STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 24093
13 juli
2026

Regeling van de Minister van Infrastructuur en Waterstaat van 3 juli 2026, kenmerk IENW/BSK-2026/105816, houdende nadere regels voor de digitale veiligheid van essentiële en belangrijke entiteiten in de sectoren vervoer, drinkwater, afvalwater, afvalstoffenbeheer, onderzoek, nucleair, keren en beheren, chemie en meteorologie (Cyberbeveiligingsregeling IenW) [Keten-ID WGK 28528]

De Minister van Infrastructuur en Waterstaat, na overleg met de Minister van Justitie en Veiligheid;

Gelet op de overeenstemming met de Minister van Justitie en Veiligheid met betrekking tot de aanwijzing van het CSIRT als bedoeld in artikel 3 en met de verplichtingen aan het CSIRT als bedoeld in artikel 4;

Gelet op de artikelen 2, tweede lid, 3, derde lid, 19 en 23, eerste lid, van het Cyberbeveiligingsbesluit;

BESLUIT:

Paragraaf 1. Begripsbepalingen

Artikel 1 (Begripsbepalingen)

In deze regeling wordt verstaan onder:
– *besluit:* het Cyberbeveiligingsbesluit;
– *BIO2:* Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stcrt. 2026, 7416);
– *essentiële dienst:* essentiële dienst als bedoeld in artikel 1 van de Wet weerbaarheid kritieke entiteiten;
– *ITS-dataverstrekkers:* aanbieders van mobiliteitsdata aan ITS-dienstverleners op basis van data ontvangen van (andere) ITS-dienstverleners;
– *ITS-dienstverleners:* exploitanten van intelligente vervoerssystemen als bedoeld in artikel 4, onderdeel 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen (PbEU 2010, L 207);
– *kritieke entiteit:* kritieke entiteit als bedoeld in artikel 6, eerste lid, van de Wet weerbaarheid kritieke entiteiten;
– *minister:* Minister van Infrastructuur en Waterstaat;
– *NEN:* norm die door de Stichting Koninklijk Nederlands Normalisatie Instituut is uitgegeven;
– *NEN-EN:* NEN die door het Europees Comité voor Normalisatie is vastgesteld;
– *NEN-EN-ISO/IEC:* NEN-EN die door de International Organization for Standardization en de International Electrotechnical Commission is vastgesteld;
– *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 L 157/1);
– *Verordening (EU) 2024/1679:* Verordening (EU) 2024/1679 van het Europees Parlement en de Raad van 13 juni 2024 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk, tot wijziging van Verordening (EU) 2021/1153 en Verordening (EU) nr. 913/2010 en tot intrekking van Verordening (EU) nr. 1315/2013 (PbEU L 2024/1679).

Paragraaf 2. Reikwijdte

Artikel 2 (Reikwijdte)

1. Deze regeling is van toepassing op alle essentiële entiteiten en belangrijke entiteiten in de volgende sectoren dan wel subsectoren:

Sector	Subsector
Vervoer	Lucht
	Spoor
	Water
	Weg
Drinkwater	
Afvalwater	
Afvalstoffenbeheer	
Vervaardiging, productie en distributie van chemische stoffen	
Overheid	Waterschappen

2. Deze regeling is verder van toepassing op door de minister aangewezen kritieke entiteiten.

3. Deze regeling is verder van toepassing op essentiële en belangrijke entiteiten in de sector onderzoek, voor zover de soort entiteit, genoemd in bijlage 2 bij de wet, betrekking heeft op de sectoren vervoer, drinkwater, afvalwater, afvalstoffenbeheer, onderzoek, nucleair, keren en beheren, chemie en meteorologie.

Paragraaf 3. CSIRT

Artikel 3 (Aanwijzing CSIRT)

In afwijking van artikel 2, eerste lid, van het besluit wordt als CSIRT voor de waterschappen aangewezen: de dienst CERT-WM die is ondergebracht bij het openbaar lichaam Het Waterschapshuis als bedoeld in de gemeenschappelijke regeling Het Waterschapshuis.

Artikel 4 (Verplichtingen CSIRT)

1. Het CERT-WM als bedoeld in artikel 3 rapporteert jaarlijks uiterlijk op 31 december aan de minister over de wijze waarop het invulling heeft gegeven aan zijn taken, bedoeld in artikel 16 van de wet en aan de eisen, bedoeld in artikel 3, eerste lid, van het besluit.

2. Het CERT-WM voldoet aan het Security Incident Management Maturity Model (SIM3) op minimaal het niveau intermediate voor zover het de taken betreft die het op grond van de wet en de daarop berustende bepalingen vervult.

3. Het niveau, bedoeld in het tweede lid, wordt vastgesteld door middel van een audit door een onafhankelijke en gekwalificeerde deskundige.

4. Het CERT-WM beschikt over een rapport van een audit, bedoeld in het derde lid, waaruit blijkt dat wordt voldaan aan het in het tweede lid bedoelde niveau, dat in ieder geval niet ouder is dan drie jaar. Het CERT-WM legt het rapport van de audit over aan de minister.

5. Indien het CERT-WM blijkens een rapport van een audit, bedoeld in het derde lid, niet meer voldoet aan het in het tweede lid bedoelde niveau, stelt het een verbeterplan op en voert het op basis daarvan wijzigingen door om aan het niveau te voldoen. Het CERT-WM legt het verbeterplan voor aan de minister.

Paragraaf 4. Nadere invulling zorgplicht

Paragraaf 4.1 Zorgplicht overheidsorganisaties

Artikel 5 (Reikwijdte paragraaf 4.1)

De paragrafen 4.1.1 en 4.1.2 zijn van toepassing op overheidsorganisaties.

Paragraaf 4.1.1 Managementsystematiek

Artikel 6 (ISO 27001)

De essentiële entiteit past de NEN-EN-ISO/IEC 27001:2023 toe op het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor de beveiliging van netwerk- en informatiesystemen, als bedoeld in artikel 6, vierde lid, van het besluit, en op het vaststellen van het toepassingsgebied van deze managementsystematiek.

Artikel 7 (Identificeren cruciale netwerk- en informatiesystemen)

1. De essentiële entiteit houdt als onderdeel van haar managementsystematiek voor de beveiliging van de netwerk- en informatiesystemen, bedoeld in artikel 6, vierde lid, van het besluit, een overzicht bij van haar cruciale netwerk- en informatiesystemen.

2. Een netwerk- en informatiesysteem van een essentiële entiteit in de sector overheid, subsector waterschappen, is cruciaal indien het systeem impactniveau 'hoog' of 'zeer hoog' uit de tabel in de bijlage bij deze regeling heeft.

Paragraaf 4.1.2 Beveiligingsmaatregelen

Artikel 8 (ISO 27002 en BIO2)

1. De essentiële entiteit gebruikt ten minste de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 voor het formuleren van passende en evenredige maatregelen voor de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 21, eerste lid, van de wet, met uitzondering van de beheersmaatregelen 5.32 en 5.34. De passende en evenredige maatregelen omvatten ten minste de voor haar relevante overheidsmaatregelen van de BIO2, met uitzondering van de overheidsmaatregelen 5.32.01 tot en met 5.34.01.

2. In afwijking van het eerste lid kunnen bij het formuleren van passende en evenredige maatregelen de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 en de overheidsmaatregelen van de BIO2, voor zover dat noodzakelijk is, worden vervangen door of gecombineerd met beheersmaatregelen uit andere normenkaders die een beveiligingsniveau bieden dat ten minste gelijkwaardig is aan het niveau van de voornoemde beheers- en overheidsmaatregelen.

3. De essentiële entiteit zorgt ervoor dat de opzet, het bestaan en de werking van de passende en evenredige maatregelen aantoonbaar zijn. Indien de entiteit bij het formuleren van passende en evenredige maatregelen gebruik heeft gemaakt van beheersmaatregelen uit andere normenkaders dan omschreven in het tweede lid, zorgt zij er ook voor dat de noodzakelijkheid van het gebruik van die andere passende en evenredige maatregelen en de gelijkwaardigheid van het beveiligingsniveau aantoonbaar zijn.

Paragraaf 4.2 Zorgplicht niet-overheidsorganisaties

Artikel 9 (Reikwijdte paragraaf 4.2)

Paragraaf 4.2 is van toepassing op essentiële en belangrijke entiteiten die geen overheidsorganisatie zijn.

Artikel 10 (Beleid over beveiliging van netwerk- en informatiesystemen)

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

Artikel 11 (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 bedrijfscontinuïteitplan, 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 plan;
   e. vereiste middelen, met inbegrip van back-ups en redundanties;
   f. voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

Artikel 12 (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 betrekking op ten minste de processen en procedures inzake:
   a. beveiligingstesten;
   b. beveiligingspatchbeheer.

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

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

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 13 (Beveiligingsaspecten ten aanzien van toegangsbeleid)

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

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

a. sterke identificatie-, authenticatie-, en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;
b. voorrechten op het gebied van systeembeheer zoveel mogelijk geïndividualiseerd en beperkt worden toegekend;
c. voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt.

Paragraaf 5. Criteria voor significante incidenten

Artikel 14 (Algemene bepalingen criteria)

Geplande dienstonderbrekingen en geplande gevolgen van geplande onderhoudswerkzaamheden die door of namens de belangrijke entiteit of essentiële entiteit worden uitgevoerd, worden niet als significante incidenten beschouwd.

Artikel 15 (Significante incidenten sector vervoer, subsector vervoer door de lucht)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervoer, subsector vervoer door de lucht, significant:
a. voor luchthavenbeheerders als door het incident is opgeschaald naar de hoogste crisisbeheersingsstructuur van de nationale luchthaven of regionale luchthaven van nationale betekenis;
b. voor een logistiek dienstverlener van vliegtuigbrandstoffen als deze voor een periode van een uur of langer geen vliegtuigbrandstoffen kan leveren die noodzakelijk zijn voor het uitvoeren van de vluchtoperatie;
c. voor luchtverkeersleidingsdiensten als de hoogst gehanteerde codering geldt, of de gehanteerde codering voor potentiële incidenten, conform het organisatie-specifieke classificatiesysteem voor crises;
d. voor luchtvaartmaatschappijen en overige entiteiten als de afhandeling niet of niet veilig kan plaatsvinden van 20% van het geplande aantal vluchten in een aaneengesloten periode van twaalf uur of langer, of als de verwachting daartoe bestaat.

Artikel 16 (Significante incidenten sector vervoer, subsector vervoer over spoor)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervoer, subsector vervoer over spoor, significant:
a. voor de infrastructuurbeheerder als het personenvervoer op de hoofdspoorweg voor een periode van vier uur of langer is gestremd;
b. voor de infrastructuurbeheerder als het goederenvervoer op de hoofdspoorweg voor een periode van twaalf uur of langer is gestremd;
c. voor een personenvervoerder als een verstoring in de bedrijfsvoering leidt tot uitval van een of meer treinen voor een periode van vier uur of langer en daarbij ten minste 100.000 reizigers worden getroffen;
d. voor een goederenvervoerder als diens dienstverlening voor een periode van twaalf uur of langer wordt gestaakt door een incident in de bedrijfsvoering.

Artikel 17 (Significante incidenten sector vervoer, subsector vervoer over water)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervoer, subsector vervoer over water, significant als:
a. dienstverlening met betrekking tot toegang tot de haven en nautische dienstverlening voor een periode van twaalf uur of langer niet beschikbaar is;
b. overslag in de haven voor een periode van twaalf uur of langer niet beschikbaar is; of
c. dienstverlening met betrekking tot transport in het maritieme achterland over, op en langs het hoofdvaarwegennet voor een periode van vierentwintig uur of langer niet beschikbaar is.

Artikel 18 (Significante incidenten sector vervoer, subsector vervoer over de weg)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervoer, subsector vervoer over de weg significant:
a. voor wegbeheerders als:
   i. de weg een onderdeel is van het trans-Europees vervoersnetwerk als bedoeld in Verordening EU/2024/1679 en voor een periode van twaalf uur of langer niet beschikbaar is; of
   ii. de weg een onderdeel is van het hoofdwegennet of het onderliggend wegennet en voor een periode van vierentwintig uur of langer niet beschikbaar is.
b. voor ITS-dienstverleners als:

i. de dienst van ITS-dataverstrekkers voor een periode van vier uur of langer niet beschikbaar is; of
ii. de dienst van de ITS-dienstverlener voor een periode van acht uur of langer niet beschikbaar is.

c. voor de dienst belast met de taken, bedoeld in de artikelen 42, tweede lid en 126, eerste lid, van de Wegenverkeerswet 1994 als de geleverde essentiële dienst voor een periode van vier uur of langer niet beschikbaar is.

Artikel 19 (Significante incidenten sector vervoer, subsector openbaar vervoer)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervoer, subsector openbaar vervoer, significant als zij in de bedrijfsvoering leidt tot uitval van het personenvervoer gedurende een periode van vier uur of langer en daarbij ten minste 100.000 reizigers worden getroffen.

Artikel 20 (Significante incidenten sector drinkwater)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector drinkwater significant:
a. voor drinkwaterbedrijven als bedoeld in artikel 1, eerste lid, van de Drinkwaterwet, als aan 10.000 aansluitingen of meer voor een periode van zes uur of langer geen drinkwater geleverd kan worden;
b. voor producenten en leveranciers van verpakt water als gedurende een periode van drie weken of langer geen water geproduceerd onderscheidenlijk geleverd kan worden.

Artikel 21 (Significante incidenten sector afvalwater)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector afvalwater significant als:
a. daardoor opgeschaald moet worden naar categorie 3 of hoger in de Gecoördineerde Regionale Incidentenbestrijdingsprocedure (GRIP);
b. daardoor opgeschaald moet worden naar dreigingsniveau 3 of hoger, bedoeld in het op grond van artikel 19.14 van de Omgevingswet door het waterschap opgestelde calamiteitenplan; of
c. voor een periode van zes uur of langer een of meer van de essentiële functies verstoord zijn bij een object dat is opgenomen op het actuele overzicht van de kritieke infrastructuur, bedoeld in artikel 5, tweede lid, van het Besluit weerbaarheid kritieke entiteiten.

Artikel 22 (Significante incidenten sector afvalstoffenbeheer)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector afvalstoffenbeheer significant als:
a. de inzameling van huishoudelijke afvalstoffen als bedoeld in artikel 1.1 van de Wet milieubeheer voor een periode van een week of langer niet kan plaatsvinden;
b. de inzameling van andere afvalstoffen dan huishoudelijke afvalstoffen als bedoeld in artikel 1.1 van de Wet milieubeheer voor een periode van 48 uur of langer niet kan plaatsvinden; of
c. de verbranding van afval in afvalverbrandingsinstallaties voor een periode van acht uur of langer verstoord is.

Artikel 23 (Significante incidenten sector nucleair)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector nucleair significant als op het terrein dat de essentiële entiteit in gebruik heeft:
a. een stralingsincident, ongeval of radiologische noodsituatie plaatsvindt waarvan op grond van artikel 6.1 van het Besluit basisveiligheidsnormen stralingsbescherming melding moet worden gemaakt bij de Autoriteit Nucleaire Veiligheid en Stralingsbescherming; of
b. een gebeurtenis plaatsvindt die in de weg staat aan onverkorte toepassing van het beveiligingspakket als bedoeld in artikel 22a van het Besluit kerninstallaties, splijtstoffen en ertsen.

