Ministerie van Infrastructuur
en Waterstaat

HOOFDDIRECTIE BESTUURLIJKE EN JURIDISCHE ZAKEN

Regeling van de Minister van Infrastructuur en Waterstaat van [datum], nr. IENW/BSK- , houdende nadere regels voor de digitale veiligheid van essentiële en belangrijke entiteiten in de sectoren vervoer, drinkwater, afvalwater, afvalstoffenbeheer, chemie, onderzoek, meteorologie, keren en beheren en nucleair (Cyberbeveiligingsregeling IenW)

(KetenID WGK XXX)

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

Gelet op artikel 68, eerste lid, van de Cyberbeveiligingswet en de artikelen 2, tweede lid, 20, 24, eerste lid, en 27 van het Cyberbeveiligingsbesluit;

BESLUIT:

Paragraaf 1. Begripsbepalingen

Artikel 1 (Begripsbepalingen)

In deze regeling wordt verstaan onder:
- *BIO2:* Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stcrt. XXX jaartal, XXX volgnummer);
- *drinkwaterbedrijf*: drinkwaterbedrijf als bedoeld in artikel 1, eerste lid, van de Drinkwaterwet;
- *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 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);
- *wet*: de Cyberbeveiligingswet.

Paragraaf 2. Reikwijdte

Artikel 2 (Reikwijdte)

1. Deze regeling is van toepassing op alle essentiële entiteiten en belangrijke entiteiten in een of meer van de volgende sectoren:

Minister	**Sector**	**Subsector**
Minister van Infrastructuur en Waterstaat	Vervoer	Lucht
		Spoor
		Water
		Weg
	Drinkwater	
	Afvalwater	
	Afvalstoffenbeheer	
	Vervaardiging, productie en distributie van chemische stoffen	
	Onderzoek	Onderzoek in de sectoren vervoer, drinkwater, afvalwater, afvalstoffenbeheer vervaardiging en distributie van chemische stoffen

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

Paragraaf 3. Aanwijzing CSIRT

Artikel 3 (Aanwijzing CSIRT)

[Gereserveerd]

Paragraaf 4. Nadere invulling zorgplicht

Paragraaf 4.1 Zorgplicht overheidsorganisaties

Artikel 4 (Reikwijdte paragraaf 4.1)
Paragraaf 4.1 is van toepassing op overheidsorganisaties.

Artikel 5 (ISO-standaarden en BIO2)
1. De entiteit past de NEN-EN-ISO/IEC 27001:2023 toe op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor beveiliging van netwerk- en informatiesystemen en het vaststellen van het toepassingsgebied van dit managementsysteem.
2. De entiteit past de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 en de overheidsmaatregelen van de BIO2, voor zover deze zien op de beveiliging van netwerk- en informatiesystemen en niet door middel van een markering in de BIO2 zijn uitgezonderd, toe op het formuleren van passende beheersmaatregelen.
3. De entiteit draagt er zorg voor dat de opzet, het bestaan en de werking van de passende beheersmaatregelen aantoonbaar zijn.

Paragraaf 4.2 Zorgplicht niet-overheidsorganisaties

Artikel 6 (Reikwijdte paragraaf 4.2)

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

Artikel 7 (Beleid over beveiliging van netwerk- en informatiesystemen)
Als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het Cyberbeveiligingsbesluit, en ter uitvoering van artikel 19 van het Cyberbeveiligingsbesluit, bepaalt de essentiële entiteit of de belangrijke entiteit:

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

Artikel 8 (Bedrijfscontinuïteit)
1. Het bedrijfscontinuïteitplan, bedoeld in artikel 9, derde lid, van het Cyberbeveiligingsbesluit, houdt rekening met de uitgevoerde beoordeling en herbeoordeling van risico's, bedoeld in artikel 7 van het Cyberbeveiligingsbesluit en omvat, in ieder geval:

a. doel en reikwijdte;
b. taken en verantwoordelijkheden;
c. belangrijkste contacten en (interne en externe) communicatiekanalen;
d. voorwaarden voor activering en de-activering van het plan;
e. vereiste middelen, met inbegrip van back-ups en redundanties;
f. de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

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

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

Artikel 9 (Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen)
1. De procedures, bedoeld in artikel 11, derde lid, van het Cyberbeveiligingsbesluit, hebben betrekking op ten minste de processen en procedures inzake:

a. beveiligingstesten;
b. beveiligingspatchbeheer.

2. De processen en procedures inzake beveiligingspatchbeheer zorgen ervoor dat:

a. waar passend, beveiligingspatches afkomstig zijn van betrouwbare bronnen en op integriteit worden gecontroleerd;
b. waar passend, beveiligingspatches worden getest voordat zij in productiesystemen worden toegepast;

c. beveiligingspatches worden toegepast binnen een redelijke termijn nadat zij beschikbaar zijn, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen. De entiteiten legt de onderbouwing van een dergelijk besluit vast.

