NOTA VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit besluit, het Cyberbeveiligingsbesluit (hierna: Cbb), strekt ter uitwerking van de Cyberbeveiligingswet (hierna: Cbw). De Cbw strekt op haar beurt tot de 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.

2. De belangrijkste onderdelen van het Cbb

2.1 Inleiding

In dit hoofdstuk wordt ingegaan op de belangrijkste onderdelen van het Cbb. Voor een nadere en uitgebreide toelichting op alle artikelen uit het Cbb wordt verwezen naar de artikelsgewijze toelichting.

2.2 Zorgplicht

Voor essentiële entiteiten en belangrijke entiteiten geldt op grond van artikel 21 Cbw de verplichting om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruiken, te beheersen. Deze verplichting wordt de zorgplicht genoemd.

De maatregelen die essentiële entiteiten en belangrijke entiteiten moeten nemen in het kader van de zorgplicht, omvatten ingevolge artikel 21, derde lid, Cbw ten minste het volgende:
a. beleid over risicoanalyse en beveiliging van informatiesystemen;
b. incidentenbehandeling;
c. bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d. de beveiliging van de toeleveringsketen;
e. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen;
f. beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h. beleid en procedures over het gebruik van cryptografie;
i. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets; en
j. wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

De maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen, zijn nader uitgewerkt in de artikelen 6 tot en met 19 Cbb. Voor een toelichting op deze artikelen wordt verwezen naar de artikelsgewijze toelichting. Daarbij geldt steeds als uitgangspunt dat de maatregelen in zijn geheel moeten voldoen aan de open geformuleerde zorgplicht uit artikel 21 Cbw en dat de artikelen 6 tot en met 19 Cbb dus steeds in dat licht moeten worden beoordeeld.

De artikelen 6 tot en met 19 Cbb zijn van toepassing op alle essentiële entiteiten en belangrijke entiteiten uit alle sectoren waar de Cbw op van toepassing is, uitgezonderd van de entiteiten die op grond van artikel 23 Cbw zijn ontheven van de zorgplicht en, met uitzondering van artikel 18, de entiteiten waarop de Uitvoeringsverordening (EU) 2024/2690[2] (hierna: de

[1] *PbEU* 2022, L 333.
[2] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant

uitvoeringsverordening) van toepassing is. Voor een toelichting op dit laatste wordt verwezen naar de artikelsgewijze toelichting op artikel 4 Cbb. Het van toepassing zijn van de artikelen 6 tot en met 19 Cbb op een groot aantal entiteiten biedt een gemeenschappelijk basisniveau voor de digitale weerbaarheid van een groot aantal essentiële entiteiten en belangrijke entiteiten.

In diverse artikelen in het Cbb, zoals de artikelen 6 en 7, is bepaald dat essentiële entiteiten en belangrijke entiteiten beleid over de in die artikelen genoemde onderwerpen schriftelijk moeten hebben vastgesteld en aantoonbaar moeten toepassen. Het doel van deze voorschriften is dat entiteiten weloverwogen beleid formuleren op de genoemde onderwerpen, dat zij dit formeel vaststellen en dat zij dit beleid daadwerkelijk ten uitvoer brengen en dat hierop ook effectief toezicht mogelijk is. Het beleid kan in één of meerdere beleidsdocumenten worden uitgewerkt of bijvoorbeeld geïntegreerd worden in een managementsysteem voor informatiebeveiliging waarmee ook aan de aantoonbaarheid kan worden voldaan.

Artikel 19 Cbb biedt de mogelijkheid om de zorgplicht nader sectoraal in te vullen middels ministeriële regelingen van de vakministers voor de sectoren waar zij verantwoordelijk voor zijn. Dit biedt de mogelijkheid om ten aanzien van de zorgplicht onderscheid te maken tussen sectoren, subsectoren, soorten entiteiten en entiteiten, bijvoorbeeld vanwege de specifieke aard van een bepaalde sector, subsector, soort entiteit of entiteit.

2.3 Training

In artikel 24, eerste lid, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten moeten nemen in het kader van de zorgplicht, de goedkeuring behoeven van het bestuur van de essentiële entiteit en belangrijke entiteit. Artikel 24, tweede lid, Cbw verplicht ieder lid van het bestuur van een essentiële entiteit en belangrijke entiteit om te beschikken over kennis en vaardigheden om onder meer risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen. In artikel 24, vijfde lid, Cbw is bepaald dat die bestuursleden met het oog op het aantonen van de hiervoor bedoelde kennis en vaardigheden moeten beschikken over een certificaat, waaruit de deelname blijkt aan een training die de hiervoor bedoelde onderwerpen behandelt. In de artikelen 21 tot en met 23 Cbb worden regels gesteld over de hiervoor bedoelde training. Deze regels zien onder meer op de eisen aan de training en het certificaat. Voor een toelichting op deze regels wordt verwezen naar de artikelsgewijze toelichting op deze bepalingen.

2.4 Aanwijzing CSIRT en coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden

In artikel 16, eerste lid, Cbw is bepaald dat voor alle essentiële entiteiten en belangrijke entiteiten bij of krachtens algemene maatregel van bestuur (hierna: amvb) een Computer security incident response team (hierna: CSIRT) wordt aangewezen. Het CSIRT heeft op grond van artikel 16, derde lid, Cbw, onder meer tot taak om genoemde entiteiten in geval van dreigingen, kwetsbaarheden en incidenten vroegtijdig te waarschuwen en bijstand te verlenen. Het CSIRT zal bij het verlenen van bijstand niet de verantwoordelijkheid overnemen van de entiteit. De entiteit blijft zelfstandig verantwoordelijk voor het oplossen van een incident en haar cyberweerbaarheid. In artikel 2, eerste en tweede lid, Cbb wordt geregeld welke partij voor essentiële entiteiten en belangrijke entiteiten als CSIRT wordt of kan worden aangewezen.

Daarnaast is in artikel 17, eerste lid, Cbw bepaald dat één van de als CSIRT aangewezen partijen bij of krachtens amvb wordt aangewezen als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. Deze coördinator heeft op grond van artikel 17, tweede lid, Cbw, onder meer tot taak om als tussenpersoon op te treden tussen degene die een kwetsbaarheid (een zwakheid, vatbaarheid of gebrek van ICT-producten of -diensten die door een cyberdreiging kan worden uitgebuit) bij de coördinator meldt en de fabrikant of aanbieder van het ICT-product of de ICT-dienst waarop de melding betrekking heeft. In artikel 3 Cbb wordt deze coördinator aangewezen. Voor een toelichting hierop wordt verwezen naar de artikelsgewijze toelichting op deze bepaling.

---

wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (*PbEU* L 2024/2690).

2.5 Na overleg met of in overeenstemming met de Minister van Justitie en Veiligheid

Waar er afstemming nodig is tussen de centraal verantwoordelijke minister, te weten de Minister van Justitie en Veiligheid, en de vakminister heeft dit er toe geleid dat in het Cbb per artikel is bepaald of dit geschiedt "na overleg met" of "in overeenstemming met" de Minister van Justitie en Veiligheid. Het verschil tussen "na overleg met" en "in overeenstemming met" is dat bij "na overleg met" eventueel verschil van inzicht kan worden opgelost via de gangbare afstemmings- en overlegstructuren, maar de vakminister uiteindelijk eigenstandig de eindbeslissing neemt. Bij "in overeenstemming met" dient de Minister van Justitie en Veiligheid bij eventueel uiteenlopende inzichten alsnog mede te beslissen. Deze variant is gekozen bij de bepalingen waarbij de handelingen van de vakminister het integrale stelsel raken, en dus van invloed zijn op de stelselverantwoordelijkheid van de Minister van Justitie en Veiligheid.

3. Gevolgen

3.1 Inleiding

Het Ministerie van Justitie en Veiligheid heeft door een onafhankelijk onderzoeksbureau een regeldrukonderzoek laten uitvoeren. Het onderzoek naar de regeldruk van de Cbw en het Cbb is gecombineerd met het onderzoek naar de regeldruk van de Wet weerbaarheid kritieke entiteiten (hierna: Wwke) en het Besluit weerbaarheid kritieke entiteiten (hierna: Bwke). Aan de hand van interviews met het bedrijfsleven en een panelbijeenkomst met het mkb is een inschatting gemaakt van de regeldruk als gevolg van de Cbw en het Cbb (en de regeldruk als gevolg van de Wwke en het Bwke). Hieronder worden de belangrijkste uitkomsten daarvan ten aanzien van de Cbw en het Cbb beschreven.
De uitkomsten van het regeldrukonderzoek, in combinatie met de consultatiereacties op een concept van het Cbb en de panelbijeenkomst met het mkb, hebben geleid tot aanpassingen in het Cbb. Een deel van die aanpassingen komen aan de orde in hoofdstuk 4.

3.2 Werkwijze regeldrukonderzoek

Bij het in kaart brengen van de regeldrukeffecten is gebruik gemaakt van de landelijke methodiek die is vastgelegd in de meest recente versie van het Handboek Meting Regeldrukkosten 2023, versie 2.1 d.d. 29 november 2023. De hierin beschreven methodiek wordt ook voorgeschreven door het Adviescollege Toetsing Regeldruk (hierna: ATR).

Er zijn interviews gehouden met verschillende bedrijven die naar verwachting regeldrukgevolgen zullen ervaren als gevolg van de Cbw en het Cbb. Tijdens de selectie van deelnemende bedrijven is rekening gehouden met de diversiteit aan bedrijven die tot de doelgroep behoren van de Cbw en Wwke. Zo is gepoogd een gevarieerde selectie samen te stellen van bedrijven uit diverse sectoren, van verschillende omvang en vallend binnen uiteenlopende wetgevende kaders.

Alleen de verplichtingen uit de Cbw die nader zijn ingevuld in het Cbb en waarvoor om die reden geen regeldrukberekening is gedaan in de memorie van toelichting op de Cbw, vormen onderdeel van dit onderzoek. Meer concreet gaat het om de regels in het Cbb over de zorgplicht, de verplichting op het terrein van governance en de registratieplicht.

In het onderzoek is op twee vlakken onderscheid gemaakt, namelijk tussen de eenmalige en de structurele regeldrukeffecten en tussen bedrijfseigen en bedrijfsvreemde kosten. Onder eenmalige effecten vallen alle kosten die tijdelijk van aard zijn. Structurele kosten omvatten kosten die periodiek terugkeren, die kunnen bestaan uit aanschafkosten (out-of-pocketkosten) voor goederen of diensten, of uit tijdbesteding. Bedrijfseigen kosten die gekwantificeerd kunnen worden, tellen niet mee in de regeldrukberekening. Bedrijfsvreemde kosten zijn alle overige kosten die bedrijven niet uit eigen beweging zouden maken, voortkomend uit verplichtingen uit wet- en regelgeving. Bedrijfsvreemde regeldrukkosten worden meegenomen in de regeldrukberekening.

In het regeldrukonderzoek is voor de berekening, naast de uitkomsten van de interviews, gebruik gemaakt van standaardaantallen. Deze aantallen omvatten onder andere het totaal aantal bedrijven of ondernemingen dat naar verwachting onder de reikwijdte van de Cbw zal vallen. Zoals ook is aangegeven in de memorie van toelichting op de Cbw wordt het toepassingsbereik van de Cbw geschat op 7.550 ondernemingen.