Artikel 24 (Significante incidenten sector keren en beheren)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector keren en beheren significant als voor een periode van vier uur of langer een of meer van de voor het keren en beheren van waterkwantiteit essentiële functies verstoord zijn bij een object dat opgenomen is op het actuele overzicht van de kritieke infrastructuur, bedoeld in artikel 5, tweede lid, van het Besluit weerbaarheid kritieke entiteiten.

Artikel 25 (Significante incidenten sector vervaardiging, productie en distributie van chemische stoffen)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector vervaardiging, productie en distributie van chemische stoffen significant als:
a. daardoor de bij een overeenkomst vastgestelde levertijden overschreden worden met een periode van drie weken of meer; of
b. daardoor een kritieke entiteit die voor haar dienstverlening afhankelijk is van de verleende dienst, daarvan voor een periode van zes uur of langer geen gebruik kan maken.

Artikel 26 (Significante incidenten sector meteorologie)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector meteorologie significant als:
a. een kritieke entiteit voor de verlening van de essentiële dienst waarvoor zij als kritieke entiteit is aangewezen, afhankelijk is van de meteorologische dienst, en deze dienst door het incident niet beschikbaar is voor een periode van zes uur of langer; of
b. het incident meldt bij de daarvoor aangewezen faciliteit bij het Ministerie van Infrastructuur en Waterstaat.

Artikel 27 (Significante incidenten sector onderzoek)

Een incident is voor essentiële entiteiten en belangrijke entiteiten in de sector onderzoek als bedoeld in artikel 2, derde lid, significant als:
a. het incident het uitlekken van bedrijfsgeheimen als bedoeld in artikel 2, eerste lid, van Richtlijn (EU) 2016/943 van de essentiële entiteit of belangrijke entiteit veroorzaakt of kan veroorzaken;
b. het incident de dood van een natuurlijk persoon heeft veroorzaakt of kan veroorzaken;
c. het incident aanzienlijke schade aan de gezondheid van een natuurlijk persoon heeft veroorzaakt of kan veroorzaken;
d. er een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen heeft plaatsgevonden die ernstige operationele verstoringen kan veroorzaken; of
e. een vermoedelijk kwaadwillige handeling de integriteit, vertrouwelijkheid of authenticiteit van opgeslagen, verzonden of verwerkte onderzoeksgegevens heeft aangetast of kan hebben aangetast, en dit leidt tot aanzienlijke materiële of immateriële schade bij andere essentiële, belangrijke of kritieke entiteiten.

Artikel 28 (Significante incidenten sector overheid, subsector waterschappen)

Een incident in de sector overheid, subsector waterschappen, is significant als het leidt of kan leiden tot:
a. uitval van de dienstverlening van de essentiële entiteit voor ten minste vier uur;
b. financiële gevolgen die niet kunnen worden opgevangen in de begroting; of
c. de ernstige verwonding of de dood van een natuurlijke persoon.

Paragraaf 6. Slotbepalingen

Artikel 29 (Inwerkingtredingsbepaling)

Deze regeling treedt in werking op het tijdstip waarop de Cyberbeveiligingswet in werking treedt.

Artikel 30 (Citeertitel)

Deze regeling wordt aangehaald als: Cyberbeveiligingsregeling IenW.

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

De Minister van Infrastructuur en Waterstaat,
V.P.G. Karremans

BIJLAGE BIJ ARTIKEL 7, TWEEDE LID – IMPACTNIVEAUS SECTOR OVERHEID, SUBSECTOR WATERSCHAPPEN

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Impact op beschikbaarheid (dataverlies – RPO[1]); hoeveel dataverlies is acceptabel	Hoeveel dataverlies is acceptabel?	Dataverlies 36 uur	Dataverlies 24 uur	Dataverlies 12 uur	Dataverlies 4 uur	Dataverlies 1 uur
Hersteltijd (RTO[2]); hoe lang mag het proces hinder ondervinden van uitval?	Hoe lang mag het proces hinder ondervinden van uitval?	Maximaal 1 week uitval (5 x 8 uur) en hersteltijd 16 uur in 2 werkdagen	Maximaal 2 dagen uitval (2 x 8 uur) en hersteltijd 8 uur in 1 werkdag	Maximaal 1 dag uitval (1 x 8 uur) en herstel in uren	Maximaal 4 uur uitval en herstel in 1 uur	Max 1 uur uitval en minimale (geen) hersteltijd
Impact op belang essentiële entiteit	Wat is de impact voor de essentiële entiteit?	Minimale invloed op kernactiviteiten; weinig invloed op strategische doelstellingen.	Beperkte invloed op sommige kernactiviteiten; enige invloed op strategische doelstellingen.	Duidelijke invloed op meerdere kernactiviteiten; strategie moet mogelijk aangepast worden.	Aanzienlijke invloed op kernactiviteiten; strategische doelstellingen ernstig in gevaar.	Kritieke invloed op de kernactiviteiten; het voortbestaan van de organisatie kan in gevaar komen.
Vervangbaarheid informatie	Is de informatie vervangbaar?	Informatie is gemakkelijk te vervangen zonder noemenswaardige kosten of inspanning.	Informatie is vervangbaar met enige inspanning of kosten.	Vervanging van de informatie is mogelijk, maar vereist aanzienlijke tijd of middelen.	Informatie is moeilijk te vervangen, met hoge kosten of aanzienlijke inspanning.	Informatie is onvervangbaar, verlies zou een onherstelbare impact hebben.
Te beschermen belangen uit de ABDO[3]/ ABRO[4] of vergelijkbaar	Te beschermen belang (TBB)		TBB 4	TBB 4	TBB 3	TBB 2 / TBB 1
Informatieclassificatie beleid	Is de informatie gerubriceerd?	Ongerubriceerd	Dep.V (niveau 1 – standaard) (oud BBN 2 uit de BIO1.04)	Dep.V (niveau 2 – weerstand tegen spionage) (Oud BBN3 uit de BIO 1.04)	Stg.C	Stg.G / Stg. ZG
Schade bij openbaarmaking	Wat is de schade bij openbaarmaking?		Indien kennisname door niet-geautoriseerden nadeel kan toebrengen aan de belangen van één of meerdere afdelingen van de essentiële entiteit	Indien kennisname door niet-geautoriseerden schade kan toebrengen aan de belangen van de essentiële entiteit	Indien kennisname door niet geautoriseerden aanzienlijke schade kan toebrengen aan een van de vitale belangen van de essentiële entiteit	Indien kennisname door niet geautoriseerden ernstige of zeer ernstige schade kan toebrengen aan een van de vitale belangen van de essentiële entiteit
Kennisnemen informatie door onbevoegden	Kennisname …		Is ongewenst	Moet zoveel mogelijk worden voorkomen	Moet worden voorkomen	Is onacceptabel
Persoonsgegevens	Bevat persoonsgegevens of bijzondere persoonsgegevens of een grote verzameling		Bevat persoonsgegevens	Bevat bijzondere persoonsgegevens of meerdere collecties van persoonsgegevens.	Bevat meerdere collecties met bijzondere persoonsgegevens	
Politieke schade	Beleidsmatige gevolg classificatie	Geen politieke aandacht of risico. De situatie heeft geen invloed op bestuurders of vertegenwoordigend orgaan, en blijft binnen de organisatie.	Beperkte politieke gevoeligheid. Mogelijk bestuurlijke notitie of korte interne afstemming, maar geen publieke aandacht of aandacht van het vertegenwoordigend orgaan.	Matige politieke impact. Er is kans op vragen van het vertegenwoordigend orgaan of lokale media-aandacht. Bestuurders moeten intern of in het vertegenwoordigend orgaan toelichten wat er is gebeurd.	Duidelijke politieke gevolgen. De kwestie leidt tot publieke discussie of mediabelangstelling, politieke druk of reputatieschade. Bestuurders worden ter verantwoording geroepen en moeten zich verantwoorden naar aanleiding van verantwoordingsvragen (vragen in het vertegenwoordigend orgaan gesteld). Er wordt een (lokaal) Parlementair onderzoek ingesteld.	Ernstige politieke impact. De kwestie veroorzaakt grote politieke en publieke ophef, mogelijk moties van wantrouwen of aftreden van bestuurders. Vertrouwen in bestuurders of vertegenwoordigers komt ernstig onder druk te staan. Er is sprake van een enquête.

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Diplomatieke schade	Is er diplomatieke schade te verwachten?	Geen diplomatieke schade. De relaties met andere landen zijn stabiel en goed onderhouden, zonder enige negatieve impact. Effect op burgergerichte processen: Geen impact. Burgers merken geen verandering in de dienstverlening, internationale samenwerking of toegang tot buitenlandse diensten.	Klein verlies aan diplomatieke goodwill. Er zijn lichte spanningen, maar deze worden snel en efficiënt opgelost zonder grote gevolgen. Effect op burgergerichte processen: Minimale invloed op internationale samenwerking, bijvoorbeeld lichte vertragingen bij grensoverschrijdende diensten of minder vloeiende samenwerking met buitenlandse partners. Burgers merken nauwelijks iets van de situatie.	Merkbare diplomatieke schade. Relaties met andere landen verslechteren tot een punt waarop samenwerking in bepaalde gebieden moeilijker wordt. Dit kan bijvoorbeeld leiden tot vertragingen in internationale handel, samenwerking of informatie-uitwisseling. Effect op burgergerichte processen: Burgers kunnen langere wachttijden ondervinden bij grensoverschrijdende diensten zoals visa-aanvragen, internationale handel of hulp in het buitenland. Er kunnen ook meer bureaucratische hindernissen ontstaan bij internationale procedures.	Aanzienlijke diplomatieke schade. De relaties met belangrijke diplomatieke partners verslechteren aanzienlijk, wat leidt tot vertragingen of beperkingen in internationale samenwerking, en tot verlies van toegang tot strategische informatie of samenwerkingsovereenkomsten. Effect op burgergerichte processen: Burgers ondervinden duidelijke problemen, zoals een aanzienlijke afname in toegang tot consulaire diensten in het buitenland, problemen bij internationale reis- of handelsregelingen, en moeilijkheden in grensoverschrijdende communicatie en samenwerking. Er is sprake van toenemende ontevredenheid.	Ernstige diplomatieke schade. De diplomatieke relaties met andere landen zijn ernstig verstoord of verbroken, wat kan leiden tot sancties, reisbeperkingen, en ernstige verstoringen in internationale samenwerkingen en handelsrelaties. Effect op burgergerichte processen: Burgers worden geconfronteerd met grote problemen, zoals reisverboden, verlies van consulaire steun in het buitenland, beperkte toegang tot internationale diensten en ernstige verstoringen in de handel. Dit kan leiden tot wijdverspreide ontevredenheid en ernstige gevolgen voor de economie en de toegang tot buitenlandse diensten.
Financiële impact	Hoeveel budget is gemoeid met het risico?	Op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de directie	Niet meer op te vangen binnen de begroting van de essentiële entiteit	Niet meer op te vangen binnen de begroting van de essentiële entiteit; leidt tot financieel toezicht.
Directe imagoschade	Verlies van publiek respect of organisatiebrede negatieve publiciteit	Geen imagoschade. De reputatie van de organisatie of overheid blijft ongeschonden. Er is geen negatieve publiciteit of perceptie van het publiek. Effect: Geen invloed op de reputatie. De essentiële entiteit wordt nog steeds als betrouwbaar, efficiënt en positief gezien.	Verlies van publiek respect – Lichte imagoschade. Er is sprake van een klein incident of negatieve publiciteit, maar dit blijft beperkt en is snel te herstellen. Effect: Kortdurende negatieve perceptie bij een beperkt publiek, zonder langdurige gevolgen. Vertrouwen wordt snel hersteld door adequate communicatie en acties.	Publieke verontwaardiging – Merkbare imagoschade. Een incident of reeks incidenten leidt tot bredere negatieve aandacht in de media en onder het publiek. Het vertrouwen in de essentiële entiteit wordt aangetast, en er is kritiek op het beleid of handelen. Effect: Zichtbare impact op de reputatie, met een afname van vertrouwen en geloofwaardigheid bij een groot deel van het publiek. Herstel vereist actieve maatregelen en verbeterde communicatie.	Verlies aan vertrouwen – Aanzienlijke imagoschade. Een grote misser of reeks van schandalen leidt tot wijdverspreide negatieve berichtgeving en publieke verontwaardiging. Het herstel van het vertrouwen vergt aanzienlijke inspanningen en tijd. Effect: Het vertrouwen in de essentiële entiteit wordt ernstig geschaad. Het publiek en de media blijven kritisch, en de negatieve impact houdt lange tijd aan. Grootschalige herziening van beleid of management is nodig om het imago te herstellen.	Structureel verlies aan vertrouwen – Ernstige imagoschade. Een crisis of schandaal leidt tot langdurige en diepgaande reputatieschade, mogelijk op internationaal niveau. Het imago van de organisatie is ernstig en mogelijk onherstelbaar beschadigd. Effect: Het vertrouwen in de essentiële entiteit is volledig verloren, met blijvende gevolgen voor de geloofwaardigheid en het functioneren. Mogelijk verlies van steun vanuit het publiek, partners of andere stakeholders. Drastische maatregelen zijn nodig, en volledig herstel kan jaren duren of nooit volledig worden bereikt.
Verlies van publiek respect of vertrouwen	Wat is het effect op het vertrouwen van burgers, bedrijven of maatschappelijke organisaties in het bestuur of de gemeentelijke organisatie?	Nauwelijks merkbaar verlies van vertrouwen; beperkt tot individuen of kleine groepen. Voorbeelden: Klacht over wachttijd bij loket, incidentele negatieve reacties op sociale media.	Lokaal verlies van vertrouwen binnen een wijk of doelgroep; beperkt media-aandacht. Voorbeelden: Onvrede over wijkontwikkeling, beperkte protesten of petities.	Breder verlies van vertrouwen; meerdere doelgroepen; lokale media-aandacht. Voorbeelden: Foutieve belastingaanslagen, langdurige ICT-storing, onduidelijke communicatie.	Aanzienlijk verlies van vertrouwen; landelijke media-aandacht. Voorbeelden: Onrechtmatige uitkeringen, datalek, bestuurlijke onrust.	Structureel verlies van vertrouwen; langdurige reputatieschade; mogelijk landelijke of juridische gevolgen. Voorbeelden: Fraude, corruptie, ernstige schending van burgerrechten, bestuurlijke crisis.