3. Ter uitvoering van artikel 21, derde lid, onderdeel e, van de wet:
   a. implementeert de essentiële entiteit of belangrijke entiteit maatregelen om het gebruik van kwaadaardige en ongeoorloofde software te detecteren en te voorkomen;
   b. voert de essentiële entiteit of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit en legt zij de resultaten van deze scans vast;
   c. evalueert de essentiële entiteit of belangrijke entiteit haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft, voor zover artikel 17 van het Cyberbeveiligingsbesluit daar niet reeds toe verplicht;
   d. verhelpt de essentiële entiteit of belangrijke entiteit onverwijld kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen, of motiveert waarom de kwetsbaarheid niet of op een later moment verholpen wordt en documenteert dit;
   e. segmenteert de essentiële entiteit of belangrijke entiteit systemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het Cyberbeveiligingsbesluit bedoelde risicoanalyse.

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

Artikel 10 (Beveiligingsaspecten ten aanzien van toegangsbeleid)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over bevoorrechte accounts en systeembeheeraccounts voor de logische en fysieke toegang tot netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.
2. Het beleid, bedoeld in artikel 15, eerste lid, van het Cyberbeveiligingsbesluit, zorgt ervoor dat:
   a. sterke identificatie-, authenticatie-, zoals multifactorauthenticatie, en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;
   b. specifieke accounts worden opgezet die uitsluitend worden gebruikt voor systeembeheer, zoals installatie, configuratie, beheer of onderhoud;
   c. voorrechten op het gebied van systeembeheer zoveel mogelijk worden geïndividualiseerd en beperkt;
   d. systeembeheeraccounts alleen worden gebruikt om te verbinden met de systemen voor systeembeheer.

Paragraaf 5. Drempelwaarden voor significante incidenten

Artikel 11 (Algemene bepalingen drempelwaarden)

1. Voor de toepassing van paragraaf 5 geldt dat een incident significant is als het betrekking heeft op een netwerk- of informatiesysteem dat verband houdt met en gebruikt wordt of noodzakelijk is voor het verlenen van een of meer diensten door de essentiële entiteit of belangrijke entiteit.
2. 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.
3. Waar in deze paragraaf sprake is van een periode, vangt die telkens aan op het vroegste moment dat een incident kan worden opgemerkt.

Artikel 12 (Significante incidenten sector drinkwater)

1. Een incident is voor drinkwaterbedrijven in de sector drinkwater significant als aan 10.000 aansluitingen of meer voor een periode van zes uur of langer geen drinkwater geleverd kan worden.
2. Een incident is voor producenten en leveranciers van verpakt water in de sector drinkwater significant als gedurende een periode van drie weken of langer geen water geproduceerd onderscheidenlijk geleverd kan worden.

Artikel 13 (Significante incidenten sector afvalwater)
Een incident is in de sector afvalwater significant als:
a. daardoor opgeschaald moet worden naar categorie 3 of hoger in de Gecoördineerde Regionale Incidentenbestrijdingsprocedure (GRIP);
b. daardoor een andere kritieke entiteit die voor haar essentiële dienst van oppervlaktewater afhankelijk is, voor een periode van 24 uur of langer geen gebruik kan maken van oppervlaktewater; of
c. voor een periode van vier 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 14 (Significante incidenten sector meteorologie)
Een incident is in de sector meteorologie significant als:
a. een andere 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. de essentiële entiteit opschaalt naar het uitvoeren van de calamiteitenregeling.

Artikel 15 (Significante incidenten sector vervoer over de weg)
1. Een incident is voor wegbeheerders in de sector vervoer, subsector vervoer over de weg significant als:
a. de weg een onderdeel is van een militaire corridor of het trans-Europees vervoersnetwerk, bedoeld in Verordening EU/2024/1679, en voor een periode van vier uur of langer niet bruikbaar is door de uitval van een of meer netwerk- en informatiesystemen;
b. de weg een onderdeel is van het hoofdwegennet en voor een periode van vier uur of langer niet bruikbaar is door vierkante wegafsluiting (rode kruisen) of een storing in een brug of tunnel of door de uitval van twee of meer netwerk- en informatiesystemen;
c. de weg een onderdeel is van het hoofdwegennet of het onderliggend wegennet en voor een periode van acht uur of langer niet bruikbaar is voor het normale verkeer;
d. de weg een onderdeel is van het hoofdwegennet of een militaire corridor of het trans-Europees vervoersnetwerk, bedoeld in Verordening EU/2024/1679, en voor de vierde keer in een maand een verstoring optreedt bij hetzelfde netwerk- en informatiesysteem; of
e. de weg een onderdeel is van het onderliggend wegennet en voor de derde keer in een maand een verstoring voor een periode van vier uur of langer optreedt bij hetzelfde netwerk- en informatiesysteem.
2. Een incident is voor ITS-dienstverleners in de sector vervoer, subsector vervoer over de weg significant als:
a. de dienst van ITS-dataverstrekkers voor een periode van vier uur of langer niet beschikbaar is;
b. de dienst van de ITS-dienstverlener voor een periode van acht uur of langer niet beschikbaar is.

