STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 25627
21 juli 2026

Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 5 juli 2026, nr. WJZ/ 101446051, houdende regels voor essentiële en belangrijke entiteiten in de EZK-sectoren (Regeling cyberbeveiliging EZK) (KetenID WGK 28487)

De Staatssecretaris van Economische Zaken en Klimaat, na overleg met de Minister van Justitie en Veiligheid, handelende in overeenstemming met de Minister van Economische Zaken en Klimaat,

Gelet op de artikelen 19, 23, eerste lid, en 28 van het Cyberbeveiligingsbesluit;

Besluit:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:
alarmnummer: alarmnummer als bedoeld in artikel 7.7, tweede lid, van de Telecommunicatiewet;
besluit: Cyberbeveiligingsbesluit;
Minister: Minister van Economische Zaken en Klimaat;
postzending: postzending als bedoeld in artikel 2, zesde lid, van Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst (PbEG 1998, L 15);
richtlijn (EU) 2016/943: Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (PbEU 2016, L 157);
ruimtevoorwerp: ruimtevoorwerp als bedoeld in artikel 1 van de Wet ruimtevaartactiviteiten;
zone: logische of fysieke groep van systemen, apparaten of processen met vergelijkbare beveiligingsvereisten.

Artikel 2. Reikwijdte

De hoofdstukken 2 en 3 zijn 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, ten aanzien waarvan de Minister ingevolge artikel 15, vierde lid, van de wet de bevoegde autoriteit is
Ruimtevaart		Operators van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten van de Europese Unie of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatienetwerken

Sector	Subsector	Soorten entiteiten
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

Ter uitvoering van artikel 6 van het besluit legt de essentiële entiteit of belangrijke entiteit als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het besluit, vast:

a. welke maatregelen voor het beheer van cyberbeveiligingsrisico's, met inbegrip van processen en controles, moeten worden gemonitord, gemeten, geanalyseerd en geëvalueerd;
b. de methoden voor het monitoren, meten, analyseren en evalueren om valide resultaten te waarborgen;
c. wanneer de monitoring en de meting moeten worden uitgevoerd;
d. wie is belast met het monitoren en meten van de doeltreffendheid van de maatregelen voor het beheer van cyberbeveiligingsrisico's;
e. wanneer de resultaten van de monitoring en meting moeten worden geanalyseerd en geëvalueerd;
f. wie is belast met het analyseren en evalueren van deze resultaten.

Artikel 4. Bedrijfscontinuïteit

1. De processen en procedures voor het maken en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens, bedoeld in artikel 9, tweede lid, van het besluit, omschrijven van welke software en gegevens een back-up wordt gemaakt en bevatten ten aanzien van die software en gegevens:
   a. hersteltijden;
   b. herstelpunten;
   c. waarborgen voor de volledigheid en nauwkeurigheid van back-ups;
   d. waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
   e. waarborgen voor herstel van software en gegevens uit back-ups;
   f. bewaartermijnen.

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

Artikel 5. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

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

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

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

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

Artikel 6. Beveiligingsaspecten ten aanzien van toegangsbeleid

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

2. Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, zorgt ervoor dat:
   a. sterke identificatie-, authenticatie- en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;
   b. voorrechten op het gebied van systeembeheer zoveel mogelijk geïndividualiseerd en beperkt worden toegekend;
   c. voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt.

HOOFDSTUK 3. CRITERIA MELDPLICHT

Artikel 7. Algemene criteria significant incident

1. Voor de toepassing van artikel 25, tweede lid, van de wet is een incident in ieder geval een significant incident als:
   a. het de dood van een of meer natuurlijke personen heeft veroorzaakt of kan veroorzaken; of
   b. het aanzienlijke schade aan de gezondheid van een of meer natuurlijke personen heeft veroorzaakt of kan veroorzaken.

2. Een incident is tevens een significant incident als het voldoet aan een of meer criteria, bedoeld in de artikelen 8 tot en met 13.

3. In afwijking van het tweede lid is een incident niet significant als het incident het gevolg is van

gepland onderhoud dat door of namens de essentiële entiteit of belangrijke entiteit wordt uitgevoerd, voor zover de onderbreking, opschorting of beëindiging van een door de essentiële entiteit of belangrijke entiteit verleende dienst een voorzien gevolg is van dat onderhoud.

Artikel 8. Criteria significant incident bij aanbieder van een openbaar elektronisch communicatienetwerk of aanbieder van een openbare elektronische communicatiedienst

Voor een essentiële entiteit of een belangrijke entiteit die aanbieder is van een openbaar elektronisch communicatienetwerk of van een openbare elektronische communicatiedienst, is een incident in ieder geval een significant incident als:

a. bij een onderbreking van de levering van een openbare elektronische communicatiedienst ten minste 50.000 gebruikers zijn getroffen voor een duur van vier uur of langer;
b. de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening van het openbare elektronische communicatienetwerk of de openbare elektronische communicatiedienst worden opgeslagen, verzonden of verwerkt, is aangetast, met gevolgen voor ten minste 1% van de gebruikers van het openbare elektronische communicatienetwerk of de openbare elektronische communicatiedienst, met een minimum van 10.000 gebruikers; of
c. het alarmnummer niet beschikbaar is.

Artikel 9. Criteria significant incident bij aanbieder van een internetknooppunt

Voor een essentiële entiteit of een belangrijke entiteit die aanbieder is van een internetknooppunt, is een incident in ieder geval een significant incident als:

a. ten minste 25% van het actuele totale verkeer dat door het internetknooppunt wordt verwerkt, gemeten in datavolume in bits per seconde, gedurende ten minste 30 minuten 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, met gevolgen voor meer dan 5% van de gebruikers.

Artikel 10. Criteria significant incident in de sector ruimtevaart

Voor een essentiële entiteit of een belangrijke entiteit in de sector ruimtevaart is een incident in ieder geval een significant incident als de integriteit, authenticiteit, beschikbaarheid of vertrouwelijkheid van gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering van een ruimtevoorwerp is aangetast tijdens een tijdvak waarin volgens de reguliere operationele planning communicatie met dat ruimtevoorwerp mogelijk en voorzien is, waardoor een risico ontstaat voor de besturing of het behoud van dat ruimtevoorwerp.

Artikel 11. Criteria significant incident in de sector post- en koerierdiensten

Voor een essentiële entiteit of een belangrijke entiteit in de sector post- en koerierdiensten is een incident in ieder geval een significant incident als:

a. ten minste 30% van de ontvangers van de post- en koerierdienst hun postzending ten minste twee bezorgdagen later ontvangt dan op grond van wettelijke of contractuele verplichtingen zou moeten; of
b. de integriteit, vertrouwelijkheid of authenticiteit van digitale gegevens die in verband met haar dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast, waardoor persoonsgegevens en adresgegevens onrechtmatig worden verwerkt of het briefgeheim wordt geschonden.

Artikel 12. Criteria significant incident in de sector vervaardiging

Voor een essentiële entiteit of een belangrijke entiteit in de sector vervaardiging is een incident in ieder geval een significant incident als:

a. veiligheidsfuncties zijn verloren gegaan;
b. de beschikbaarheid of integriteit van essentiële besturings- of monitoringsfuncties is verloren gegaan;
c. de continuïteit van het productieproces in gevaar is gekomen of kan komen;
d. milieuschade als bedoeld in artikel 17.6, eerste lid, van de Wet milieubeheer is opgetreden; of
e. ongeoorloofde toegang tot een industrie-specifiek netwerk- en informatiesysteem heeft plaatsgevonden en zich naar meerdere zones of omgevingen heeft verspreid.

Artikel 13. Criteria significant incident in de sector onderzoek

Voor een essentiële entiteit of een belangrijke entiteit in de sector onderzoek als bedoeld in bijlage 2 bij de wet, ten aanzien waarvan de Minister ingevolge artikel 15, vierde lid, van de wet de bevoegde autoriteit is, is een incident in ieder geval een significant incident als:

a. het incident heeft geleid of kan leiden tot de ongeoorloofde openbaarmaking van bedrijfsgeheimen als bedoeld in artikel 2, eerste lid, van Richtlijn (EU) 2016/943 van de essentiële entiteit of belangrijke entiteit; of
b. de integriteit, vertrouwelijkheid of authenticiteit van onderzoeksgegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast, waardoor aanzienlijke materiële of immateriële schade ontstaat bij andere entiteiten.

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 en Klimaat, uit hoofde van de Wet ruimtevaartactiviteiten;
b. de Minister van Economische Zaken en Klimaat, uit hoofde van Verordening (EU) 2019/881;
c. de Minister van Economische Zaken en Klimaat, uit hoofde van Verordening (EU) 2024/2847;
d. de Minister van Economische Zaken en Klimaat, uit hoofde van de Telecommunicatiewet;
e. de Autoriteit Consument en Markt, uit hoofde van de Postwet 2009.

Artikel 15. Intrekking Regeling aanwijzing aanbieders essentiële diensten EZK

De Regeling aanwijzing aanbieders essentiële diensten EZK wordt ingetrokken.

Artikel 16. Inwerkingtreding

Indien het bij koninklijke boodschap van 2 juni 2025 ingediende voorstel van wet houdende regels ter implementatie van 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 (PbEU 2022, L 333) (Cyberbeveiligingswet) (Kamerstukken 36 764) tot wet is of wordt verheven en die wet in werking treedt, treedt deze regeling op hetzelfde tijdstip in werking.

Artikel 17. Citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging EZK.

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

's-Gravenhage, 5 juli 2026

De Staatssecretaris van Economische Zaken en Klimaat,
W.J.M. Aerdts

TOELICHTING

I. Algemeen

1. Inleiding

Deze regeling strekt tot nadere uitwerking van de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb). De Cbw implementeert de NIS2-richtlijn[1] en heeft tot doel om een hoger niveau van cyberweerbaarheid voor de onder haar werkingssfeer vallende essentiële en belangrijke entiteiten te bewerkstelligen.
De Cbw verplicht deze entiteiten onder andere 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.

Deze regeling bevat een nadere uitwerking van de Cbw en het Cbb voor de volgende sectoren ten aanzien waarvan de Minister van Economische Zaken en Klimaat ingevolge artikel 15, van de wet de bevoegde autoriteit is:
– ruimtevaart;
– post- en koeriersdiensten;
– vervaardiging;
– onderzoek, en
– binnen de sector digitale infrastructuur voor de soorten entiteiten aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten en aanbieders van internetknooppunten.

Bij de sector vervaardiging gaat het om de volgende subsectoren:
– vervaardiging van informaticaproducten en van elektronische en optische producten;
– vervaardiging van elektrische apparatuur;
– vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd;
– vervaardiging van motorvoertuigen, aanhangers en opleggers; en
– vervaardiging van andere transportmiddelen.

Voor de overige soorten entiteiten binnen de sector digitale infrastructuur die onder de Cbw vallen, geldt voor de uitwerking van de zorgplicht en de meldplicht rechtstreeks de Uitvoeringsverordening (EU) 2024/2690[2]. De bepalingen van hoofdstukken 2 en 3 zijn voor deze soorten entiteiten niet van toepassing. Het gaat hierbij om DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud en verleners van vertrouwensdiensten. Deze uitvoeringsverordening is ook van toepassing op aanbieders van beheerde diensten en aanbieders van beheerde beveiligingsdiensten en op digitale aanbieders. Bij deze laatste sector gaat het om aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten.

Bij het opstellen van deze regeling is waar mogelijk afstemming gezocht met en om input gevraagd van bedrijven en brancheverenigingen uit de betrokken sectoren, om de maatregelen zo goed mogelijk te laten aansluiten bij de bestaande praktijk, de uitvoerbaarheid te waarborgen en onnodige regeldruk voor essentiële en belangrijke entiteiten te voorkomen.

