt, of wanneer sprake is geweest van ongeoorloofde toegang waardoor de kwaadwillenden gegevens van de entiteit hebben ontvreemd. Ook de integriteit van de dienstverlening kan worden geraakt. Bij kwaadwillige toegang kunnen gegevens zijn aangetast die noodzakelijk zijn voor de correcte werking van de netwerk- en informatiesystemen van internetknooppunten, hetgeen eveneens gevolgen kan hebben voor derden.
De meldplicht is echter niet beperkt tot kwaadwillige toegang. Ook menselijke fouten vallen hieronder. Daarbij kan worden gedacht aan het onbedoeld openbaar maken van vertrouwelijke gegevens of het onjuist uitvoeren van een systeemupdate, waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Artikel 10 - Criteria significante incidenten in de sector ruimtevaart
De ruimtevaartsector levert een directe bijdrage aan onder meer vitale maatschappelijke en economische processen. Netwerk en informatiesystemen worden binnen deze sector ingezet voor communicatie, navigatie, aardobservatie en tijdsynchronisatie, en ondersteunen daarmee onder meer telecommunicatie, transport, energievoorziening, landbouw, veiligheid en wetenschappelijk onderzoek. Een verstoring in deze infrastructuur kan daardoor gevolgen hebben voor meerdere sectoren binnen en buiten Nederland.
Ruimtevaartactiviteiten worden uitgevoerd met behulp van netwerk- en informatiesystemen die essentieel zijn voor de besturing en veilige werking van ruimtevoorwerpen. Deze systemen verzorgen onder meer telemetrie-, tracking- en commando-verbindingen en vormen daarmee het operationele hart van satellietmissies. Het is daarom van belang dat significante incidenten die de besturing of continuïteit van dergelijke systemen raken tijdig worden gemeld.

Onderdeel a
Dit onderdeel ziet op situaties waarin gedurende een door de entiteit vastgestelde periode geen communicatie met het ruimtevoorwerp mogelijk is. De technische omstandigheden zijn sterk afhankelijk van het type aardbaan. Daarom is gekozen voor criteria die voor alle aardbanen werkbaar zijn. De verantwoordelijkheid voor het contact houden met het ruimtevoorwerp ligt bij de entiteit. Wanneer communicatie zonder voorafgaande planning of buiten reguliere operaties uitvalt, kan daardoor verlies van controle over een ruimtevoorwerp optreden en daarmee risico voor veilige besturing van het ruimtevoorwerp. Het criterium is daarom gericht op het tijdig onderkennen van onverwachte of langdurige uitval van telemetrie-, tracking- en commandoverbindingen.

Onderdeel b
In dit onderdeel is geregeld dat een incident een significant incident is wanneer een netwerk- en informatiesysteem uitvalt of wordt verstoord dat noodzakelijk is voor het verlenen van diensten of het verrichten van ruimtevaartactiviteiten die van economisch of publiek belang zijn, waaronder het verlies van dataverbindingen of navigatiesignalen. Dergelijke storingen kunnen aanzienlijke gevolgen hebben voor publieke en private organisaties die van deze diensten gebruikmaken.

Onderdeel c
In dit onderdeel is geregeld dat een incident significant is indien sprake is van manipulatie of corruptie van vlucht- of besturingsgegevens, waardoor risico ontstaat voor de besturing of het behoud van het ruimtevoorwerp.
Dit omvat zowel interne als externe cyberincidenten die kunnen leiden tot verlies van controle of verstoring van missiekritieke functies. Interne cyberincidenten zijn