Artikel 16 (Significante incidenten sector vervoer door de lucht)

Een incident is in de sector vervoer, subsector vervoer door de lucht significant:
a. voor luchthavens als door het incident na een aaneengesloten periode van 24 uur is opgeschaald naar de hoogste crisisbeheersingsstructuur van de nationale luchthaven of regionale luchthaven van nationale betekenis;
b. voor een brandstofleverancier 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 de luchtverkeersleiding 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 17 (Significante incidenten sector vervoer over water)
1. Een incident is in de sector vervoer, subsector vervoer over water significant als:
a. het proces scheepvaartafwikkeling en de toegang tot en de nautische dienstverlening in het gebied waar het proces scheepvaartafwikkeling plaatsvindt voor een periode van vier uur of langer niet beschikbaar zijn en 20% van de gebruikelijke scheepvaartafwikkeling, toegang en nautische dienstverlening in een periode van 24 uur geen doorgang kan vinden;
b. maritieme achterlandverbindingen als onderdeel van het proces scheepvaartafwikkeling over, op en langs het hoofdvaarwegennet voor een periode van acht uur of langer niet beschikbaar zijn en 20% van de gebruikelijke vervoersbewegingen in een periode van 24 uur geen doorgang kan vinden; of
c. bij host nation support of militaire mobiliteit het proces scheepvaartafwikkeling, de toegang tot en de nautische dienstverlening in het gebied waar het proces scheepvaartafwikkeling plaatsvindt voor een periode van vier uur of langer niet beschikbaar zijn.
2. Een incident is in de sector vervoer, subsector vervoer over water verder significant als:
a. ten minste 20% van de gebruikers voor een periode van vier uur of langer geen toegang heeft tot de dienst die de essentiële entiteit of belangrijke entiteit verleent;
b. een door de entiteit niet vast te stellen aantal gebruikers meer dan vier uur geen toegang hebben tot de dienst die de essentiële entiteit of belangrijke entiteit verleent;
c. voor de tweede keer in de afgelopen zes maanden gebruikers geen toegang hebben tot de dienst die de essentiële entiteit of belangrijke entiteit verleent en beide incidenten dezelfde oorzaak hebben; of
d. als een andere kritieke entiteit voor zijn dienstverlening afhankelijk is van dienst en deze voor een periode van een uur of langer daartoe geen toegang heeft.
3. Voor het bepalen van de impact op gebruikers worden de eindgebruikers van de dienstverlening in aanmerking genomen. Voor ondernemingen gaat het om natuurlijke personen of rechtspersonen die op grond van een overeenkomst toegang hebben tot de verleende dienst.

Artikel 18 (Significante incidenten sector vervoer over spoor)
Een incident is in de sector vervoer, subsector vervoer over spoor significant als:
a. personenvervoer op de hoofdspoorweg ten minste vier uur is gestremd;
b. goederenvervoer op de hoofdspoorweg ten minste twaalf uur is gestremd;

c. de dienstverlening van een personenvervoerder ten minste vier uur wordt gestaakt door een incident in de bedrijfsvoering; of
d. de dienstverlening van een goederenvervoerder ten minste twaalf uur wordt gestaakt door een incident in de bedrijfsvoering.

Artikel 19 (Significante incidenten sector vervaardiging, productie en distributie van chemische stoffen)
Een incident is 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;
b. daardoor een andere 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 20 (Significante incidenten sector afvalstoffenbeheer)
Een incident is 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 21 (Significante incidenten sector onderzoek)
Een incident is in de sector onderzoek 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 22 (Significante incidenten sector keren en beheren)
Een incident is in de sector keren en beheren significant als voor een periode van vier uur of langer een of meer van de 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 23 (Significante incidenten sector nucleair)
Een incident is in de sector nucleair significant als op of rondom het terrein dat de essentiële entiteit in gebruik heeft:
a. een stralingsincident, ongeval of radiologische noodsituatie plaatsvindt als bedoeld in artikel 6.1 van het Besluit basisveiligheidsnormen stralingsbescherming;

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; of
c. een gebeurtenis plaatsvindt met gevolgen of potentiële gevolgen die mogelijk niet verwaarloosbaar zijn voor de nucleaire veiligheid, het milieu of de stralingsbescherming.

Paragraaf 6. Aanwijzing toezichthouders

Artikel 24 (Aanwijzing toezichthouders)
1. Voor de sectoren en entiteiten genoemd in artikel 2 wordt de Inspecteur-generaal van de Inspectie Leefomgeving en Transport aangewezen als toezichthouder.
2. In afwijking van het eerste lid wordt in de sector drinkwater voor andere entiteiten dan drinkwaterbedrijven de Nederlandse Voedsel- en Warenautoriteit aangewezen als toezichthouder.
3. Het eerste lid is niet van toepassing op de sector nucleair als bedoeld in artikel 3 van de Regeling weerbaarheid kritieke entiteiten IenW.

Paragraaf 7. Slotbepalingen

Artikel 25 (Inwerkingtredingsbepaling)
Deze regeling treedt in werking op het tijdstip waarop het bij koninklijke boodschap van 2 juni 2025 ingediende voorstel van wet Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet) in werking treedt.

Artikel 26 (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,

R. Tieman

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, 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 drempelwaarden voor meldplichtige incidenten grotendeels gelijkluidend vormgegeven, om de uitvoerbaarheid voor entiteiten die onder beide wetten vallen te waarborgen, evenals de uitvoerbaarheid en handhaafbaarheid voor de toezichthouders.