Verder worden structurele tijdbestedingen geregeld uitgedrukt in fte's in plaats van individuele uren. Omdat het aantal werkzame uren van een voltijds dienstverband significant kan verschillen tussen werkgevers en tussen cao's, wordt gerekend met een standaardaantal uren. Gekozen is om het aantal van 1.720 werkzame uren op jaarbasis te hanteren. Dit aantal berust op een schatting van het Ministerie van Sociale Zaken en Werkgelegenheid.

Ook voor de uurtarieven van medewerkers van de bedrijven die activiteiten moeten verrichten om te voldoen aan wettelijke verplichtingen worden standaardaantallen gebruikt. Dit regeldrukonderzoek volgt hiervoor de methode uit het Handboek Meting Regeldrukkosten, versie 2.1 d.d. 29 november 2023. Onderdeel van deze methode is het aanhouden van standaard interne uurtarieven per type functie. Per activiteit die verricht wordt om te voldoen aan een verplichting is bepaald welk type functie de medewerkers die deze activiteit uitvoeren naar alle waarschijnlijkheid zullen hebben. Dit is afgestemd met de respondenten. Op basis hiervan is gerekend met het bijbehorende uurtarief. Sommige bedrijven hebben aangegeven dat zij voor het verrichten van dezelfde werkzaamheden in sommige gevallen een ander type medewerker inzetten.

3.3 Bevindingen regeldrukonderzoek

De geïnterviewde bedrijven geven aan dat zij al maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen, met als basis de eisen uit de Wet beveiliging netwerk- en informatiesystemen of sectorspecifieke wetgeving. Veel bedrijven gaan echter verder dan wettelijk is vereist. Hun motieven zijn complex en niet eenduidig te herleiden tot bedrijfseigen of wettelijke redenen. ISO- en NEN-standaarden vormen het ijkpunt voor alle geïnterviewde bedrijven en worden voortdurend aangepast aan technologische en wettelijke ontwikkelingen. Om gecertificeerd te blijven, moeten bedrijven daarom blijvend investeren. Of deze investeringen voortkomen uit intrinsieke beweegredenen of wetgeving is niet altijd evident. De hier gerapporteerde regeldrukkosten zijn gebaseerd op een kwantitatieve inschatting van de meerkosten die bedrijven verwachten voor het voldoen aan de Cbw en het Cbb.

De bevindingen met betrekking tot de zorgplicht, de opleidingsverplichting voor bestuursleden en de verplichting tot het registreren worden hieronder toegelicht. De uiteenzetting van de verwachte regeldrukgevolgen wordt hierna uitgesplitst in eenmalige en structurele regeldrukkosten.

Artikel 21 Cbw en de artikelen 6 tot en met 17 en 19 Cbb (zorgplicht)
De eenmalige kosten die gemaakt moeten worden om te voldoen aan de zorgplicht zijn primair het gevolg van de voorbereidingen die bedrijven moeten treffen om de voorgeschreven maatregelen ten aanzien van de zorgplicht uit te voeren, en de eenmalige meerkosten bij de implementatie van deze maatregelen. Voor de meeste bedrijven vormt het uitvoeren van een *gap assessment* en het herzien van de overeenkomsten met ketenpartners het meest kostbare onderdeel van deze voorbereiding. Bedrijven verwachten hierbij zowel gebruik te zullen maken van hun eigen werknemers, alsook van de diensten van externe partijen. Sommige bedrijven geven aan te verwachten extra personeel in dienst te nemen voor de duur van de transitieperiode.
Bedrijven verwachten dat het inregelen en aanpassen aan de nieuwe wet- en regelgeving minstens enkele maanden, maar in sommige gevallen enkele jaren in beslag zal gaan nemen. Gemiddeld verwachten middelgrote ondernemingen individueel 614 uur per onderneming aan eenmalige extra tijdbesteding nodig te hebben voor de voorbereiding en implementatie van de te nemen maatregelen ten aanzien van de zorgplicht. Voor grote ondernemingen ligt dit getal aanzienlijk hoger, namelijk op gemiddeld 6.708 uur per onderneming.
De betrokken medewerkers kunnen worden ingedeeld in verschillende functietypen variërend van "administratief medewerker" tot "leidinggevenden en managers". De meeste handelingen worden echter verricht door "hoogopgeleide medewerkers", zij worden hierna aangeduid als "theoretisch opgeleide medewerkers". De gemiddelde uurtarieven van de betrokken medewerkers bij middelgrote (€ 49,-) en grote ondernemingen (€ 54,-) wijken niet significant af van het standaard uurtarief voor theoretisch opgeleide medewerkers volgens het Handboek Meting Regeldrukkosten, versie 2.1 d.d. 29 november 2023.
Naast tijdbesteding zullen bedrijven ook *out-of-pocket*-investeringen moeten doen. Wederom verwachten middelgrote ondernemingen gemiddeld lagere kosten te moeten maken dan grote ondernemingen: € 25.000,- respectievelijk € 44.400,- per bedrijf.
Naast eenmalige kosten voor het voorbereiden en implementeren van maatregelen in het kader van de zorgplicht verwachten bedrijven ook structurele meerkosten te zullen maken. Bedrijven geven aan dat zij op veel thema's die worden uitgewerkt in het Cbb al staand beleid hebben. De ISO27001- en NEN7510-standaarden vereisen dit immers al. De structurele meerkosten voor bedrijven volgen dan ook primair uit verplichtingen die meer diepgang of een bredere scope van

toepassing vereisen dan de maatregelen die bedrijven op dit moment al nemen. Veel genoemd zijn de voorschriften met betrekking tot de beveiliging van de toeleveringsketen. Bedrijven geven aan dat, hoewel zij vaak al maatregelen nemen op dit gebied, zij verwachten dat dit huidige beleid ontoereikend zal zijn om te voldoen aan de voorschriften op dit punt uit het Cbb. Bedrijven die veel op projectbasis werken met ketenpartners verwachten dat het sluiten van overeenkomsten met deze partijen structureel meer tijd zal kosten. Ook geven veel bedrijven aan meerkosten te verwachten ten aanzien van de voorschriften op het gebied van incidentenbehandeling. De structurele kosten van een licentie voor een *Incident Security Management System* (ISMS), en de inhuur van externe monitoringsdiensten ter ondersteuning van het *Security Operations Centre* (SOC) worden hierbij meermaals genoemd. Andere structurele kostenposten zijn de inhuur van een *Chief Information Security Officer* (CISO), de kosten in verband met de voorschriften ten aanzien van logging, en het schriftelijk vastleggen en bijhouden van het beleid in algemene zin.
Op basis van de inschattingen van de geïnterviewde bedrijven zijn de gemiddelde en de totale structurele regeldrukgevolgen als gevolg van de zorgplicht berekend. Bedrijven verwachten zowel kosten te maken als gevolg van tijdbesteding om aan de zorgplicht te voldoen, alsook als gevolg van *out-of-pocket*-investeringen die gedaan zullen moeten worden. Gemiddeld verwachten middelgrote bedrijven structureel 1.246 uur per jaar kwijt te zijn aan tijdbesteding om te voldoen aan de zorgplicht. Bij grote ondernemingen ligt dit aantal aanmerkelijk hoger, namelijk op gemiddeld 3.465 uur per jaar per bedrijf. Ook het type medewerker dat deze handelingen zal verrichten verschilt tussen middelgrote en grote ondernemingen. Bij bedrijven in die eerste categorie is de verwachting dat leidinggevenden en/of managers in de meeste gevallen verantwoordelijk zullen zijn voor de structurele werkzaamheden ten gevolge van de zorgplicht. Het gemiddelde corresponderend uurtarief van deze medewerkers ligt op € 73,-. Bij grote ondernemingen zal dit werk meestal verricht worden door hoogopgeleide medewerkers van de IT-afdeling of administratief personeel. Het gemiddelde corresponderend uurtarief van deze medewerkers ligt op € 51,-. De structurele *out-of-pocket*-kosten van middelgrote en grote ondernemingen liggen niet ver uit elkaar, deze bedragen gemiddeld € 30.000,- respectievelijk € 32.800,-.

Artikel 24 Cbw en de artikelen 22 en 23 Cbb (governance)
De kosten die geïnterviewde bedrijven verwachten te maken om te voldoen aan de eisen op het gebied van governance bestaan uit tijdbesteding door leden van het bestuur enerzijds, en *out-of-pocket*-kosten als gevolg van de vergoeding die betaald moet worden aan de externe trainer anderzijds. De geïnterviewde bedrijven verwachten deze kosten eenmalig te moeten maken voor het voltallige bestuur, en vervolgens periodiek naarmate de samenstelling van het bestuur verandert en de stand van de techniek evolueert. Omdat geen inschatting gegeven kon worden van de gemiddelde *turnover* van de raad van bestuur, en omdat technische innovaties zich niet laten voorspellen, is de aanname gedaan dat de helft van het aantal bestuursleden gedurende een periode van 10 jaar wordt vervangen.
De regeldrukgevolgen van de governanceverplichtingen zijn afzonderlijk in kaart gebracht voor middelgrote en grote ondernemingen. Hieruit blijkt dat middelgrote bedrijven gemiddeld genomen lagere kosten per bedrijf voorzien dan grote bedrijven, zowel ten gevolge van de tijdbesteding van het bestuur[3], alsook ten gevolge van de *out-of-pocket*-investeringen die gedaan zullen moeten worden. Middelgrote ondernemingen verwachten eenmalig € 1.954,- aan tijdbesteding kwijt te zijn voor de training van het bestuur en € 3.958,- aan *out-of-pocket*-investeringen te moeten doen. Voor grote ondernemingen zijn deze bedragen € 2.808,- respectievelijk € 11.071,- per bedrijf. Het verschil in de kosten van de tijdbesteding tussen middelgrote en grote bedrijven is te verklaren door de verwachting van grote bedrijven dat hun bestuurders meer tijd kwijt zullen zijn aan de te volgen training dan bestuurders van middelgrote bedrijven, namelijk bijna 9 uur per bestuurder van een grote onderneming tegenover bijna 5 uur per bestuurder van een middelgrote onderneming. De divergentie in de te maken *out-of-pocket*-kosten is minder eenduidig te verklaren. Wel geven respondenten namens middelgrote bedrijven vaker aan dat zij de verplichting tot het inhuren van een externe trainer bezwaarlijk vinden. Een mogelijke verklaring zou daarom kunnen zijn dat zij zullen proberen om de kosten van externe inhuur te verlagen, bijvoorbeeld door de voorbereiding op deze training zoveel mogelijk intern op te pakken. Grote bedrijven daarentegen hebben in sommige gevallen al ervaring met trainingen en/of cursussen van externe partijen. De verwachting van de respondenten namens grote bedrijven is veelal dat zij deze partijen simpelweg opnieuw zullen inschakelen en de bijkomende kosten accepteren.
De structurele kosten voor het voldoen aan de verplichtingen in het kader van de governance zijn naar verwachting beperkt.

[3] Hoewel middelgrote ondernemingen verwachten minder tijd per bestuurder kwijt te zijn aan de training dan grote ondernemingen (ca. 5 uur om ca. 9 uur), geven zij aan gemiddeld meer bestuurders de training te zullen laten volgen dan grote ondernemingen (5,6 personen om 4,4 personen).