incidenten die hun oorsprong vinden binnen de eigen netwerk- en informatiesystemen van de entiteit die direct wordt gebruikt voor de aansturing van het ruimtevoorwerp of het grondstation. In dergelijke gevallen heeft de entiteit doorgaans directe invloed op het herstel van het incident, bijvoorbeeld bij een interne systeemfout, een configuratiefout of bij het uitvallen van een eigen softwarecomponent. Hierbij kan ook worden gedacht aan een verstoring bij een rechtstreekse leverancier of dienstverlener waarvan de entiteit afhankelijk is, zoals een leverancier van cloud- of netwerkdiensten. Externe cyberincidenten daarentegen betreffen incidenten waarbij de entiteit geen directe invloed heeft op het herstel van de dienstverlening, zoals aan een verstoring van een externe communicatielink die buiten de operationele controle van de entiteit ligt.
Het begrip manipulatie van gegevens ziet op het opzettelijk wijzigen van gegevens met als doel de betrouwbaarheid of juistheid ervan te beïnvloeden. Dit kan het gevolg zijn van kwaadwillige handelingen, zoals cyberaanvallen waarbij commando's of telemetriedata worden aangepast of vervalst, of spoofing, waarbij een actor zich voordoet als een vertrouwde bron binnen het netwerk. Manipulatie kan leiden tot verlies van betrouwbaarheid van gegevens en risico's voor de bestuurbaarheid van het ruimtevoorwerp.
Corruptie van gegevens ziet op het bedoeld of onbedoeld beschadigen van gegevens, bijvoorbeeld door technische storingen, systeemfouten, opslagproblemen of door elektromagnetische of stralingsinvloeden in de ruimteomgeving. Hierdoor kunnen gegevens onleesbaar of onbruikbaar worden, wat kan leiden tot verkeerde interpretatie of verlies van kritieke gegevens waarmee het ruimtevoorwerp wordt bestuurd. Ook vormen van jamming, waarbij communicatie- of navigatiesignalen worden verstoord of geblokkeerd, vallen hieronder.

Artikel 11 - Criteria significante incidenten in de sector post- en koerierdiensten
Post- en koeriersdiensten blijven belangrijk voor burgers, bedrijven en overheidsorganisaties. De bezorgnetwerken worden gebruikt voor communicatie en voor het verzenden en ontvangen van commerciële zendingen. Deze markt is sterk aan verandering onderhevig. Door digitalisering dalen de volumes van post al jaren, waardoor het belang van post als communicatiemiddel afneemt. De markt zal komende jaren naar verwachting overgaan in een brede bezorgmarkt voor post en pakketten. Voor de goede functionering van post- en koeriersdiensten blijft het daarom noodzakelijk dat belangrijke entiteiten in deze sector significante incidenten melden.
Er is sprake van een incident wanneer netwerk- en informatiesystemen uitvallen, waardoor de dienst niet meer of met voor klanten aanzienlijke vertraging wordt geleverd.

Onderdeel a
Een incident in de post- en koerierssector wordt als significant beschouwd wanneer het leidt tot een forse vertraging met landelijke impact. Dat is het geval wanneer ten minste 30% van de klanten in het post- of koeriersnetwerk de dienst meer dan één bezorgdag later ontvangt dan contractueel of wettelijk voorzien, als gevolg van een verstoring in de systemen. Een dergelijk percentage impliceert dat meerdere bezorgcentra zijn geraakt, waardoor er niet langer sprake is van alleen regionale impact. De oorzaak van de verstoring kan zowel in de systemen zelf liggen, bijvoorbeeld bij systeemfalen, als extern, zoals bij een stroomstoring.
Bezorgdagen zijn de dagen waarop normaal gesproken post- en koeriersdiensten geleverd worden. Op zondag en maandag wordt bijvoorbeeld geen post bezorgd. Een brief die op zaterdag zou aankomen, maar als gevolg van een

systemenstoring pas op woensdag wordt geleverd, komt derhalve twee bezorgdagen later aan dan gepland.