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Organisatiebrede negatieve publiciteit	Wat is het effect van organisatiebrede negatieve publiciteit op het imago, het vertrouwen van inwoners en partners, en op de bestuurlijke stabiliteit?	Interne of zeer beperkte externe aandacht; geen blijvende schade. Voorbeeld: Kritiek in een bewonersbrief of kleine online discussie.	Lokale media-aandacht of social media-ophef; beperkt tot één onderwerp of wijk. Voorbeeld: Artikel in lokale krant over fout in vergunningverlening of afvalinzameling.	Entiteit-brede aandacht; meerdere afdelingen betrokken; reputatieschade binnen de grenzen van de essentiële entiteit. Voorbeeld: Nieuwsitem over falende dienstverlening, datalek, of onduidelijke communicatie.	Landelijke media-aandacht; langdurige negatieve beeldvorming; bestuurlijke verantwoording vereist. Voorbeeld: Nieuwsuuritem over mismanagement, integriteitskwestie of fraude.	Structurele reputatieschade; landelijke of internationale aandacht; mogelijk juridische of politieke gevolgen. Voorbeeld: Onderzoek door toezichthouder, Parlementaire vragen, of internationale media-aandacht.
Significant verlies van motivatie medewerkers	Wat is het effect op de motivatie van de medewerkers?	Geen waarneembaar effect op de burgergerichte processen. De dienstverlening blijft op het verwachte niveau zonder vertragingen of fouten. Effect op burgergerichte processen: Geen merkbare invloed op de kwaliteit van de dienstverlening. Burgers ervaren dezelfde efficiëntie en betrouwbaarheid.	Een lichte afname in motivatie die minimale gevolgen heeft voor de prestaties. Mogelijk kleine vertragingen of minder efficiëntie, maar zonder significante verstoring van de processen. Effect op burgergerichte processen: Kleine vertragingen of incidentele fouten in de dienstverlening, maar geen structurele problemen. Burgers merken mogelijk een lichte afname in de respons of efficiëntie.	Merkbare daling in motivatie wat leidt tot verminderde productiviteit. Dit kan leiden tot vertragingen in besluitvorming, langere doorlooptijden en mogelijk meer fouten. Effect op burgergerichte processen: Verlengde wachttijden voor burgers, fouten in de afhandeling van aanvragen, en lagere kwaliteit van dienstverlening. Burgers kunnen ontevreden raken over de snelheid en kwaliteit van de overheidsdiensten.	Aanzienlijk verlies van motivatie, resulterend in frequente fouten, lange vertragingen en verminderd vermogen om op vragen of klachten van burgers te reageren. Effect op burgergerichte processen: Veel voorkomende vertragingen en kwaliteitsproblemen, waardoor burgers regelmatig problemen ondervinden bij het verkrijgen van diensten. Dit kan leiden tot een afname van het vertrouwen in de overheid.	Extreme demotivatie die leidt tot ernstige verstoringen in de dienstverlening, inclusief aanzienlijke fouten, langdurige vertragingen en mogelijk ook hogere niveaus van verloop onder medewerkers. Effect op burgergerichte processen: Ernstige verstoringen in de burgergerichte processen. Burgers ervaren langdurige wachttijden, fouten in administratieve processen, en een drastische afname in de kwaliteit van dienstverlening, wat resulteert in grote publieke ontevredenheid en mogelijk een vertrouwenscrisis in de overheid.
Belangrijk verlies van management control	Kan de organisatie haar processen nog effectief en efficiënt uitvoeren?	Geen verlies van management control. Processen verlopen zoals gepland, met duidelijke sturing en toezicht. Effect op burgergerichte processen: Geen impact. De overheid blijft effectief in het leveren van consistente en betrouwbare diensten aan burgers.	Klein verlies van management control. Er zijn lichte inefficiënties, maar deze worden snel opgemerkt en opgelost zonder grote verstoringen. Effect op burgergerichte processen: Sporadische kleine inefficiënties in de dienstverlening, zoals lichte vertragingen of communicatiemisverstanden. Burgers ervaren incidenteel minder optimale processen, maar dit leidt niet tot serieuze klachten.	Merkbaar verlies van management control. Er ontstaan significante inefficiënties en miscommunicatie tussen verschillende afdelingen, wat resulteert in trager besluitvormingsproces en problemen met het naleven van vastgestelde procedures. Effect op burgergerichte processen: Burgers ondervinden langere wachttijden, inconsistenties in informatieverstrekking of behandeling van aanvragen. Er is een duidelijke afname in de kwaliteit en voorspelbaarheid van overheidsdiensten, wat tot verhoogde frustratie kan leiden.	Aanzienlijk verlies van management control. Het gebrek aan sturing leidt tot fouten in kritieke processen, langdurige vertragingen, en het niet volgen van protocollen. Management reageert langzaam of inadequaat op problemen. Effect op burgergerichte processen: Burgers ervaren systematische vertragingen, onvolledige of foutieve dienstverlening, en gebrek aan adequate opvolging van aanvragen of klachten. Het vertrouwen in de efficiëntie en betrouwbaarheid van de overheid neemt merkbaar af.	Extreem verlies van management control. Het management is vrijwel niet in staat om de operationele processen te beheersen. Er is sprake van een chaotische situatie met frequente fouten, gebrek aan samenhang en ernstige vertragingen. Effect op burgergerichte processen: Ernstige verstoringen in de dienstverlening aan burgers. Diensten worden slecht uitgevoerd of komen zelfs geheel tot stilstand. Burgers ervaren langdurige vertragingen, administratieve chaos en aanzienlijke fouten in hun aanvragen of diensten, wat resulteert in een groot verlies van vertrouwen in de overheidsinstellingen.
Schade vitale processen	Is er impact op de vitale/kritieke processen van de organisatie?	Geen verstoring van vitale processen.	Beperkte verstoring van vitale processen; processen kunnen snel worden hervat.	Duidelijke verstoring; vitale processen worden tijdelijk gehinderd.	Aanzienlijke verstoring; vitale processen worden ernstig gehinderd.	Catastrofale verstoring; vitale processen worden onwerkbaar of volledig stilgelegd.
Maatschappelijke impact	Incidenten die mogelijk negatieve publiciteit veroorzaken of het vertrouwen van burgers in publieke instellingen beïnvloeden.	Geen of nauwelijks merkbare impact voor de samenleving. De verstoring is beperkt tot een kleine groep mensen of heeft nauwelijks effect op het dagelijks leven van burgers.	Enige impact op een beperkte groep mensen of specifieke gemeenschap. Het dagelijks leven van burgers wordt licht verstoord, maar er zijn alternatieven beschikbaar of de verstoring is kortdurend.	Duidelijke impact op meerdere gemeenschappen of een significante groep mensen. Het dagelijks leven van deze mensen wordt merkbaar beïnvloed, bijvoorbeeld door verstoring van een publieke dienst gedurende meerdere dagen.	Aanzienlijke impact op de samenleving als geheel of op een groot deel van de bevolking. Diensten of voorzieningen die essentieel zijn voor burgers worden onderbroken, wat leidt tot verstoringen op sociaal, economisch of fysiek gebied.	Ernstige impact die de hele samenleving raakt. Essentiële diensten vallen langdurig uit of falen, wat mogelijk leidt tot onrust, massale verstoring van dagelijks leven, en maatschappelijke ontwrichting.

Impactniveau	Omschrijving	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Letsel		Geen of minimale fysieke of psychische schade.	Lichte verwondingen of stress die zonder blijvende gevolgen zijn.	Ernstige verwondingen of stress met tijdelijke gevolgen.	Zeer ernstige verwondingen of blijvende psychische schade.	Dodelijke verwondingen of onherstelbare psychische schade.
Inbreuk op persoonlijke levenssfeer		Geen of minimale inbreuk op privacy, geen impact op betrokkenen.	Beperkte inbreuk op privacy; gering risico voor betrokkenen.	Duidelijke inbreuk op privacy; aanzienlijke impact op betrokkenen.	Aanzienlijke inbreuk op privacy; ernstige impact en grote impact voor betrokkenen en verlies van vertrouwen.	Catastrofale inbreuk op privacy; ernstige gevolgen voor betrokkenen, mogelijk juridische gevolgen.

[1] Recovery Point Objective: De herstelpuntdoelstelling, die weergeeft wat het maximaal toegestane dataverlies is voor de organisatie. Deze hoeveelheid is gemeten in tijd, namelijk de periode tussen de laatste succesvolle data back-up en de verstorende gebeurtenis.
[2] Recovery Time Objective: De hersteltijddoelstelling, die weergeeft wat de maximaal toegestane tijd is dat een systeem of proces offline kan zijn na een incident zonder dat dit gevolgen heeft voor de bedrijfsvoering.
[3] Algemene Beveiligingseisen voor Defensieopdrachten.
[4] Algemene Beveiligingseisen Rijksoverheidsopdrachten.

TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Deze regeling, de Cyberbeveiligingsregeling IenW, strekt tot uitwerking van de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb). De Cbw heeft tot doel om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. De Cbw strekt tot uitvoering van de 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[1]. Die richtlijn wordt ook wel aangeduid als de NIS2-richtlijn.

Gelijktijdig met de NIS2-richtlijn is de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad[2] vastgesteld. Deze richtlijn wordt ook wel aangeduid als de CER-richtlijn. De CER-richtlijn ziet op het verhogen van de weerbaarheid van kritieke entiteiten, en wordt geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke). Kritieke entiteiten zijn aanbieders van essentiële diensten. De weerbaarheid van deze kritieke entiteiten ziet op natuurlijke en door de mens veroorzaakte risico's die negatieve gevolgen kunnen hebben voor de verlening van essentiële diensten. Voorbeelden van zulke risico's zijn ongevallen, natuurrampen, noodsituaties op het gebied van de volksgezondheid (zoals pandemieën) en dreigingen (zoals terroristische misdrijven, criminele infiltratie en sabotage).

Uitgangspunt is dat de Cbw en de Wwke en de onderliggende regelgeving zoveel mogelijk op elkaar aansluiten, zodat entiteiten niet met (dubbele) administratieve lasten te maken krijgen die verder gaan dan nodig is om de doelstellingen van de Wwke en de Cbw te verwezenlijken.

2. Hoofdlijnen van de ministeriële regeling

Deze regeling bevat de aanwijzing van de dienst CERT-WM van het openbaar lichaam Het Waterschapshuis als bedoeld in de gemeenschappelijke regeling Het Waterschapshuis als CSIRT voor de waterschappen. Ook worden enkele verplichtingen opgelegd aan het CERT-WM in zijn rol als CSIRT.

Deze regeling bevat voorts, in aanvulling op de Cbw en het Cbb, nadere regels voor de sectoren waarvoor de Minister van Infrastructuur en Waterstaat (IenW) is aangewezen als bevoegde autoriteit op grond van de Cbw. De regeling bevat allereerst de nadere regels over de maatregelen die essentiële entiteiten en belangrijke entiteiten uit de in artikel 2 bedoelde sectoren moeten treffen op grond van artikel 21 van de Cbw (zorgplicht).

Deze regeling bevat verder regels inzake de criteria aan de hand waarvan bepaald wordt of incidenten significant zijn als bedoeld in artikel 25 van de Cbw. Voor deze incidenten geldt een meldplicht als bedoeld in genoemde bepaling. De terminologie en scope van de meldplicht in de Cbw en die in de Wwke verschillen. In de onderscheiden ministeriële regelingen echter (de voorliggende regeling en de Regeling weerbaarheid kritieke entiteiten) zijn de criteria voor meldplichtige incidenten (drempelwaarden) grotendeels gelijkluidend vormgegeven, om de uitvoerbaarheid voor entiteiten die onder beide wetten vallen te waarborgen, evenals de uitvoerbaarheid en handhaafbaarheid voor de toezichthouders.

De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

3. CSIRT

In artikel 2, eerste lid, van het Cyberbeveiligingsbesluit wordt de Minister van Justitie en Veiligheid aangewezen als CSIRT, bedoeld in artikel 16, eerste lid, van de wet. Het tweede lid van artikel 2 bepaalt dat bij ministeriële regeling van de minister die het aangaat, voor entiteiten uit specifieke sectoren en voor specifieke soorten entiteiten een andere instantie kan worden aangewezen als CSIRT. Van deze mogelijkheid wordt in de voorliggende ministeriële regeling gebruik gemaakt, door voor de waterschappen als CSIRT aan te wijzen: de dienst CERT-WM die is ondergebracht in het openbaar lichaam

[1] PbEU 2022, L 333/80.
[2] PbEU 2022, L 333/164.

Het Waterschapshuis als bedoeld in de gemeenschappelijke regeling Het Waterschapshuis[3]. Voor de aanwijzing van CERT-WM is gekozen, omdat het CERT-WM nu al als ondersteuning van de waterschappen fungeert in cyberkwesties, en daar zijn goede ervaringen mee. CERT-WM is namelijk goed bekend met de structuren van en processen binnen de watersector. Hierdoor blijft kennis behouden bij de sector.
Voor een verdere toelichting zij verwezen naar het artikelsgewijze deel van deze toelichting.

4. Nadere regels zorgplicht

In deze ministeriële regeling worden voor de in artikel 2 genoemde sectoren nadere regels gesteld ten aanzien van de zorgplicht uit de Cbw en het Cbb. Het doel van deze nadere invulling is om de algemene normen uit de Cbw en het Cbb verder te concretiseren op onderdelen die worden gezien als van groot belang voor de beveiliging van netwerk- en informatiesystemen. Dit biedt duidelijkheid aan essentiële en belangrijke entiteiten en zorgt voor een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen.

Bij het opstellen van deze nadere regels is getracht aan te sluiten bij de systematiek uit de Cbw, het Cbb en Uitvoeringsverordening (EU) 2024/2690[4]. Daarmee zou de regeling goed toepasbaar moeten zijn voor entiteiten die tevens binnen het bereik van de uitvoeringsverordening vallen op basis van artikel 4 van het Cbb.

Net als voor de uitwerking van de zorgplicht in de Cbw en het Cbb zijn voor het nader uitwerken van de zorgplicht in deze regeling bestaande normenkaders gehanteerd als uitgangspunt, zoals ISO27001. Hierbij is gecontroleerd of de zorgplicht in deze regeling deze normenkaders niet doorkruist. In de toelichting wordt, waar van toepassing, naar bestaande normenkaders verwezen. Dit is in lijn met de aanpak in de toelichtingen op de Cbw en het Cbb. Entiteiten behouden hiermee de ruimte om hun bestaande normenkader te hanteren, waarbij ze wel moeten zorgen dat de maatregelen uit de Cbw, het Cbb en deze regeling geborgd zijn. Ook staat het doel van specifieke eisen in deze nota van toelichting verder uitgewerkt. Deze regeling hanteert, net als de Cbw en het Cbb, een risicogebaseerde aanpak en schrijft daarom niet overal voor hoe invulling gegeven moet worden aan de maatregelen.

4.1 Zorgplicht sector overheid, subsector waterschappen

Bij de overheid bestond al de Baseline Informatiebeveiliging Overheid (BIO) als interbestuurlijk convenant met een groot aantal zorgplichtbepalingen. Los daarvan zijn er veel andere informatiebeveiligingseisen of zorgplichtbepalingen die vanuit verschillende interbestuurlijke voorzieningen en informatieprocessen wettelijk zijn verplicht.