Artikel 44 Cbw en artikel 28 Cbb (registratie in het nationaal register en informatieverstrekking ten behoeve van die registratie)
Sommige geïnterviewde bedrijven geven aan al geregistreerd te zijn naar aanleiding van het huidige wettelijke kader (de Wet beveiliging netwerk- en informatiesystemen). Zij zijn echter niet geregistreerd bij het Nationaal Cyber Security Centrum (hierna: NCSC), maar bij de Rijksinspectie Digitale Infrastructuur (hierna: RDI), en zullen zich dus nog moeten registreren bij het NCSC. Meerdere bedrijven geven daarnaast aan op dit moment niet in te kunnen schatten wat de exacte implicaties van de registratieverplichting voor hun organisatie zullen zijn. Wat hierbij een rol speelt is dat sommige bedrijven uit vele tientallen, soms honderden juridische eenheden bestaan actief zijn in meerdere lidstaten van de Europese Unie, ieder met een eigen registratieplicht die volgt uit de NIS2-richtlijn.
De meeste bedrijven geven aan enkel eenmalige kosten te verwachten ten gevolge van de registratieplicht, of de structurele kosten als verwaarloosbaar te beschouwen. Gemiddeld verwachten bedrijven dat één medewerker een dagdeel (circa 4 uur) kwijt zal zijn aan het registeren van het bedrijf bij het NCSC. De medewerker die deze werkzaamheden uit zal voeren is naar verwachting in de meeste gevallen een hoogopgeleide IT'er met een corresponderend uurtarief van € 54,-.
Toch voorzien enkele bedrijven ook significante structurele regeldrukgevolgen, bijvoorbeeld omdat de informatie in het register, waaronder informatie over de domeinnamen van de entiteit, continu bijgewerkt zal moeten worden. Deze opvatting wordt echter uitsluitend gedeeld door grote bedrijven. Daarom wordt in het kader van de berekening van de regeldrukkosten aangenomen dat, naast de incidentele kosten van het registreren van de onderneming bij het NCSC, alle 1.742 grote bedrijven die naar verwachting onder het toepassingsbereik van de Cbw vallen jaarlijks tijd kwijt zullen zijn om de geregistreerde informatie actueel te houden. Gemiddeld verwachten grote bedrijven dat enkele medewerkers hier gezamenlijk 10 uur per jaar aan zullen besteden, tegen een gemiddeld uurloon van € 52,-.

Tabel 1: eenmalige regeldrukgevolgen Cbw en Cbb[4]

Artikelen	**Tijdbesteding in uren**	**Uurtarief (€)**	***Out-of-pocket*-kosten (€)**	**Totale kosten per bedrijf (P)**	**Aantal (Q)**	**Kosten (P×Q)**
Artikel 21 Cbw en de artikelen 6 tot en met 17 en 19 Cbb (zorgplicht)	2.020	€ 53,-	€ 29.476,-	€ 136.536,-	7.550	€ 1.030.847.000,-
Artikel 24 Cbw en de artikelen 22 en 23 Cbb (governance)	€ 2.151		€ 5.599,-	€ 7.750,-	7.550	€ 58.513.000,-
Artikel 44 Cbw en artikel 28 Cbb (registratie in het nationaal register en informatieverstrekking ten behoeve van die registratie)	4	€ 54,-	-	€ 216,-	7.550	€ 1.631.000,-
Totaal	€ 1.090.991.000,-					
Gemiddeld per bedrijf	€ 145.000,-					

Tabel 2: structurele regeldrukgevolgen Cbw en Cbb[5]

Artikelen	**Tijdbesteding in uren**	**Uurtarief (€)**	***Out-of-pocket*-kosten (€)**	**Totale kosten per bedrijf (P)**	**Aantal (Q)**	**Kosten (P×Q)**
Artikel 21 Cbw en de artikelen 6 tot en met 17 en 19 Cbb (zorgplicht)	1.758	€ 63,-	€ 30.646,-	€ 141.400,-	7.550	€ 1.067.570.000,-
Artikel 24 Cbw en de artikelen 22 en 23 Cbb (governance)	€ 108,-		€ 280,-	€ 388,-	7.550	€ 2.926.000,-
Artikel 44 Cbw en artikel 28 Cbb (registratie in het nationaal register en informatieverstrekking ten behoeve van die registratie)	10	€ 52,-	-	€ 520,-	7.550	€ 906.000,-
Totaal	€ 1.071.402.000,-					
Gemiddeld per bedrijf	€ 142.000,-					

[4] De resultaten zijn gewogen gemiddelden voor middelgrote- en grote ondernemingen.
[5] De resultaten zijn gewogen gemiddelden voor middelgrote- en grote ondernemingen.

3.4 Panel mkb

Inleiding
Bij de voorbereiding van het onderhavige besluit is tevens een panel van mkb-ondernemers gevraagd mee te denken over deze regelgeving. Deze ondernemers hebben op basis van hun praktijkervaring aangegeven of de plannen werkbaar zijn, waar eventuele knelpunten zitten en hoe regeldruk voor het mkb zo veel mogelijk beperkt of voorkomen kan worden. Tijdens een bijeenkomst is gesproken over de deelthema's waar de meeste regeldruk wordt voorzien, te weten: de zorgplicht, governanceverplichting en registratieplicht.

Ondersteuning
Met betrekking tot de zorgplicht gaven de panelleden aan dat het vereiste van het nemen van specifieke maatregelen voor de beveiliging van netwerk- en informatiesystemen niet onredelijk is, waarbij het mkb-panel zich wel af vroeg hoe haalbaar en betaalbaar dit voor het mkb is. Daarbij pleitten de deelnemers voor zo veel mogelijk duidelijkheid over het toepassingsbereik en over de betekenis van specifieke begrippen. Voor mkb'ers is het bijvoorbeeld lastig in te schatten wat de risico's in hun netwerk- en informatiesystemen zijn. Daarom zouden mkb'ers graag zien dat de overheid hen ondersteuning biedt door bijvoorbeeld handreikingen, tools en sjablonen aan te bieden, zodat zij een beter idee krijgen wat er van hen wordt verwacht. In reactie hierop wordt erop gewezen dat organisaties bij het NCSC en het Digital Trust Center (hierna: DTC) terecht kunnen voor kennis, informatie en advies op thema's rondom cyberweerbaarheid. Daarnaast bieden het NCSC en het DTC verschillende handreikingen en tools die organisaties kunnen gebruiken. Het DTC heeft op grond van de Wet bevordering digitale weerbaarheid bedrijven de wettelijke taak om (onder andere) het mkb hierin specifiek te voorzien. Met de komst van de Cbw worden deze vormen van ondersteuning verder uitgebreid.

Toezicht
De NIS2-richtlijn en de Cbw hanteren het principe van een risicogebaseerde benadering, waardoor organisaties discretionaire ruimte hebben voor de specifieke invulling van de eisen die de Cbw en het Cbb stellen. De panelleden pleitten ervoor dit principe van risicobeheersing ook te hanteren bij het toezicht en de handhaving van de Cbw en het Cbb.
Het toezicht onder de Cbw is risicogestuurd sectoraal en wordt gedaan door een onafhankelijke toezichthouder. Op welke wijze essentiële entiteiten en belangrijke entiteiten invulling moeten geven aan de maatregelen in het kader van de zorgplicht is afhankelijk van de risicoanalyse, waaruit voortvloeit welke invulling passend en evenredig is voor de betreffende entiteit. De toezichthouder zal per entiteit beoordelen of de specifieke invulling van de maatregelen voldoen aan de zorgplicht, bedoeld in artikel 21 Cbw. Toezichthoudende instanties werken op grond van artikel 55 Cbw zoveel mogelijk samen bij het (onderling gecoördineerd) toezicht houden op essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, ook gericht op het beperken van de regeldruk bij entiteiten. In het bijzonder in gevallen waarbij meerdere toezichthoudende instanties onder de Cbw toezicht houden op eenzelfde entiteit is het vanuit het belang van doeltreffend en doelmatig toezicht en het beperken van toezichtslasten gewezen om deze informatie uit te wisselen.

Focus op administratie
Verder geeft het mkb-panel aan dat voorkomen dient te worden dat de focus van de verplichtingen op de administratie komt te liggen. Dit gaat ten koste van de inspanning en de middelen die ondernemers kunnen aanwenden voor het daadwerkelijk nemen van maatregelen. Mkb'ers zouden graag zien dat hen minder gedetailleerd wordt opgelegd hóe zij bepaalde doelen moeten behalen, en dat in plaats daarvan een algemene inspanningsverplichting geldt. Het is van belang dat de eisen die de Cbw en het Cbb stellen duidelijk, evenredig en proportioneel zijn. De eisen voor bedrijfscontinuïteit en crisisbeheer zijn nu nog (te) breed geformuleerd, aldus het mkb-panel. Gepleit wordt voor het werken met doelvoorschriften, waarbij precieze invulling aan de ondernemers wordt gelaten. Zij roepen op om maatwerk te faciliteren. Daarnaast wordt de suggestie gedaan om de ISO27001-standaard als kapstok te hanteren, omdat veel mkb'ers al bekend zijn met dit normenkader.
De reactie op het voorgaande is als volgt. Zowel voor de Cbw als voor de uitwerking van de zorgplicht in het Cbb zijn bestaande normenkaders gehanteerd als uitgangspunt, zoals de ISO27001 en NEN7510. In de memorie van toelichting op de Cbw en nota van toelichting op het Cbb wordt, waar van toepassing, naar bestaande normenkaders verwezen. Ook staat het doel van specifieke eisen in deze nota van toelichting verder uitgewerkt. De Cbw en het Cbb gaan uit van een risicogebaseerde aanpak en schrijven niet voor hoe invulling gegeven met worden aan de maatregelen.

Effecten op de markt
Tevens signaleren mkb'ers het risico dat bepaalde partijen onevenredig kunnen profiteren van deze nieuwe wetgeving, omdat zij als enigen bepaalde diensten aanbieden die ondernemers nodig hebben om de verplichtingen van de Cbw te kunnen voldoen. De reactie hierop is als volgt. De Cbw en onderliggende regelgeving beoogt geen invloed uit te oefenen op (al bestaande) marktwerkingen. Waar mogelijk bieden overheidsorganisaties zoals het NCSC en het DTC ondersteuning, zoals eerder omschreven. Een organisatie blijft echter zelf verantwoordelijk voor het beveiligen van haar netwerk- en informatiesystemen en voor het besluit of gebruik wordt gemaakt van externe partijen in het implementeren van de Cbw en het Cbb.

Ingroeiperiode
Met betrekking tot de inwerkingtreding van de Cbw en onderliggende regelgeving wordt de suggestie gedaan een ingroeiperiode te hanteren, zodat mkb-ondernemers zich adequaat kunnen voorbereiden. Dit heeft ook te maken met onzekerheid over de datum van inwerkingtreding en onduidelijkheid over de vraag welke mkb-ondernemers nu precies onder de reikwijdte van de Cbw zullen vallen.
De reactie op het voorgaande is als volgt. Over de inwerkingtreding van de Cbw en onderliggende regelgeving zal tijdig worden gecommuniceerd. Hierbij wordt opgemerkt dat organisaties al meermaals via verschillende kanalen zijn opgeroepen om de inwerkingtreding van de Cbw en onderliggende regelgeving niet af te wachten, maar om alvast aan de slag te gaan ter voorbereiding op de komst van die wet- en regelgeving. Daarbij kan gebruik worden gemaakt van de eerder omschreven ondersteuning die al wordt geboden. Voor de reikwijdte van de Cbw kunnen organisaties terecht op verschillende websites van de rijksoverheid, waar onder andere een zelfevaluatietool beschikbaar. Deze tool kan helpen bij het bepalen of een organisatie onder de Cbw valt. Iedere organisatie is hier zelf verantwoordelijk voor.