2. Hoofdlijnen van de regeling

2.1 Algemeen

In deze regeling zijn verschillende verplichtingen uit de Cbw en het Cbb nader uitgewerkt ter bevordering van de beveiliging van de netwerk- en informatiesystemen. Verder omvat deze regeling een

[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 (PbEU 2022, L 333).
[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).

nadere invulling van de criteria voor de beoordeling of sprake is van een incident significant. Ook voorziet zij in de mogelijkheid voor het CSIRT, de bevoegde autoriteit en het centrale contactpunt om met de in deze regeling aangewezen autoriteiten informatie uit te wisselen ten behoeve van een doelmatige uitvoering van hun taken. Deze drie onderwerpen worden hieronder nader toegelicht.

2.2 Nadere regels zorgplicht

In deze regeling worden voor de in artikel 2 genoemde sectoren en subsectoren nadere regels gesteld ten aanzien van de zorgplicht, bedoeld in artikel 21 van de Cbw en zoals nader uitgewerkt in het Cbb. Het doel van deze nadere invulling is om de 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 draagt bij aan een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen.
Bij het opstellen van deze nadere regels is aangesloten bij de systematiek van de Cbw, het Cbb en Uitvoeringsverordening (EU) 2024/2690. Daarmee is de regeling afgestemd op de systematiek van Uitvoeringsverordening (EU) 2024/2690, zodat entiteiten op wie die uitvoeringsverordening van toepassing is, beide kaders naast elkaar kunnen toepassen. Net zoals bij de uitwerking van de zorgplicht in de Cbw en het Cbb zijn bij het nader uitwerken van de zorgplicht in deze regeling bestaande normenkaders als uitgangspunt gehanteerd, zoals ISO 27001. Daarbij is gecontroleerd of de zorgplicht in deze regeling deze normenkaders niet doorkruist. In de toelichting wordt, waar van toepassing, naar bestaande normenkaders verwezen. Entiteiten behouden hiermee de ruimte om hun bestaande normenkader te blijven hanteren, mits zij ervoor zorgen dat de maatregelen die voortvloeien uit de in artikel 21 van de Cbw neergelegde zorgplicht en de uitwerking daarvan in het Cbb en deze regeling, zijn geborgd. Net zoals de Cbw en het Cbb, gaat deze regeling uit van een risicogebaseerde aanpak en schrijft daarom niet in alle gevallen voor hoe invulling moet worden gegeven aan de maatregelen. Essentiële en belangrijke entiteiten dienen overeenkomstig de zorgplicht van artikel 21 van de Cbw deze maatregelen op passende en evenredige wijze in te vullen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken te beheersen en incidenten te voorkomen of de gevolgen ervan te beperken.

2.3 Nadere regels meldplicht

De Cbw heeft tot doel 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. Door het melden van significante incidenten door essentiële en belangrijke entiteiten kan de bevoegde autoriteit, in de praktijk de toezichthouder, patronen en kwetsbaarheden signaleren en entiteiten indien nodig gerichte aanwijzingen geven voor verdere verbetering van hun cyberweerbaarheid.

De meldplicht geldt als zich een significant incident voordoet. Ingevolge artikel 25, tweede lid, van de Cbw is een incident significant als het:
a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of
b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

In artikel 23, eerste lid, van het Cbb is bepaald dat de betrokken Minister, 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, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten. Van deze bevoegdheid is met deze regeling gebruikgemaakt.

Deze regeling bevat regels inzake de criteria aan de hand waarvan wordt bepaald of incidenten significant zijn als bedoeld in artikel 25, tweede lid, van de Cbw.
In artikel 1 van de Cbw 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.*' Met deze definitie wordt een incident expliciet gekoppeld aan de beveiliging van de netwerk- en informatiesystemen van een entiteit. In deze regeling zijn de meldcriteria veelal ook geformuleerd in termen van beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid. 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.

De meldcriteria vormen een gedeeltelijke nadere uitwerking van de wettelijke norm en beogen

duidelijkheid te bieden over wanneer in ieder geval sprake is van een meldplichtig incident. Met het oog op de uitvoerbaarheid en de beperking van regeldruk voor entiteiten is ervoor gekozen om niet alle parameters uit artikel 25, tweede lid, van de Cbw nader uit te werken. Dit zou ertoe leiden dat entiteiten voor al die criteria specifieke processen zouden moeten inrichten om tijdig te kunnen vaststellen of zij aan die criteria voldoen, zoals het vaststellen van een meldcriterium voor financieel verlies. De meldplicht is in deze regeling dan ook niet uitputtend geregeld. Incidenten die voldoen aan de algemene criteria in de wet blijven in beginsel meldplichtig. De in de regeling opgenomen criteria zijn bedoeld als het primaire beoordelingskader voor entiteiten en voor het uitoefenen van toezicht en handhaving. De wettelijke criteria uit artikel 25, tweede lid, van de Cbw blijven onverkort van toepassing als vangnet voor gevallen die niet onder de in deze regeling opgenomen criteria vallen.

Zodra een incident voldoet aan één of meerdere van de in deze regeling opgenomen meldcriteria, is er in ieder geval sprake van een significant incident en dient een essentiële of belangrijke entiteit dat incident te melden.
Een essentiële entiteit of belangrijke entiteit meldt een significant incident bij het eigen CSIRT en de bevoegde autoriteit. 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 Cbw en worden in deze regeling niet verder uitgewerkt.

2.4 Aanwijzing autoriteiten

Een aantal wetten heeft nauwe raakvlakken 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, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cbw.
In het Cbb is ervoor gekozen de betrokken Minister de bevoegdheid te geven om de autoriteiten, bedoeld in artikel 51, tweede lid, onderdeel i, van de wet bij regeling aan te wijzen. 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 Cbw vallen. Derhalve ligt de keuze voor de hand om de aanwijzing op het niveau van de ministeriële regeling te beleggen.
De aanwijzing van autoriteiten in deze regeling maakt het in het bijzonder voor bevoegde autoriteiten mogelijk om in het geval van overlappend toezicht nauwer samen te werken en informatie uit te wisselen. Dit bevordert doelmatig en doeltreffend toezicht, waarmee ook onnodige toezichtslasten voor entiteiten worden beperkt.

3. Toezicht en handhaving

Met het toezicht op de naleving van deze regeling worden ambtenaren van de Rijksinspectie Digitale Infrastructuur (hierna: RDI) belast. De betreffende ambtenaren oefenen hun bevoegdheden uit met inachtneming van artikel 69 van de Cbw.

4. Notificatie

Deze regeling bevat geen technische voorschriften in de zin van richtlijn nr. 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PbEU 2015, L 241). Er is derhalve geen notificatie krachtens deze richtlijn nodig.

5. Regeldruk

Deze regeling veroorzaakt geen incidentele of structurele aanvullende regeldruk ten opzichte van de reeds berekende regeldruk voor essentiële en belangrijke entiteiten onder de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb). De meld- en zorgplicht in deze regeling betreffen een uitwerking van de Cbw en Cbb en kunnen niet los worden gezien van het gehele pakket aan regels in de zorg- en meldplicht uit de NIS2-richtlijn, Cbw en Cbb.
Van de artikelen die de zorgplicht in deze regeling concretiseren bevat het merendeel aspecten die een entiteit bij de beleidsvorming moet betrekken. Die artikelen betreffen een verduidelijking en de administratieve lasten zijn reeds verdisconteerd in de omvang van de lasten die zijn beschreven in de memorie van toelichting bij de Cbw en de nota van toelichting bij het Cbb. De zorgplicht in deze regeling is daarbij onlosmakelijk verbonden met de verplichte risicoanalyse die essentiële en belangrijke entiteiten moeten uitvoeren. Om deze redenen wordt de zorgplicht in deze regeling niet gezien als aanvullende verplichtingen ten aanzien van de Cbw en Cbb.

De meldcriteria onder de Cbw, brengen ook geen aanvullende uitvoeringslasten met zich mee voor essentiële en belangrijke entiteiten. De meldcriteria zijn zo gekozen dat het aantal meldingen dat gedaan moet worden, niet hoger zal liggen dan waar al rekening mee is gehouden bij de Cbw en het Cbb. De last van deze meldingen is reeds becijferd in de memorie van toelichting bij de Cbw.

Kortom, de regeldruk voor essentiële en belangrijke entiteiten in alle sectoren, zoals vermeld in bijlage 2 bij de Cbw, is becijferd en verantwoord in de toelichtingen bij de Cbw en Cbb. Daarbij is reeds rekening gehouden met de kosten die entiteiten moeten maken om maatregelen te treffen (de zorgplicht) en om meldplichtige incidenten te doen (meldplicht).

6. Advies en consultatie

6.1 Internetconsultatie

6.1.1 Opmerkingen betreffende de zorgplicht

Over een concept van deze regeling is een internetconsultatie gehouden via www.internetconsultatie.nl. De consultatie heeft 16 reacties opgeleverd, waarvan 8 openbaar zijn.
Gelijktijdig vonden internetconsultaties plaats over de concepten van de Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector, de Cyberbeveiligingsregeling IenW, en de Regeling cyberbeveiliging levensmiddelensector. In het kader daarvan zijn eveneens reacties ingediend. De reacties die met betrekking tot de zorgplicht op de vier hierboven genoemde concept-regelingen zijn binnengekomen zijn door de betrokken ministeries gezamenlijk en integraal beoordeeld om zodoende tot een gelijkluidende uitwerking van de zorgplicht in de betreffende regelingen te komen.

Meerdere partijen hebben in hun reacties gesteld dat deze aanpak efficiënt en doeltreffend is voor bedrijven die in meerdere sectoren actief zijn en dat dit aansluit bij *best practices* en bestaande standaarden. Cyberveilig Nederland heeft gesteld dat naar haar oordeel de zorgplicht in alle regelingen op consistente wijze is uitgewerkt en goed aansluit bij nationaal en internationaal erkende en toegepaste normen, wat de harmonisatie en implementatie bevordert.

BTG heeft in haar reactie verzocht een verwijzing naar bestaande normen, zoals ISO- en NEN-normen, op te nemen. Naar aanleiding van deze reactie en soortgelijke reacties op de concept-regelingen van de andere ministeries, is de algemene inleiding van de toelichting op de zorgplicht aangevuld.

6.1.2 Algemene en sector-overstijgende opmerkingen betreffende de meldplicht

Meerdere partijen hebben in hun reactie gesteld dat uit artikel 7 en de toelichting niet duidelijk blijkt wat het toepassingsbereik is van een significant incident. Er zijn zorgen geuit dat bijvoorbeeld bedrijfsongevallen ook op grond van deze regeling ook meldplichtig zouden zijn. Een incident is volgens artikel 1 van de wet 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. Dit betekent dat significante incidenten in de context van deze definitie moeten worden beschouwd en die dus verband houden met de opgeslagen, verzonden of verwerkte gegevens dan wel de diensten die via deze netwerk- en informatiesystemen van een entiteit worden aangeboden. In deze regeling zijn in artikel 7 sectoroverstijgend en in de artikelen 8 tot en met 13 sectorspecifiek nader gedefinieerd wat significante incidenten zijn en daarmee meldplichtig zijn.

Meerdere partijen hebben gevraagd in hoeverre bedrijfsongevallen onder de regeling vallen. Bedrijfsongevallen zijn als zodanig niet meldplichtig op grond van deze regeling. Indien een netwerk- of informatiesysteem echter uitvalt of wordt verstoord, bijvoorbeeld als gevolg van een bedrijfsongeval, en deze uitval of verstoring voldoet aan een of meer van de in deze regeling opgenomen criteria, dan wel aan een van de parameters van artikel 25, tweede lid, van de Cbw die in deze regeling geen nadere uitwerking hebben gekregen, is dat incident meldplichtig. Een bedrijfsongeval kan ook een direct gevolg zijn van een incident, bijvoorbeeld bij een verstoring van veiligheidsfuncties. Als het incident voldoet aan een of meer criteria van deze regeling, dan wel aan een van de criteria van artikel 25, tweede lid, van de Cbw, die in deze regeling geen nadere uitwerking hebben gekregen, dient het te worden gemeld.