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

Ten slotte worden in deze regeling de Inspectie Leefomgeving en Transport als toezichthouder aangewezen, behalve voor de nucleaire sector. Voor die laatste sector wordt het bestuur van de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) bij separaat besluit gemandateerd om de toezichthouders op die sector aan te wijzen.

De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

2. Nadere regels zorgplicht

In deze ministeriële regeling worden voor de in artikel 2 genoemde sectoren nadere regels gesteld over de zorgplicht uit de Cbw en het Cbb. Het doel van deze nadere invulling is om de algemene normen uit de wet en het besluit verder te concretiseren op onderdelen die als van groot belang worden gezien voor de beveiliging van netwerk- en informatiesystemen. Deze nadere invulling 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[3]. 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.

3. 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 sectoren en daarbinnen genoemde subsectoren 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 Wet weerbaarheid kritieke entiteiten (verder: 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 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

[3] 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).

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.

4. 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.

[aanvullen met uitkomsten UDO]

5. Regeldruk

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

6. Uitvoering

[resultaten HUF-toetsen en beschrijving eventuele aanpassingen].

7. Consultaties

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

8. Evaluatie

Deze regeling zal periodiek worden geëvalueerd en waar nodig aangepast of aangevuld. Ingevolge artikel 24, tweede lid van het Cbb en artikel 16, derde lid, van het Bwke evalueert de Minister van Justitie en Veiligheid 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 5 (ISO-standaarden en BIO2)
Deze bepaling verplicht de toepassing van de NEN-EN-ISO/IEC 27001:2023, de beheersmaatregelen van de NEN-EN-ISO 27002:2022 en de overheidsmaatregelen van de BIO2. Overheidsorganisaties zijn al bekend met

beide ISO standaarden en de BIO2. De voorganger van de BIO2, de Baseline Informatiebeveiliging Overheid, gold als verplichtende zelfregulering.
Met deze bepaling wordt de toepassing van deze standaarden wettelijk vastgelegd, voor zover de standaarden zien op de beveiliging van netwerk- en informatiesystemen. Deze beperking is noodzakelijk, omdat deze standaarden 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 lagere regelgeving. Toepassing ervan kan dus niet in deze regeling worden verplicht.

De verwijzingen naar de beide ISO-standaarden en naar de BIO2 betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging van de ISO-standaarden en de BIO2 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.

Het eerste lid verplicht de entiteit om de NEN-EN-ISO/IEC 27001:2023 toe te passen op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor beveiliging van informatie in netwerk- en informatiesystemen. Ook moet deze standaard worden toegepast op het vaststellen van het toepassingsgebied van het managementsysteem. Doorgaans zal een dergelijk managementsysteem ook zien op beveiliging van informatie buiten netwerk- en informatiesystemen. Dat is vanzelfsprekend toegestaan, maar zoals hiervoor is uiteengezet, beperkt deze regeling zich tot netwerk- en informatiesystemen.
Verder moet de entiteit passende beheersmaatregelen formuleren. Hiervoor gelden op grond van het tweede lid de beheersmaatregelen uit de NEN-EN-ISO/IEC 27002:2022 en de overheidsmaatregelen uit deel 2 van de BIO2 als kader. De overige teksten uit de NEN-EN-ISO/IEC 27002:2022 en BIO2 bestaan uit inleiding en toelichting en zijn louter informatief van aard. Deze teksten kunnen nuttig zijn bij het formuleren van de beheersmaatregelen, maar worden niet verplicht gesteld in deze regeling.
Dat de entiteit ‘passende’ beheersmaatregelen moet formuleren, betekent dat rekening moet worden gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico’s gelden, gebaseerd op de scope en de onderkende risico’s. ‘Passend’ houdt ook in dat de beheersmaatregelen uit NEN-EN-ISO/IEC 27002 en de overheidsmaatregelen uit de BIO2 kunnen worden vervangen door of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen. Hierbij kan worden gedacht aan NEN 7510 voor zorginformatie en de CyberSecurity ImplementatieRichtlijn (CSIR) en IEC 62443 Industriële cybersecurity voor Operationele Technologie (OT). De entiteit dient wel aannemelijk te maken dat het vervangen door of combineren met beheersmaatregelen uit andere normen en richtlijnen noodzakelijk is. Ook is het aan de entiteit om aannemelijk te maken dat die beheersmaatregelen gelijkwaardig zijn.
Enkele beheersmaatregelen uit de NEN-EN-ISO/IEC 27002:2022 en daaraan gekoppelde 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. In de BIO2 is door middel van het aanbrengen van een grijze tekstmarkering duidelijk gemaakt welke overheidsmaatregelen buiten de reikwijdte van de Cbw en dus van deze regeling vallen. Voor de in de BIO2 gemarkeerde overheidsmaatregelen geldt dat ook de bijbehorende beheersmaatregelen uit de