Toeleveranciers
De panelleden signaleren dat de kleinere toeleveranciers van hun ondernemingen moeilijk aan de eisen met betrekking tot de beveiliging van de toeleveringsketen zullen kunnen voldoen. Grotere bedrijven hebben wellicht de mogelijkheid om hun toeleveranciers te helpen, maar voor het mkb is dat niet altijd haalbaar. Ook hier wordt gepleit voor een risicogebaseerde benadering, zodat mkb'ers zelf kunnen inschatten welke van hun toeleveranciers een mogelijk risico voor de beveiliging van hun netwerk- en informatiesystemen vormen. Daarnaast voorzien panelleden een risico in de slagkracht die zij hebben tegenover grote(re) bedrijven in hun toeleveringsketen.
De reactie op het voorgaande is als volgt. De artikelen uit de Cbw en het Cbb die zien op de toeleveringsketen zijn alleen van toepassing op de leveranciers die van invloed zijn op het netwerk- en informatiesysteem van een organisatie. Uit de risicoanalyse van de organisatie vloeit voort welke maatregelen voor de toeleveringsketen genomen moeten worden.

Governance
De gestelde eisen op het gebied van governance van de Cbw en het Cbb zijn behoorlijk uitgebreid, zo merken de deelnemers van het mkb-panel op. De eis dat een trainer een onafhankelijke partij, dat wil zeggen een externe partij, moet zijn wordt voor het mkb als belastend ervaren. De deelnemers aan het mkb-panel begrijpen dat het bestuur een zeker begrip van cyberbeveiliging moet hebben, maar geven aan dat ervoor gewaakt moet worden dat het middel het doel voorbijschiet. De training is bedoeld dat bestuurders adequate beslissingen kunnen nemen met betrekking tot de beveiliging van de netwerk- en informatiesystemen van hun organisatie, niet dat zij tot in detail kunnen uitleggen hoe een bijvoorbeeld DdoS-aanval werkt. Ook in dit geval pleiten zij voor proportionele en evenredige eisen.
Ten aanzien van het voorgaande is de reactie als volgt. De eis van een onafhankelijke trainer is na de internetconsultatie geschrapt. De verplichting van een training voor het bestuur is een (dwingend) vereiste uit de NIS2-richtlijn en kan om die reden niet gewijzigd worden.

Registratie
De panelleden gaven tot slot aan behoefte te hebben aan meer en betere voorlichting over de registratieplicht. Zo waren niet alle deelnemers op de hoogte van het feit dat entiteiten die onder de reikwijdte van de Cbw vallen, zich dienen te registreren bij het NCSC die namens de Minister van Justitie en Veiligheid en het nationale register zal beheren. Met betrekking tot de registratieplicht ziet het mkb-panel voorts graag harmonisatie en afstemming tussen lidstaten. Het is niet werkbaar wanneer sommige mkb'ers zich mogelijk 27 keer moeten registreren.
De reactie op het voorgaande is als volgt. Er wordt actief ingezet op communicatiemiddelen die onder andere de boodschap om te registreren met zich meedragen. Er zal in aanloop naar de

inwerkingtreding van de Cbw grootschaliger campagne worden gevoerd met communicatiemiddelen die wederom deze boodschap met zich mee zullen dragen. Voor wat betreft het punt over de harmonisatie en afstemming tussen lidstaten wordt erop gewezen dat de NIS2-richtlijn van elk lidstaat van de Europese Unie vereist te voorzien in de registratieplicht.

4. Adviezen, consultatie en uitvoerings- en handhaafbaarheidstoetsen

4.1 Inleiding

Een eerdere versie van dit besluit is voor advies voorgelegd aan de Autoriteit persoonsgegevens (hierna: AP) en het ATR, opengesteld voor consultatie op www.internetconsultatie.nl en voor commentaar toegezonden aan belangenorganisaties en entiteiten. Hieronder volgt een globale bespreking van de adviezen en reacties.

4.2 Advies AP

De AP geeft in haar advies aan dat onvoldoende duidelijk is welke persoonsgegevens in het kader van de Cbw verwerkt mogen worden. De AP concludeert dat de te verwerken persoonsgegevens waar mogelijk in de wettekst gespecificeerd dienen te worden, of dat verduidelijking en onderbouwing in de toelichting nodig is. De reactie op dit punt is als volgt. De gevraagde specificering is niet mogelijk. Voor een CSIRT is het bijvoorbeeld niet mogelijk om van tevoren te zien welke persoonsgegevens zich bevinden in dreigings- en incidentinformatie. Daardoor is het niet mogelijk dit vooraf te identificeren. Door dit wel te specificeren kan dit een belemmering vormen voor de wettelijke taakuitvoering van een CSIRT.

Voorts wijst de AP in haar advies op artikel 30, tweede lid, Cbb en hetgeen daarover in de nota van toelichting is aangegeven. Volgens de AP wordt in de nota van toelichting aangegeven dat de verwachting is dat het nationaal register steeds aangepast of bijgewerkt wordt zodat deze gegevens in de praktijk oneindig bewaard worden. De maximale bewaartermijn van 60 maanden begint voor veel van deze persoonsgegevens steeds opnieuw te lopen, waardoor de termijn geen effectieve waarborg meer is, aldus de AP. Naar aanleiding van dit advies is in artikel 30, tweede lid, Cbb “na de laatste wijziging van de betreffende persoonsgegevens” vervangen door “na de laatste bevestiging van de juistheid van de betreffende persoonsgegevens”. Hierop is ook de artikelsgewijze toelichting bij de bepaling aangepast.

4.3 Advies ATR

Nut en noodzaak
Het ATR adviseert om het nut en de noodzaak van het wetsvoorstel Cbw in de memorie van toelichting beter te onderbouwen, door te verduidelijken op welke onderdelen de bestaande wetgeving tekortschiet. In reactie op dit advies wordt verwezen naar hoofdstuk 2.2 van de memorie van toelichting op de Cbw. Hierin is reeds toegelicht dat de NIS2-richtlijn onder meer verplichtingen bevat waarvan het wenselijk is dat deze door de entiteiten uit de verschillende sectoren van de NIS2-richtlijn uniform worden toegepast. Bovendien bevat de NIS2-richtlijn onderwerpen waarvan de regeling per definitie alleen centraal kan worden geregeld (bijvoorbeeld het beheer van een nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen).

Minder belastende alternatieven
Het ATR stelt dat zoveel mogelijk gekozen moet worden voor de minst belastende invulling van verplichtingen uit de NIS2-richtlijn (en van de implementatiewetgeving als gevolg daarvan). Daarbij geeft het ATR aan dat toegelicht moet worden welke alternatieven voor nationale koppen zijn bezien en toe te lichten waarom niet is gekozen voor die (minder belastende) alternatieven. De reactie hierop is als volgt. In het Cbb zijn er geen nationale koppen. Wel is in het Cbb de zorgplicht uit de Cbw nader ingevuld. Ten aanzien van het punt over minder belastende alternatieven wordt opgemerkt dat bij de invulling van de zorgplicht uit de Cbw in het Cbb telkens is gekozen voor de invulling die entiteiten duidelijkheid geeft en daarmee dus ook bijdraagt aan de rechtszekerheid voor entiteiten. De gekozen invulling zorgt in zekere zin voor een regeldrukbeperking voor de entiteit.
Daarnaast adviseert het ATR om aan te sluiten bij bestaande kaders. Daarbij refereert het ATR aan een onderdeel van de regeldrukparagraaf waarin mkb’ers bestaande normenkaders hebben aangehaald voor minder belastende regeldruk. De reactie hierop is als volgt. Zowel voor de Cbw als voor de uitwerking van de zorgplicht in het Cbb zijn bestaande normenkaders gehanteerd als

uitgangspunt, zoals de ISO27001 en NEN7510. Hierbij is gecontroleerd of de Cbw en het Cbb deze normenkaders niet doorkruist. In de memorie van toelichting op de Cbw en de nota van toelichting op het Cbb wordt, waar van toepassing, naar bestaande normenkaders verwezen. Eén verplicht normenkader, zoals het ATR adviseert, levert niet noodzakelijkerwijs lastenvermindering op. Entiteiten houden met de Cbw en het Cbb de ruimte om hun bestaande normenkader te blijven hanteren, waarbij ze wel moeten zorgen dat de maatregelen uit het Cbb geborgd zijn.

Mkb
Het ATR heeft bij het wetsvoorstel Cbw geadviseerd om een mkb-toets uit te laten voeren voor de lagere regelgeving waarmee de verplichtingen uit de Cbw nader worden uitgewerkt. Aansluitend adviseert het ATR om de werkbaarheid van het Cbb te onderzoeken en consequent toe te lichten hoe met de zorgen en kritiek van de relevante entiteiten is omgegaan. Conform het advies van het ATR is een mkb-toets uitgevoerd op het Cbb. Hiervoor wordt verwezen naar hoofdstuk 3, waarin de belangrijkste uitkomsten worden omschreven, evenals hoe is omgegaan met de door entiteiten aangehaalde aandachtspunten.
Het ATR vraagt of aan mkb'ers dezelfde eisen moeten worden gesteld als aan grotere entiteiten. De reactie hierop is als volgt. Voor differentiatie tussen de verplichtingen die gelden voor essentiële entiteiten en die gelden voor belangrijke entiteiten biedt de NIS2-richtlijn geen ruimte, anders dan de reeds opgenomen differentiatie in het toezichtregime.
Ten aanzien van het mkb wordt tot slot opgemerkt dat in het kader van de Cbw en het Cbb gericht aanvullende hulpmiddelen worden geboden aan het mkb, om de werkbaarheid voor het mkb te vergroten. Er zullen onder meer handreikingen worden gepubliceerd die als hulpmiddel kunnen worden gebruikt voor het implementeren van de verschillende vereisten die de Cbw en het Cbb bevatten. Ook wordt in deze handreiking handelingsperspectief geboden aan entiteiten die onder meerdere sectoren vallen.

Regeldruk
Het ATR heeft bij het wetsvoorstel Cbw geadviseerd om meer inzicht te geven in de regeldrukgevolgen van het Cbb. Omdat het Cbb met name regels bevat ter uitwerking van de zorgplicht, de nadruk van deze regeldrukgevolgen voornamelijk op het voldoen aan de zorgplicht. Conform het advies van het ATR is een regeldrukonderzoek uitgevoerd met betrekking tot het Cbb door een onafhankelijk onderzoeksbureau. Hiervoor wordt verwezen naar hoofdstuk 3, waarin de belangrijkste uitkomsten worden omschreven en hoe hiermee om is en wordt gegaan. De berekening van de regeldrukgevolgen is conform de Rijksbrede methodiek uitgevoerd.
Het ATR stelt dat een onderbouwing ontbreekt van de berekening van sommige onderdelen van de regeldrukkosten. Naar aanleiding van deze observatie van het ATR zijn waar nodig de bevindingen in hoofdstuk 3 aangevuld, mede op basis van een uitbreiding van de mkb-toets.
Het ATR signaleert dat de gevolgen voor de toeleveringsketen niet in de regelruktoets zijn meegenomen. In reactie daarop is het van belang om hierbij te benadrukken dat het wat de Cbw en het Cbb betreft gaat om leveranciers die relevant zijn voor de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten en belangrijke entiteiten en waarvoor maatregelen moeten worden genomen vanuit de risicoanalyse van de entiteit zelf. Daardoor is de inschatting dat op dit punt de Cbw en het Cbb geen hogere regeldruk veroorzaken.