De Cbw en het Cbb vestigen een algemene zorgplicht voor een groot aantal maatschappelijke sectoren, waaronder de sector overheid. Naast de grondslag om deze onderwerpen nader uit te werken, biedt de delegatiegrondslag van het Cbb de ruimte om per ministeriële regeling ook zorgplichtbepalingen op te nemen over andere dan de genoemde onderwerpen, zolang die binnen de scope van de NIS2-richtlijn en de Cbw vallen. Met het stellen van nadere regels voor de zorgplicht ontstaat er voor overheidsinstanties, waaronder de waterschappen, een algemeen wettelijk uniform en afdwingbaar kader met betrekking tot de zorgplicht voor de beveiliging van netwerk- en informatiesystemen. De noodzaak om deze eisen vanuit andere wet- en regelgeving nogmaals te stellen vervalt daarmee.

De keuze is gemaakt om toepassing van de Baseline Informatiebeveiliging Overheid versie 2 (BIO2)[5], de vernieuwde versie van de BIO die al als verplichtende zelfregulering werd toegepast door overheidsinstanties, in deze regeling op te nemen als minimale invulling van het formuleren van passende en evenredige maatregelen, bedoeld in artikel 21, eerste lid, van de Cbw. In de regeling zijn om die reden de volgende verplichtingen opgenomen.

De entiteit heeft de verplichting tot het toepassen van de NEN-EN-ISO/IEC 27001 (ISO 27001) op het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor

---

[3] Blad gemeenschappelijke regeling 2024, 1163.
[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).
[5] Stcrt. 2026, 7416.

informatiebeveiliging en het vaststellen van het toepassingsgebied van die managementsystematiek. De beheersmaatregelen van de NEN-EN-ISO/IEC 27002 (ISO 27002) en de verplichte overheidsmaatregelen uit de BIO2 worden toegepast op het formuleren van passende en evenredige maatregelen. Hierbij wordt voor de beheersmaatregelen uit de ISO 27002 rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's voorkomen, gebaseerd op de scope en de onderkende risico's. De beheers- en overheidsmaatregelen uit de ISO 27002 en de BIO2 kunnen, voor zover dat noodzakelijk is én daarmee een gelijkwaardig beveiligingsniveau wordt gegarandeerd, worden vervangen door of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie NEN 7510 en voor Operationele Technologie (OT) de CSIR en IEC 62443 Industriële cybersecurity. Dat kan bijvoorbeeld wanneer het ingeschatte risico beter afgedekt is met een gelijkwaardige beheersmaatregel vanuit andere, specifiekere normenkaders.
De essentiële entiteit draagt er zorg voor dat de opzet, het bestaan en de werking van de passende en evenredige maatregelen aantoonbaar zijn. Dit is een specificering van de eis uit artikel 18 van het Cbb om de doeltreffendheid van de genomen maatregelen periodiek te evalueren. De eis sluit aan bij de BIO2 en specificeert wat aangetoond moet worden over de implementatie van de maatregelen.
Als er gebruik is gemaakt van passende en evenredige maatregelen uit andere normenkaders, is daarbij ook vereist dat de noodzakelijkheid van het gebruik van die andere normen en de gelijkwaardigheid van het beveiligingsniveau die ze bieden, aantoonbaar worden gemaakt in de Verklaring van Toepasselijkheid.

4.2 Identificeren cruciale netwerk- en informatiesystemen

Daarnaast zijn er bepalingen opgenomen die het identificeren van de cruciale netwerk- en informatiesystemen voor waterschappen verplicht stelt. Eenzelfde verplichting geldt ingevolge de Cyberbeveiligingsregeling sector overheid voor andere overheidsorganisaties. Het doel daarvan is meervoudig:
- Het helpt organisaties bij het proportioneel beveiligen van hun netwerk- en informatiesystemen. Het is een onderdeel van het risicomanagement en het geeft inzicht bij welke diensten de beveiliging de hoogste mate van zorgvuldigheid vraagt. Deze verplichting leidt er echter niet toe dat aan de zorgplicht wordt voldaan als er alleen maatregelen worden genomen ter bescherming van deze cruciale systemen;
- Het helpt entiteiten bij het voldoen aan de meldplicht. Deze drempelwaarden sluiten aan op de criteria die zijn gebruikt voor het identificeren van de cruciale netwerk- en informatiesystemen. Hierdoor is het bij incidenten op cruciale netwerk- en informatiesystemen aannemelijker dat er gemeld zou moeten worden; bij de inschatting van de netwerk- en informatiesystemen is immers reeds gekeken naar de mogelijke impact die aantasting van deze systemen kan hebben.

Voor de inschatting wat cruciale netwerk- en informatiesystemen binnen de sector overheid zijn, is gekeken naar de tabel met te beschermen belangen uit de Leidraad te beschermen belangen (TBB's) en de impacttabel die de Informatiebeveiligingsdienst van de Vereniging van Nederlandse Gemeenten (IBD) bij gemeenten toepast en die ook door enkele provincies wordt gebruikt. Deze tabellen werden al gebruikt door overheidsorganisaties voor het inschatten van het belang van de systemen voor de organisatie op basis van de mogelijke impact die het niet-functioneren van deze systemen kan hebben.

Voor de subsector waterschappen zijn er vijf impactniveaus. Het model gebruikt voor de inschatting van deze niveaus criteria die overeenkomen met de gevolgen van een incident zoals benoemd in de Cbw:
- schade aan personen, denk aan doden of ernstig gewonden als gevolg van het incident;
- materiële en immateriële schade, denk aan financieel verlies dat niet binnen de reguliere begroting van de organisatie is op te vangen;
- integriteit en vertrouwelijkheid, denk aan de openbaarmaking van informatie op het niveau Confidentieel;
- beschikbaarheid, denk aan uitval van dienstverlening van kernprocessen die een bepaalde tijd voortduurt, of herstel dat niet binnen afzienbare tijd mogelijk is.

Voor het bepalen of er sprake is van een cruciaal netwerk- en informatiesysteem kijken entiteiten naar de mogelijke impact die een aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van dit netwerk- en informatiesysteem kan hebben. Daarvoor gebruiken de waterschappen de tabel in de bijlage. Zij lopen de verschillende categorieën van deze tabellen langs en bepalen de mogelijke impact van het betreffende netwerk- en informatiesysteem op die categorie. Uiteindelijk bepaalt de hoogstgeclassificeerde categorie op welk niveau het netwerk- en informatiesysteem wordt ingeschaald. Een netwerk- en informatiesysteem is cruciaal indien het systeem impactniveau 'hoog' of 'zeer hoog' uit de tabel heeft.

4.3 Uitwerking zorgplicht niet-overheidsorganisaties

De uitwerking van de zorgplicht is gelijkluidend voor entiteiten in de sectoren waarvoor de Minister van Economische Zaken (EZ), Klimaat en Groene Groei (KGG), Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN) en Infrastructuur en Waterstaat (IenW) de bevoegde autoriteit zijn. Deze gelijkluidende uitwerking beoogt verschillen in interpretatie van regelgeving te beperken en daarmee bij te dragen aan een gemeenschappelijk hoog niveau van cyberweerbaarheid.

5. Nadere regels meldplicht

De nadere regels inzake de meldplicht beogen duidelijkheid te verschaffen over wanneer een essentiële of belangrijke entiteit een melding moet doen bij het door de bevoegde autoriteit ingerichte meldpunt. Deze nadere regels zijn van toepassing op de (sub)sectoren en soorten entiteiten waarvoor de Minister van IenW beleidsverantwoordelijk is. Het gaat om de sectoren genoemd in artikel 2. Daarnaast geldt de meldplicht voor de kritieke entiteiten die zijn aangewezen op grond van artikel 7 van de Wwke. Kritieke entiteiten kwalificeren op grond van artikel 8, eerste lid, onder i, van de Cbw tevens als essentiële entiteiten als bedoeld in de Cbw.

De meldplicht geldt als zich een significant incident voordoet. Ingevolge artikel 1 van de Cbw is een incident: 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. 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.

Ingevolge het derde lid van artikel 25 van de Cbw kunnen bij of krachtens algemene maatregel van bestuur de criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en soorten entiteiten. In paragraaf 5 van deze regeling worden per sector de criteria (drempelwaarden) bepaald.

Bij het opstellen van deze drempelwaarden is afstemming gezocht met diverse stakeholders en vertegenwoordigers van stakeholders in de desbetreffende sectoren en betrokken toezichthouders. Deze afstemming had als doel de regels goed te laten aansluiten op de praktijk en bestaande kaders, zoals de Wet beveiliging netwerk- en informatiesystemen en onderliggende regelgeving, de meldplicht uit de Wwke en sectorale regelgeving, om de uitvoerbaarheid en handhaafbaarheid te borgen en onnodige regeldruk te beperken.
Bij het formuleren van de drempelwaarden is nadrukkelijk gezocht naar een benadering die onafhankelijk is van de oorzaak van een incident. Er is geen onderscheid gemaakt tussen een fysieke of digitale oorzaak. Daardoor konden de drempelwaarden worden geharmoniseerd met die onder de Wwke. Dit komt de uitvoerbaarheid ten goede, omdat, zoals hierboven opgemerkt, kritieke entiteiten tevens kwalificeren als essentiële entiteit onder de Cbw. Er is wel enig onderscheid in de meldplicht tussen de Cbw en de Wwke. Waar relevant wordt dat toegelicht in het artikelsgewijze deel van deze toelichting.

Conform artikel 25, derde lid, van de Cbw, is er in deze regeling onderscheid gemaakt tussen sectoren, subsectoren en categorieën van entiteiten bij het opstellen van de nadere regels voor de meldplicht. In de regeling zijn dus alleen sectorspecifieke drempelwaarden opgenomen. Het bleek niet goed mogelijk om generieke drempelwaarden op te stellen, omdat er te grote verschillen tussen, maar ook binnen de sectoren waren, en er om die reden ook verschil was in de impact op de samenleving.

Een essentiële entiteit of een belangrijke entiteit meldt op basis van artikel 25, eerste lid, van de Cbw, zonder onnodige vertraging een significant incident bij het door de bevoegde autoriteit ingericht meldpunt. Hiertoe wordt één centraal meldloket onder regie van de Minister van Justitie en Veiligheid ingericht. De kritieke entiteit doet die melding uiterlijk binnen 24 uur nadat zij kennis heeft genomen van dat incident, eerder mag ook. De termijn voor het doen van de melding start op het moment wanneer een entiteit kennis heeft genomen van een incident en wanneer redelijkerwijs moet worden aangenomen dat dit incident de drempelwaarde overschrijdt of kan overschrijden. Indien een drempelwaarde geformuleerd is als een verstoring voor een bepaalde (langere) tijdsperiode kan de termijn dus ook aanvangen voordat die periode is verstreken, maar wanneer er een redelijke mate van zekerheid is dat de verstoring langer dan die periode zal duren.

6. Gevolgen voor decentrale overheden

De regeling bevat regels die betrekking hebben op decentrale overheden. Het gaat daarbij over de

waterschappen, maar ook over andere decentrale overheden, als gemeenten en provincies. De regeling bevat voorschriften voor deze overheden over de maatregelen die ze moeten treffen in het kader van de zorgplicht. Deze voorschriften zijn gelijkluidend aan de voorschriften die de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) aan deze overheden stelt.
Voorts gelden voor deze overheden de drempelwaarden in de respectieve sectoren die voor hen van toepassing zijn. Over de inhoud van de concepten van deze regeling is overleg gevoerd, zowel gezamenlijk met het Ministerie van BZK als met vertegenwoordigers van de decentrale overheden.

Gedurende de totstandkoming van deze regeling is een Uitvoeringstoets Decentrale Overheden (UDO) met beperkte omvang uitgevoerd. Daarbij werd aandacht gevraagd voor duidelijkheid over de aanwijzing van het CERT-Wm als sectorale CSIRT en de drempelwaarden voor significante incidenten. Naar aanleiding van ontvangen opmerkingen daarover is de drempelwaarde in de sector overheid voor waterschappen opgenomen. Daarbij is aangesloten bij de wijze waarop het Ministerie van BZK daaraan uitwerking heeft gegeven.
Medeoverheden hebben, bij monde van het Interprovinciaal Overleg (IPO), de Unie van Waterschappen en de Vereniging van Nederlandse Gemeenten, in hun reacties aangegeven dat deze graag meewerken aan de totstandkoming van een normenkader, voor de objecten die niet informatietechnologie (IT) betreffen. Voor de beveiliging van informatietechnologie is in paragraaf 4.1 van deze regeling een normenkader uitgewerkt. De totstandkoming van zo'n normenkader dat op operationele technologie (OT) en op de fysieke weerbaarheid van objecten ziet is ook een beleidsmatige wens, maar kon niet plaatsvinden voorafgaand aan de inwerkingtreding van de wet en daarmee van deze regeling. Wel wordt de handschoen samen met hen opgepakt om dat normenkader te ontwikkelen.

7. Regeldruk

De regeling veroorzaak beperkt nieuwe regeldruk ten opzichte van de Cbw en het Cbb. De regeldruk voor essentiële entiteiten en belangrijke entiteiten is verantwoord in de memorie van toelichting bij de Cbw en de nota van toelichting bij het Cbb. Daarbij is reeds rekening gehouden met de kosten die entiteiten moeten maken om maatregelen te treffen (de zorgplicht) en om meldplichtige incidenten te melden.

Aantal bedrijven

Het Adviescollege toetsing regeldruk (ATR) adviseert aan te sluiten bij de gebruikelijke methodiek. In de sectoren van het Ministerie van IenW hebben de Cbw, het Cbb en deze regeling gevolgen voor ongeveer 600–800 bedrijven. Deze marge is het gevolg van het feit dat betrouwbare gegevens ontbreken over welke bedrijven in welke sectoren diensten aanbieden. De gegevens in het handelsregister bieden onvoldoende duidelijkheid over welke bedrijven in de IenW-sectoren diensten aanbieden of voldoen aan de criteria voor middelgrote ondernemingen van de Aanbeveling 2003/361/EG. Daarnaast zijn er meerdere bedrijven die onder meerdere sectoren vallen. De aantallen per ministerie houden dus dubbelingen in. Deze dubbelingen vertekenen het beeld van de regeldruk. Voor een bedrijf is de uitvoeringslast hetzelfde, ongeacht of het onder een of meerdeere sectoren valt. Dit is het gevolg van een identieke zorgplicht, en meldplicht met een melding via een centraal loket.

Minder belastende alternatieven

Het ATR heeft over het concept van de regeling geadviseerd. In het advies stelt het adviescollege dat het noodzakelijk is dat een nadere toelichting wordt gegeven van en onderbouwing op de afgewogen alternatieven, de werkbaarheid van de bepalingen voor de sectoren en entiteiten en dat de regeldrukeffecten kwalitatief en kwantitatief worden uitgewerkt.
In deze regeling worden enkele bepalingen van de zorgplicht uit de Cbw en het Cbb verder geconcretiseerd. Behoudens de verplichting tot kwetsbaarheidsscans en de verplichtingen tot segmentering, is deze concretisering een verduidelijking van de verplichtingen uit het Cbb. Voor die verduidelijking zijn de uitvoeringslasten reeds bij de Cbw en het Cbb becijferd. Bij het formuleren van de bepalingen van paragraaf 4.2 van deze regeling, waarin de zorgplicht op onderdelen nader geconcretiseerd wordt, is met de volgende facetten nadrukkelijk rekening gehouden om de regeldruk zo laag mogelijk te houden. De regeling onderkent dat een entiteit onder verschillende sectoren kan vallen. Om die reden is een uniform luidende zorgplicht opgenomen voor de entiteiten voor sectoren van de Ministers van EZ en KGG, LVVN en IenW.