NEN-EN-ISO/IEC 27002:2022, waarnaar de eerste drie cijfers van de overheidsmaatregelen in de BIO2 verwijzen, buiten de reikwijdte van deze regeling vallen.
Het derde lid verplicht de entiteit om ervoor zorg te dragen dat de opzet, het bestaan en de werking van de passende beheersmaatregelen aantoonbaar zijn. De BIO2 omvat maatregelen op tactisch niveau. Dit betekent dat deze maatregelen door de entiteit eerst geoperationaliseerd worden voordat ze geïmplementeerd kunnen worden. Deze implementatie moet risicogericht zijn en voldoen aan best practices en marktstandaarden. Onderdeel van de operationalisatie is het kunnen detecteren of de maatregel goed functioneert. Over het hele ontwerp moet worden geborgd dat uitval van één maatregel niet leidt tot een directe kwetsbaarheid in het hele systeem. Hoe de maatregelen zijn geoperationaliseerd, moet via verwijzingen worden vastgelegd. Hiermee toont een entiteit de 'opzet' van maatregelen aan. Al dan niet met behulp van externe partijen of via self-assessments, audits, pentesten, redteam-testen en dergelijke toont een entiteit het 'bestaan' en de 'werking' van maatregelen aan.

Artikel 7 (Beleid over beveiliging van netwerk- en informatiesystemen)
Artikel 7 bevat een nadere uitwerking van artikel 6 van het Cbb, ten aanzien van het beleid over de beveiliging van netwerk- en informatiesystemen en ten aanzien van de managementsystematiek. De essentiële en de belangrijke entiteit moeten, als onderdeel van hun managementsystematiek, bepalen welke maatregelen voor het beheer van cyberbeveiligingsrisico's worden gemonitord en gemeten, hoe dit gebeurt, wanneer dit plaatsvindt en wie daarvoor verantwoordelijk is. Het doel van de managementsystematiek is ervoor te zorgen dat de netwerk- en informatiebeveiligingsrisico's van de organisatie inzichtelijk zijn, dat passende en evenredige maatregelen worden genomen om de risico's te beheersen en dat deze maatregelen structureel worden beoordeeld en waar nodig bijgesteld. Door in de systematiek vast te leggen welke maatregelen worden gevolgd, met welke methoden, met welke frequentie en door wie de beoordeling wordt uitgevoerd, ontstaat een sluitende cyclus van plannen, uitvoeren, toetsen en bijsturen. Daarmee wordt geborgd dat het inzicht in de effectiviteit van de maatregelen actueel is en dat resultaten tot verdere verbetering van de beveiliging leiden. Deze elementen sluiten aan bij de werkwijze die in de praktijk gebruikelijk is in managementsystemen voor informatiebeveiliging, zoals die zijn ontwikkeld op basis van internationale normen.

Artikel 8 (Bedrijfscontinuïteit)
Artikel 8 beschrijft de nadere maatregelen die de belangrijke entiteit of essentiële entiteit moet nemen op het vlak van bedrijfscontinuïteitplan, bedoeld in artikel 9 van het Cbb.

Bedrijfscontinuïteitsplan
De essentiële entiteit en belangrijke entiteit moeten een bedrijfscontinuïteitsplan opstellen, om zo voorbereid te zijn op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen en om op dergelijke incidenten goed en tijdig te kunnen reageren, om zo de duur en gevolgen van dergelijke incidenten te beperken. Bij het opstellen daarvan moet de entiteit rekening houden met de risicobeoordelingen op grond van artikel 7 van het Cbb, zodat de entiteit alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen. De onderdelen van het eerste lid omschrijven de onderdelen die normaliter geadresseerd zouden moeten worden in het plan. In de praktijk kan het bedrijfscontinuïteitsplan zoals hier bedoeld deel uitmaken van een algemeen bedrijfs- en continuïteitsplan van de belangrijke en essentiële entiteit.
Door te zorgen voor ten minste gedeeltelijke redundantie van netwerk- en informatiesystemen, assets (met inbegrip van faciliteiten, uitrusting en benodigdheden), personeel met de nodige verantwoordelijkheid, bevoegdheid en

bekwaamheid en passende communicatiekanalen, zorgen de essentiële entiteit en belangrijke entiteit ervoor dat er voldoende middelen beschikbaar zijn om de primaire processen doorgang te laten vinden.