4.4 Toepassingsbereik

In meerdere (internet)consultatiereacties zijn vragen gesteld over het toepassingsbereik van het Cbb, geregeld in artikel 4 Cbb, met name als het gaat om entiteiten die zowel onder het Cbb als de uitvoeringsverordening vallen. De artikelsgewijze toelichting op artikel 4 Cbb is in verband hiermee verduidelijkt.

4.5 CSIRT

In meerdere (internet)consultatiereacties is gevraagd naar de samenhang van de Cbw, het Cbb en het rapport over het herinrichten van het CSIRT-stelsel.[6] Dit zal verder worden uitgewerkt in beleid. Hierbij is ook aandacht voor de informatie vanuit het CSIRT-stelsel ten behoeve van het Cyberweerbaarheidsnetwerk zoals toegelicht in de Toekomstvisie van 23 mei 2024. Ook zal nader worden ingegaan op de invulling van taken door CSIRT's, zoals bij het leveren van bijstand.

[6] *CSIRT-stelsel - Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland*, Petra Oldengarm, 2023.

Een aantal partijen, waaronder het Verbond van Nederlandse Ondernemingen – Nederlands Christelijk Werkgeversverbond (hierna: VNO-NCW) en Cyberveilig Nederland, vragen in de consultatie naar de bijstand die een entiteit van het CSIRT kan verwachten. De toelichting hierop is als volgt. Het CSIRT zal geen taken en verantwoordelijkheden van essentiële entiteiten en belangrijke entiteiten overnemen. De bijstand door een CSIRT laat dus de eigen verantwoordelijkheid voor het naleven van de verplichtingen die voortvloeien uit de Cbw en het Cbb onverlet. De door het CSIRT geleverde bijstand zal worden uitgewerkt in beleid.

4.6 Zorgplicht

In een aantal consultatiereacties, waaronder die van FME, VNO-NCW, Pasquil, Energie Nederland en de Nederlandse Vereniging van Ziekenhuizen, wordt opgemerkt dat duidelijker naar voren moet komen dat in het kader van de Cbw en het Cbb er sprake is van een *risk-based* aanpak in plaats van een *rule-based* aanpak. Naar aanleiding van deze reacties is deze nota van toelichting op meerdere plekken aangepast om duidelijk te maken dat de invulling van de te nemen maatregelen afhankelijk is van de uitkomsten van de risicoanalyse. In diverse artikelen in het Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten bepaald beleid moeten hebben vastgesteld. Hiermee kunnen entiteiten aantonen dat zij hebben nagedacht over de mogelijke risico's. Er wordt niet voorgeschreven wat de exacte omvang en inhoud van dit beleid moet zijn.

Omni-U Services B.V. en Netbeheer Nederland hebben in hun consultatiereacties aangegeven dat processen en procedures geen onderdeel zijn van het beleid, maar aparte documenten die uitvoering geven aan het beleid. Hierop is het Cbb en de nota van toelichting op verschillende punten aangepast.

In een aantal consultatiereacties, waaronder die van FERM en de koninklijke Vereniging van de Nederlandse Chemische Industrie (hierna: VNCI), is aangegeven dat het scheiden van conflicterende rollen voor het mkb niet altijd mogelijk is en risicogebaseerd moet zijn. Naar aanleiding van dit commentaar is artikel 6, tweede lid, Cbb aangepast.

Meerdere partijen vragen in de consultatie wat er met termen als "periodiek" en "tijdig" wordt bedoeld. De reactie hierop is als volgt. Afhankelijk van de geïdentificeerde risico's zal een entiteit zelf moeten bepalen en onderbouwen welke periode passend is en wat tijdig is in de context van die entiteit.

Meerdere partijen hebben in de consultatie commentaar gegeven op artikel 9 Cbb. Zo hebben Omni-U Services B.V. en MSP ISAC aangegeven dat niet voor ieder incident een bedrijfscontinuïteitsplan nodig is. Daarnaast wordt aangegeven dat een noodvoorzieningenplan een heel ander plan is. Sunbites Cybersecurity geeft aan dat er geen apart plan hoeft te zijn voor de Cbw, maar dat dit geïntegreerd kan worden in bestaande plannen. Daarnaast geeft VNO-NCW aan dat ook hier een risicogebaseerde aanpak nodig is. Een aantal andere partijen vragen aandacht voor de OT-omgeving in verband met back-ups. Verder vraag Brainport om verduidelijking over hoe er gecommuniceerd kan worden met het CSIRT. In reactie hierop wordt toegelicht dat dit zal gaan via het meld- en registratieportaal waar entiteiten zich kunnen registeren en incidenten en de voortgang daarvan kunnen melden. Op basis van deze commentaren is artikel 9 Cbb aangepast, evenals de artikelsgewijze toelichting op dat artikel.

In een aantal consultatiereacties, waaronder die van VNO-NCW, Energie Nederland en Cyberveilig Nederland, wordt gevraagd wat bedoeld wordt met de term "waar mogelijk" in artikel 10, eerste lid, Cbb. Naar aanleiding hiervan is artikel 10 Cbb aangepast. Ook is de passage in dit artikel over het beëindigen van overeenkomsten aangepast.

In de consultatie geven VNO-NCW en FERM aan dat zij een toelichting wensen over de relatie tussen het Cbb en de zogeheten Verordening cyberweerbaarheid[7] (*Cyber Resilience Act*). Naar aanleiding van deze vraag wordt het volgende toegelicht. De *Cyber Resilience Act* is toekomstige wet- en regelgeving die de cyberbeveiliging van producten met een digitaal component verbetert. Dit ontslaat entiteiten er niet van zelf vast te stellen of het gebruik van dergelijke producten en diensten de beveiliging van hun netwerk- en informatiesystemen verhoogt of verlaagt.

[7] Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (*PbEU* 2024/2847).

Diverse partijen, waaronder VNO-NCW en Energie Nederland, geven aan dat de term "opleiding" in artikel 12, tweede lid, Cbb te ver gaat en hier de term "training" moet worden gehanteerd. De reactie hierop is als volgt. De term "opleiding" komt uit de NIS2-richtlijn en is ter implementatie daarvan ook in de Cbw gehanteerd.

Door verschillende partijen is in de consultatie aangegeven dat artikel 15 Cbb niet juist is vanwege de term "authenticaties". Naar aanleiding van deze commentaren is artikel 15 Cbb aangepast.

Diverse partijen, waaronder Nederlandse Federatie van Universitair Medische Centra (NFU), VNCI, NVZ en Brainport, hebben vragen gesteld over de uitleg van artikel 17 Cbb en dan met name over op welke attenderingen entiteiten nu wel en niet moet reageren. Hierop is de artikelsgewijze toelichting op artikel 17 Cbb verduidelijkt.

4.7 Training

Uit de consultatie volgt dat meerdere partijen, waaronder de G4, kritisch zijn over artikel 22 Cbb, over de eisen die worden gesteld aan de trainer. Er wordt met name aangegeven dat deze bepaling verder gaat dan de NIS2-richtlijn, onder meer ten aanzien van de onafhankelijkheid van de trainer. Dit artikel is mede vanwege deze commentaren heroverwogen en geschrapt.

Ook waren er kritische reacties op de eisen aan het certificaat, met name ten aanzien van het vereiste over het aantal uren dat de training is gevolgd. Hierover is onder meer aangegeven dat het aantal uur niets zegt over de kwaliteit van de training. Naar aanleiding van deze reacties is in artikel 23, eerste lid, Cbb het vereiste over het aantal uren geschrapt.

Enkele consultatiereacties gingen ook in op het stellen van een opleidingsvereiste aan de bestuurder van een entiteit. De toelichting hierop is als volgt. Dit is een vereiste uit de NIS2-richtlijn. In dit verband wordt overigens benadrukt dat het uitdrukkelijk geen opleiding betreft waarin van de bestuurder wordt verwacht technische kennis te verkrijgen en netwerk- en informatiesystemen te kunnen uitleggen. Wel wordt van de bestuurder op strategisch niveau kennis verwacht op de genoemde onderwerpen, zodat de bestuurder in staat is de maatregelen die de entiteit moet nemen in het kader van de zorgplicht te beoordelen en de risico's te (laten) beheersen. Hiervoor is een bepaalde basiskennis vereist.

4.8 Meldplicht

In enkele consultatiereacties, waaronder die van NLdigital, Energie Nederland, de N.V. Nederlandse Spoorwegen en Cyberveilig Nederland, wordt aandacht gevraagd voor de meld- en registratieplicht van groepen van entiteiten. De reactie hierop is als volgt. Op dit moment wordt gewerkt aan een functionaliteit in het meld- en registratieportaal waarmee groepen van entiteiten meerdere entiteiten die tot een groep behoren, gebundeld kunnen registreren en meldingen kunnen doen. Entiteiten die zowel een essentiële entiteit als belangrijke entiteit zijn onder verschillende sectoren, moeten zich registreren als essentiële entiteit.

In de consultatie is door een aantal partijen, waaronder Brainport, gevraagd wat wordt bedoeld met soort entiteit. De toelichting hierop is als volgt. De Cbw kent een onderscheid tussen sectoren en indien van toepassing subsectoren en soorten entiteiten. Dit onderscheid is te vinden in bijlage 1 en 2 van de Cbw.

Door de Vereniging van Nederlandse Gemeenten (VNG) en het Interprovinciaal Overleg (IPO) is gevraagd om twee jaar na de invoering van de Cbw de inhoud van de meldplicht te evalueren. De reactie hierop is als volgt. De termijn van vier jaar voor het evalueren van de drempelwaarden in het kader van de meldplicht betreft een uiterlijke termijn; een eerdere evaluatie is ook mogelijk. Het is de verwachting dat de vakministers (ruim) voor die uiterlijke termijn zullen overgaan op het evalueren van de drempelwaarden. Het moment waarop zij de drempelwaarden zullen evalueren wordt uitgewerkt in beleid en zal vanwege de in artikel 24, tweede lid, Cbb opgenomen termijn in ieder geval binnen vier jaar na de vaststelling van de drempelwaarden zijn.

4.9 Overige opmerkingen

Een aantal partijen, waaronder Energie Nederland, Forum Standaardisatie en Netbeheer Nederland, vragen wat er onder domeinnamen wordt verstaan. Onder domeinnamen wordt verstaan: de publiek beschikbare domeinen die de entiteit in eigendom heeft en niet de interne

domeinen of de domeinnamen die zij namens derden beheert. De data vanuit Stichting Internet Domeinregistratie Nederland (SIDN) evenals de gegevens uit het Register Internetdomeinen Overheid zijn een goed startpunt, maar niet volledig. De artikelsgewijze toelichting op artikel 28 Cbb is hierop aangepast.

De G4 geeft aan dat een bewaartermijn van 60 maanden, zeker voor loggegevens, lang is en de nodige kosten met zich meebrengt. De reactie hierop is als volgt. De in artikel 30, eerste en tweede lid, Cbb opgenomen maximale bewaartermijn van 60 maanden geldt voor de persoonsgegevens die door het CSIRT, de bevoegde autoriteit, het centrale contactpunt en de Minister van Justitie en Veiligheid bij of krachtens de Cbw worden verwerkt.