Onderdeel b
In dit onderdeel is geregeld dat een incident een significant incident is wanneer de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast. Gegevens die noodzakelijk zijn voor de dienstverlening van post- en koerierdienst kunnen van vertrouwelijke aard zijn en lopen daarmee risico op onbedoelde openbaarmaking of verlies.
De vertrouwelijkheid van gegevens kan bijvoorbeeld worden aangetast wanneer de encryptie van een dienst niet correct heeft gewerkt, of wanneer sprake is van ongeoorloofde toegang waarbij de kwaadwillenden gegevens van de entiteit hebben ontvreemd. Ook de integriteit van de dienstverlening kan worden geraakt, bijvoorbeeld doordat gegevens worden gecorrumpeerd die noodzakelijk zijn voor de correcte werking van de netwerk- en informatiesystemen van post- en koerierdiensten.
De meldplicht is echter niet beperkt tot incidenten die het gevolg zijn van kwaadwillige toegang. Ook menselijke fouten vallen hieronder, bijvoorbeeld. Hierbij kan gedacht worden aan het onbedoeld openbaar maken van vertrouwelijke gegevens of het onjuist uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Artikel 12 - Criteria significante incidenten in de sector vervaardiging
De sector vervaardiging vormt een diverse en sterk geautomatiseerde sector, waarin productieprocessen grotendeels afhankelijk zijn van industriële besturingssystemen (Operational Technology, OT). Een verstoring in deze systemen kan directe gevolgen hebben voor de continuïteit van het productieproces, de kwaliteit en veiligheid van de gefabriceerde producten en de veiligheid van medewerkers en de directe omgeving.
Om incidentmeldingen proportioneel en uitvoerbaar te maken, is ervoor gekozen om de meldplicht te baseren op internationaal erkende impactclassificaties die de ernst van verstoringen in OT-omgevingen betrouwbaar beschrijven. De IEC 62443-normenreeks biedt hiervoor de meest gebruikte referentie. Deze norm is ontwikkeld door de International Electrotechnical Commission (IEC) en wordt wereldwijd toegepast in onder meer de procesindustrie, machinebouw en high-techsector. In deze normenreeks wordt beschreven hoe organisaties de beveiliging van industriële automatiserings- en controlesystemen systematisch kunnen beoordelen, beheren en verbeteren. De onderdelen die hier relevant zijn, zijn met name:

- IEC 62443-2-1: Security program requirements for IACS
- IEC 62443-2-3: Patch & incident management for IACS
- IEC 62443-3-2: Security risk assessment and system design

Deze onderdelen bevatten eveneens een geharmoniseerde classificatie van incidenten op basis van impactniveau's (Negligible – Minor – Major – Critical – Catastrophic). Een incident met impactniveau "Major" of hoger betekent dat één of meer kritieke functies van het productieproces zijn aangetast of dat herstel handmatige interventie vereist. Deze grens vormt in de praktijk een goede, bruikbare referentie voor wat binnen de Cyberbeveiligingswet als een significant incident kan worden beschouwd.
IEC 62443 is te beschouwen als een internationale normenreeks voor industriële cybersecurity. De reeks richt zich primair op IACS, maar vereist dat ook ondersteunende IT-systemen die de OT-zones beïnvloeden in scope zijn.

De meldingscriteria in dit artikel sluiten aan bij de praktijk in de vervaardigingssector, waar procesautomatisering en machineveiligheid sterk verweven zijn. Incidenten leiden niet vaak tot massale ICT-uitval, maar veelal wel tot verlies van bijvoorbeeld productiekwaliteit of traceerbaarheid van gegevens (organisaties moeten in staat zijn de gegevensstromen te reconstrueren, vanaf herkomst en toegang tot aan eventuele wijzigingen en gebruik). Door de meldingscriteria met name te baseren op de IEC 62443-impactniveaus wordt aangesloten bij bestaande risicobeoordelingen en beveiligingsprogramma's van bedrijven. Tegelijkertijd zorgt het voor uniformiteit en internationale vergelijkbaarheid binnen de OT-toeleveringsketen die veelal conform deze norm werken (o.a. in de automobiel- en halfgeleidersector). Tot slot zijn de criteria zo geformuleerd dat kleine storingen, zoals sensorfouten of netwerkvertragingen die frequent voorkomen niet meldingsplichtig zijn. Hiermee wordt het overmatig rapporteren van incidenten voorkomen en worden de gevolgen voor regeldruk beperkt.