Meerdere partijen hebben gevraagd in hoeverre bedrijfsongevallen onder de regeling vallen. Bedrijfsongevallen zijn als zodanig niet meldplichtig op grond van deze regeling. Indien een netwerk- of informatiesysteem echter uitvalt of wordt verstoord, bijvoorbeeld als gevolg van een bedrijfsongeval, en deze uitval of verstoring voldoet aan een of meer van de in deze regeling opgenomen criteria, dan wel aan een van de criteria van artikel 25, tweede lid, van de Cbw die in deze regeling geen nadere uitwerking hebben gekregen, is dat incident meldplichtig. Een bedrijfsongeval kan ook een

direct gevolg zijn van een incident, bijvoorbeeld bij een verstoring van veiligheidsfuncties. Indien het incident voldoet aan een of meer criteria van deze regeling, dient het te worden gemeld.

BTG en Netbeheer Nederland hebben in hun reacties gesteld dat artikel 7, eerste lid, onderdelen a en b, nadere verduidelijking behoeven. Volgens hen is niet duidelijk of schade aan de gezondheid zich beperkt tot directe schade dan wel mede indirecte keteneffecten omvat. Tevens is onduidelijk welke criteria gelden voor het begrip 'aanzienlijke schade'. Naar aanleiding hiervan is de artikelsgewijze toelichting op artikel 7 verduidelijkt met situaties die onder de onderdelen a en b als significant incident worden aangemerkt. Hierbij is verduidelijkt wat onder 'aanzienlijke schade' wordt verstaan.

6.1.3 Opmerkingen betreffende de meldplicht voor aanbieders van elektronische communicatienetwerken of -diensten

Meerdere partijen hebben in hun reactie gesteld dat artikel 8, onderdeel a, ertoe zou leiden dat ook regelmatig voorkomende operationele verstoringen gemeld zouden moeten worden. Als voorbeeld wordt onder andere een defecte kaart in de transmissie-apparatuur genoemd. Deze partijen geven aan dat de meeste verstoringen van de dienstverlening binnen vier uur worden opgelost en hierbij de impact op gebruikers veelal gering is. Daarom is er ook voor gekozen om verstoringen korter dan 4 uur niet meldplichtig te laten zijn. Naar aanleiding hiervan is aan artikel 8, onderdeel a, een minimale tijdsduur van vier uur toegevoegd.

Daarnaast hebben ook meerdere partijen gesteld dat de drempel van minimaal 50.000 gebruikers te laag is. Zo wordt voorgesteld om deze drempel te verhogen naar 100.000 gebruikers. Bij een incident zou de drempel van 50.000 gebruikers namelijk al relatief snel kunnen worden bereikt, omdat bij grote aanbieders 50.000 gebruikers een relatief klein deel van hun totale klantenbestand is. Dit voorstel is niet overgenomen. Het verhogen van de drempel van 50.000 gebruikers naar 100.000 gebruikers zou ertoe leiden dat middelgrote en kleinere aanbieders van openbare elektronische communicatienetwerken- en diensten bij incidenten niet of nauwelijks aan het meldcriterium zullen voldoen, omdat zij over een kleiner klantenbestand beschikken. Als gevolg hiervan zouden incidenten buiten het zicht van de toezichthouder en het CSIRT kunnen blijven. Daarnaast waarborgt een meldcriterium van 50.000 gebruikers dat de toezichthouder een goede inschatting kan maken van de geografische impact van een incident.

Meerdere partijen stellen dat een incident onder artikel 8, onderdeel b, al snel gemeld zou moet worden, wat volgens deze partijen onevenredig is. Onder het meldcriterium zou elke aantasting van integriteit, vertrouwelijkheid, of authenticiteit van gegevens meldplichtig zijn. Zij stellen voor om bij deze bepaling een drempelwaarde van minimaal 10.000 getroffen gebruikers te hanteren. Naar aanleiding hiervan is het criterium aangepast. Een aantasting is nu alleen meldplichtig indien een incident ten minste 1% van de gebruikers treft, met een minimum van 10.000 gebruikers. Voor grote aanbieders zal 1% gebruikers in absolute zin boven de 10.000 gebruikers liggen. Voor kleine aanbieders zou het hanteren van een meldcriterium van 1% getroffen gebruikers geen of amper maatschappelijke impact hebben; derhalve is een ondergrens van 10.000 gebruikers geïntroduceerd.
Daarnaast hebben meerdere partijen verzocht de term 'gegevens' nader te specificeren. Naar aanleiding hiervan is de artikelsgewijze toelichting op artikel 8 aangevuld. Bij gegevens kan het bijvoorbeeld gaan om verkeersgegevens of persoonsgegevens.

Meerdere partijen hebben gesteld dat artikel 8, onderdeel d, moet worden geschrapt, omdat deze bepaling zou leiden tot een dubbele meldplicht voor uitval van NL-Alert. In artikel 8 van de Regeling alarmeringsdienst NL-Alert 2023 is reeds een meldplicht voor storingen bij NL-Alert aan de Minister van Justitie en Veiligheid opgenomen. Met het oog op beperking van de regeldruk is ervoor gekozen om de meldplicht in deze regeling te laten vervallen.

Netbeheer Nederland en BTG hebben vragen gesteld over de toepasbaarheid van de meldcriteria voor machine-to-machine toepassingen (hierna: M2M-toepassingen). Dit zijn toepassingen waarbij apparaten autonoom functioneren en automatisch met elkaar communiceren. Netbeheer Nederland en BTG vragen of deze M2M-toepassingen onder de reikwijdte van de meldplicht vallen en, zo ja, of de drempel van 50.000 gebruikers dan niet te laag is. Er worden voorbeelden genoemd van M2M-toepassingen voor slimme meters, bij sluizen of in ziekenhuizen.
M2M-toepassingen kunnen ook een elektronische communicatiedienst zijn. In de Cbw wordt voor de definitie van een elektronische communicatiedienst verwezen naar artikel 1.1 van de Telecommunicatiewet. De meldplicht in artikel 8 is echter alleen van toepassing op aanbieders van *openbare* elektronische communicatiediensten en -netwerken. Veel organisaties maken gebruik van M2M-toepassingen zonder zelf te kwalificeren als aanbieder van een openbare elektronische communicatiedienst. De connectiviteit voor de M2M-toepassingen wordt bijvoorbeeld door een derde partij geleverd. Deze derde partijen zijn veelal aanbieders van openbare elektronische communicatiediensten of -netwerken, en voor hen geldt de meldplicht zoals geformuleerd in artikel 8.

6.1.4 Opmerkingen betreffende de meldplicht voor de sector post- en koerierdiensten

PostNL heeft in haar reactie gesteld dat artikel 11, onderdeel a, niet duidelijk specificeert wat er wordt verstaan onder de term 'gebruiker'. De term 'gebruiker' omvat zowel de afzender van een poststuk als de ontvanger. Ter verduidelijking is de term 'gebruiker' vervangen door de term 'ontvanger'. Voor de ontvanger is gekozen omdat de afzender voor het bepalen van de ernst van een incident onder dit criterium geen rol speelt. De ernst van het incident wordt afgemeten aan de hand van de impact op de ontvangende partij.

Zowel PostNL als TLN hebben in hun reacties gesteld dat artikel 11, onderdeel b, onvoldoende duidelijkheid biedt over wanneer een incident moet worden gemeld. Volgens TLN leidt de bepaling ertoe dat elke aantasting van de integriteit, vertrouwelijkheid of authenticiteit van opgeslagen, verzonden of verwerkte gegevens in verband met de dienstverlening moet worden gemeld. Naar aanleiding hiervan is de bepaling aangescherpt, zodat duidelijker is in welke gevallen onder artikel 11, onderdeel b, een meldplicht geldt. Een incident is nu alleen meldplichtig indien de aantasting van opgeslagen, verzonden of verwerkte gegevens risico oplevert voor de bescherming van persoons- en adresgegevens of van het briefgeheim.

6.1.5 Opmerkingen betreffende de meldplicht voor de sector vervaardiging

Een partij heeft in haar reactie gesteld dat artikel 12, onderdeel e, impliciet verplicht tot een risicoanalysemethodiek, terwijl de Cbw en de daarop berustende regelgeving uitgaan van een risicogebaseerde aanpak. Het is niet de bedoeling dat de meldcriteria- al dan niet indirect – nieuwe verplichtingen introduceren die niet reeds uit de zorgplicht voortvloeien. Naar aanleiding hiervan is artikel 12, onderdeel e, geschrapt.

Een partij heeft daarnaast opgemerkt dat de meldcriteria voor de vervaardigingssector te ruim zijn geformuleerd en ruimte laten voor verschillende interpretaties. Daarnaast heeft een partij opgemerkt dat de meldcriteria in artikel 12 niet zijn gekwantificeerd naar gevolgen, terwijl dit wel wenselijk is. De meldcriteria in de regeling zijn bewust niet uitputtend opgesteld. De opgenomen criteria voor significant incident vormen een gedeeltelijke uitwerking van de wettelijke norm en beogen entiteiten en toezichthouders duidelijkheid te geven over wanneer in ieder geval sprake is van een meldplichtig incident. Gelet op de uitvoerbaarheid en de beperking van regeldruk is gekozen niet alle parameters van artikel 25, tweed lid, Cbw nader te specificeren.

Verder is bij sommige meldcriteria de impact op de maatschappij in ogenschouw genomen, gelet op artikel 12, onderdeel d, waar het om milieuschade en daarmee maatschappelijke gevolgen gaat. Voor andere meldcriteria in de regeling is veelal niet expliciet gekwantificeerd naar de gevolgen voor de maatschappij, belanghebbenden of medewerkers. Dat zou te veel afwijken van het normenstelsel waarop artikel 12 mede is gebaseerd en zou de uitvoerbaarheid bemoeilijken en regeldruk verhogen. De gevolgen voor belanghebbenden zullen niet altijd direct te kwantificeren zijn, waardoor het risico bestaat dat te laat, te weinig of juist te snel gemeld wordt.

Een andere partij vraagt aandacht voor ketenafhankelijkheden in de maakindustrie. Volgens deze partij zijn de huidige criteria te veel gericht op schade of gevolgen bij de betrokken entiteit zelf, in plaats van op gevolgen voor klanten en leveranciers.

De regeling is opgesteld om duidelijk te maken wanneer er in ieder geval sprake is van een meldplichtig incident. De meldplicht geldt enkel voor significante incidenten. Dat zijn incidenten die een ernstige operationele verstoring of financiële verliezen voor de betrokken entiteit veroorzaken of kunnen veroorzaken, of die aanzienlijke materiële of immateriële schade bij andere entiteiten veroorzaken of kunnen veroorzaken. Dat betreft mogelijk ook incidenten die kunnen leiden tot schade bij andere entiteiten in de keten. Het concreet maken en verwerken van de gevolgen voor klanten en leveranciers in de criteria zou voor entiteiten extra regeldruk opleveren, aangezien dan processen moeten worden ingericht om vast te stellen in hoeverre sprake is van significante gevolgen in de keten.

Tot slot benadrukt een partij dat een aantal begrippen onvoldoende duidelijk is en daardoor vatbaar voor interpretatie. Naar aanleiding hiervan is de artikelsgewijze toelichting op artikel 12 waar nodig aangevuld en zijn enkele begrippen gedefinieerd in artikel 1 van deze regeling.