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

Niet-reguleren had als nadeel dat er onduidelijkheid is over de norm, wat leidt tot hogere transactiekosten voordat (rechts-)zekerheid van compliance wordt verkregen. Het reguleren van het 'hoe' betekent dat de entiteiten minder ruimte of vrijheidsgraden hebben, en daarmee tegen hogere lasten compliant worden. Daarbij geldt voor regulering van het 'hoe', dat onvoldoende rekening kan worden gehouden met de verschillen tussen sectoren en entiteiten. In deze regeling wordt de mogelijkheid behouden voor essentiële en belangrijke entiteiten om hun eigen normenkaders te hanteren voor het beheersen van hun risico's ten aanzien van de beveiliging van netwerk- en informatiesystemen, zoals de ISO/IEC of sectorale normen. Het voldoen aan een eigen normenkader betekent op zichzelf niet dat een entiteit aan de zorgplicht van de Cbw, Cbb en deze regeling voldoet. De entiteit dient te borgen dat de maatregelen die zij neemt op grond van de Cbw in ieder geval onderdeel zijn van het maatregelenpakket.
Het ATR vraagt over de drempelwaarden voorts in welke mate daarbij sprake is van ontwrichting van de samenleving. Voor het bepalen van de hoogte van de drempelwaarden is gekeken naar de potentiële effecten van een incident. Deze effecten zijn nog niet zo ernstig dat de samenleving daardoor ontwricht raakt. In het overgrote deel van de gevallen gaat het om een ernstige verstoring van een proces waar anderen van afhankelijk zijn, of dat er aanzienlijke schade optreedt. Beoogd is een drempelwaarde in een sector zo vast te stellen dat uitsluitend de meest ernstige verstoringen gemeld moeten worden, die hooguit enkele keren per jaar voor komen. Naar aanleiding van dit advies van het ATR is in de toelichting extra toegelicht hoe de drempelwaarden tot stand zijn gekomen en welke alternatieven zijn overwogen.

Werkbaarheid

Het ATR adviseert om in de toelichting nader in te gaan op de werkbaarheid van de drempelwaarden en de zorgplicht en de inbreng van bedrijven o.a. uit de pre-consultatie daarbij te benoemen en aan te geven hoe met die input is omgegaan. In paragraaf 9 van deze toelichting wordt ingegaan op de aandachtspunten van bedrijven.

Het ATR merkt op dat bedrijven extra lasten ervaren als zij te maken krijgen met stapeling van verplichtingen of knelpunten. Het college adviseert in de toelichting in te gaan op hoe deze voorkomen worden. Ten aanzien van stapeling van verplichtingen streven de Ministeries van Economische Zaken en Klimaat, Klimaat en Groene Groei, Landbouw, Visserij, Voedselzekerheid en Natuur en Infrastructuur en Waterstaat naar een uniform geformuleerde zorgplicht. Dit is de beste garantie voor het voorkomen van stapeling of knelpunten. Ten aanzien van stapeling van toezicht maken de toezichthouders ten aanzien van entiteiten die in meerdere sectoren vallen in abstracto en in concreto werkafspraken. Onderdeel van die afspraken is dat dubbele toezichtslasten worden voorkomen. Ten aanzien van stapeling van drempelwaarden zij opgemerkt dat deze drempelwaarden zo veel mogelijk geoperationaliseerd zijn voor een specifieke sector en dat deze hoog liggen, in veel gevallen duidelijk hoger dan andere meldplichten voor vergelijkbare incidenten. Onderkend wordt dat dit kan betekenen dat een incident op meerdere plekken, bij meerdere instanties moet worden gemeld.

Het ATR vraagt in welke mate de concretisering van de zorgplicht een verandering in de ingeschatte lasten meebrengt. De concretisering van de zorgplicht zou mogelijk de enige extra lasten meebrengen. Alle bepalingen die de zorgplicht concretiseren betreffen aspecten die een entiteit reeds op grond van de Cbw, het Cbb en een richtlijn-conforme interpretatie daarvan, bij de beleidsvorming moet betrekken. Die bepalingen betreffen een verduidelijking en zijn reeds verdisconteerd in de omvang van de lasten die zijn beschreven in de memorie van toelichting op de Cbw en de nota van toelichting op het Cbb. De hoogte van de drempelwaarde voor het doen van een melding brengt geen aanvullende uitvoeringslasten mee. De drempelwaarde is zo gekozen dat het aantal meldingen dat gedaan moet worden, niet hoger zal liggen dan waar al rekening mee is gehouden bij de Cbw en het Cbb. Voor de 600 tot 800 bedrijven in IenW-sectoren geldt dat per entiteit gemiddeld een melding per jaar wordt verwacht. Dat wil zeggen 600 tot 800 meldingen per jaar. De last van deze meldingen is reeds becijferd in de memorie van toelichting bij de Cbw en de nota van toelichting bij het Cbb.

Invoeringstoets

Het ATR adviseert om een invoeringstoets uit te voeren. De Cbw is op dat punt geamendeerd, waardoor een bepaling is opgenomen die een invoeringstoets regelt (artikel 94, eerste lid). Bij die invoeringstoets kunnen alle knelpunten aan de orde komen, ook de knelpunten die het gevolg zijn van nadere regels.

8. Uitvoering

Voor deze regeling hebben de Inspectie Leefomgeving en Transport (ILT), de Nederlandse Voedsel- en Warenautoriteit en de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) een handhaafbaarheids-, uitvoerings- en fraudebestendigheidstoets (HUF-toets) uitgebracht. De genoemde

instanties beoordelen de regeling als handhaafbaar, uitvoerbaar en fraudebestendig, en hebben daarbij enkele aandachtspunten.

ILT

De ILT merkt op dat er samenwerkingsafspraken met andere toezichthouders moeten worden gemaakt, waarbij ook rekening gehouden moet worden met reeds bestaande sector-regelgeving. De ILT merkt op dat de drempelwaarde bij de scheepvaartafwikkeling gerelateerd is aan een gebruikelijke situatie, die lastig kenbaar is voor de toezichthouder. Mede naar aanleiding van deze opmerking is de drempel geherformuleerd. De ILT merkt voorts op dat het wenselijk is om beter zicht te krijgen op de normadressaten in enkele sectoren. Onderkend wordt dat dat wenselijk is. Het ministerie spant zich in om daar beter zicht op te krijgen. Communicatie rond de inwerkingtreding van de wet moet daaraan bijdragen. Voorts vraagt de ILT aandacht voor de kwaliteit van het register en de mogelijkheid om concerns daar als zodanig in te registreren. Die behoefte wordt onderschreven.

NVWA

De NVWA vraagt om aandacht voor de benodigde capaciteit. De NVWA maakt opmerkingen over de wijze waarop de toezichthouders worden aangewezen. De aanwijzing van toezichthouders gebeurt mede daarom bij separaat besluit. De NVWA constateert dat er noodzaak bestaat om werkafspraken te maken met andere toezichthouders. Dat punt wordt onderkend.

ANVS

De HUF-toets van de ANVS heeft betrekking op zowel de Regeling weerbaarheid kritieke entiteiten IenW als de Cyberbeveiligingsregeling IenW. Op deze HUF-toets is gereageerd in paragraaf 7 van het algemeen deel van de toelichting bij de Regeling weerbaarheid kritieke entiteiten IenW. Kortheidshalve zij daarnaar hierbij verwezen.

9. Consultaties

Een concept van de regeling is geconsulteerd op www.internetconsulatie.nl.

Gezamenlijke paragraaf internetconsultatie

Omdat de nadere uitwerking van de zorgplicht gezamenlijk is opgesteld door de Ministers van EZ, KGG, LVVN en IenW, zijn de binnengekomen consultatiereacties gezamenlijk geanalyseerd en verwerkt. Om deze reden zal in deze consultatieparagraaf op de binnengekomen reacties vanuit verschillende sectoren worden ingegaan.

Algemeen

Meerdere partijen, zoals BTG en Elaad, vragen om een verwijzing naar bestaande normen, zoals ISO/NEN en sectorspecifieke normen. Naar aanleiding van deze reacties is de toelichting op de algemene inleiding zorgplicht aangepast in lijn met de Cbw en het Cyberbeveiligingsbesluit Cbb. NOREA stelt in haar reactie voor om netwerksegmentatie uit te breiden naar leveranciersscreening en ketenaudits. Dit voorstel is niet in de zorgplicht in de regeling opgenomen, aangezien deze verplichting voor een verhoogde regeldruk en aanzienlijk verhoogde kosten bij essentiële en belangrijke entiteiten zorgt, en in sommige gevallen moeilijk uitvoerbaar is. Daarbij werkt deze regeling het artikel over beveiliging van de toeleveringsketen uit het Cbb bewust niet verder uit, omdat dit een nieuwe verplichting is uit de richtlijn en de regels uit het Cbb voor nu als voldoende worden geacht.

Artikel 11. Bedrijfscontinuïteit

Schiphol vraagt om te verduidelijken dat het bedrijfscontinuïteitsplan uit verschillende deelplannen kan bestaan. Dat is verduidelijkt.

Artikel 12. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Meerdere partijen, zoals Holland Solar en Energie Nederland, vragen om een duidelijker onderscheid aan te brengen tussen IT en OT, waaronder voor patchmanagement. Dit onderscheid is doorgevoerd in meerdere onderdelen van de toelichting op artikel 12. Wat betreft patchmanagement is bijvoorbeeld nader toegelicht op artikel 12, tweede lid, onderdeel c, dat bij het toepassen van beveiligingspatches op OT-systemen de noodzaak van continuïteit van dienstverlening en de verouderde aard van veel industriële componenten meegewogen kan worden om te bepalen of de nadelen van deze toepassing

zwaarder wegen dan de voordelen voor cyberbeveiliging.

Artikel 13. Beveiligingsaspecten ten aanzien van toegangsbeleid

RWE onderschrijft het belang van sterke identificatie- en authenticatieprocedures, en een zorgvuldig gereguleerde autorisatie. Het energiebedrijf benadrukt in zijn reactie dat niet alle OT-systemen technisch in staat zijn om deze functionaliteit te ondersteunen en adviseert om een clausule op te nemen, zoals 'waar mogelijk', of de verplichting om 'alternatieve maatregelen te definiëren' voor systemen die deze functionaliteit niet kunnen implementeren. Als reactie hierop is dit artikel aangepast, en is er ruimte geboden om dit mee te nemen in het beleid over bevoorrechte accounts en systeembeheeraccounts. Bovendien geldt voor alle zorgplicht maatregelen dat deze passend en evenredig worden ingevuld.

Cyberjaarverslag

NOREA vraagt onder andere in haar reactie om een verplichting aan entiteiten op te leggen om op basis van de Internationale Digitale Rapportage Standaard (IDRS) een cyberjaarverslag op te stellen. Dit wordt niet geregeld in deze regeling, aangezien die een implementatie is van de NIS2-richtlijn, waarbij aan entiteiten geen aanvullende verplichtingen worden opgelegd. Momenteel verkennen de Ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Economische Zaken en Klimaat (EZK), naar aanleiding van de motie-Kathmann[6], hoe het cyberjaarverslag, op basis van de IDRS, ingevoerd kan worden als brede standaard op een wijze die leidt tot lastenverlichting en het verbeteren van de veiligheid.

Drempelwaarden

Meerdere partijen hebben in een reactie aangegeven dat de concept-regeling drempelwaarden bevatte die ook bereikt worden onder 'normale' omstandigheden. In reactie daarop zijn de drempelwaarden voor de relevante sectoren aangepast.
Meerdere partijen gaven aan dat onduidelijk was welke drempelwaarden voor hen specifiek zouden gelden. In reactie daarop is dat in de formulering van de verschillende drempelwaarden verduidelijkt.
Een partij heeft gevraagd om ook de waarneming van ongeïdentificeerde luchtvaartuigen onder de meldplicht te laten vallen. Dit verzoek is niet overgenomen omdat een dergelijke waarneming op zichzelf niet leidt tot een aanzienlijke verstoring.

Specifiek over enkele sectorale drempelwaarden zijn in de consultatie de volgende opmerkingen gemaakt.

Luchthavens

Schiphol vraagt om te verduidelijken dat artikel 15, onder a, de voor haar relevante drempelwaarde is, en om het eerste lid van artikel 14 uit de conceptregeling te laten vervallen. Dit is overgenomen.

Vervoer, vervoer over water

FERM-Zeehavens heeft gevraagd om verduidelijking van onderdelen van de drempelwaarden van artikel 17. Mede naar aanleiding daarvan zijn de drempelwaarden aangepast en verduidelijkt.
FERM-Zeehavens vraagt voorts naar de mogelijkheid om kennis te blijven ontvangen, die voorheen met OKTT's werd gedeeld (organisaties die 'objectief kenbaar tot taak' hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen). Dat is mogelijk en wordt in een separaat traject verder uitgewerkt.
De (Rijks)havenmeesters hebben opmerkingen over enkele drempelwaarden voor die sector. Met name een drempelwaarde van een uur wordt disproportioneel gevonden. In reactie daarop zijn de drempelwaarden voor de havens aangepast en wordt een langere termijn gehanteerd.
De Nederlandse Loodsencorporatie maakt overige opmerkingen die geen bespreking behoeven en in bilateraal overleg worden geadresseerd.

Chemie

De Vereniging van de Nederlandse Chemische Industrie (VNCI) bepleitte in de internetconsultatie over de drempelwaarde voor de chemische industrie door de entiteiten zelf te laten bepalen wanneer er sprake is van een ernstige verstoring en door hen zelf te laten aangeven welke van hun diensten het meest kritisch is in het kader van bedrijfscontinuïteit. Dit is onder de Cbw niet mogelijk. Bedrijven zijn

[6] Kamerstukken II 2025/26, 26 643, nr. 1342.

van rechtswege een essentiële of belangrijke entiteit of zij worden vanwege de levering van een bepaalde essentiële dienst als kritieke entiteit aangewezen. Het ligt daarmee dus vast om welke dienst het gaat. Daarnaast bepleitte de VNCI dat entiteiten niet kunnen voldoen aan drempelwaarde van artikel 25, onder b, omdat de lijst van kritieke entiteiten niet openbaar is. In de artikelsgewijze toelichting op artikel 25 is daar nader op ingegaan. De VNCI heeft voorts opmerkingen ingediend over de overlap in meldplicht met overige regelgeving en de toezichtslast. De regeling is hierop niet aangepast. Bestaande wetgeving, zoals de Omgevingswet waarin onder meer de zogeheten Seveso-richtlijn[7] is omgezet, ziet niet op de weerbaarheid van entiteiten. De Wwke kent een all hazard-karakter en treedt naar de opvatting van de regering niet terug voor de bedrijven waarop tevens de Seveso-richtlijn van toepassing is, omdat deze laatste geen specifieke eisen kent voor weerbaarheid. De verplichtingen uit de Cbw zijn dus van toepassing naast de Seveso-richtlijn en de Seveso-toezichthouder is niet belast met het toezicht op de Cbw. Wel kan het zo zijn dat een incident onder de Cbw samenvalt met of gerelateerd is aan een incident zoals bedoeld in de Seveso-richtlijn. De entiteit zal dan voor beide zaken een melding moeten doen bij de betreffende bevoegde autoriteit.