Onderdeel a
Het eerste criterium, zoals opgenomen in dit onderdeel, betreft de veiligheid (Safety). Ten aanzien van veiligheid moet er gemeld worden als er sprake is van verlies of degradatie van veiligheidsfuncties door een defect of anderszins niet normaal functionerend industrie specifiek netwerk- en informatiesysteem. Bij veiligheidsfuncties kan gedacht worden aan Safety Instrumented Systems (instrumentele beveiliging die een veilige staat van het productieproces behoudt op het moment dat gevaarlijke of onacceptabele procescondities worden gedetecteerd), noodstops en gasdetectie. Dergelijke incidenten leiden tot verhoogd risico op letsel of gevaarlijke situaties. Zo kan een defect in de veiligheids-PLC ervoor zorgen dat een noodstop niet meer functioneert tijdens onderhoudswerkzaamheden.

Onderdeel b
Het in dit onderdeel opgenomen criterium betreft de beschikbaarheid van essentiële besturings- of monitoringsfuncties door een niet-normaal functionerend industriespecifiek netwerk- en informatiesysteem. (Availability). Het gaat hier om tijdelijke of langdurige verlies van besturing (Loss of Control (LOC)), of verlies van proceszicht of monitoring (Loss of View (LOV)). Als voorbeeld van een dergelijk incident kan worden gedacht aan een aanval op het Manufacturing Execution System (MES) die tijdelijk de communicatie tussen productielijnen en het ERP-systeem stillegt, waardoor de productie niet kan worden aangestuurd of bewaakt.

Onderdeel c
Het derde criterium betreft de inbreuk op de integriteit van het industriespecifieke netwerk- en informatiesysteem waardoor kwaliteit van het product of het productieproces in gevaar is gekomen of kan komen. Hierbij kan gedacht worden aan manipulatie van procesparameters, recepturen of meetwaarden waardoor productkwaliteit, materiaalconformiteit of wettelijke eisen (zoals voedselveiligheid, CE-markering) in gevaar komen of kunnen komen. Een voorbeeld hiervan is wanneer een wijziging in de PLC-logica (programmable logic controller, in feite een computer die speciaal is ontwerpen voor industriële toepassingen) leidt tot afwijkende temperatuurinstellingen bij kunststofextrusie, wat resulteert in ondeugdelijke producten.

Onderdeel d
Het in dit onderdeel opgenomen criterium betreft het melden van significante incidenten die leiden tot milieuschade als gevolg van een inbreuk op de beveiliging van netwerk- en informatiesystemen. Als voorbeeld kan gedacht worden aan een

cyberaanval op een waterzuiveringsinstallatie wat bij een entiteit zorgt voor ongecontroleerde lozing van afvalwater.

Onderdeel e
Het vijfde criterium is een beveiligingsinbreuk (Security Level breach). In IEC 62443 wordt per systeem of zone een beveiligingsniveau (*Security Level; SL1–SL4)* vastgesteld, passend bij het dreigingsprofiel. Een incident significant wanneer een actor succesvol een aanval uitvoert die het beoogde beveiligingsniveau overstijgt, bijvoorbeeld een SL2-geclassificeerd systeem dat wordt gecompromitteerd door een aanval met SL3-capaciteiten. Dit wijst op een structureel tekort in de beveiligingsarchitectuur.