6.1.6 Opmerkingen betreffende de meldplicht voor de sector onderzoek

BTG heeft in haar reactie gesteld dat de Regeling cyberbeveiliging EZK en de Cyberbeveiligingsregeling IenW verschillende meldcriteria hanteren voor de sector onderzoek. BTG heeft voorgesteld om de meldcriteria voor deze sector in beide regelingen te harmoniseren. Dit voorstel is overgenomen. Artikel 13 is daartoe afgestemd op de meldcriteria uit de Cyberbeveiligingsregeling IenW. Om overlap

te voorkomen beperken de wijzigingen in artikel 13 zich echter tot de meldcriteria die niet reeds zijn opgenomen in artikel 7 van deze regeling.

6.1.7 Aanwijzing CSIRT

TLN en Cyberveilig Nederland hebben in hun reacties gesteld dat in de regeling geen verwijzing is opgenomen naar het bevoegde CSIRT.
In artikel 2, eerste lid, van het Cbb is de Minister van Justitie en Veiligheid als het CSIRT aangewezen. De Minister van Justitie en Veiligheid zal dit uitvoeren voor de sectoren en subsectoren die onder de beleidsverantwoordelijkheid van de Minister van Economische Zaken en Klimaat vallen. Omdat dit reeds in het Cyberbeveiligingsbesluit is geregeld, hoeft dit niet afzonderlijk in deze regeling te worden opgenomen.

6.1.8. Overige opmerkingen

Tot slot beveelt TLN aan in de regeling op te nemen dat deze na een periode van twee jaar wordt geëvalueerd. Dit voorstel is niet overgenomen. In artikel 94 van de Cbw is geregeld dat de wet twee jaar na inwerkingtreding zal worden geëvalueerd op de doeltreffendheid en de effecten van de wet in de praktijk. Hierbij zal worden bezien op welke manier ook de lagere regelgeving, waaronder deze regeling, wordt meegenomen.

6.2 Advies Adviescollege toetsing regeldruk

Gelijktijdig met de internetconsultatie is het Adviescollege toetsing regeldruk (hierna: ATR) gevraagd om deze regeling te beoordelen op nut en noodzaak, minder belastende alternatieven, werkbaarheid van de regeling en de gevolgen voor de regeldruk. In deze paragraaf wordt nader ingegaan op het advies van het ATR[3] en de wijze waarop de aanbevelingen zijn verwerkt. Op het onderdeel nut en noodzaak wordt niet nader ingegaan, omdat het ATR daarover geen advies heeft uitgebracht.

6.2.1 Totstandkoming meldcriteria en minder belastende alternatieven

Het ATR heeft geadviseerd nader te onderbouwen hoe de uitwerking van de zorgplicht en hoe de criteria voor de meldplicht tot stand zijn gekomen, in welke mate bij de meldcriteria de samenleving wordt ontwricht en welke mogelijk minder belastende alternatieven zijn overwogen. Dit advies is voor de zorgplicht opgevolgd door de algemene toelichting in paragraaf 2.2 op dit punt nader uit te werken.

Bij het bepalen van de meldcriteria is gekeken naar de potentiële gevolgen van een incident met name voor de samenleving alsmede naar de regeldruk.
Bij potentiële gevolgen van een incident voor de samenleving zal het veelal gaan om een ernstige verstoring van de dienstverlening waarvan anderen afhankelijk zijn. Het kan ook betrekking hebben op aanzienlijke schade voor de maatschappij of voor de entiteit zelf die ontstaat als bijvoorbeeld kwaadwillenden inbreuk plegen op de netwerk- en informatiesystemen van een entiteit waarbij gevoelige gegevens worden ontvreemd, bijvoorbeeld klantgegevens. Bij het bepalen van de meldcriteria en de keuze voor minder belastende alternatieven is hierbij onder andere rekening gehouden met de volgende aspecten. Allereerst zijn meldcriteria per sector vastgesteld waarbij uitsluitend de meest ernstige incidenten moeten worden gemeld, zoals ook wettelijk is bepaald. Om te kunnen bepalen of een incident aan een of meerdere meldcriteria voldoet, is daarnaast ook gekeken naar de uitvoerbaarheid en werkbaarheid voor entiteiten. Sommige meldcriteria sluiten ook aan waar reeds bestaande monitorings- en detectiesystemen van entiteiten ook op gericht zijn en inzicht in moeten geven, bijvoorbeeld (mate van) verstoring van een bepaalde dienst. Eveneens is er gekozen voor een beperkt aantal meldcriteria per sector. Tot slot is ook input opgehaald bij bedrijven of brancheorganisaties, zodat de meldcriteria zo goed mogelijk aansluiten bij de bestaande praktijk in een bepaalde sector. Dit is ook het voordeel van sectorale meldcriteria. Mede naar aanleiding van reacties uit de internetconsultatie en uit gevoerde gesprekken zijn diverse meldcriteria waar nodig aangepast, waarbij met name de reikwijdte is verduidelijkt of de meldcriteria is verhoogd. Dit ook met het oog op reductie van de regeldruk.

Het ATR verzoekt ook om nog in te gaan op de ontwrichting van de samenleving. In hoeverre er sprake is van ontwrichting van de samenleving kan niet op voorhand worden vastgesteld. Allereerst geven de meldcriteria een ondergrens aan; in de praktijk kunnen zich ernstiger incidenten voordoen dan de in deze regeling geformuleerde meldcriteria. Daarnaast kan de maatschappelijke impact bijvoorbeeld worden beïnvloed door de maatregelen die de entiteit treft om de gevolgen van het incident zo klein

[3] Brief van 19 december 2025 met kenmerk MvH/RvZ/ATR4306/2025-U201.

mogelijk te houden en bijvoorbeeld in hoeverre getroffen gebruikers van de dienst (snel) kunnen overschakelen naar een alternatieve dienst.

6.2.2 Werkbaarheid

Met betrekking tot de werkbaarheid van de regeling heeft het ATR geadviseerd om de werkbaarheid nader toe te lichten en die per sector uit te splitsen, vanwege de aard en activiteiten van de verschillende sectoren die onder de reikwijdte van deze regeling vallen.
Voor wat betreft de zorgplicht wordt een goede werkbaarheid van deze regeling gerealiseerd door bij de uitwerking zoveel mogelijk aan te sluiten bij bestaande normenkaders, zoals ISO 27001. Daarnaast zijn de bepalingen inzake de zorgplicht in samenwerking met de ministeries van LVVN en IenW opgesteld, waarmee een eenduidig normenkader is gecreëerd. Hiermee wordt tevens beoogd eenduidige en werkbare regels te waarborgen voor entiteiten die onder meerdere sectoren vallen.
Voor wat betreft de werkbaarheid van de meldplicht wordt verwezen naar paragraaf 6.2.1. Bij de totstandkoming van de meldcriteria is gekozen voor een uniforme aanpak waarbij de uitvoerbaarheid en werkbaarheid belangrijke factoren zijn geweest.
Verder stelt het ATR dat niet duidelijk is of de regeling voor de vervaardigingssector uitvoerbaar en realistisch is. Bij het opstellen van de meldcriteria is bewust aangesloten bij de praktijk die al gangbaar is in de sector. In de toelichting op artikel 12 is hier nader op ingegaan. De criteria zijn daarom met name gebaseerd op de IEC 62443-normenreeks, de meest gebruikte referentie voor Operational Technology-omgevingen. Daarmee is aangesloten bij bestaande risicobeoordelingen en beveiligingsprocessen.

Het ATR vraagt daarnaast hoeveel bedrijven worden geraakt door deze regelgeving. Voor de bedrijven die onder deze regeling en onder de in paragraaf 1 genoemde Uitvoeringsverordening (EU) 2024/2690[4] vallen, gaat het om ongeveer 2200–2600 bedrijven.

6.2.3 Invoeringstoets

Het ATR adviseert om een jaar na de inwerkingtreding van deze regeling een invoeringstoets uit te voeren. Naar aanleiding van een aangenomen amendement door de Tweede Kamer is in artikel 94, eerste lid, Cbw geregeld dat een invoeringstoets plaatsvindt 18 maanden na inwerkingtreding van de wet. Hiermee wordt gehoor gegeven aan dit advies van het ATR.

6.3 Uitvoering- en handhavingstoets

De RDI heeft een uitvoerbaarheids- en handhaafbaarheidstoets (UHT) uitgevoerd. De RDI acht de regeling uitvoerbaar, handhaafbaar en fraudebestendig, mits met een aantal aandachtspunten rekening wordt gehouden. In deze paragraaf worden deze aandachtspunten besproken.
De meldcriteria voor de sector vervaardiging waren ten tijde van het uitbrengen van de UHT nog niet volledig uitgewerkt en zijn derhalve niet in de UHT meegenomen. De RDI heeft in de UHT te kennen gegeven graag betrokken te willen worden zodra ook de regels voor de sector vervaardiging verder zijn uitgewerkt. Aan dit verzoek is gevolg gegeven. Er heeft niet alleen afstemming met de RDI plaatsgevonden over de meldcriteria voor de sector vervaardiging, maar ook over de andere artikelen in deze regeling. Daarnaast heeft de RDI meerdere verduidelijkingsvragen gesteld over de conceptregeling. Deze zijn met de RDI besproken en tekstuele opmerkingen van de RDI zijn verwerkt.

Aangezien de zorgplicht gezamenlijk is uitgewerkt door de ministeries van EZK, LVVN en IenW, zijn de bij deze ministeries binnengekomen UHT's gezamenlijk geanalyseerd en verwerkt. Om deze reden zijn ten aanzien van de zorgplicht ook punten geadresseerd die uit UHT's van andere toezichthouders dan de RDI naar voren zijn gekomen.

6.3.1 Zorgplicht

De RDI heeft in de toets gevraagd om in de toelichting bij de zorgplicht te verduidelijken hoe de verplichtingen uit deze regeling zich verhouden tot de meer open geformuleerde zorgplicht in de Cbw en wat dit in de praktijk betekent voor de invulling van de verplichtingen door entiteiten. Daarbij noemt de RDI artikel 4 (bedrijfscontinuïteit) als voorbeeld. Tevens heeft de RDI gewezen op het belang

[4] 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).

van consistente terminologie in de Cbw, het Cbb, deze regeling en de bijbehorende toelichtingen. Naar aanleiding hiervan is de algemene toelichting op de zorgplicht aangevuld. Daarbij is verduidelijkt waarom onderdelen van de zorgplicht nader zijn uitgewerkt in deze regeling en hoe deze uitwerking zich verhoudt tot de zorgplichtbepalingen in de Cbw en het Cbb. Daarbij is tevens toegelicht dat de regeling moet worden gelezen in samenhang met de wet en het besluit en dat de wettelijke norm onverkort van toepassing blijft. Deze regeling bevat een concretisering van een aantal zorgplichtmaatregelen om meer duidelijkheid te bieden over de wijze waarop de zorgplicht in de praktijk moet worden toegepast en geoperationaliseerd, om daarmee de algehele cyberbeveiliging van entiteiten te verhogen. Tevens is de toelichting op artikel 4 ten aanzien van bedrijfscontinuïteit verduidelijkt, waarbij de verhouding met het bedrijfscontinuïteitsplan, bedoeld in artikel 9, derde lid, van het Cbb, en de risicobeoordelingen, bedoeld in artikel 7 van het Cbb, is uiteengezet. Voorts zijn de onderdelen van artikel 4, eerste lid, die in het bedrijfscontinuïteitsplan moeten worden opgenomen, nader toegelicht. Ook is de terminologie zoveel mogelijk gelijkgetrokken.