Overige opmerkingen

Enkele respondenten, waaronder FERM-Zeehavens en de Nederlandse Loodsencorporatie, vragen om verduidelijking van het begrip 'overheidsorganisaties' met het oog op het beantwoorden van de vraag of de artikelen van paragraaf 4.1 of 4.2 voor hen relevant zijn. De definitie van het begrip kan niet nader verduidelijkt worden in deze regeling of de toelichting erop. Tegelijkertijd wordt wel, in samenspraak met het Ministerie van BZK, gekeken of dit voor individuele organisaties verduidelijkt kan worden.
Een respondent merkt op dat in theorie kwetsbaarheden ook gelden als incident. Door drempelwaarden vast te stellen, is naar verwachting niet iedere kwetsbaarheid een meldplichtig incident.
Een respondent vraagt om branche-specifieke regelgeving, op basis van daadwerkelijke risico's. Dit wordt niet overgenomen.

10. Evaluatie

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

ARTIKELSGEWIJS DEEL

Artikel 2 (Reikwijdte)

Artikel 2 bepaalt de reikwijdte van deze regeling. Zij is van toepassing op alle essentiële entiteiten en belangrijke entiteiten die onder de verantwoordelijkheid vallen van de Minister van Infrastructuur en Waterstaat (IenW) als bevoegde autoriteit (eerste lid). De regeling is voorts van toepassing op door deze minister aangewezen kritieke entiteiten, die immers, ingevolge artikel 8, eerste lid, aanhef en onder i, van de Cyberbeveiligingswet (Cbw) ook kwalificeren als essentiële entiteit als bedoeld in de Cbw (tweede lid). Deze regeling is ten slotte van toepassing op essentiële en belangrijke entiteiten in de sector onderzoek, voor zover de desbetreffende onderzoeksorganisatie betrekking heeft op een van de IenW-sectoren.

Artikel 3 (CSIRT)

Zoals is toegelicht in het algemeen deel van deze toelichting, wordt de dienst CERT-WM, ondergebracht in het openbaar lichaam Het Waterschapshuis als bedoeld in de gemeenschappelijke regeling Het Waterschapshuis[8], aangewezen als CSIRT (Computer Security Incident Response Team) voor de waterschappen. De waterschappen maken deel uit van verschillende sectoren, te weten: de sector keren en beheren, de sector vervoer, subsector weg, de sector afvalwater en de sector overheid, subsector waterschappen. Het CERT-WM fungeert als CSIRT voor de waterschappen ten behoeve van hun taakuitvoering binnen al deze sectoren.

---

[7] Richtlijn 2012/18/EU van het Europees Parlement en de Raad van 4 juli 2012 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken, houdende wijziging en vervolgens intrekking van Richtlijn 96/82/EG van de Raad (PbEU 2012, L 197).
[8] Blad gemeenschappelijke regeling 2024, 1163.

Artikel 4 (Verplichtingen CSIRT)

In artikel 3, eerste lid, van het Cyberbeveiligingsbesluit worden eisen gesteld aan CSIRT's. Het derde lid van dit artikel maakt het mogelijk om bij ministeriële regeling van de minister die het aangaat, nadere regels te stellen over de functionele, financiële, technische en organisatorische vereisten ten aanzien van een organisatie die op grond van artikel 2, tweede lid, van het Cyberbeveiligingsbesluit is aangewezen als CSIRT. Van deze mogelijkheid is gebruik gemaakt door in artikel 4 van deze regeling enkele verplichtingen aan CERT-WM op te leggen. Concreet moet jaarlijks uiterlijk op 31 december een rapport worden opgeleverd over de manier waarop CERT-WM invulling heeft gegeven aan de taken, bedoeld in artikel 16 van de Cyberbeveiligingswet en aan de eisen, bedoeld in artikel 3, eerste lid, van het Cyberbeveiligingsbesluit.
Het tweede lid bepaalt dat het CERT-WM voldoet aan het SIM3 Model (Security Incident Management Maturity Model) op minimaal het niveau intermediate. Het derde lid bepaalt dat dit niveau wordt vastgesteld door een audit die wordt uitgevoerd door een onafhankelijke en gekwalificeerde deskundige. Daarmee wordt de neutraliteit van de beoordeling van het volwassenheidsniveau gewaarborgd. Omdat een SIM3-auditcertificaat maximaal drie jaar geldig is, is in aansluiting hierop in het vierde lid bepaald dat het auditrapport, waarmee wordt aangetoond dat aan bovenbedoeld niveau wordt voldaan, niet ouder is dan drie jaar. Het is mogelijk dat er voor deze driejaarstermijn een hernieuwde onafhankelijke audit wordt uitgevoerd, bijvoorbeeld als het CERT-WM significante organisatorische wijzigingen ondergaat. Voor het geval het CERT-WM blijkens genoemde audit niet meer voldoet aan het gestelde niveau, wordt in het vijfde lid bepaald dat het een verbeterplan moet opstellen en op basis daarvan wijzigingen moet doorvoeren om weer aan dat niveau te voldoen. Daarmee wordt ook beoogd om het CERT-WM een redelijke termijn te geven om alsnog te kunnen voldoen aan het gestelde niveau. Ook regelt het vijfde lid dat het CERT-WM de Minister van IenW informeert over (de uitvoering van) het verbeterplan. Die kan deze informatie betrekken bij de besluitvorming over de continuering van de aanwijzing als CSIRT.

Artikel 6 (ISO 27001)

Dit artikel verplicht de waterschappen om de ISO 27001 toe te passen op het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsystematiek voor beveiliging van informatie in netwerk- en informatiesystemen. Hiermee wordt bedoeld dat de managementsystematiek van de essentiële entiteit moet voldoen aan de eisen uit deze standaard. Ook moet deze standaard worden toegepast op het vaststellen van het toepassingsgebied van de managementsystematiek. Doorgaans zal een dergelijk managementsystematiek ook zien op beveiliging van informatie buiten netwerk- en informatiesystemen. Gelet op de scope van de Cbw en lagere regelgeving, beperkt dat zich in deze regeling tot netwerk- en informatiesystemen.

De verwijzingen naar deze ISO-standaard betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging van deze standaard niet automatisch leidt tot het verplicht worden van de nieuwe versie onder deze regeling. In plaats daarvan zal er altijd een wijziging moeten worden aangebracht in deze regeling om die nieuwe versie van toepassing te laten zijn. Zo wordt gegarandeerd dat een wijziging van de inhoud van deze regeling altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen. Indien een nieuwe versie van de ISO-standaard beschikbaar is, maar deze regeling hierop nog niet is aangepast en een essentiële entiteit wil deze nieuwe versie toepassen, dan is het gebruik daarvan mogelijk, mits dit niet leidt tot een lager beveiligingsniveau dan de in deze regeling voorgeschreven versie.

Artikel 7 (identificeren cruciale netwerk- en informatiesystemen)

Deze bepaling verplicht waterschappen om hun cruciale netwerk- en informatiesystemen te identificeren en daarvan een overzicht bij te houden als onderdeel van de managementsystematiek voor de beveiliging van netwerk- en informatiesystemen, bedoeld in artikel 6, vierde lid, van het Cbb.

Het vaststellen van de cruciale netwerk- en informatiesystemen wordt gedaan door middel van de tabel die is opgenomen in de bijlage bij deze regeling. Deze tabel is gebaseerd op de impacttabel die is uitgegeven door de Informatiebeveiligingsdienst van de Vereniging van Nederlandse Gemeenten (IBD). Een netwerk- en informatiesysteem is cruciaal als dit het impactniveau 'Hoog' of 'Zeer hoog' heeft uit de tabel in de bijlage bij deze regeling. Als bijvoorbeeld in de categorie financiële impact sprake is van niveau 'Hoog' en in de rest van de categorieën gevolgen van niveau 'Laag', dan is er niettemin sprake van een cruciaal netwerk- en informatiesysteem, omdat de gevolgen van het incident in ten minste één categorie van de impacttabel de drempelwaarde overschrijden. Als er dus sprake is van schades op verschillende impactniveaus, moet worden uitgegaan van de categorie gevolgen die de hoogste impact heeft.
In de categorieën waar ook een passage is opgenomen over het "effect op burgergerichte processen", hoeft niet aan beide genoemde situaties voldaan te zijn. Om in die categorie te vallen is het voldoende

dat wordt voldaan aan de eerste alinea van de betreffende categorie.

Artikel 8 (ISO 27002 en BIO2)

De kern van de zorgplicht is het komen tot een passende set aan maatregelen die de geïnventariseerde risico's afdoende beheersen. Het eerste lid verplicht essentiële entiteiten tot het gebruikmaken van de beheersmaatregelen van de ISO 27002:2022 voor het formuleren van passende maatregelen voor de beveiliging van netwerk- en informatiesystemen, bedoeld in artikel 21, eerste lid, van de Cbw. De beheersmaatregelen uit de ISO 27002 moeten risicogedreven toegepast worden. Dat volgt uit de verplichting om deze ISO-standaard te gebruiken voor 'het formuleren van passende en evenredige maatregelen'. Dit is waartoe de ISO-standaard zelf ook verplicht. Dat impliceert dat een essentiële entiteit aanvullende maatregelen moet treffen als het risico daarom vraagt. Om die reden is de verplichting opgenomen dat zij 'ten minste' deze ISO-standaard moet toepassen. Tegelijkertijd betekent de risicogedreven benadering ook dat toepassing van bepaalde beheersmaatregelen achterwege gelaten kan worden als het risico beperkt is, of als de betreffende beheersmaatregel niet relevant is, omdat de essentiële entiteit bijvoorbeeld niet beschikt over bepaalde systemen waar een beheersmaatregel op ziet.

Ingevolge het eerste lid omvatten deze passende en evenredige maatregelen ten minste de relevante overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stcrt. 2026, 7416). Deze overheidsmaatregelen uit de BIO2 komen niet "bovenop" de ISO-beheersmaatregelen, maar vormen al een gedeeltelijke invulling van de passende en evenredige maatregelen die geformuleerd moeten worden op basis van de ISO 27002. Essentiële entiteiten moeten deze overheidsmaatregelen implementeren ongeacht het ingeschatte risico. Dit betreft echter wel een minimale invulling: waar het risico groter is, zullen meer passende en evenredige maatregelen moeten worden genomen. Als een BIO2-overheidsmaatregel niet toe te passen is, omdat de essentiële entiteit bijvoorbeeld niet beschikt over een systeem waarop deze maatregel ziet, kan het gebruik van die overheidsmaatregel achterwege worden gelaten. Om die reden is in de tweede zin van het eerste lid de formulering 'de voor haar relevante overheidsmaatregelen' opgenomen.

Met het eerste lid wordt de toepassing van deze standaarden vastgelegd, voor zover zij zien op de beveiliging van netwerk- en informatiesystemen. Deze beperking is noodzakelijk, omdat deze standaarden in principe zien op informatiebeveiliging in bredere zin, inclusief bijvoorbeeld informatie die op papier staat. Dit valt buiten de reikwijdte van de NIS2-richtlijn en daardoor ook van de Cbw en de daarop gebaseerde regelgeving. Toepassing ervan kan dus niet in deze regeling worden verplicht.

Enkele beheersmaatregelen uit de ISO 27002 en overheidsmaatregelen uit de BIO2 vallen buiten de reikwijdte van de Cbw. Toepassing daarvan wordt daarom in deze regeling niet verplicht gesteld. Een voorbeeld hiervan is een beheersmaatregel die ziet op de bescherming van intellectuele-eigendomsrechten. Dit is een onderwerp dat de Cbw niet regelt. Het eerste lid voorziet daarom in een expliciete uitzondering van deze beheers- en overheidsmaatregelen. In de BIO2 is dit voor de uitgezonderde overheidsmaatregelen duidelijk gemaakt door middel van het aanbrengen van een vetgedrukte tekstmarkering. Voor de uitgezonderde beheers- en overheidsmaatregelen blijft wel de verplichtende zelfregulering van toepassing die voor de gehele BIO2 geldt. Deze verplichting staat echter los van de Cbw.

De verwijzingen naar de ISO 27002:2022 en de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stcrt. 2026, 7416) betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging niet automatisch leidt tot het verplicht worden van de nieuwe versie onder deze regeling. Om een nieuwe versie van deze standaarden van toepassing te laten zijn, zal eerst een wijziging in deze regeling moeten worden aangebracht. Zo wordt gegarandeerd dat een wijziging van de materiële eisen die op grond van deze standaarden worden gesteld aan de entiteit altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen. Indien een nieuwe versie van een standaard beschikbaar is, maar deze regeling hierop nog niet is aangepast en een essentiële entiteit wil deze nieuwe versie toepassen, dan is dat mogelijk, zolang dit niet leidt tot een lager beveiligingsniveau.

Tweede lid

Op basis van het tweede lid kunnen de beheersmaatregelen uit de ISO 27002 en de overheidsmaatregelen uit de BIO2 worden vervangen door of gecombineerd met beheersmaatregelen uit andere normenkaders voor informatiebeveiliging. De essentiële entiteit moet wel aannemelijk maken dat het vervangen door of combineren met andere passende en evenredige maatregelen noodzakelijk is en dat deze maatregelen een gelijkwaardig beveiligingsniveau bieden.

Derde lid

De verplichting in het derde lid voor de essentiële entiteit om te zorgen voor aantoonbaarheid van opzet, bestaan en werking van maatregelen geldt voor alle netwerk- en informatiesystemen. Daarbij is er ruimte om deze aantoonbaarheid risicogedreven vorm te geven als onderdeel van de operationalisering van de beheersmaatregelen. De controle op en aantoonbaarheid van opzet, bestaan en werking van de maatregelen ter bescherming van netwerk- en informatiesystemen die het meest cruciaal zijn, of waar de hoogste dreiging voor geldt, moet het strengste zijn. Voor netwerk- en informatiesystemen met een laag risicoprofiel is het toegestaan deze controle minder uitgebreid in te vullen. De wijze waarop deze controle wordt ingevuld, moet kunnen worden onderbouwd met een risicoafweging. Indien de entiteit gebruik heeft gemaakt van andere passende en evenredige maatregelen, geldt naast de bovenstaande verplichting om de opzet, bestaan en werking aan te tonen, ook de verplichting om de noodzakelijkheid en gelijkwaardigheid van de andere normen en richtlijnen aantoonbaar te maken. Dit wordt aangetoond in de Verklaring van Toepasselijkheid.