Back-upplannen
Op basis van de risicobeoordelingen op grond van artikel 7 van het Cbb en het bedrijfscontinuïteitsplan moeten de belangrijke entiteit en essentiële entiteit back-upplannen vaststellen. De onderdelen in artikel 9, tweede lid, omschrijven welke aspecten in de back-upplannen 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),* heeft betrekking op de frequentie van de back-ups. Het voorschrift dat back-ups volledig zijn, ziet erop dat alle gegevens die nodig zijn voor het herstellen van de betreffende netwerk- en informatiesystemen zijn opgenomen, waaronder configuratiegegevens en gegevens die in cloudcomputingdiensten zijn opgeslagen. Dit is noodzakelijk om te waarborgen dat systemen en processen bij een herstel weer volledig functioneren. Daarnaast moeten de back-ups nauwkeurig zijn, wat inhoudt dat er een integere backup van de software en gegevens moet worden gemaakt die in het geval van herstel succesvol kan worden teruggeplaatst en weer kan worden gebruikt. Daarnaast dient de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups gewaarborgd te worden, zodat de back-ups ook daadwerkelijk ingezet kunnen worden. In het bijzonder is hierbij van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door acties van kwaadwillenden, zoals ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups moet gewaarborgd worden, om zo ongeautoriseerde toegang tot gegevens te voorkomen. De risicobeoordelingen op grond van artikel 7 van het Cbb zijn dus zowel relevant voor het bepalen van welke software en gegevens in back-ups moeten worden opgenomen, als voor het bepalen van de eerdergenoemde waarborgen. Het is tevens van belang dat de vertrouwelijkheid, integriteit en beschikbaarheid van de back-ups doorlopend gemonitord worden, zodat de essentiële en belangrijke entiteit tijdig worden geïnformeerd over tekortkomingen. Het plan moet tevens omschrijven hoe de gegevens hersteld kunnen worden. Ook moeten de back-upplannen omschrijven hoe lang de betreffende back-ups bewaard moeten worden. Ten slotte moeten de essentiële entiteit en belangrijke entiteit, waar mogelijk, periodiek het terugzetten van back-ups testen, om zo de werking van back-ups in de praktijk te testen. Enerzijds beschikken belangrijke entiteiten en essentiële entiteiten bij incidenten op deze wijze over de nodige kennis en vaardigheden op dit punt. Anderzijds biedt het testen meer zekerheid dat er geen technische belemmeringen zijn om de back-ups daadwerkelijk terug te zetten.

Artikel 9 (Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen)
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. In artikel 9, eerste lid, van deze regeling is gespecificeerd dat deze procedures ten minste betrekking moeten hebben op beveiligingstesten en beveiligingspatchbeheer. Beveiligingstesten zijn noodzakelijk om vast te stellen of de getroffen maatregelen in de praktijk doeltreffend functioneren en of kwetsbaarheden tijdig aan het licht komen. Door structureel processen en procedures voor beveiligingstesten vast te leggen, wordt geborgd dat testen systematisch, herhaalbaar en volgens vooraf bepaalde criteria plaatsvinden. Dit voorkomt dat testen ad hoc of onvolledig worden uitgevoerd en draagt eraan bij dat tekortkomingen tijdig kunnen worden verholpen voordat deze tot incidenten leiden.

Om potentiële risico's voor de beveiliging van netwerk- en informatiesystemen weg te nemen, 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 het tweede lid, onderdeel a, geldt dat waar passend gecontroleerd moet worden of beveiligingspatches afkomstig zijn van betrouwbare bronnen en of de integriteit van deze patches gewaarborgd is. Het vereiste geldt "waar passend", omdat bij patches zoals reguliere systeemupdates van besturingssystemen doorgaans geen afzonderlijke controle door de essentiële en belangrijke entiteit op herkomst en integriteit nodig is, vanwege reeds ingebouwde technische controles.
Op grond van onderdeel b geldt dat beveiligingspatches, waar passend, getest moeten worden voordat zij in de productieomgeving worden toegepast. De noodzaak van een dergelijke test is afhankelijk van de risico's die het installeren van de patch meebrengt. Voorgenoemde 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 zwaarder wegen dan de voordelen op het gebied van cyberbeveiliging. Hierbij kan gedacht worden aan het ongepland stilzetten van kritieke bedrijfsprocessen van een entiteit ter uitvoering van de patch, terwijl de patch ook uitgevoerd kan worden op een al ingepland moment van breder onderhoud aan de netwerk- en informatiesystemen. Indien een essentiële of belangrijke entiteit hiervoor kiest, dient de motivatie voor het niet of niet direct toepassen van de beveiligingspatch gedocumenteerd te worden, zodat het voor de toezichtspraktijk mogelijk is om te toetsen is of dit een terechte keuze was.

Ter bescherming van hun netwerk- en informatiesystemen moeten essentiële en belangrijke entiteiten op grond van het derde lid, onderdeel a, 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.
Op grond van onderdeel b moeten essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uitvoeren en de resultaten daarvan vastleggen. Deze scans maken inzicht mogelijk in bekende kwetsbaarheden in systemen en applicaties; zij vormen daarmee een belangrijk hulpmiddel om risico's tijdig te onderkennen. Door de resultaten te documenteren, kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.
Op grond van onderdeel c evalueren essentiële en belangrijke entiteiten hun blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van hebben. Door deze evaluatie structureel uit te voeren, ontstaat een actueel beeld van het risicolandschap en kan tijdig worden bepaald welke aanvullende maatregelen nodig zijn om de weerbaarheid te vergroten.
Op grond van onderdeel d nemen essentiële entiteiten en belangrijke entiteiten maatregelen om kwetsbaarheden te adresseren. 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, wordt zo voor de toezichtspraktijk duidelijk waarom er wordt afgeweken, en kan de toezichthouder oordelen of deze beslissing terecht is genomen.
Essentiële entiteiten 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 derde lid, onderdeel e, moeten essentiële entiteiten en belangrijke entiteiten hun netwerken segmenteren overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het Cbb bedoelde risicobeoordeling. Hierbij kunnen entiteiten zelf in acht nemen hoe ze de netwerksegmentatie toepassen, waarbij rekening gehouden wordt 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.