6.3.2 Meldplicht. Algemene criteria significante incidenten

In de toets heeft de RDI gesteld dat uit artikel 7 en de bijbehorende toelichting onvoldoende duidelijk blijkt in hoeverre de daarin opgenomen criteria uitputtend zijn, dan wel of buiten deze criteria ook sprake kan zijn van een significant incident als bedoeld in de Cbw.
De meldcriteria in deze regeling zijn niet uitputtend. Dit betekent dat buiten de in deze regeling opgenomen criteria ook kan worden getoetst aan de criteria van artikel 25, tweede lid, van de Cbw om te beoordelen of een incident significant is. De criteria in de regeling vormen echter het primaire kader voor de beoordeling of sprake is van een significant incident. Naar aanleiding van deze reactie is de toelichting in paragraaf 2.3 aangevuld.

6.3.3 Specifieke criteria significant incident aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten

Met betrekking tot de meldcriteria voor aanbieders van openbare elektronische communicatienetwerken of -diensten heeft de RDI opgemerkt dat artikel 8, onderdeel b, onvoldoende duidelijk is. Artikel 8, onderdeel b, verplicht een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst een incident te melden indien de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast, met gevolgen voor meer dan 10.000 gebruikers van het openbaar elektronische communicatienetwerk of openbare elektronische communicatiedienst. Volgens de RDI is onvoldoende duidelijk wat in dit verband onder dienstverlening moet worden verstaan.
Naar aanleiding hiervan is de artikelsgewijze toelichting aangevuld. Daarbij is verduidelijkt dat onder dienstverlening niet alleen het daadwerkelijk aangeboden netwerk of de daadwerkelijk aangeboden dienst, zoals een telefoniedienst, wordt verstaan, maar ook diensten van een entiteit die noodzakelijk zijn om die openbare elektronische communicatiedienst- of dat openbare elektronische communicatienetwerk operationeel aan te bieden.

6.3.4 Specifieke criteria significant incident aanbieders van internetknooppunten

Eveneens bij aanbieders van openbaar elektronische communicatienetwerken of -diensten heeft de RDI verzocht te verduidelijken wat wordt verstaan onder ‘dienstverlening’ in de meldcriteria voor aanbieders van internetknooppunten. Met dienstverlening wordt in dit verband bedoeld het aanbieden van een netwerkplatform aan de leden of klanten van de dienstaanbieder, waarop deze leden of klanten IP-verkeer met elkaar kunnen uitwisselen. Ook diensten van een internetknooppunt die noodzakelijk zijn voor het aanbieden van dit netwerkplatform, vallen onder dit begrip.

6.3.5 Specifieke criteria significant incident sector onderzoek

Met betrekking tot de meldcriteria voor de sector onderzoek heeft de RDI opgemerkt dat onvoldoende duidelijk is wat wordt verstaan onder de aantasting van gegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt. Gevraagd wordt wanneer sprake is van aantasting van gegevens.
Van aantasting van gegevens is sprake indien de integriteit, vertrouwelijkheid, of authenticiteit van de in verband met het verrichte onderzoek opgeslagen, verzonden, of verwerkte gegevens niet langer kan worden gegarandeerd. Dit is verduidelijkt in de artikelsgewijze toelichting op artikel 13, alsmede in de artikelsgewijze toelichting op de andere sectoren waarin soortgelijke bepalingen zijn opgenomen.
Naar aanleiding van de reacties uit de internetconsultatie is daarnaast besloten de aantasting van deze gegevens alleen meldplichtig te maken indien deze leidt tot aanzienlijke materiële of immateriële schade bij andere entiteiten. Dit biedt duidelijkheid over wanneer een incident op grond van deze bepaling meldplichtig is.

6.3.6 Integraliteit regelgeving

De RDI heeft aandacht gevraagd voor de samenhang tussen de Regeling cyberbeveiliging EZK en de Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector. De RDI heeft geconstateerd dat de formulering van verschillende artikelen in beide regelingen van elkaar afwijkt. Naar aanleiding hiervan zijn de formuleringen in beide regelingen zoveel mogelijk op elkaar afgestemd. Daarnaast heeft de RDI in het kader van de integraliteit aandacht gevraagd voor een eenduidig standpunt over de vraag in hoeverre de meldcriteria uitputtend zijn. Hierop is nader ingegaan in de paragrafen 2.3. en 6.3.2.

7. Inwerkingtreding

Deze regeling treedt in werking op het tijdstip waarop de Cyberbeveiligingswet in werking treedt. Er is afgeweken van het systeem van vaste verandermomenten omdat deze regeling samenhangt met de implementatie van bindende Europese regelgeving in de Cyberbeveiligingswet.

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 Cbw of het Cbb, sluiten de definities in deze regeling daarbij aan. Een aantal definities is 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 op welke entiteiten de in deze regeling opgenomen bepalingen over de zorg- en meldplicht van toepassing zijn. Het betreft aanbieders van internetknooppunten, aanbieders van openbare elektronische communicatienetwerken en aanbieders van openbare elektronische communicatiediensten, alsmede entiteiten in de sectoren ruimtevaart, post- en koerierdiensten en vervaardiging die kwalificeren als essentiële of belangrijke entiteit. Op de entiteiten in de sector onderzoek is deze regeling van toepassing voor zover de betrokken belangrijke of essentiële entiteit onderzoeksactiviteiten verricht binnen een sector of subsector die onder de verantwoordelijkheid van de Minister van Economische Zaken en Klimaat valt.

Hoofdstuk 2. Nadere regels zorgplicht

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen

Dit artikel geeft nadere invulling aan artikel 6 van het Cbb ten aanzien van het beleid over beveiliging van netwerk- en informatiesystemen.
Dit artikel regelt dat essentiële en belangrijke entiteit, als onderdeel van de managementsystematiek, de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's toetst door vast te leggen welke maatregelen worden gemonitord, gemeten, geanalyseerd en geëvalueerd, hoe dit gebeurt, wanneer dit plaatsvindt en wie daarmee belast is. Dit is een doorlopend proces.
Het doel van de managementsystematiek is te waarborgen dat de netwerk- en informatiebeveiligingsrisico's van de entiteit 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 vast te leggen welke maatregelen worden gemonitord, met welke methoden, met welke frequentie en door wie, ontstaat een sluitende cyclus van plannen, uitvoeren, toetsen en bijsturen.
Opvolging van deze evaluatie en beoordeling dient plaats te vinden. Deze verplichting is niet in dit artikel opgenomen, aangezien zij al volgt uit artikel 6, vierde lid, en artikel 18 van het Cbb. Daarmee wordt geborgd dat het inzicht in de effectiviteit van de maatregelen actueel blijft en dat de resultaten van deze cyclus leiden tot verdere verbetering van de beveiliging. Deze elementen sluiten aan bij de werkwijze die in de praktijk gebruikelijk is in managementsystemen voor informatiebeveiliging en bij internationale normen, zoals ISO-normen.

Artikel 4 – Bedrijfscontinuïteit

Op grond van artikel 9, tweede lid, van het Cbb stelt de belangrijke entiteit of essentiële entiteit processen en procedures vast voor back-ups van software en gegevens en past die toe. De risicobe-

oordelingen op grond van artikel 7 van het Cbb zijn derhalve relevant voor zowel het bepalen van welke software en gegevens in back-ups dienen te worden opgenomen, als voor de hierna genoemde waarborgen.

De onderdelen van het eerste lid omschrijven welke aspecten in de processen en procedures voor back-ups van software en gegevens moeten worden opgenomen. Het bepalen van hersteltijden, in het Engels ook wel aangeduid als *recovery time objective (RTO),* heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. De term herstelpunten, in het Engels ook wel aangeduid als *recovery point objective (RPO),* heeft betrekking op de frequentie van de back-ups. Het voorschrift dat de processen en procedures waarborgen 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 processen en procedures te waarborgen dat de back-ups nauwkeurig zijn. Hiermee wordt bedoeld dat de informatie in geval van herstel succesvol kan worden gebruikt, bijvoorbeeld door ervoor te zorgen dat de gegevens in de back-up zich in een staat bevinden die een succesvol herstel mogelijk maakt.

Daarnaast dienen de processen en procedures de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups te waarborgen, zodat de back-ups daadwerkelijk ingezet kunnen worden. Met integriteit wordt bedoeld dat de entiteit borgt dat de back-ups niet zijn gemanipuleerd of beschadigd, bijvoorbeeld door derden. Dit voorkomt dat de geback-upte gegevens zijn gewijzigd, beschadigd of aangetast tijdens het back-upproces, de opslag of het herstel. Voor de beschikbaarheid is het van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door toedoen van kwaadwillenden, zoals bij ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups dient te worden gewaarborgd, om ongeautoriseerde toegang tot gegevens te voorkomen. Daarnaast dienen de processen en procedures waarborgen te bevatten voor het herstellen van software en gegevens. Dit omvat zowel de wijze waarop back-ups hersteld kunnen worden als de waarborg dat back-ups zo nodig daadwerkelijk teruggezet kunnen worden. Een gangbare praktijk hierbij is het periodiek testen van het terugzetten van back-ups, om de werking van back-ups in de praktijk te verifiëren. Ten slotte dienen de processen en procedures te omschrijven hoe lang de betreffende back-ups bewaard moeten worden.

Bedrijfscontinuïteitsplan

De essentiële entiteit of belangrijke entiteit stelt op grond van artikel 9, derde lid, Cbb een bedrijfscontinuïteitsplan op. Daarmee kan zij zich voorbereiden op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen, hierop doeltreffend en tijdig reageren en de duur en gevolgen van dergelijke incidenten beperken. Op grond van het tweede lid van dit artikel dient de entiteit bij het opstellen van het bedrijfscontinuïteitsplan rekening te 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 tweede lid omschrijven de elementen die het bedrijfscontinuïteitsplan moet bevatten. Allereerst dient het plan het doel en de reikwijdte ervan te omschrijven, zodat de context en het toepassingsbereik van het bedrijfscontinuïteitsplan op voorhand duidelijk zijn. Daarbij ligt het voor de hand dat de entiteit bij het opstellen van het bedrijfscontinuïteitsplan prioriteit geeft aan haar kritieke processen. Dit laat onverlet dat de zorgplicht van artikel 21 van de wet van toepassing blijft op alle netwerk- en informatiesystemen van de entiteit.

Het vastleggen van de belangrijkste contacten en interne en externe communicatiekanalen in een bedrijfscontinuïteitsplan is van belang voor snelle, gecoördineerde actie en communicatie tijdens incidenten of crises. Hierbij kan worden gedacht aan contacten voor directe actie, zoals noodnummers van hulpdiensten, sleutelpersoneel in de organisatie zoals crisisteams, IT/OT-specialisten, directie, evenals externe partners als leveranciers, klanten of overheidsorganisaties. Wat betreft overheidsorganisaties kan in ieder geval worden gedacht aan de bevoegde autoriteit en het CSIRT waar significante incidenten gemeld dienen te worden.
De voorwaarden voor activering en de-activering beschrijven in welke gevallen of onder welke omstandigheden het bedrijfscontinuïteitsplan of onderdelen ervan in werking treden dan wel worden beëindigd.
De vereiste middelen, met inbegrip van back-ups en redundanties, beschrijven welke middelen nodig zijn voor een goede uitvoering van het bedrijfscontinuïteitsplan.
Ten slotte dient het bedrijfscontinuïteitsplan de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen te bevatten, zodat de overgang naar een normale bedrijfsvoering wordt gewaarborgd.