In enkele consultatiereacties is gewezen op fouten in het conceptbesluit op het gebied van de interpunctie, spelling, grammatica en opmaak en verwijzingsfouten. Deze fouten zijn hersteld.

4.10 Uitvoerings- en handhaafbaarheidstoetsen

De betrokken vakdepartementen hebben uitvoerings- en handhaafbaarheidstoetsen laten uitvoeren op een concept van het Cbb en hebben deze als volgt beoordeeld.

4.10.1 Ministerie van Binnenlandse Zaken en Koninkrijkrelaties

Op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft de RDI een uitvoerings- en handhavingstoets (UHT) uitgevoerd op het concept van het Cbb en de bijbehorende nota van toelichting. De RDI acht het concept van het Cbb uitvoerbaar, handhaafbaar en fraudebestendig, mits verschillende aandachtspunten nader worden verduidelijkt dan wel aangepast in het concept. Deze aandachtspunten betreffen niet specifiek de sector overheid, maar zijn algemeen van aard.

In het kader van artikel 2 Financiële-verhoudingswet is in de memorie van toelichting op de Cbw aangegeven dat de gevolgen van de Cbw voornamelijk voort zullen vloeien uit de lagere regelgeving. Voor de overheid gelden reeds sinds 1 december 2008 de ISO27001- en ISO27002-standaarden, aangezien zij toen zijn opgenomen in de *pas-toe-of-leg-uit*-lijst van het Bureau Forum Standaardisatie. Voorts vormen deze standaarden de basis voor de bij de centrale en decentrale overheden verplichte normatiek van de Baseline Informatiebeveiliging Overheid (BIO).

De verplichtingen ten aanzien van de zorgplicht in het Cbb gaan in grote lijnen niet verder dan reeds bestaande verplichtingen van genoemde ISO-standaarden en de BIO. Verder bevat het Cbb enkele eisen ten aanzien van de opleiding van de bestuurder. De inschatting is dat deze opleiding geen merkbaar effect zal hebben op de begroting van de overheidsentiteiten en zal opgaan in reguliere scholings- en opleidingsinspanningen.

In de ministeriële regeling onder de Cbw voor de sector overheid zullen de specifieke bepalingen uit de BIO worden opgenomen. De impact van de Cbw op overheidsorganisaties zal met name voortvloeien uit deze ministeriële regeling.

4.10.2 Ministerie van Economische Zaken en Ministerie van Klimaat en Groene Groei

De RDI acht het concept-Cbb en de bijbehorende ministeriële regeling uitvoerbaar, handhaafbaar en fraudebestendig, mits op enkele onderdelen aanvullende toelichting wordt gegeven. Het gaat daarbij onder meer om de verhouding tussen de open norm van de zorgplicht in de Cbw en de in het Cbb uitgewerkte maatregelen. In de toelichting is verduidelijkt dat deze maatregelen het minimumniveau vormen en passend en evenredig toegepast moeten worden, afhankelijk van de risicoanalyse van de betreffende entiteit. Hiermee is geborgd dat de open norm uit de Cbw leidend blijft, met ruimte voor sectorspecifieke toepassing.

Daarnaast is in de toelichting per maatregel het doel en beoogde resultaat toegelicht, zodat voor entiteiten en toezichthouders duidelijk is wat een adequate invulling inhoudt. Ook zijn begrippen als “crisis” en “cryptografie” nader toegelicht, net als het gebruik van termen als “waar passend” en “waar mogelijk”, om interpretatieverschillen bij de uitvoering te voorkomen. Verder is op verzoek van de RDI de samenhang tussen de verschillende beleidsdocumenten binnen hoofdstuk 4 van het Cbb verduidelijkt, zoals tussen het incidentenplan en het bedrijfscontinuïteitsplan, zodat deze in de praktijk integraal kunnen worden toegepast. Waar signalen van overlap zijn benoemd,

zoals bij artikelen over toeleveringsketens, is de reikwijdte nader afgebakend in de artikelsgewijze toelichting.

Ook wijst de RDI op het belang van integraliteit tussen de Cbw, het Cbb en andere relevante wet- en regelgeving, zowel nationaal als Europees. Dit punt wordt herkend. Daarbij wordt rekening gehouden met de uitvoerbaarheid voor entiteiten en uitvoeringsorganisaties. Waar volledige afstemming niet mogelijk is – bijvoorbeeld als gevolg van vastgestelde Europese verplichtingen – wordt bij de inrichting van processen gezocht naar zoveel mogelijk coördinatie en centralisatie, met als doel de uitvoeringslasten en regeldruk voor betrokken partijen te beperken.

Tot slot zijn naar aanleiding van de uitvoerings- en handhavingstoets van de RDI nog technische aanpassingen in de telecommunicatiewetgeving (het Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten en het Besluit veiligheid en integriteit telecommunicatie) doorgevoerd.

4.10.3 Ministerie van Financiën

Gelijktijdig met de NIS2-richtlijn is de zogeheten *Digital Operational Resilience Act* (hierna: DORA) vastgesteld.[8] Deze verordening is van toepassing op de financiële sector. De Nederlandsche Bank (DNB) en Autoriteit Financiële Markten (AFM) zijn verantwoordelijk voor het toezicht uit hoofde van DORA.

De bepalingen van de DORA over risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), het beheer van ICT-gerelateerde incidenten en met name de rapportage van grote ICT-gerelateerde incidenten, alsmede die over digitale operationele weerbaarheidstests, informatie-uitwisselingsregelingen en risico van derden op het gebied van ICT, zijn van toepassing op een groot gedeelte van de financiële sector in plaats van de bepalingen uit de NIS2-richtlijn. In artikel 1, tweede lid, DORA is namelijk expliciet bepaald dat de verordening voor de toepassing van artikel 4 NIS2-richtlijn moet worden beschouwd als een sectorspecifieke rechtshandeling. Dit betekent dat de bepalingen uit de Cbw over de zorgplicht, governance en de meldplicht niet van toepassing zijn op financiële entiteiten die onder de verordening vallen, voor zover zij niet tevens kwalificeren als ander soort entiteit onder de Cbw. Dit geldt vanzelfsprekend ook voor de uitwerking van de hiervoor genoemde verplichtingen in het Cbb. Wel regelt het Cbb de dubbele meldplicht voor banken, handelsplatformen, centrale effectenbewaarinstellingen en centrale tegenpartijen. Deze instellingen melden bij zowel de toezichthouder als het CSIRT. Ook hierop houdt de relevante toezichthouder toezicht.

De verplichting uit artikel 44 Cbw (over het verstrekken van informatie ten behoeve van het nationale register) is wel van toepassing, voor zover deze entiteiten onder het toepassingsbereik van de Cbw vallen. De verplichtingen uit de artikelen 42 (over de aanwijzing van een vertegenwoordiger), 47 (over het verstrekken van informatie ten behoeve van het Enisa-register) en 49 (over een database met domeinnaamregistratiegegevens) Cbw zijn alleen van toepassing voor zover de betrokken financiële entiteit kwalificeert als één van de in die artikelen genoemde entiteiten en onder het toepassingsbereik van de Cbw valt.

Onder de Cbw is de Minister van Financiën aangewezen als bevoegde autoriteit voor entiteiten in de sectoren bankwezen en infrastructuur voor de financiële markt. Het Ministerie van Financiën acht het Cbb, waar het de taak als bevoegde autoriteit ten aanzien van financiële instellingen betreft, uitvoerbaar en handhaafbaar.

4.10.4 Ministerie van Infrastructuur en Waterstaat

Door de Inspectie voor Leefomgeving en Transport (hierna: ILT) en de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (hierna: ANVS) is het Cbb beoordeeld op handhaafbaarheid, uitvoerbaarheid en fraudebestendigheid.

De ILT oordeelt dat het Cbb op hoofdlijnen handhaafbaar, uitvoerbaar en fraudebestendig is. Daarbij wordt wel aandacht gevraagd voor de consequentie van de overlap tussen sectoren. Daarnaast geeft de ILT aan dat de uitvoerbaarheid samenhangt met de krapte op de arbeidsmarkt voor gekwalificeerde inspecteurs.

[8] Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (*PbEU* 2022, L 333).

De ANVS merkt op dat nog enkele relevante aspecten onduidelijk zijn, zoals de wijze waarop de (nucleaire) sector zal worden aangewezen. De ANVS geeft aan nog niet te beschikken over bestuurlijke boetes als handhavingsinstrument. Daarnaast vraagt de ANVS aandacht voor het belang dat haar huidige onafhankelijkheid in stand blijft, ook als zij er op grond van de Wwke toezichthoudende taken zou bij krijgen. Het Ministerie van Infrastructuur en Waterstaat houdt bij de verdere uitwerking van de ministeriële regeling nadrukkelijk rekening met deze punten.

4.10.5 Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur

Een concept van het Cbb is voorgelegd aan de Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA). Volgens de NVWA is het Cbb in potentie handhaafbaar, uitvoerbaar en fraudebestendig mits normen duidelijker zijn beschreven en de NVWA de juiste technische expertise in huis kan halen. Daarnaast moet vooraf duidelijk zijn welke bedrijven in Nederland onder het Cbb zullen vallen en zullen deze bedrijven geïnformeerd moeten worden over het Cbb. Ook zal samenwerking en informatie-uitwisseling tussen verschillende toezichthouders en de opdrachtgevers van de NVWA ingericht moeten zijn.

4.10.6 Ministerie van Volksgezondheid, Welzijn en Sport

Een concept van het Cbb is voorgelegd aan de Inspectie Gezondheidszorg en Jeugd (hierna: IGJ). De IGJ stelt dat het Cbb op enkele punten aanscherping behoeft. Zo ziet de IGJ dat enkele artikelen van het Cbb bepalingen bevatten die (tekstueel en inhoudelijk) afwijken van de normen voor informatiebeveiliging in de zorgsector. Dit zal tot verwarring leiden bij zorgaanbieders die op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) al wettelijk verplicht zijn te voldoen aan de NEN7510. Er ontstaan daarnaast nieuwe Nederlandse regels die afwijken van gangbare internationale normen, voor entiteiten die internationaal werken (zoals fabrikanten van medische hulpmiddelen). Volgens de IGJ leidt dit tot extra regeldruk. Het Ministerie van Volksgezondheid, Welzijn en Sport zal bij de sectorale invulling van de zorgplicht rekening houden met de door de IGJ genoemde aandachtspunten en waar mogelijk tegemoet komen aan de gangbare normen binnen de zorgsector.

Daarnaast verzoekt de IGJ om artikel 25 Cbb uit te breiden door entiteiten te vragen om extra informatie aan te leveren, zodat de significantie van incidenten beter beoordeeld kan worden. Naar aanleiding hiervan is artikel 25 Cbb uitgebreid.

5. Overgangsrecht en inwerkingtreding

Het Cbb voorziet niet in overgangsrecht.

Met betrekking tot de inwerkingtreding van het Cbb is in artikel 36 Cbb bepaald dat het Cbb in werking treedt op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld. Op grond van dit artikel kan worden gekozen voor een gefaseerde inwerkingtreding. Dit is denkbaar in het geval dat bepaalde onderdelen van het Cbb nog niet in werking kunnen treden, terwijl dat bij andere onderdelen van het Cbb wel het geval is. De verwachting is dat bij de inwerkingtreding van (onderdelen van) het Cbb een uitzondering wordt gemaakt op de vaste verandermomenten en de minimuminvoeringstermijn, omdat het Cbb strekt tot de uitvoering van de Cbw en de Cbw ziet op de implementatie van een bindende EU-rechtshandeling.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1 (begripsbepaling)

Artikel 1 Cbb bevat de definitie van enkele begrippen uit het Cbb. Zo wordt, daar waar in het Cbb "de wet" wordt genoemd, daaronder verstaan: de Cbw.