Hoe de maatregelen zijn geoperationaliseerd, moet via verwijzingen worden vastgelegd, bijvoorbeeld in een beleids- of ontwerpdocument. Hiermee toont de essentiële entiteit de 'opzet' van maatregelen aan. Al dan niet met behulp van externe partijen of via self-assessments, audits, pentesten, redteamtesten en dergelijke toont de essentiële entiteit het 'bestaan' en de 'werking' van maatregelen aan. Met bestaan wordt bedoeld dat de maatregelen daadwerkelijk zijn geïmplementeerd, met werking wordt bedoeld dat de organisatie aantoont dat de maatregelen effectief zijn.

Artikel 10 (Beleid over beveiliging van netwerk- en informatiesystemen)

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

Artikel 11 (Bedrijfscontinuïteit)

Op basis van artikel 9, tweede lid, van het Cbb moet de belangrijke entiteit of essentiële entiteit processen en procedures vaststellen en toepassen voor back-ups van software en gegevens. De risicobeoordelingen op grond van artikel 7 van het Cbb zijn dus relevant voor zowel het bepalen van welke software en gegevens in back-ups moeten 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 terug moeten komen. Het bepalen van hersteltijden, in het Engels ook wel bekend als *recovery time objective* (RTO), heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. Herstelpunten, in het Engels ook wel bekend als *recovery point objective* (RPO), hebben betrekking op de frequentie van de back-ups. Het voorschrift dat de processen en procedures moeten waarborgen dat back-ups volledig zijn, ziet erop dat alle gegevens die nodig zijn voor het herstellen van de betreffende netwerk- en informatiesystemen moeten 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 moeten de processen en procedures waarborgen dat de back-ups nauwkeurig zijn. Hiermee wordt bedoeld dat de informatie ingeval van herstel succesvol kan worden gebruikt, bijvoorbeeld door ervoor te zorgen dat de gegevens in de back-up zich in een staat bevinden die een succesvol herstel mogelijk maken.

Daarnaast moeten de processen en procedures ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups gewaarborgd worden, zodat de back-ups ook daadwerkelijk ingezet

kunnen worden. Met integriteit wordt bedoeld dat de entiteit borgt dat de back-ups niet zijn gemanipuleerd of beschadigd, bijvoorbeeld door derden. Dit voorkomt dat de geback-upte gegevens zijn gewijzigd, beschadigd of aangetast tijdens het backupproces, 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 moet gewaarborgd worden, om ongeautoriseerde toegang tot gegevens te voorkomen. Ook moeten de processen en procedures waarborgen 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 wanneer noodzakelijk 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 en testen. Ten slotte moeten de processen en procedures omschrijven hoe lang de betreffende back-ups bewaard moeten worden.

Bedrijfscontinuïteitsplan

De essentiële of belangrijke entiteit moet op grond van artikel 9, derde lid, van het Cbb een bedrijfscontinuïteitsplan opstellen. Daarmee kan zij zich voorbereiden op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen, hierop goed en tijdig reageren en de duur en gevolgen van dergelijke incidenten beperken. Op grond van het tweede lid van artikel 11 van deze regeling moet de entiteit bij het opstellen van het bedrijfscontinuïteitsplan rekening houden met de risicobeoordelingen op grond van artikel 7 van het Cbb, zodat zij alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen.

De onderdelen van het tweede lid omschrijven de onderdelen die geadresseerd moeten worden in het plan. Allereerst moet het plan het doel en de reikwijdte ervan bevatten, zodat de context en het toepassingsbereik op voorhand duidelijk zijn. Daarbij ligt het voor de hand dat de entiteit zich met name richt op de voor haar kritieke processen. 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 moeten worden. De voorwaarden voor activering en deactivering beschrijven in welke gevallen of onder welke omstandigheden het bedrijfscontinuïteitsplan of onderdelen ervan worden geactiveerd dan wel gedeactiveerd. De vereiste middelen, met inbegrip van back-ups en redundanties, beschrijven welke middelen nodig zijn om een goede uitvoering aan het bedrijfscontinuïteitsplan te geven. Ten slotte moet het bedrijfscontinuïteitsplan de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen bevatten, om zo de overgang naar een normale bedrijfsvoering te waarborgen.

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

Artikel 12 (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 te hebben voor het onderhoud en beheer van hun 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, moeten essentiële en belangrijke entiteiten processen en procedures inrichten 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 er bij reguliere systeemupdates van besturingssystemen doorgaans al sprake van ingebouwde technische controles op herkomst en integriteit van beveiligingspatches. De essentiële of belangrijke entiteit moet zich hiervan echter wel 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 meebrengt. Voornoemde stappen dragen ertoe bij dat de toepassing van patches geen nieuwe kwetsbaarheden of verstoringen veroorzaakt. Vervolgens bepaalt onderdeel c dat beveiligingspatches binnen een redelijke termijn nadat zij beschikbaar zijn moeten worden toegepast, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen op het gebied van cyberbeveiliging. Dit kan bijvoorbeeld het geval zijn voor het toepassen van beveiligingspatches op OT-systemen waarbij het belang van continuïteit van dienstverlening en de verouderde aard van veel industriële componenten een rol 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, moet de motivatie voor het niet of niet direct toepassen van de beveiligingspatch gedocumenteerd worden.

Derde lid, onderdeel a

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

Onderdeel b

Op grond van dit onderdeel voeren essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uit op hun netwerk- en informatiesystemen en leggen zij de resultaten daarvan vast. Deze scans maken het mogelijk om inzicht te krijgen in bekende kwetsbaarheden in systemen en applicaties en vormen daarmee een belangrijk hulpmiddel om risico's tijdig te onderkennen. De entiteit voert de scans waar passend toe door rekening te houden met de blootstelling van systemen aan dreigingen en hun netwerktoegankelijkheid, alsmede met de kritikaliteit van die systemen voor de continuïteit van de dienstverlening en de potentiële impact van uitval of misbruik. Kwetsbaarheidsscans 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 en belangrijke entiteiten om een passende vorm van kwetsbaarheidsscan in te zetten, gegeven hun omgeving van netwerk- en informatiesystemen en de mogelijke risico's die zich 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 evalueren essentiële en belangrijke entiteiten hun blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van hebben ten aanzien van hun netwerk- en informatiesystemen. Dit is voor zover artikel 17 van het Cbb daar niet reeds toe verplicht. Onderdeel c regelt daarmee aanvullend dat kwetsbaarheden uit de uitgevoerde kwetsbaarheidsscans of meldingen van interne werknemers ook geëvalueerd en verholpen moeten worden. Door deze evaluatie structureel uit te voeren, ontstaat een actueel beeld van het risicolandschap en kan tijdig worden bepaald welke aanvullende maatregelen nodig zijn om de weerbaarheid te vergroten.

Onderdeel d

Op grond van dit onderdeel nemen essentiële en belangrijke entiteiten onverwijld maatregelen om kwetsbaarheden die een risico vormen voor de beveiliging van hun netwerk- en informatiesystemen te verhelpen. Indien een kwetsbaarheid niet of op een later moment verholpen wordt, moet de essentiële of belangrijke entiteit dit motiveren en 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 toezichthouder oordelen of deze keuze terecht is gemaakt.

Vierde lid, onderdeel a

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

Onderdeel b

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

Artikel 13 (Beveiligingsaspecten ten aanzien van toegangsbeleid)

Het beleid, bedoeld in artikel 15, eerste lid, van het Cbb, moet ook beleid omvatten over bevoorrechte accounts en systeembeheeraccounts. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Systeembeheeraccounts zijn een specifieke categorie bevoorrechte accounts die worden gebruikt voor het beheer van systemen, zoals het uitvoeren van updates, het wijzigen van configuraties of het beheren van gebruikersrechten. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.
Het tweede lid geeft nadere invulling aan het beleid voor bevoorrechte accounts en systeembeheeraccounts door te specificeren welke maatregelen en procedures moeten worden toegepast. Het beleid waarborgt dat bij bevoorrechte accounts en systeembeheeraccounts sterke identificatie- en authenticatieprocedures worden toegepast en dat autorisaties zorgvuldig worden toegekend en beheerd. Bij sterke authenticatie kan gedacht worden aan phishing-bestendige multifactorauthenticatie, waarmee de dreiging van phishing en ander misbruik van dergelijke accounts zoveel mogelijk wordt tegengegaan. 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.

Paragraaf 5. Criteria voor significante incidenten

Een incident is 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 (artikel 1 van de Cbw).

Een incident is ingevolge artikel 25, tweede lid, van de Cbw 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.

Op grond van artikel 23, eerste lid, van het Cbb worden bij ministeriële regeling de criteria vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident. Daarin voorziet paragraaf 5 van deze regeling. Een incident is significant wanneer het aan een van de in paragraaf 5 genoemde criteria voldoet of kan gaan voldoen (drempelwaarden). Onder 'kan gaan voldoen' wordt verstaan: een door een incident veroorzaakte reële kans op de in de drempelwaarden benoemde gevolgen in de (nabije) toekomst waarvan het gevaar op dat moment nog niet is geweken.
Indien de entiteit in meerdere sectoren valt, moet zij rekening houden met alle drempelwaarden die voor deze sectoren gelden.
Als een of meer van de drempelwaarden gehaald worden, gelden de verplichtingen om het incident te melden (paragraaf 8.1 van de Cbw).

Artikel 14 (Algemene bepalingen criteria)

Dit artikel bepaalt dat van een significant incident geen sprake is als het gaat om een geplande dienstonderbreking met geplande gevolgen. Als de gevolgen van een geplande dienstonderbreking anders zijn dan gepland, kan er wel sprake zijn van een significant incident dat gemeld moet worden, namelijk als de gevolgen zelf uitkomen boven een van de genoemde drempelwaarden.
Onderhoudswerkzaamheden die leiden tot beperkte beschikbaarheid of niet-beschikbaarheid van de diensten worden niet als significante incidenten beschouwd indien de beperkte beschikbaarheid of niet-beschikbaarheid van de dienst plaatsvindt volgens een geplande onderhoudsactiviteit en de gevolgen van deze onderhoudswerkzaamheden voorzien waren.
Wanneer een dienst niet beschikbaar is als gevolg van geplande onderbrekingen, zoals onderbrekingen of niet-beschikbaarheid op basis van een vooraf bepaalde contractuele overeenkomst, mag dit ook niet als een significant incident worden beschouwd.

Artikel 15 (Significante incidenten vervoer door de lucht)

In deze bepaling worden de drempelwaarden voor significante incidenten in de subsector vervoer door de lucht vastgesteld.
Voor luchthavenbeheerders (onderdeel a) wordt aangesloten bij de hoogste crisisbeheersingsstructuur van de nationale en regionale luchthavens. Op het moment van schrijven zijn de hoogste crisisbeheersingsstructuren: het (gemeentelijk) beleidsteam of de lokale driehoek. Daarbij kan het calamiteitenplan voorzien in samenwerking met de veiligheidsregio. Door aan te sluiten bij bestaande opschalingsniveaus wordt gebruikgemaakt van reeds bestaande procedures op de luchthavens.
Voor logistiek dienstverleners van vliegtuigbrandstoffen (onderdeel b) geldt dat een periode van één uur of langer zonder levering van noodzakelijke brandstoffen wordt aangemerkt als een significant incident. Hierbij is van belang dat het gaat om brandstoffen die noodzakelijk zijn voor het uitvoeren van de vluchtoperatie; incidentele of beperkte verstoringen zonder operationele impact vallen hierbuiten. De drempelwaarde geldt voor de in Nederland gevestigde logistiek dienstverlener van vliegtuigbrandstoffen waarmee een overeenkomst is gesloten. De dienstverlener meldt ook als de oorzaak van het incident zich voordoet bij eventuele onderaannemers.
Voor luchtverkeersleidingsdiensten (onderdeel c) wordt aangesloten bij het reeds bestaande organisatie-specifieke classificatiesysteem voor crises. Indien de hoogste gehanteerde codering van toepassing is, of de codering voor potentiële incidenten, wordt het incident als significant beschouwd.
Voor luchtvaartmaatschappijen en overige entiteiten (onderdeel d) wordt een kwantitatieve drempelwaarde gehanteerd. Indien de afhandeling van 20% of meer van het geplande aantal vluchten gedurende een aaneengesloten periode van twaalf uur of langer niet of niet veilig kan plaatsvinden, is sprake van een significant incident. Dit criterium ziet zowel op feitelijke verstoringen als op situaties waarin redelijkerwijs te verwachten is dat deze drempel wordt bereikt. Deze drempelwaarde is van toepassing op luchtverkeer deel uitmakend van het proces vlucht- en vliegtuigafhandeling.

Artikel 16 (Significante incidenten vervoer over spoor)

Voor de sector spoor is bepaald dat voor een significant incident sprake moet zijn van een stremming van ten minste vier uur bij personenvervoer (onderdeel a). Dit is lijn met de gehanteerde treinincidentscenario-meldingen (TIS-meldingen) die de sector hanteert om incidenten te classificeren. In afstemming met de sector is gebleken dat alle significante verstoringen met deze drempelwaarde zijn gedekt.
In onderdeel b is bepaald dat de drempelwaarde voor goederenvervoer hoger ligt. Een stremming van het spoorgoederenvervoer heeft minder impact, omdat er minder vervoer plaatsvindt en een meldplicht van vier uur daarmee niet proportioneel zou zijn voor bijvoorbeeld de Havenspoorlijn.

Omdat er ook sprake kan zijn van een significant incident waarvan de oorzaak niet 'op het spoor' ligt maar in de bedrijfsvoering van een personen- of goederenvervoerder, is in onderdelen c en d bepaald dat die vervoerders verplicht zijn om incidenten te melden die de dienstverlening stilleggen met meer dan vier uur voor personenvervoer en twaalf uur voor goederenvervoer. Dit sluit aan bij de tijden genoemd in onderdelen a en b. Bij een incident dat de dienstverlening van personenvervoer meer dan 4 uur stillegt (onderdeel c), moeten ten minste 100.000 reizigers getroffen worden voordat sprake is van een meldplichtig incident. Onder het aantal getroffen reizigers wordt verstaan: het verwachte aantal reizigers dat ten gevolge van het incident niet kan reizen per spoor. Dit aantal wordt bepaald aan de hand van reizigersprognoses voor de uitgevallen treinen, op grond van historische (check-in) gegevens.

Artikel 17 (Significante incidenten vervoer over water)

Voor de subsector vervoer over water zijn de verschillende stappen in de keten onderscheidend geweest voor de drempelwaarden van een significant incident. De drempelwaarden gelden voor entiteiten in de subsector vervoer over water, met een op maat gemaakte driedeling in drempelwaarden voor entiteiten voor wat betreft 1) dienstverlening met betrekking tot toegang tot de haven en nautische dienstverlening, 2) de overslag in de haven en 3) dienstverlening met betrekking tot transport in het maritieme achterland (het hoofdvaarwegennet). Het uitgangspunt van de drempelwaarden is de continuïteit van vervoer over water.
Met dienstverlening met betrekking tot toegang tot de haven en nautische dienstverlening (onderdeel a) wordt bedoeld: alle activiteiten, diensten, middelen en systemen die noodzakelijk zijn om een schip veilig en efficiënt vanaf de vastgestelde buitengrens van het havenaanloop- of VTS-gebied tot en met het afmeren aan de toegewezen ligplaats in de haven te begeleiden en weer terug.
Met overslag in de haven (onderdeel b) wordt bedoeld: alle activiteiten, diensten, middelen en systemen die in de haven noodzakelijk zijn om goederen en passagiers van een schip veilig en efficiënt over te zetten naar een andere modaliteit, opslagfaciliteit of bewerkingsplaats binnen de haven.
Met dienstverlening met betrekking tot transport in het maritieme achterland (onderdeel c) wordt bedoeld: alle activiteiten, diensten, middelen en systemen die noodzakelijk zijn om goederen veilig, efficiënt en tijdig over het Nederlandse hoofdvaarwegennet te vervoeren.