Onderdeel f
Het zesde criterium is cross-zone propagatie. Industriële netwerk- en informatiesystemen zijn veelal ingedeeld in *zones* (afgesloten beveiligingsdomeinen) die via zogeheten *conduits* (communicatiekanaal tussen zones waarover gegevensverkeer plaatsvindt) met elkaar communiceren. Een incident is significant wanneer de aanval zich verspreidt naar een of meerdere zones of via een *conduit* overstapt naar een hoog risico-omgeving (het geheel van systemen waarbij een onderbreking of aantasting van normale functioneren ervan kan leiden tot grote gevolgen zoals letsel of milieuschade), zoals de productiebesturing of beveiligingsslaag. Als voorbeeld kan gedacht worden aan malware die vanuit een kantoor-IT-systeem tot het PLC-netwerk binnendringt.

Artikel 13 - Criteria significante incidenten in de sector onderzoek
In dit artikel is een criterium opgenomen dat bepaalt wanneer een incident als significant moet worden beschouwd. Voor de sector onderzoek wordt een incident als significant aangemerkt indien de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast. Gegevens die noodzakelijk zijn voor de uitvoering van (toegepast) onderzoek met het oog op een commerciële toepassing zijn door de aard van het onderzoek doorgaans vertrouwelijk en lopen daardoor risico op onbedoelde openbaarmaking of verlies.
De vertrouwelijkheid van gegevens kan bijvoorbeeld worden aangetast wanneer de encryptie van een dienst niet correct heeft gewerkt, of wanneer sprake is van ongeoorloofde toegang waarbij de kwaadwillenden gegevens van de entiteit hebben ontvreemd. Ook kan er sprake zijn van de aantasting van de integriteit van het onderzoek. Bij kwaadwillige toegang kunnen onderzoeksgegevens gecorrumpeerd worden, wat gevolgen kan hebben voor de betrouwbaarheid of juistheid van onderzoeksresultaten.
De meldplicht is echter niet beperkt tot kwaadwillige toegang. Ook menselijke fouten vallen hieronder. Hierbij kan gedacht worden aan het onbedoeld openbaar maken van vertrouwelijke gegevens of het onjuist uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Hoofdstuk 4. Overige en slotbepalingen

Artikel 14 – Aanwijzing autoriteiten
Dit artikel geeft uitvoering aan de bevoegdheid van de Minister van Economische Zaken om op grond van artikel 51, tweede lid, onderdeel i, van de Cyberbeveiligingswet autoriteiten aan te wijzen waarmee de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt als bedoeld in de wet (de zogenoemde Cbw-instanties) samenwerken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van de wet.

In dit artikel is de Minister van Economische Zaken, uit hoofde van de Wet ruimtevaartactiviteiten, Verordening (EU) 2019/881, Verordening (EU) 2024/2847 en de Telecommunicatiewet, aangewezen als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet. In alle gevallen gaat het om dezelfde toezichthouder: de Rijksinspectie Digitale Infrastructuur (RDI).
Dit artikel waarborgt dat de toezichthouders op deze sectorspecifieke regelgeving effectief kunnen samenwerken en informatie kunnen uitwisselen met de Cbw-instanties, met het oog op doelmatig en samenhangend toezicht en het beperken van toezichtlasten voor entiteiten.

Artikel 15 – Intrekking Regeling aanwijzing aanbieders essentiële diensten EZK
Met dit artikel wordt de Regeling aanwijzing aanbieders essentiële diensten EZK die uitvoering gaf aan de Wet beveiliging netwerk- en informatiesystemen (Wbni), ingetrokken.
De Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de NIS-richtlijn) was geïmplementeerd in de Wbni. De NIS-richtlijn is vervangen door de NIS2-richtlijn. De Cyberbeveiligingswet (Cbw) implementeert de NIS2-richtlijn in Nederland. Met de inwerkingtreding van de Cbw worden de Wbni en de daarop gebaseerde regelgeving ingetrokken. Voor zover het betreft regelingeving van de Minister van Economische Zaken gaat het hierbij om de Regeling aanwijzing aanbieders essentiële diensten EZK. Deze regeling was tevens van toepassing op de energiesector, die thans onder de verantwoordelijkheid valt van de Minister van Klimaat en Groene Groei.

De Minister van Economische Zaken,