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

Artikel 5 – Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Eerste lid

Artikel 11, derde lid, van het Cbb verplicht essentiële en belangrijke entiteiten om processen en procedures vast te stellen voor het onderhoud en beheer van haar netwerk- en informatiesystemen. Deze processen en procedures hebben ten minste betrekking op het configuratiebeheer en het wijzigingsbeheer van de netwerk- en informatiesystemen van de entiteit, alsmede, op grond van het eerste lid, 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, stelt de essentiële entiteit of belangrijke entiteit processen en procedures vast 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 onderdeel a geldt dat, waar passend, gecontroleerd moet worden of beveiligingspatches afkomstig zijn van betrouwbare bronnen en of de integriteit van deze patches gewaarborgd is. Dit vergt niet in alle gevallen handmatige actie van de essentiële entiteit of belangrijke entiteit. Zo is bij reguliere systeemupdates van besturingssystemen doorgaans al sprake van ingebouwde technische controles op herkomst en integriteit van beveiligingspatches. De essentiële of belangrijke entiteit dient zich hiervan echter wel te vergewissen.
Op grond van onderdeel b geldt dat beveiligingspatches, waar passend, getest moeten worden voordat zij in de productieomgeving worden toegepast. De noodzaak van een dergelijke test is afhankelijk van de risico's die het installeren van de patch met zich meebrengt. Voornoemde stappen dragen ertoe bij dat de toepassing van patches geen nieuwe kwetsbaarheden of verstoringen veroorzaakt. Onderdeel c bepaalt 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. Dit kan bijvoorbeeld het geval zijn voor het toepassen van beveiligingspatches op OT-systemen, waarbij het belang van continuïteit van de dienstverlening en de verouderde aard van veel industriële componenten een rol spelen. 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 tijdig toepassen van de beveiligingspatch gedocumenteerd te worden.

Derde lid

Onderdeel a

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

Onderdeel b

Op grond van dit onderdeel voert de essentiële of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit op haar netwerk- en informatiesystemen en legt zij de resultaten daarvan vast. Deze scans maken het mogelijk om inzicht te krijgen in bekende kwetsbaarheden in systemen en applicaties en vormen daarmee een belangrijk hulpmiddel om risico's tijdig te onderkennen. De entiteit voert de scans, waar passend, uit waarbij rekening wordt gehouden met de blootstelling van systemen aan dreigingen en de netwerktoegankelijkheid van die systemen?, alsmede met de

criticaliteit van die systemen voor de continuïteit van de dienstverlening en de potentiële gevolgen van uitval of misbruik.
Kwetsbaarheidsscans van OT-systemen vereisen vaak een andere aanpak dan die van IT-systemen, vanwege het belang van de continuïteit van de operationele diensten of de aanwezigheid van verouderde apparatuur. Het is daarom aan de essentiële of belangrijke entiteit om een passende vorm van kwetsbaarheidsscan in te zetten, gegeven de omgeving van haar netwerk- en informatiesystemen en de mogelijke risico's die zich daarin kunnen voordoen. Zo kan het in OT-omgevingen noodzakelijk zijn om dit op een passieve wijze vorm te geven, om zo verstoring van processen te voorkomen. Door de resultaten te documenteren kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.

Onderdeel c

Op grond van dit onderdeel evalueert de essentiële of belangrijke entiteit structureel haar blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van heeft ten aanzien van haar netwerk- en informatiesystemen, voor zover artikel 17 van het Cbb daar niet reeds toe verplicht. Dit onderdeel regelt daarmee aanvullend dat kwetsbaarheden uit de uitgevoerde kwetsbaarheidsscans van de essentiële of belangrijke entiteit of meldingen van interne werknemers worden geëvalueerd en verholpen. 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 verhelpt de essentiële entiteit of belangrijke entiteit onverwijld kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen. Indien een kwetsbaarheid niet of op een later moment verholpen wordt, dient de essentiële entiteit of belangrijke entiteit dit te motiveren en te documenteren. Evenals bij het niet toepassen van een beveiligingspatch (zie het tweede lid) wordt voor de toezichtspraktijk daarmee duidelijk waarom wordt afgeweken en kan de bevoegde autoriteit oordelen of deze keuze terecht is gemaakt.

Vierde lid

Onderdeel a

De essentiële entiteit of belangrijke entiteit waarborgt 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 onderdeel a segmenteert de essentiële entiteit of belangrijke entiteit haar netwerken overeenkomstig de resultaten van de in artikel 7, derde lid, van het Cbb bedoelde risicobeoordeling. De entiteit bepaalt zelf op welke wijze zij de netwerksegmentatie toepast. Netwerksegmentatie betreft het onderverdelen van systemen en netwerken in verschillende, van elkaar gescheiden segmenten, waardoor er geen automatische toegang is tussen systemen en netwerken. Daarbij wordt rekening gehouden wordt met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen. De essentiële entiteit of 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.
Als goede praktijken kunnen worden genoemd- toegang tot een netwerk of zone te verlenen 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.

Onderdeel b

Op grond van onderdeel b segmenteert de essentiële entiteit of belangrijke entiteit, waar passend, haar netwerk- en informatiesystemen van de netwerk- en informatiesystemen 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 voorkomen dat een beveiligingsincident of

een kwetsbaarheid bij een derde partij zich verspreidt naar de systemen van de entiteit. 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 noodzakelijke minimum.

Artikel 6 – Beveiligingsaspecten ten aanzien van toegangsbeleid

Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, dient ook beleid te omvatten over bevoorrechte accounts en systeembeheeraccounts. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Systeembeheeraccounts zijn een specifieke categorie bevoorrechte accounts die worden gebruikt voor het beheer van systemen, zoals het uitvoeren van updates, het wijzigen van configuraties of het beheren van gebruikersrechten.
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 waarborgt dat bij bevoorrechte accounts en systeembeheeraccounts sterke identificatie-, authenticatie- en autorisatieprocedures worden toegepast. Bij sterke identificatie kan gedacht worden aan het vooraf betrouwbaar vaststellen van de identiteit van de gebruiker voordat accounts worden uitgegeven. Bij sterke authenticatie kan worden gedacht aan phishing-bestendige multifactorauthenticatie, waarmee de dreiging van phishing en ander misbruik van dergelijke accounts zoveel mogelijk wordt tegengegaan. Bij sterke autorisatie kan worden gedacht aan een strikte scheiding van rollen en bevoegdheden. Daarnaast waarborgt het beleid dat de voorrechten van deze accounts zoveel mogelijk geïndividualiseerd en beperkt worden toegekend. Dit zorgt ervoor dat misbruik beter te herleiden is tot specifieke accounts. Tevens waarborgt het beleid dat voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt. Deze maatregelen verkleinen tezamen het risico op misbruik of onbedoelde gevolgen van het inzetten van deze voorrechten.

Hoofdstuk 3. Nadere criteria meldplicht

Artikel 7 – Algemene criteria significant incident

Dit artikel bevat algemene criteria op grond waarvan wordt bepaald of een incident significant is. Deze criteria gelden voor alle essentiële en belangrijke entiteiten waarop hoofdstuk 3 van deze regeling van toepassing is. Een significant incident is meldplichtig.

Eerste lid

In het eerste lid zijn algemene criteria opgenomen voor incidenten op grond waarvan incidenten in ieder geval als significant worden aangemerkt. Daarvan is sprake indien een incident heeft geleid, of kan leiden, tot de dood van een of meer personen of tot aanzienlijke schade aan de gezondheid van een of meer personen. Onder aanzienlijke schade aan de gezondheid wordt verstaan ernstig lichamelijk of psychisch letsel dat leidt tot een substantiële en langdurige vermindering van het fysieke of mentale functioneren van een of meer personen. Het gaat daarbij om schade die niet slechts tijdelijk of licht van aard is, maar die gevolgen heeft voor het dagelijks functioneren of de kwaliteit van leven.
Een entiteit meldt een incident dat voldoet aan de criteria in de onderdelen a en b, zodra zij kennis heeft van het feit dat een dergelijk incident heeft plaatsgevonden. Dit omvat ook situaties waarin pas na verloop van tijd, bijvoorbeeld twee maanden, duidelijk wordt dat zich dergelijke gevolgen hebben voorgedaan.

Van entiteiten wordt niet verlangd dat zij aanvullende informatie verzamelen waartoe zij redelijkerwijs geen toegang hebben. Een incident kan bijvoorbeeld meldplichtig zijn indien de entiteit op basis van eigen informatie of informatie van derden redelijkerwijs kan vaststellen dat het incident heeft geleid of kan leiden tot gezondheidsschade aan personen. Daarvan kan ook sprake zijn indien een derde de entiteit informeert over dergelijke gevolgen van het incident. Zo kan bijvoorbeeld bij een gebruiker of afnemer van de dienst van een entiteit gezondheidsschade ontstaan als gevolg van een incident bij die entiteit. Dit kan worden gezien als een keteneffect.
Een incident is niet meldplichtig indien de entiteit op basis van eigen waarneming of beschikbare informatie niet redelijkerwijs kan vaststellen dat sprake is van mogelijke dood van individuen of gezondheidsschade aan individuen en zij evenmin beschikt over informatie van derden waaruit dit blijkt.

Tweede lid

Het tweede lid verduidelijkt dat een incident ook significant kan zijn indien wordt voldaan aan een of meer van de criteria, bedoeld in de artikelen 8 tot en met 13. Deze artikelen bevatten nadere criteria

voor de beoordeling van de significantie van een incident.

Derde lid

Het derde lid ziet op incidenten die het gevolg zijn van gepland onderhoud dat door of namens de essentiële of belangrijke entiteit wordt uitgevoerd. Geplande gevolgen van dergelijke onderhoudswerkzaamheden worden in beginsel niet aangemerkt als een significant incident. Daarbij kan bijvoorbeeld worden gedacht aan een vooraf aangekondigde tijdelijke onderbreking van de dienstverlening of een tijdelijk verminderde beschikbaarheid van een dienst.

Deze uitzondering geldt uitsluitend ten aanzien van de geplande onderhoudswerkzaamheden. Indien tijdens of als gevolg van de geplande onderhoudswerkzaamheden ongeplande gevolgen ontstaan, is deze uitzondering niet van toepassing. Zo kan bijvoorbeeld een onjuist uitgevoerde 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 moet worden beoordeeld of aan een of meer criteria van deze regeling wordt voldaan, of aan de parameters van artikel 25, tweede lid, van de wet.

Artikel 8 – Criteria significant incident bij aanbieders van elektronische communicatienetwerken of aanbieders van elektronische communicatiediensten

Openbare elektronische communicatienetwerken- en diensten zijn essentieel voor de communicatie tussen personen, bedrijven, overheidsorganisaties en andere instituties. Voor de goede functionering en continuering van deze diensten is het van belang dat de desbetreffende essentiële en belangrijke entiteiten significante incidenten melden bij de toezichthouder en het CSIRT.

Onderdeel a

Van een incident met betrekking tot beschikbaarheid is sprake als de openbare elektronische communicatiedienst niet meer wordt geleverd. Het kan hierbij bijvoorbeeld gaan om een storing waarbij gebruikers niet meer kunnen bellen of 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 voor een periode van langer dan vier uur. Indien de dienst voor een dergelijk aantal gebruikers gedurende die tijdsduur niet beschikbaar is, kan ervan worden uitgegaan dat sprake is van significante maatschappelijke impact en de hinder die gebruikers ondervinden neemt ook snel toe. Verstoringen die korter duren dan vier uur hebben naar verwachting een beperktere maatschappelijke impact.

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 de openbare elektronische communicatiedienst van de entiteit gebruik maken voor particuliere – of zakelijke doeleinden.
Daarbij hoeven zij niet noodzakelijkerwijs op die dienst te zijn geabonneerd. Immers, bij bepaalde openbare elektronische communicatiediensten, zoals nummeronafhankelijke interpersoonlijke 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 zoals een rechtspersoon zal er veelal sprake zijn van meerdere natuurlijke personen die toegang hebben tot en gebruik maken van de verleende dienst van de entiteit, zonder dat zij zelf een overeenkomst hebben gesloten met die entiteit, zoals de werknemers van een zakelijke gebruiker. Deze werknemers kunnen in het kader van deze regeling als afzonderlijke gebruikers worden beschouwd. Indien de essentiële of belangrijke entiteit niet in staat is het exacte aantal getroffen gebruikers te bepalen, schat zij het totale aantal getroffen gebruikers in op basis van informatie waarover zij beschikt. Het gaat hierbij om diensten die in Nederland worden aangeboden, waaronder internettoegangsdiensten (vast en mobiel) en telefonie (vast en mobiel), ongeacht waar de gebruiker zich bevindt.