Artikel 18 (Significante incidenten vervoer over de weg)

De wegbeheerders hebben drempelwaarden die een onderscheid maken naar het belang van de weg. Als de weg voor een bepaalde periode niet bruikbaar is als gevolg van het incident, is de impact daarvan verschillend. Een incident is significant als onderdelen van het trans-Europees vervoersnetwerk langer dan twaalf uur niet bruikbaar zijn. Met het niet beschikbaar zijn van de weg wordt bedoeld dat minimaal één volledige rijbaan (of rijrichting) niet beschikbaar is voor het verkeer.
Voor wegen die wel onderdeel zijn van het hoofdweggennet, maar niet van het trans-Europees vervoersnetwerk en voor wegen die onderdeel zijn van het onderliggend weggenet geldt een drempelwaarde van vierentwintig uur waarin de weg niet beschikbaar is.
Een incident is bij ITS-dienstverleners significant als deze gedurende enige tijd niet langer de gegevens kunnen verstrekken die gebruikelijkerwijs verstrekt worden. Daarbij wordt een onderscheid gemaakt naar ITS-dienstverleners en ITS-dataverstrekkers. De dataverstrekkers bundelen en verwerken de ontvangen data, die door meerdere organisaties worden benut. Een verstoring bij hen heeft sneller ernstige effecten. Vandaar dat reeds sprake is van een significant incident na een periode van vier uur. ITS-dienstverleners, die vooral ITS-gegevens verstrekken omdat ze als wegbeheerder beschikken over de relevante informatie, zijn verantwoordelijk voor hun eigen systemen. Deze wegbeheerders leveren informatie aan, onder andere over wegafsluitingen, met een bepaalde regelmaat. Dat kan ook wekelijks zijn. Als de gebruikelijke regelmatige verstrekking van ITS-gegevens verstoord is, voor een periode van acht uur, is er sprake van een significant incident.
Een incident bij de dienst die belast is met het beheer van de registers, bedoeld in de artikelen 42, tweede lid en 126, eerste lid, van de Wegenverkeerswet 1994 is significant als het register gedurende vier uur of langer niet beschikbaar is. Met het niet beschikbaar zijn wordt bedoeld dat het voor overheidsorganen bij de uitoefening van publieke taken niet mogelijk is om toegang te krijgen of gebruik te maken van de gegevens in de registers.

Artikel 19 (Significante incidenten openbaar vervoer)

Voor de sector vervoer, subsector openbaar vervoer, is van een significant incident sprake als daardoor het personenvervoer gestremd wordt voor een periode van vier uur of langer en daardoor 100.000 reizigers of meer zijn getroffen. Deze drempelwaarde is gelijk aan die van personenvervoer over spoor, als bedoeld in artikel 16, aanhef en onder c. De drempelwaarde geldt gelijkelijk voor personenvervoer door bus, tram, metro of trein. Onder het aantal getroffen reizigers wordt verstaan: het verwachte aantal reizigers dat ten gevolge van het incident niet kan reizen met de aanbieder. Dit

aantal wordt bepaald aan de hand van reizigersprognoses voor de uitgevallen vervoersmodaliteiten, op grond van historische (check-in) gegevens.

Artikel 20 (Significante incidenten drinkwater)

Het eerste lid regelt dat een incident bij een drinkwaterbedrijf significant is, als dit daardoor voor 10.000 aansluitingen of meer, voor een aaneengesloten periode van zes uur of meer geen drinkwater kan leveren. De impact van een dergelijk incident wordt ernstig geacht, omdat veel ondernemingen, overheden, huishoudens en andere organisaties afhankelijk zijn van de levering van drinkwater. Voor de volledigheid zij erop gewezen dat voor een meldplichtig incident aan beide voorwaarden moet zijn voldaan: het moet gaan om 10.000 aansluitingen of meer én de verstoring moet zes uur of langer duren. Een verstoring van een uur bij 20.000 aansluitingen, of een verstoring van acht uur bij 1.000 aansluitingen levert geen meldplichtig incident op (al kan het betreffende drinkwaterbedrijf natuurlijk altijd op vrijwillige basis een melding doen; zie artikel 33 van de Cbw).
Het tweede lid regelt dat een incident voor een producent of leverancier van verpakt water significant is als deze producent of leverancier gedurende een periode van drie weken geen water kan produceren dan wel leveren. Deze drempel is hoog, omdat de impact van een dergelijk incident op de maatschappij niet groot wordt geacht. De Nederlandse situatie wijkt namelijk af van die in het buitenland, omdat de leveringszekerheid van drinkwater is geregeld in de Drinkwaterwet. Dat wettelijke regime legt de verantwoordelijkheid bij drinkwaterbedrijven, en is niet afhankelijk van commerciële producenten van gebotteld drinkwater.

Artikel 21 (Significante incidenten afvalwater)

Dit artikel bevat de drempelwaarden voor de essentiële entiteiten of belangrijke entiteiten in de sector afvalwater. Het incident kan aanleiding zijn voor de veiligheidsregio om op te schalen naar een bepaalde categorie in de gecoördineerde regionale incidentenbestrijdingsprocedure. Vanaf GRIP 3 is er sprake van een meldplichtig incident als deze opschaling veroorzaakt is door een incident in de afvalwaterketen.
Onderdeel b sluit aan bij de calamiteitenbestrijding van waterschappen. Vanaf het dreigingsniveau 3 is er sprake van een meldplichtig incident als deze opschaling veroorzaakt is door een incident in de afvalwaterketen.
Onderdeel c bepaalt dat een incident significant is als een object (bijvoorbeeld een pomp) dat is opgenomen in het actuele overzicht van de kritieke infrastructuur, zes uur of langer niet een of meer essentiële functies kan uitvoeren. Deze drempelwaarde is alleen relevant voor essentiële entiteiten die ook een kritieke entiteit zijn.

Artikel 22 (Significante incidenten afvalstoffenbeheer)

Voor afvalstoffenbeheer zijn drempelwaarden in de keten aflopend. Vooraan in de keten van afvalstoffenbeheer is het effect van een verstoring pas na langer tijdsverloop ernstig te noemen. Daarom is er voor de inzameling van huishoudelijke afvalstoffen sprake van een significant incident als dit langer dan een week aanhoudt. Andere afvalstoffen dan huishoudelijke afvalstoffen, zoals bedrijfsafvalstoffen waaronder de huishoudelijke afvalstoffen die reeds zijn ingezameld en in beheer zijn bij een bedrijf, onderneming of afvalstoffenverwerker, hebben een lagere drempelwaarde. Voor die afvalstoffen is een incident significant na verloop van 48 uur. Voor de verbrandingsinstallaties, dus helemaal aan het eind van de keten, is een incident significant als de verstoring acht uur of langer aanhoudt. Hierbij zij opgemerkt dat afvalverbrandingsinstallaties ook onder andere sectoren, specifiek elektriciteitsproductie of warmteproductie, rekening moeten houden met drempelwaarden van de Minister van Klimaat en Groene Groei.

Artikel 23 (Significante incidenten nucleair)

Voor de kritieke entiteiten in de nucleaire sector is grotendeels aangesloten bij de meldplicht die reeds op grond van de kernenergieregelgeving geldt.

Artikel 24 (Significante incidenten keren en beheren)

Dit artikel bepaalt dat een incident in de sector keren en beheren significant is als een object (bijvoorbeeld een pomp, een sluis, of een waterkering) dat is opgenomen in het actuele overzicht van de kritieke infrastructuur, vier uur of langer niet een of meer voor het keren en beheren van waterkwantiteit essentiële functies kan uitvoeren. Er is dus geen sprake van een significant incident als de voor het keren en beheren essentiële functie niet direct in het geding komt. Zo kan een pomp, sluis of waterkering tijdelijk niet beschikbaar zijn terwijl er geen hoogwater is, en er dus geen verlies is van de functie waterkeren.
Objecten kunnen meerdere functies hebben; zo is voor een sluis relevant dat deze een functie heeft in

het bewaken van de waterstand, maar ook in het doorlaten van scheepvaartverkeer. Als een sluis die tot de kritieke infrastructuur behoort, niet open kan is er even goed een probleem als wanneer deze niet dicht kan.

Artikel 25 (Significante incidenten vervaardiging, productie en distributie van chemische stoffen)

De chemische industrie is een sector waar veel verschillende bedrijfsprocessen onder vallen. Dat maakt het onwenselijk om hele specifieke drempelwaarden vast te stellen voor wanneer een incident onder de wet als significant beschouwd moet worden. Wel kan over de chemische industrie gesteld worden dat de processen en diensten die zij levert aan de basis liggen van veel productieketens. De weerbaarheid en continuïteit van de chemische industrie is dan ook met name van belang voor andere bedrijfsprocessen. Om aan dat belang invulling te geven, worden er twee drempelwaarden gesteld voor wanneer er in de sector chemie sprake is van een significant incident.
Allereerst is er sprake van een significant incident als de vastgestelde levertijden van de verleende essentiële dienst van een kritieke entiteit in de sector chemie met drie of meer weken wordt overschreden. Het gaat hierbij dus specifiek om de dienst die geleverd wordt waarvoor de entiteit onder de Cbw valt of waarvoor zij is aangewezen als kritieke entiteit. Diensten die geleverd worden op niet-gerelateerde onderdelen, zoals de bedrijfscatering, vallen niet onder deze drempelwaarde. Na gesprekken met entiteiten uit de sector is gekozen voor een termijn van drie weken vanwege de voorraden die in veel gevallen beschikbaar zijn. Chemische entiteiten en hun klanten hebben vaak een voorraad van hun product zodat zij incidenten en tegenslagen kunnen opvangen. Uit ervaring van chemische entiteiten blijkt dat zij hiermee vaak een periode van twee weken kunnen overbruggen. Pas wanneer een incident een zodanige verstoring oplevert dat de voorraden op zijn, heeft dit effecten op de continuïteit in het proces plaats. Er is daarom gekozen voor een overschrijding van levertijden met drie of meer weken.
De tweede drempelwaarde voor een significant incident ziet op de levering van de essentiële dienst aan een kritieke entiteit die direct afhankelijk is van de verleende dienst voor haar eigen continuïteit. Indien er een incident plaatsvindt waardoor de afhankelijke kritieke entiteit voor een periode van zes aaneengesloten uren of langer geen gebruik kan maken van de verleende dienst, wordt het incident als significant beschouwd. Aangezien een verstoring in de verleende dienst vervolgens ook kan leiden tot een verstoring in de dienst van de ontvangende kritieke entiteit, is het mogelijk dat ook daar een Wwkemelding uit volgt. Om stapeling van meldingen te voorkomen zou beargumenteerd kunnen worden dat enkel de ontvangende kritieke partij een melding moet doen. Echter, het doel van de Wwke is om de weerbaarheid van een essentiële dienst te verhogen zodat de continuïteit beter geborgd is. De meldplicht dient zodat de bevoegde autoriteit in het geval van verstoringen ondersteuning kan bieden (artikel 10 van de Wwke) om de verstoring zo snel mogelijk op te lossen. Het is daarvoor wel van belang dat de bevoegde autoriteit weet waar de bron van de verstoring zit om zo snel mogelijk de juiste bijstand te kunnen verlenen. Daarom blijft de drempelwaarde voor de leverende belangrijke entiteit in de chemische sector van toegevoegde waarde.

De aanwijzing van een kritieke entiteit door de bevoegde autoriteit is niet altijd openbaar. Het kan daarom zijn dat belangrijke entiteiten in de sector chemie niet op de hoogte zijn welke entiteiten die van hun dienst afhankelijk zijn ook als kritieke entiteit zijn aangewezen. Een meldplichtige entiteit is niet gehouden tot het onmogelijke. Als de aanwijzing als kritieke entiteit niet bekend is gemaakt aan de meldplichtige entiteit, en niet openbaar is, dan kan de entiteit niet aan deze drempelwaarde gehouden worden. Het is niet in te schatten hoe vaak deze situatie voor zou komen. Niet alle aanwijzingen als kritieke entiteit zullen als vertrouwelijk behandeld worden en die informatie is dan openbaar toegankelijk. Daarnaast dienen kritieke entiteiten volgens artikel 15 van de Wwke (zorgplicht) continuïteitsmaatregelen te nemen en in hun toeleveringsketen te kijken naar alternatieven. Het is dus zeer goed mogelijk dat kritieke entiteiten directe leveranciers waarvan zij afhankelijk zijn inlichten over hun aanwijzing als kritieke entiteit en de daarbij behorende zorgplicht.

Artikel 26 (Significante incidenten meteorologie)

In dit artikel staan de drempelwaarden voor de meteorologische dienst die het KNMI verricht als kritieke entiteit als bedoeld in de Wwke, en dus ook als essentiële entiteit onder de Cbw. Omdat andere kritieke entiteiten van deze meteorologische gegevens afhankelijk zijn, heeft een verstoring van de dienstverlening van het KNMI snel impact. Zodra het KNMI deze dienst niet meer kan leveren voor een periode van zes uur of langer, is er een meldplichtig incident. Kritieke entiteiten die afhankelijk zijn van de meteorologische diensten van het KNMI zijn onder meer de luchthavens en luchtverkeersleiding.
Voorts is een incident significant als het KNMI dit op grond van zijn interne calamiteitenregeling moet melden bij het Meldloketpunt van Rijkswaterstaat.

Artikel 28 (Significante incidenten sector overheid, subsector waterschappen)

In deze bepaling worden de drempelwaarden geregeld voor significante incidenten voor de sector overheid, subsector waterschappen. De drempelwaarden komen voort uit de impacttabel in de bijlage bij deze regeling.
Met de formulering ‘leidt of kan leiden’ wordt bedoeld dat dat het niet alleen gaat om de situatie dat de gevolgen van het incident zich daadwerkelijk voordoen, maar ook de situaties dat die drempelwaarden mogelijk gehaald kunnen worden. De verplichte inschatting of systemen cruciaal of niet-cruciaal zijn aan de hand van de tabel uit de bijlage, kan voor die laatste situatie behulpzaam zijn.

Artikel 29 (Inwerkingtredingsbepaling)

Deze regeling treedt in werking op het tijdstip waarop de Cyberbeveiligingswet in werking treedt. Weliswaar bepaalt artikel 107 van de Cyberbeveiligingswet dat de verschillende artikelen of onderdelen daarvan een verschillend moment van inwerkingtreding kunnen hebben, maar de regering is niet voornemens om te voorzien in een gefaseerde inwerkingtreding van de Cyberbeveiligingswet.

De Minister van Infrastructuur en Waterstaat,
V.P.G. Karremans