Het Cbb bevat ook andere begrippen, zoals "risico" en "incident", die ook voorkomen in de Cbw en al in artikel 1 Cbw zijn gedefinieerd. De in artikel 1 Cbw opgenomen definitie van die begrippen geldt ook als de definitie van diezelfde begrippen in het Cbb. In artikel 1 Cbw is namelijk bepaald dat de daarin opgenomen definities gelden voor de begrippen in de Cbw én in de daarop berustende bepalingen. Bij het Cbb is sprake van dat laatste; de bepalingen uit het Cbb berusten immers op de Cbw.

Artikel 2 (aanwijzing CSIRT)

In artikel 2, eerste lid, Cbb wordt de Minister van Justitie en Veiligheid voor essentiële entiteiten en belangrijke entiteiten aangewezen als het CSIRT. In afwijking daarvan kan op grond van artikel 2, tweede lid, Cbb voor essentiële entiteiten en belangrijke entiteiten uit specifieke sectoren en subsectoren, voor specifieke soorten entiteiten en voor specifieke entiteiten een andere instantie als CSIRT worden aangewezen.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Economische Zaken, de Minister van Financiën, de Minister van Infrastructuur en Waterstaat, de Minister van Klimaat en Groene Groei en de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur hebben in samenspraak met de Minister van Justitie en Veiligheid besloten de CSIRT-taak te beleggen bij de Minister van Justitie en Veiligheid voor de sectoren waar zij politiek verantwoordelijk voor zijn. De taken die de Minister van Justitie en Veiligheid als CSIRT op grond van de Cbw moet verrichten zullen in de praktijk worden uitgevoerd door het NCSC. Voor de aanwijzing van de Minister van Justitie en Veiligheid is, in samenspraak met de andere betrokken departementen, reden gezien vanwege diens coördinerende verantwoordelijkheid voor cybersecurity.

Op grond van artikel 2, tweede lid, Cbb kan bij regeling van de betrokken vakminister, na overleg met de Minister van Justitie en Veiligheid, voor entiteiten uit specifieke sectoren en subsectoren, voor specifieke soorten entiteiten en voor specifieke entiteiten een andere instantie dan de Minister van Justitie en Veiligheid als CSIRT worden aangewezen. De reden daarvoor kan bijvoorbeeld zijn dat een dergelijke andere instantie beschikt over specifieke kennis met betrekking tot de beveiliging van netwerk- en informatiesystemen in een bepaalde sector en daarom meer aangewezen is om de rol van CSIRT ten aanzien van bepaalde essentiële entiteiten of belangrijke entiteiten in die sector te vervullen.

Inmiddels is besloten dat voor entiteiten in de zorgsector bij ministeriële regeling de Stichting Z-CERT, dat momenteel ook al als computercrisisteam voor deze sector fungeert, zal worden aangewezen. Ook is reeds besloten dat voor gemeenten bij ministeriële regeling de Informatiebeveiligingsdienst, onderdeel van VNG Realisatie B.V., die thans ook al computercrisisteam voor die entiteiten is, als CSIRT zal worden aangewezen. Voor beide instanties geldt dat hiertoe, naast bijvoorbeeld hun specifieke deskundigheid van cybersecurity in die sectoren, ook is besloten op basis van de vaststelling dat zij voldoen aan de eisen die artikel 11, eerste lid, NIS2-richtlijn aan een CSIRT stelt. Bovendien hebben zij een voldoende mate van volwassenheid. Het voornemen is voorts om voor de waterschappen het CERT Watermanagement (CERT-WM) aan te wijzen als het CSIRT, die nu nog een onderdeel is van de gemeenschappelijke regeling van waterschappen (Het Waterschapshuis).

Met het oog op het voorgaande wordt momenteel interdepartementaal beleid ontwikkeld ten behoeve van onder meer de onderlinge samenwerking tussen CSIRT's en het bevorderen van uniformiteit in hun taakuitoefening.

Artikel 3 (aanwijzing coördinator bekendmaking kwetsbaarheden)

In artikel 3 Cbb wordt de Minister van Justitie en Veiligheid aangewezen als de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden, bedoeld in artikel 17 Cbw. Die rol van coördinator zal in de praktijk worden uitgevoerd door het NCSC. Voor deze aanwijzing is gekozen, niet alleen omdat de Minister van Justitie en Veiligheid zoals hierboven toegelicht onder

artikel 2 Cbb voor de meeste essentiële entiteiten en belangrijke entiteiten als CSIRT wordt aangewezen, maar ook omdat het NCSC momenteel in de praktijk namens de Minister van Justitie en Veiligheid reeds een met de aanwijzing in dit artikel vergelijkbare rol vervult.

Artikel 4 (verhouding tot Uitvoeringsverordening (EU) 2024/2690)

In artikel 21, vijfde lid, NIS2-richtlijn is bepaald dat de Europese Commissie uiterlijk op 17 oktober 2024 uitvoeringshandelingen vaststelt met betrekking tot de technische en methodologische vereisten van de maatregelen die een aantal specifiek genoemde entiteiten in het kader van de zorgplicht ten minste moeten nemen. Die vereisten gelden onder meer voor DNS-dienstverleners, aanbieders van cloudcomputingdiensten en aanbieders van vertrouwensdiensten.

In artikel 23, elfde lid, NIS2-richtlijn is bepaald dat de Europese Commissie uiterlijk op 17 oktober 2024 uitvoeringshandelingen vaststelt waarin nader wordt gespecificeerd in welke gevallen een incident als significant wordt beschouwd als bedoeld in artikel 23, derde lid, NIS2-richtlijn. Deze regels gelden voor dezelfde entiteiten als de hiervoor genoemde uitvoeringshandelingen over de zorgplicht (waaronder DNS-dienstverleners, aanbieders van cloudcomputingdiensten en aanbieders van vertrouwensdiensten).

Ter uitvoering van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn heeft de Europese Commissie de Uitvoeringsverordening (EU) 2024/2690[9] (hierna: de uitvoeringsverordening) vastgesteld. De uitvoeringsverordening is op grond van artikel 16 van de uitvoeringsverordening rechtstreeks van toepassing; implementatie in nationale wet- en regelgeving hoeft niet plaats te vinden. Met de uitvoeringsverordening wordt voor de entiteiten waarop deze van toepassing is (waaronder DNS-dienstverleners, aanbieders van cloudcomputingdiensten en aanbieders van vertrouwensdiensten) in direct op hen van toepassing zijnde regelgeving uitwerking gegeven aan de maatregelen die zij in het kader van de zorgplicht moeten nemen en wordt nader gespecificeerd in welke gevallen voor hen een incident als significant wordt beschouwd. Gelet hierop kunnen de bepalingen in dit besluit, waarin dezelfde onderwerpen worden geregeld, niet van toepassing zijn op de entiteiten waarop de uitvoeringsverordening van toepassing is In artikel 4 Cbb is daarom uitdrukkelijk geregeld dat voor de hierin genoemde essentiële entiteiten en belangrijke entiteiten de artikelen 6 tot en met 17 en 19 Cbb buiten toepassing blijven. Deze artikelen blijven alleen buiten toepassing wanneer een entiteit uitsluitend van een soort is die onder de reikwijdte van de uitvoeringsverordening valt, als bedoeld in artikel 1 uitvoeringsverordening. Dan gelden de technische en methodologische vereisten van de maatregelen die zij in het kader van de zorgplicht ten minste moeten nemen en de nadere criteria voor het bepalen of er sprake is van een significant incident uit de uitvoeringsverordening. Op basis van de uitvoeringsverordening kunnen meerdere criteria voor het bepalen van een significant incident gelden als een entiteit van meerdere soorten is die binnen de reikwijdte van de uitvoeringsverordening vallen, bijvoorbeeld als aanbieder van een datacentrumdienst en aanbieder van cloudcomputingdiensten. Echter, indien een entiteit zowel van een soort als bedoeld in artikel 1 uitvoeringsverordening als een ander soort als bedoeld in bijlage 1 en 2 van de Cbw is, dan zijn zowel de zorgplicht- en meldplichtverplichtingen uit de uitvoeringsverordening als die bij of krachtens het Cbb van toepassing. Een voorbeeld hiervan is een entiteit die zowel een aanbieder van cloudcomputingdiensten als een aanbieder van internetknooppunten is. Deze entiteit heeft zowel nadere zorg- en meldplichtverplichtingen op grond van de uitvoeringsverordening, namelijk in haar hoedanigheid als aanbieder van cloudcomputerdiensten, als op grond van het Cbb in haar hoedanigheid van internetknooppunt. Belangrijk is om op te merken dat een entiteit in verschillende sectoren kan vallen en daardoor voor wat betreft de zorgplicht en de meldplicht zowel onder de uitvoeringsverordening, als onder het Cbb kan vallen in welk geval de entiteit aan beide dient te voldoen.

Artikel 5 (uitvoering van artikel 21 van de wet)

[9] 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).

In artikel 5 Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten in elk geval de maatregelen, bedoeld in de artikelen 6 tot en met 19 Cbb, moeten nemen, waarmee zij uitvoering geven aan de zorgplicht uit artikel 21 Cbw.

In de genoemde artikelen wordt gesproken over het vaststellen van beleid, processen, procedures en plannen. Processen en procedures werken het beleid uit, dat geldt ook voor plannen. Dit zijn losse maar nauw met elkaar verbonden elementen. Ten aanzien van het vaststellen van beleid wordt het volgende opgemerkt. Door beleid vast te stellen en beleid schriftelijk vast te leggen, kan de entiteit aantonen dat zij over de invulling van de te nemen maatregelen heeft nagedacht en welke invulling van de maatregelen passend en evenredig is. Dit kan in theorie betekenen dat er gezien de risico's op beperkte wijze invulling wordt gegeven aan de betreffende maatregel. Desalniettemin betekent dit wel dat er, wanneer dit in het Cbb vereist wordt, er altijd beleid dient te zijn.

De vraag op welke wijze invulling moet worden gegeven aan de maatregelen is afhankelijk van de risicoanalyse, bedoeld in artikel 7 Cbb, waaruit voortvloeit welke invulling van de maatregelen passend en evenredig is voor de betreffende entiteit. De uitkomsten van de risicoanalyse en daarmee de invulling van de genomen maatregelen zullen daarom per entiteit verschillen vanwege de specifieke en unieke kenmerken van iedere entiteit.

Artikel 6 (beleid over beveiliging van netwerk- en informatiesystemen)

In artikel 21, derde lid, onderdeel a, Cbw is bepaald dat essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht beleid moeten hebben over de beveiliging van de netwerk- en informatiesystemen, die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken.

In artikel 6, eerste lid, Cbb is opgenomen dat het hiervoor bedoelde beleid schriftelijk moet zijn vastgelegd en aantoonbaar moet worden toegepast. Het beleid formuleert de doelstellingen van de entiteit voor de beveiliging van de netwerk- en informatiesystemen, evenals de aanpak ervan en de organisatie-inrichting met bijhorende rollen, verantwoordelijkheden en bevoegdheden.