Onderdeel b

Dit onderdeel bevat een criterium op grond waarvan een essentiële of belangrijke entiteit verplicht is een incident te melden indien de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast, met gevolgen voor ten minste 1% van de gebruikers van het openbare elektronische communicatienetwerk of openbare elektronische communicatiedienst, met en minimum van 10.000 gebruikers. Van aantasting van gegevens is sprake indien de integriteit, vertrouwelijkheid, of authenticiteit van de in

verband met de dienstverlening opgeslagen, verzonden, of verwerkte gegevens niet langer kan worden gegarandeerd.
Met dienstverlening dient niet alleen het aangeboden openbare elektronische communicatienetwerk en of de openbare elektronische communicatiedienst te worden verstaan, maar ook de ondersteunende diensten of netwerk- en informatiesystemen van de entiteit die noodzakelijk zijn voor het aanbieden ervan.
Bij gegevens kan bijvoorbeeld worden gedacht aan verkeersgegevens, gegevens die worden verwerkt voor het overbrengen van communicatie over een openbaar elektronisch communicatienetwerk of voor de facturering ervan. Deze gegevens betreffen onder meer de herkomst, tijd en duur van telefoongesprekken. Ook kan worden gedacht aan persoonsgegevens. Deze gegevens zijn vertrouwelijk van aard en kunnen worden blootgesteld aan het risico van onbedoelde openbaarmaking of verlies.

De vertrouwelijkheid van gegevens kan bijvoorbeeld worden aangetast indien de encryptie van een dienst niet correct heeft gewerkt of indien sprake is geweest van ongeoorloofde toegang waarbij kwaadwillenden gegevens van de entiteit hebben ontvreemd.
Ook de integriteit van gegevens kan worden aangetast, bijvoorbeeld doordat gegevens worden gecorrumpeerd die noodzakelijk zijn voor het correct functioneren van de netwerk- en informatiesystemen van de essentiële of belangrijke entiteit. Dergelijke aantastingen kunnen niet alleen de systemen zelf verstoren, maar ook gevolgen hebben voor de dienstverlening aan derden. Onder aantasting van integriteit vallen ook gevallen waarbij gegevens permanent ontoegankelijk zijn geworden.
Authenticiteit is eveneens als criterium opgenomen. Een voorbeeld hiervan is spoofing. Spoofing is vervalsing van afzenderinformatie verstrekt via het systeem voor nummerdoorgifte. Zo kunnen oplichters zich voordoen als bankhelpdeskmedewerkers, inloggegevens ontfutselen of mensen misleiden om geld over te maken.
De meldplicht is niet beperkt tot incidenten die het gevolg zijn van kwaadwillige handelingen; ook incidenten die het gevolg zijn van menselijke fouten vallen hieronder. Hierbij kan gedacht worden aan een incident waarbij vertrouwelijke gegevens onbedoeld openbaar worden gemaakt.

Onderdeel c

Aangezien een verstoring van het alarmnummer 112 significante maatschappelijke gevolgen teweeg kan brengen, in het uiterste geval met doden of gewonden als gevolg, is sprake van een meldplichtig incident indien de dienst van het alarmnummer 112 niet beschikbaar is, ongeacht de aard en omvang van de verstoring.

Bij het alarmnummer 112 is sprake van een keten, bestaande uit een openbaar elektronische communicatienetwerk of een openbare elektronische communicatiedienst (de vaste of mobiele telefoonaanbieder van de beller) en vervolgens het telefonienetwerk dat het 112-verkeer doorstuurt naar de landelijke meldkamer. Daarna gaat het 112-verkeer via een besloten spraak- en datanetwerk van de landelijke meldkamer naar één van de meldkamers van de regionale hulpdiensten. Tot slot alarmeert de regionale meldkamer de benodigde hulpdienst(en).
Alleen het gedeelte van deze keten tot aan de landelijke meldkamer valt onder de reikwijdte van de meldplicht van deze regeling. Een incident is onder dit onderdeel alleen meldplichtig indien het plaatsvindt binnen de 112-keten bij of onder de verantwoordelijkheid van de aanbieder van het openbare elektronische communicatienetwerk of de openbare elektronische communicatiedienst. Immers, alleen die aanbieders zijn op grond van deze regeling de normadressaten.

Artikel 9 – Criteria significant incident 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 onder andere gevolgen hebben voor de beschikbaarheid van de dienstverlening van internetknooppunten, gemeld worden bij het CSIRT en de toezichthouder.

Onderdeel a

Dit onderdeel ziet op situaties wanneer ten minste 25% van het actuele totale verkeer dat door het internetknooppunt wordt verwerkt, gedurende 30 minuten of langer is uitgevallen. Dit is een uitwerking van artikel 25, tweede lid, onderdeel a, van de wet. Onder het totale verkeer van een internetknooppunt wordt verstaan het totale verkeer uitgedrukt in datavolume in bits per seconde, gewoonlijk uitgedrukt in gigabit of terrabit per seconde, dat wordt uitgewisseld via het internetknooppunt.

Onderdeel b

Op grond van dit onderdeel meldt een essentiële of belangrijke entiteit een incident indien de

integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening van het internetknooppunt worden opgeslagen, verzonden of verwerkt, is aangetast, met gevolgen voor meer dan 5% gebruikers van het internetknooppunt. Met dienstverlening dient te worden verstaan zowel het aanbieden van een netwerkplatform aan de leden of klanten van de dienstaanbieder, waarop deze leden of klanten IP-verkeer met elkaar kunnen uitwisselen, als de ondersteunende diensten van de entiteit die noodzakelijk zijn voor het aanbieden van dit netwerkplatform.
Van aantasting van gegevens is sprake indien de integriteit, vertrouwelijkheid of authenticiteit van de in verband met de dienstverlening opgeslagen, verzonden of verwerkte gegevens niet langer kan worden gegarandeerd.
Voor het criterium dat ten minste 5% van de gebruikers gevolgen moet ondervinden van de aantasting, is aansluiting gezocht bij bestaande meldcriteria onder de Uitvoeringsverordening (EU) 2024/2690 voor meerdere subsectoren binnen de sector digitale infrastructuur, om vanuit het oogpunt van regeldruk herkenbare regels te stellen.
Voor zover het de integriteit, vertrouwelijkheid of authenticiteit betreft, kunnen incidenten niet alleen gevolgen 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 gegevens van de entiteit zijn ontvreemd.
Bij authenticiteit kan bijvoorbeeld sprake zijn van *spoofing*, waarbij het verkeer dat via een internetknooppunt wordt uitgewisseld afkomstig is van een andere bron dan de daadwerkelijke bron van het verkeer.
Ook de integriteit van de gegevens kan worden aangetast, met gevolgen voor de dienstverlening. Bij ongeoorloofde 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. Onder aantasting van integriteit vallen ook situaties waarbij gegevens permanent ontoegankelijk zijn geworden.
De meldplicht is niet beperkt tot incidenten als gevolg van ongeoorloofde 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 significant incident in de sector ruimtevaart

De ruimtevaartsector levert een directe bijdrage aan 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. Deze systemen zijn essentieel voor de besturing en veilige werking van ruimtevoorwerpen. Zij verzorgen onder meer de telemetrie, tracking en commandovoering van ruimtevoorwerpen 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.

Dit artikel laat de meldplicht op grond van artikel 10 van de Wet ruimtevaartactiviteiten onverlet. Die geldt voor de vergunninghouder en ziet op voorvallen die gevaar kunnen opleveren voor personen en goederen, het milieu in de ruimte, de openbare orde, de veiligheid van de staat of anderszins schade kunnen veroorzaken in het kader van een ruimtevaartactiviteit. De onderhavige regeling ziet op significante incidenten die verband houden met de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten in de sector ruimtevaart. Het kan voorkomen dat hetzelfde feitencomplex onder beide meldplichten valt.

Dit artikel ziet op aantasting van de integriteit, authenticiteit, beschikbaarheid of vertrouwelijkheid van gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering van een ruimtevoorwerp via de door de entiteit beheerde grondfaciliteit, voor zover daardoor een risico ontstaat voor de veilige besturing of het behoud van dat ruimtevoorwerp. Onder besturing wordt ook de controle en positionering verstaan. Onder behoud wordt in dit verband verstaan dat het ruimtevoorwerp veilig en functioneel behouden blijft.

Het criterium is alleen van toepassing op een verstoring tijdens een tijdvak waarin communicatie met het ruimtevoorwerp volgens de reguliere operationele planning mogelijk en voorzien is. Bij de beoordeling of dergelijke gegevens noodzakelijk zijn voor telemetrie, tracking of commandovoering wordt rekening gehouden met de aardbaan, de missiearchitectuur, vooraf geplande contactmomenten en reguliere operationele procedures. Normale perioden waarin geen contact mogelijk of voorzien is, bijvoorbeeld omdat een ruimtevoorwerp zich door zijn baan tijdelijk buiten bereik van een grondfacili-

teit bevindt, vallen niet onder dit criterium. De technische omstandigheden zijn sterk afhankelijk van het type aardbaan. Daarom is gekozen voor een criterium dat voor alle aardbanen werkbaar is.

Bij gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering kan onder meer worden gedacht aan commando's, telemetriedata, attitude and orbit control-gegevens (stand- en baanregeling) en gegevens die relevant zijn voor manoeuvreplanning of veilige besturing.

Van aantasting van de integriteit is sprake wanneer gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering onjuist, gewijzigd, beschadigd, onvolledig of anderszins niet langer betrouwbaar zijn. Dit kan bijvoorbeeld het geval zijn wanneer commando's of telemetriedata worden gewijzigd of vervalst, of wanneer gegevens door een technische storing, systeemfout, opslagprobleem of andere oorzaak onbruikbaar worden. Hierdoor kunnen gegevens verkeerd worden geïnterpreteerd of kunnen kritieke gegevens ontbreken die nodig zijn voor de besturing of monitoring van het ruimtevoorwerp.
Van aantasting van de authenticiteit is sprake wanneer onvoldoende zekerheid bestaat over de herkomst van gegevens, berichten, signalen of commando's. Dit kan zich bijvoorbeeld voordoen wanneer niet kan worden vastgesteld dat een commando daadwerkelijk afkomstig is van de daartoe bevoegde bron, of wanneer een partij zich voordoet als een vertrouwde grondfaciliteit, een vertrouwde operator of een andere vertrouwde bron. Spoofing kan onder dit criterium vallen wanneer daardoor de authenticiteit, integriteit of beschikbaarheid van gegevens, signalen of commando's wordt aangetast.
Van aantasting van de vertrouwelijkheid is sprake wanneer gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering toegankelijk worden voor of bekend worden bij onbevoegde derden. Dit kan bijvoorbeeld het geval zijn bij het onderscheppen, afvangen, uitlekken of ongeautoriseerd raadplegen van gevoelige gegevens.
Van aantasting van de beschikbaarheid is sprake wanneer gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering niet beschikbaar, toegankelijk of bruikbaar zijn op het moment dat deze nodig zijn voor de besturing of het behoud van het ruimtevoorwerp. Dit kan bijvoorbeeld het geval zijn wanneer relevante telemetrie-, tracking- of commandogegevens tijdelijk of blijvend niet beschikbaar zijn, of wanneer communicatie- of trackingsignalen worden verstoord of geblokkeerd. Jamming kan onder dit criterium vallen wanneer daardoor de beschikbaarheid van gegevens die noodzakelijk zijn voor telemetrie, tracking of commandovoering wordt aangetast en daardoor een risico ontstaat voor de besturing of het behoud van het ruimtevoorwerp.