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

Artikel 10 (Beveiligingsaspecten ten aanzien van toegangsbeleid)
De essentiële entiteit of belangrijke entiteit moet vastgesteld beleid hebben voor het gebruik van bevoorrechte accounts en systeembeheeraccounts voor de logische en fysieke toegang tot netwerk- en informatiesystemen. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Het beleid legt vast hoe deze accounts worden toegewezen, gebruikt en beheerd. Dat gebeurt schriftelijk, zodat de toepassing aantoonbaar is.

Het tweede lid geeft nadere invulling aan het beleid voor bevoorrechte accounts en systeembeheeraccounts, door te specificeren welke maatregelen en procedures moeten worden toegepast. Het beleid moet ervoor zorgen dat sterke identificatie- en authenticatieprocedures, zoals multifactorauthenticatie, worden toegepast en dat autorisatie zorgvuldig wordt geregeld. Zo wordt de dreiging van phishing en andere misbruik van dergelijke accounts zoveel mogelijk tegengegaan. Daarnaast schrijft het lid voor dat specifieke accounts uitsluitend worden gebruikt voor systeembeheer en dat de voorrechten van deze accounts zoveel mogelijk worden geïndividualiseerd en beperkt tot het strikt noodzakelijke. Dit draagt bij aan een duidelijke scheiding van functies, en het voorkomt dat

accounts voor meerdere doeleinden worden gebruikt en dat acties niet herleidbaar zijn tot specifieke personen, waardoor het risico op fouten of misbruik wordt verminderd. Tevens is vastgelegd dat systeembeheeraccounts alleen verbinding maken met de systemen waarvoor zij zijn bedoeld, zodat activiteiten traceerbaar en controleerbaar blijven en de veiligheid van de netwerk- en informatiesystemen gewaarborgd is.

Paragraaf 5. Drempelwaarden 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 een significant wanneer het aan een van de in paragraaf 5 genoemde drempelwaarden voldoet of kan gaan voldoen. 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 de entiteit rekening houden met alle drempelwaarden die voor deze sectoren gelden.
Als één of meer van de drempelwaarden gehaald wordt, gelden de verplichtingen om het incident te melden, als bedoeld in paragraaf 8.1 van de Cbw.

Artikel 11 (Algemene bepalingen drempelwaarden)
Het eerste lid bepaalt dat incidenten op netwerk- en informatiesystemen alleen significant zijn, als deze netwerk- en informatiesystemen verband houden met, gebruikt worden voor of noodzakelijk zijn voor een of meer van de diensten van de essentiële entiteiten of belangrijke entiteit. Hiermee is beoogd te voorkomen dat een entiteit gehouden is een melding te doen van een verstoring in een systeem dat niet verbonden is met de dienst die maakt dat er sprake is van een essentiële entiteit of belangrijke entiteit.

Het tweede lid 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, als de gevolgen zelf voldoen uitkomen boven een van de andere genoemde drempelwaarden. In dat geval is er wel sprake van een significant incident dat gemeld moet worden.
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.

Het derde lid regelt dat de perioden die in deze paragraaf genoemd zijn, telkens aanvangen op het vroegste moment dat het incident kan worden opgemerkt.

Artikel 12 (Significante incidenten sector 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.

Artikel 13 (Significante incidenten sector 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.
In onderdeel b is een drempelwaarde opgenomen over de bruikbaarheid van oppervlaktewaterlichamen voor andere kritieke entiteiten als bedoeld in de Wwke. Omdat afvalwater uiteindelijk terecht komt in het oppervlaktewater, zijn verschillende soorten incidenten denkbaar die de bruikbaarheid van dat oppervlaktewater verstoren. Denk daarbij aan een onbedoelde lozing van chemisch materiaal, of van rioolwater. Een aantal kritieke entiteiten zijn voor hun essentiële dienst afhankelijk van oppervlaktewater, denk aan koeling of transport. Als het oppervlaktewater zodanig verontreinigd is, dat deze kritieke entiteiten daardoor voor een periode van 24 uur of langer geen gebruik meer kunnen maken van de oppervlaktewater, is er sprake van een aanzienlijke maatschappelijke effecten en om die reden sprake van een meldplichtig incident.
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, vier 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 14 (Significante incidenten sector meteorologie)
In artikel 14 zijn de drempelwaarden voor de meteorologische dienst opgenomen, 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 de wettelijke taken niet meer kan uitvoeren en daarom, op grond van zijn interne beleid, opschaalt naar het uitvoeren van de calamiteitenregeling van het instituut.