Artikel 11 – Criteria significant incident in de sector post- en koerierdiensten

Post- en koeriersdiensten blijven van belang voor burgers, bedrijven en overheidsorganisaties. De bezorgnetwerken worden gebruikt voor communicatie en voor het verzenden en ontvangen van commerciële zendingen. Voor de goede functionering van deze sector is het noodzakelijk dat essentiële en belangrijke entiteiten significante incidenten melden.

Onderdeel a

Dit onderdeel ziet op situaties waarin een incident leidt tot een forse vertraging voor de ontvanger (geadresseerde) van de dienst met landelijke impact. Dat is het geval wanneer ten minste 30% van de ontvangers in het post- of koeriersnetwerk de dienst ten minste twee bezorgdagen later ontvangt dan contractueel of wettelijk voorzien, als gevolg van een verstoring in de netwerk- en informatiesystemen.
Een dergelijk percentage impliceert dat meerdere bezorg- en sorteercentra zijn geraakt, waardoor niet langer sprake is van alleen regionale impact. De oorzaak van de verstoring kan zowel in de systemen zelf liggen, bijvoorbeeld bij systeemfalen, als buiten de systemen, zoals bij een stroomstoring.
Bezorgdagen zijn de dagen waarop de dienstverlener op grond van wettelijke verplichtingen, contractuele afspraken of algemene voorwaarden van de betreffende dienstverlener gehouden is post- en koeriersdiensten te leveren.

Onderdeel b

In dit onderdeel is geregeld dat een incident een significant incident is wanneer de integriteit, vertrouwelijkheid of authenticiteit van digitale gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt, is aangetast. Van aantasting van gegevens is sprake indien de integriteit, vertrouwelijkheid, of authenticiteit van digitale gegevens die in verband met de dienstverlening worden opgeslagen, verzonden, of verwerkt niet langer kan worden gegarandeerd. In onderdeel b is de meldplicht beperkt tot aantastingen die leiden tot onrechtmatige verwerking van persoons- en adresgegevens of schending van het briefgeheim.
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. Hierbij

kan worden gedacht aan de mobiele applicatie voor klanten voor het volgen van een postzending. De vertrouwelijkheid van digitale gegevens kan bijvoorbeeld worden aangetast wanneer de encryptie van een dienst niet correct heeft gewerkt, of wanneer sprake is van ongeoorloofde toegang waarbij de digitale gegevens zijn ontvreemd. Ook de integriteit van de dienstverlening kan worden aangetast, bijvoorbeeld doordat gegevens worden gecorrumpeerd die noodzakelijk zijn voor de correcte werking van de netwerk- en informatiesystemen van post- en koerierdiensten. Onder aantasting van integriteit vallen ook gevallen waarbij gegevens permanent ontoegankelijk zijn geworden.
De meldplicht is niet beperkt tot incidenten die het gevolg zijn van kwaadwillige handelingen. Ook menselijke fouten vallen hieronder. Hierbij kan worden gedacht aan het onbedoeld openbaar maken van vertrouwelijke digitale gegevens of het onjuist uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Artikel 12 – Criteria significant incident 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 de verplichting tot het melden van incidenten 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 (IACS) systematisch kunnen beoordelen, beheren en verbeteren. De reeks richt zich primair op IACS, maar vereist dat ook ondersteunende IT-systemen die de OT-zones beïnvloeden in scope zijn. Door de meldingscriteria 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). De criteria zijn zo geformuleerd dat kleine storingen, zoals sensorfouten of netwerkvertragingen die frequent voorkomen, niet meldplichtig zijn. Hiermee wordt overmatige rapportage van incidenten voorkomen en worden de gevolgen voor de regeldruk beperkt.
De onderdelen, die hier relevant zijn, zijn:
- 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 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 bruikbare referentie voor wat binnen de Cbw als een significant incident kan worden beschouwd binnen de sector vervaardiging.

Onderdeel a

Dit onderdeel ziet op de veiligheid van het productieproces (Safety). Een incident is meldplichtig indien sprake is van verlies van veiligheidsfuncties, bijvoorbeeld door een defect. Bij veiligheidsfuncties kan worden gedacht 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 (gespecialiseerde controllers die de veiligheid in industriële omgevingen bewaken) ervoor zorgen dat een noodstop niet meer functioneert tijdens onderhoudswerkzaamheden.

Onderdeel b

Het in dit onderdeel opgenomen criterium betreft verlies van beschikbaarheid of integriteit van essentiële besturings- of monitoringsfuncties. Dit zijn functies die cruciaal zijn voor de veiligheid, prestaties en betrouwbaarheid van systemen en machines, doordat zij real-time monitoring bieden op basis waarvan ingegrepen kan worden bij afwijkende waarden. Het gaat hierbij bijvoorbeeld om tijdelijk of langdurig verlies van besturing (Loss of Control (LOC)), of verlies van proceszicht of monitoring (Loss of View (LOV)) dan wel manipulatie hiervan. 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 (Enterprise Resource Planning-systeem, een

systeem wat kernprocessen integreert en automatiseert) stillegt, waardoor de productie niet kan worden aangestuurd of bewaakt.

Onderdeel c

Dit onderdeel ziet op het in gevaar komen of kunnen komen van de continuïteit van het productieproces. Als productieprocessen stil komen te liggen, kan dat leiden tot tekort aan voorraden die noodzakelijk zijn in andere belangrijke productieketens. Hierbij kan worden gedacht aan manipulatie van procesparameters, recepturen of meetwaarden waardoor productkwaliteit, materiaalconformiteit of naleving van wettelijke eisen (zoals voedselveiligheid, CE-markering) in gevaar komen of kunnen komen. Een voorbeeld hiervan is een wijziging in de PLC-logica (programmable logic controller, in feite een computer die speciaal is ontwerpen voor industriële toepassingen) die leidt tot afwijkende temperatuurinstellingen bij kunststofextrusie.

Onderdeel d

Dit onderdeel ziet op milieuschade als gevolg van een inbreuk op de beveiliging van netwerk- en informatiesystemen. Als voorbeeld kan gedacht worden aan een situatie waarbij een cyberaanval op de controlesystemen ertoe leidt dat gas of andere gevaarlijke stoffen weglekken zonder dat dit tijdig wordt opgemerkt, met mogelijke verontreiniging en gevaar voor personeel als gevolg.

Onderdeel e

Dit onderdeel ziet op situaties waarin ongeoorloofde toegang tot een industriespecifiek netwerk- of informatiesysteem heeft plaatsgevonden en zich naar meerdere zones of omgevingen heeft verspreid. Industriële netwerk- en informatiesystemen zijn veelal ingedeeld in *zones* (een afgebakende groep van netwerk- en informatiesystemen) die via zogeheten *conduits* (communicatiekanaal tussen zones waarover gegevensverkeer plaatsvindt) met elkaar verbonden zijn. Een incident is significant wanneer de ongeoorloofde toegang zich verspreidt naar meerdere zones. Als voorbeeld kan gedacht worden aan malware die vanuit een kantoor-IT-systeem doordringt tot het PLC-netwerk.

Artikel 13 – Criteria significant incident in de sector onderzoek

Bij de sector onderzoek als bedoeld in bijlage 2 bij de wet gaat het om entiteiten die als hoofddoel hebben het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden. De onderzoeksgegevens die bij de uitvoering van het onderzoek worden gegenereerd, vertegenwoordigen vaak een commerciële waarde. Afhankelijk van het onderwerp van het onderzoek kunnen deze gegevens daarnaast persoonsgegevens of vertrouwelijke gegevens over organisaties bevatten. De ongeoorloofde openbaring van dergelijke gegevens – al dan niet moedwillig – kan daarom grote gevolgen hebben voor de onderzoeksorganisatie zelf of voor derden. Daarom bevat dit artikel nadere criteria voor de beoordeling of sprake is van een significant incident.

Onderdeel a ziet op incidenten waarbij bedrijfsgeheimen als bedoeld in artikel 2, eerste lid, van Richtlijn (EU) 2016/943 van de essentiële entiteit of belangrijke entiteit ongeoorloofd openbaar worden gemaakt.

Onderdeel b ziet op incidenten waarbij de integriteit, vertrouwelijkheid of authenticiteit van onderzoeksgegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast en deze aantasting leidt tot aanzienlijke materiële of immateriële schade bij andere entiteiten. Van aantasting van gegevens is sprake indien de integriteit, vertrouwelijkheid, of authenticiteit van de in verband met het verrichte onderzoek opgeslagen, verzonden, of verwerkte gegevens niet langer kan worden gegarandeerd.

Onderzoeksgegevens die noodzakelijk zijn voor de uitvoering van toegepast onderzoek met het oog op een commerciële toepassing zijn vanwege de aard van het onderzoek doorgaans vertrouwelijk. Daardoor bestaat verhoogd risico op onbedoelde openbaarmaking. Daarnaast kunnen de resultaten van onderzoeken worden beïnvloed indien de integriteit wordt aangetast van gegevens die noodzakelijk zijn voor de uitvoering van dat onderzoek. Hieronder valt ook de situatie waarin gegevens permanent ontoegankelijk zijn worden.

De vertrouwelijkheid van gegevens kan bijvoorbeeld worden aangetast wanneer de encryptie van een dienst niet correct heeft gefunctioneerd, of wanneer sprake is van ongeoorloofde toegang waarbij gegevens van de entiteit zijn ontvreemd.

De meldplicht is niet beperkt tot kwaadwillige handelingen. 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 en Klimaat om op grond van artikel 51, tweede lid, onderdeel i, van de Cbw 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. Dit artikel zorgt ervoor dat de Cbw-instanties, waarbij het met name zal gaan om de bevoegde autoriteit, effectief kunnen samenwerken en informatie kunnen uitwisselen met autoriteiten die taken en bevoegdheden hebben op grond van de in artikel 14 genoemde sectorspecifieke regelgeving. Dit artikel maakt het mogelijk dat in de praktijk toezichthouders die op grond van verschillende wetten toezicht houden op dezelfde (sub)sectoren of soorten entiteiten toch informatie kunnen uitwisselen en samenwerken. Dit is belangrijk met het oog op doelmatig en samenhangend toezicht en het beperken van toezichtlasten voor entiteiten. Zoals ook het ATR stelt wordt met de aanwijzing van autoriteiten onder artikel 14 overlappende handhavingsacties en inconsistenties in risico-inschattingen voorkomen.

In dit artikel is de Minister van Economische Zaken en Klimaat, 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 bijna alle gevallen gaat het feitelijk om dezelfde toezichthouder: de RDI. Daarnaast wordt ook de Autoriteit Consumenten en Markt (hierna: ACM) uit hoofde van de Postwet 2009 aangewezen onder dit artikel. De ACM houdt in algemene zin toezicht op onder andere een goede kwaliteit van de universele postdienst. Cybersecurity-incidenten kunnen daar impact op hebben. Daarnaast houdt ACM een register bij van post- en koeriersdiensten. Dit maakt het van belang dat er zich ook situatie kunnen voordoen inzake de postsector dat de bevoegde autoriteiten, het centrale contactpunt en de CSIRT's ook met de ACM zouden moeten kunnen samenwerken.

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 (hierna: 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 (hierna: NIS-richtlijn) was geïmplementeerd in de Wbni. De NIS-richtlijn is vervangen door de NIS2-richtlijn.
De 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 regelgeving betreft van de Minister van Economische Zaken en Klimaat 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 Staatssecretaris van Economische Zaken en Klimaat,
W.J.M. Aerdts