Artikel 15 (Significante incidenten sector 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 een militaire corridor of het trans-Europees vervoersnetwerk langer dan vier uur niet bruikbaar zijn.
Voor het hoofdwegennet wordt wel een onderscheid gemaakt naar de oorzaak van het incident. Daarvoor geldt dat er sprake is van een significant incident als er specifieke oorzaken zijn (rode kruisen, storing in brug of tunnel of een verstoring van twee of meer assets) en de verstoring langer duurt dan vier uur. Andere oorzaken leiden tot een significant incident als de verstoring langer duurt dan acht uur. Voor het onderliggend wegennet geldt ook een drempelwaarde van acht uur. Voor de wegbeheerders is ook een herhaald incident significant, wanneer de verstoring op zichzelf korter duurt dan de periode van vier of acht uur, opgenomen in onderdelen a tot en met c, maar plaatsvindt in hetzelfde bedrijfsmiddel. Zo wordt een korte verstoring van de beveiligingsinstallatie in een tunnel, waardoor deze niet gebruikt kan worden, voor de derde keer in een maand wel aangemerkt als een significant incident. De onderbouwing daarvoor is dat er dan sprake is van overlast, maar ook dat deze herhaling een indicatie is dat het onderliggende probleem niet adequaat is opgelost.

In het tweede lid is opgenomen dat een incident bij ITS-dienstverleners significant is 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.

Artikel 16 (Significante incidenten sector vervoer door de lucht)
In artikel 16 worden de drempelwaarden voor significante incidenten in de subsector vervoer door de lucht vastgesteld.
De drempelwaarde die is opgenomen in onderdeel b is van toepassing op vluchten die onderdeel zijn van het kritieke luchtverkeer. Bepaalde categorieën van vluchten, zoals lesvluchten, zijn hier geen onderdeel van. Een vlucht bestaat uit twee vliegtuigbewegingen (opstijgen en landen).
In onderdeel c is de drempelwaarde opgenomen die geldt voor in Nederland gevestigde brandstofleveranciers waarmee een overeenkomst is afgesloten. Dit betekent dat de leverancier ook meldt als de oorzaak van het incident zich voordoet bij eventuele onderaannemers.

Artikel 17 (Significante incidenten sector vervoer over water)
Voor de subsector vervoer over water zijn verschillende stappen in de keten onderscheidend geweest voor de drempelwaarden van een significant incident. De drempelwaarden gelden voor entiteiten die aangewezen worden in het gehele proces scheepvaartafwikkeling, met een op maat gemaakte tweedeling in drempelwaarden voor entiteiten in 1) de toegang tot en de nautische dienstverlening in het gebied waar het proces scheepvaartafwikkeling plaatsvindt, de scheepvaartafwikkeling zelf (overslag) en 2) entiteiten in de maritieme achterlandverbindingen.
In het tweede lid is opgenomen dat een verstoring aanzienlijk is als een significant aantal gebruikers geen toegang heeft tot de essentiële dienst voor een aanzienlijke periode van vier uur of langer. In het derde lid wordt bepaald wie onder gebruikers wordt verstaan. Dit betreft aangewezen kritieke entiteiten

binnen de sector vervoer, subsector water die niet tot het proces scheepvaartafwikkeling behoren.

Artikel 18 (Significante incidenten sector 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 (sub 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. Onder sub 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 aanzienlijke verstoring waarvan de oorzaak niet 'op het spoor' ligt maar in de bedrijfsvoering van een personen- of goederenvervoerder, is onder sub 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 sub a en b.

Artikel 19 (Significante incidenten sector vervaardiging, productie en distributie van chemische stoffen)
Van een significant incident in de sector chemie is sprake als de vastgelegde levertijden van diensten door een belangrijke of essentiële entiteit meer dan drie weken overschreden worden. Daarnaast is een incident significant als een essentiële entiteit die afhankelijk is van de dienst van een belangrijke of essentiële entiteit uit de sector vervaardiging, productie en distributie van chemische stoffen voor een periode van zes aaneengesloten uur of langer geen gebruik kan maken van deze dienst. Dit vanwege de belangrijke positie die de sector heeft aan het begin van verschillende essentiële productketens.

Artikel 20 (Significante incidenten sector 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 22 (Significante incidenten sector 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 essentiële functies kan uitvoeren. Objecten kunnen meerdere functies hebben; zo is voor een sluis relevant dat deze een functie heeft in het bewaken van de waterstand, maar ook een functie 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. Deze

drempelwaarde geldt uitsluitend voor de essentiële entiteiten in deze sector, die ook voor deze sector als kritieke entiteiten zijn aangewezen.

Artikel 23 (Significante incidenten sector 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 (Aanwijzing toezichthouders)
De ILT wordt aangewezen als toezichthouder op naleving door essentiële en belangrijke entiteiten van de regels die bij en krachtens de Cbw zijn gesteld. Voor verpakt water in de sector drinkwater is dat de Nederlandse Voedsel- en Waren autoriteit (NVWa) (tweede lid). In het derde lid wordt de nucleaire sector uitgezonderd. De Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) zal worden gemandateerd om de toezichthouders voor deze sector aan te wijzen. De reden daarvoor is dat de toezichtstaken in deze sector in de praktijk zullen worden uitgeoefend door ambtenaren van de ANVS die ook het toezicht uitoefenen op de naleving van hetgeen bij en krachtens de Kernenergiewet is bepaald. Deze ambtenaren staan daarbij onder het gezag van de ANVS. Het verdient de voorkeur dat deze gezagsverhouding in stand blijft voor wat betreft de toezichts- en handhavingstaken op grond van de Cbw.

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

NAAM