In artikel 6, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van dat beleid de rollen, verantwoordelijkheden en bevoegdheden in relatie tot de beveiliging van hun netwerk- en informatiesystemen vaststellen. Hiermee bewerkstelligt de entiteit dat alle rollen, verantwoordelijkheden en bevoegdheden met betrekking tot de beveiliging van haar netwerk- en informatiesystemen kenbaar zijn. Daarnaast worden conflicterende rollen zoveel als mogelijk gescheiden. Hiermee wordt bedoeld dat hierbij het principe van pas toe of leg uit geldt, waarbij de entiteit dient te kunnen onderbouwen waarom een conflicterende rol in een gegeven geval niet gescheiden kon worden en welke compenserende maatregelen getroffen zijn om bijkomende risico's te beheersen, zoals logging van handelingen en managementgoedkeuring.

In artikel 6, derde lid, Cbb is geregeld dat essentiële entiteiten en belangrijke entiteiten van hun personeel en andere binnen de entiteit werkzame personen moeten verlangen dat zij de beveiliging van hun netwerk- en informatiesystemen toepassen overeenkomstig het hiervoor bedoelde beleid. Het is aan de entiteit om bij haar personeel en andere binnen de entiteit werkzame personen af te dwingen dat het beleid in de praktijk ook daadwerkelijk wordt toegepast en om daarop toe te zien.

In artikel 6, vierde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten voor de beveiliging van hun netwerk- en informatiesystemen een managementsystematiek hanteren. Het is aan de entiteit zelf om te bepalen welke managementsystematiek voor hen passend is. Deze systematiek zorgt ervoor dat informatie over onder andere de beveiliging van netwerk- en informatiesystemen op basis van een *Plan-Do-Check-Act*-cyclus (PDCA) wordt vastgelegd en inzichtelijk, begrijpelijk en toegankelijk is. Daarmee kunnen afgewogen besluiten worden genomen over de beveiliging van de netwerk- en informatiesystemen en is het aantoonbaar welke maatregelen er zijn genomen of welk beleid is vastgesteld. Voorbeelden hiervan zijn een managementsysteem voor informatiebeveiliging (*Information Security Management Systeem*, ISMS) zoals de ISO27000-reeks of het *Cyber Security Management System* (CSMS) op basis van IEC62443.

Artikel 7 (beleid over risicomanagement)

In artikel 21, derde lid, onderdeel a, Cbw is bepaald dat essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht beleid moeten hebben over risicoanalyse. In artikel 7 Cbb wordt deze verplichting verder uitgewerkt.

In artikel 7, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten voor de beveiliging van hun netwerk- en informatiesystemen vastgesteld beleid hebben over risicomanagement. De entiteit moet het hiervoor bedoelde beleid schriftelijk vastleggen en aantoonbaar toepassen.

Er is ervoor gekozen om risicomanagement als terminologie te hanteren in plaats van het begrip risicoanalyse, zoals dat in de Cbw staat opgenomen, omdat dit een meer gangbare term is en het gehele proces van risicobeheersing, inclusief risicoanalyse, omvat. Het doel van risicomanagement is om risico's voor de entiteit in kaart te brengen en deze vervolgens te beheersen. Onder risicomanagement wordt het geheel aan processen en procedures voor de beheersing van risico's van de entiteit verstaan. De entiteit houdt bij het in kaart brengen van de risico's rekening met de dreigingen, kwetsbaarheden en afhankelijkheden ten aanzien van de te beschermen belangen van de entiteit.

Artikel 7, tweede lid, Cbb vereist onder meer dat het beleid, bedoeld in het eerste lid, een risicomanagementmethodiek omvat. Het doel van een risicomanagementmethodiek is om op gestructureerde wijze risico's te identificeren en te beheersen. Deze bepaling vereist eveneens criteria voor risicoacceptatie.

Artikel 7, derde lid, Cbb, bepaalt dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vaststelt voor risicoanalyse, risicobeoordeling en risicobehandeling. Ook dient de entiteit deze processen en procedures aantoonbaar toe te passen.
Bij de risicoanalyse wordt een *all hazard*-benadering gebruikt waarbij de te beschermen belangen met betrekking tot de beveiliging van de netwerk- en informatiesystemen in kaart worden gebracht. Een te beschermen belang is datgene wat belangrijk is voor de netwerk- en informatiesystemen van de entiteit om goed te kunnen functioneren en om de continuïteit van haar dienstverlening te borgen. Denk hierbij aan personen, informatie, informatiesystemen, materieel, goederen, imago en objecten, waarbij in geval van compromittering of uitval van voorgenoemde, of de mogelijkheid van compromittering of uitval ervan, nadelige gevolgen kunnen hebben op het functioneren van de netwerk- en informatiesystemen van de entiteit en daarmee haar dienstverlening.
In de risicoanalyse kunnen de risico's tegen elkaar afgewogen worden. Zo kan verdere digitalisering van de entiteit bekende risico's doen afnemen ten koste van nieuwe risico's. Dit kan worden afgewogen in de bredere context van de entiteit zoals: organisatiedoelen, operationele activiteiten, technische- of financiële beperkingen of relaties met leveranciers of dienstverleners. Risico's met betrekking tot de beveiliging van de netwerk- en informatiesystemen kunnen daarnaast niet los gezien worden van alle andere risico's waar de entiteit aan bloot gesteld wordt. Daarom behoort het beheersen van de risico's met betrekking tot de beveiliging van de netwerk- en informatiesystemen een onderdeel van het bredere risicobeheerproces van de entiteit te zijn. De risicoanalyse die op basis van de Cbw moeten worden gedaan kan een onderdeel zijn van een grotere of gecombineerde risicoanalyse. Dit betekent concreet dat er een integrale risicoanalyse plaats kan vinden voor bijvoorbeeld de Wwke en de Cbw, mits alle relevante elementen van de betreffende regelgeving worden meegenomen in de risicoanalyse.

Artikel 7, vierde lid, Cbb, schrijft voor dat essentiële entiteiten en belangrijke entiteiten op basis van de uitgevoerde risicoanalyse een overzicht moeten vaststellen van de risico's met betrekking tot de beveiliging van hun netwerk- en informatiesystemen. Het doel van dit overzicht is om een goede afweging te kunnen maken voor de beheersing van de risico's.

Artikel 7, vijfde lid, Cbb, vereist dat essentiële entiteiten en belangrijke entiteiten op basis van het overzicht van de risico's, bedoeld in het derde lid, eisen met betrekking tot de beveiliging van hun netwerk- en informatiesystemen formuleren. Deze beveiligingseisen moet de entiteit, waar mogelijk, gebruiken bij het uitvoering geven aan de in de artikelen 10, tweede lid, en 11, eerste lid, Cbb voorgeschreven maatregelen.

Artikel 8 (incidentenbehandeling)

In artikel 21, derde lid, onderdeel b, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval incidentenbehandeling moeten omvatten. In artikel 8 Cbb wordt deze verplichting verder uitgewerkt.

In artikel 8, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten vastgesteld beleid moeten hebben over incidentenbehandeling. Dat beleid moet schriftelijk zijn vastgelegd en aantoonbaar worden toegepast.

Artikel 8, tweede lid, Cbb, bepaalt dat essentiële entiteiten en belangrijke entiteiten, in het kader van de toepassing van het beleid, bedoeld in het eerste lid, de rollen, verantwoordelijkheden, bevoegdheden vaststellen voor het tijdig detecteren van, analyseren en beoordelen van, reageren op, beperken van de gevolgen van, wegnemen van de oorzaak van, herstellen van, documenteren van, rapporteren van en leren van incidenten. Het doel van deze bepaling is dat het gehele proces en uitvoering van processen en procedures van incidentbehandeling, zoals beschreven in artikel 8, vierde lid, Cbb helder is belegd binnen de organisatie, zodat daar in de praktijk goede uitvoering aan gegeven kan worden.

Artikel 8, derde lid, Cbb schrijft voor dat essentiële entiteiten en belangrijke entiteiten, in het kader van de toepassing van het beleid, processen en procedures moeten vaststellen om relevante gebeurtenissen in hun netwerk- en informatiesystemen te monitoren en te registreren. Ook dient de entiteit deze processen en procedures aantoonbaar toe te passen. Die processen en procedures zijn bedoeld om incidenten te detecteren, analyseren en classificeren. Met relevante gebeurtenissen wordt in elk geval gedoeld op alle gebeurtenissen die de beveiliging van de netwerk- en informatiesystemen van de entiteit in gevaar brengen of kunnen brengen. Hierbij wordt opgemerkt dat de monitoring extern kan worden uitbesteed. Het is ook mogelijk dat de monitoring plaatsvindt door een andere vestiging van de entiteit die zich in het buitenland bevindt.

Artikel 8, vierde lid, Cbb schrijft voor dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast moeten stellen voor het tijdig detecteren van, analyseren en beoordelen van, reageren op, beperken van de gevolgen van, wegnemen van de oorzaak van, herstellen van, documenteren van, rapporteren van en leren van een incident. Deze processen en procedures hebben het doel om snel te kunnen handelen wanneer een incident zich voordoet, zodat de impact zoveel mogelijk beperkt kan worden. Artikel 8, vijfde lid, Cbb schrijft voor dat de hiervoor bedoelde processen en procedures aantoonbaar moeten worden toegepast.

Artikel 8, zesde lid, Cbb ziet op het loggen van relevante gebeurtenissen in de netwerk- en informatiesystemen die relevant zijn voor de beveiliging van de netwerk- en informatiesystemen, voor zover logging mogelijk is. Hierbij wordt opgemerkt dat de logging extern kan worden uitbesteed. Logging is belangrijk, omdat het onder meer monitoring en detectie mogelijk maakt, waarmee essentiële entiteiten en belangrijke entiteiten opvolging kunnen geven aan de bevindingen die hieruit voortkomen. De entiteit kan onder meer op basis van geïdentificeerde risico's, bedoeld in artikel 7 Cbb, bepalen welke gegevens worden gelogd, hoelang deze moeten worden bijgehouden en welke loggegevens moeten worden beschermd tegen ongeautoriseerde toegang of wijzigingen. De periode voor het bijhouden van logbestanden dient in verhouding te staan tot de aard van de risico's waaraan de entiteit is blootgesteld, alsmede tot de tijd die doorgaans verstrijkt tussen het plaatsvinden van een incident en de ontdekking ervan.

Artikel 9 (bedrijfscontinuïteit en crisisbeheer)

In artikel 21, derde lid, onderdeel c, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval bedrijfscontinuïteit en crisisbeheer moet omvatten. In artikel 9 Cbb wordt deze verplichting verder uitgewerkt.

Artikel 9, eerste lid, Cbb bepaalt dat essentiële entiteiten en belangrijke entiteiten bedrijfscontinuïteitsbeleid moeten hebben vastgesteld. Dat beleid moet schriftelijk zijn vastgelegd en aantoonbaar worden toegepast.

In artikel 9, tweede lid, Cbb is opgenomen dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures moeten vaststellen voor het borgen van hun bedrijfscontinuïteit, waaronder in ieder geval processen en procedures voor het herstellen van hun netwerk- en informatiesystemen en voor het maken en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens. Dit moeten zij doen om een passend niveau van vertrouwelijkheid, beschikbaarheid en integriteit van hun netwerk- en informatiesystemen te borgen. Hierbij is het in het bijzonder van belang dat de entiteit processen en procedures vaststelt voor incidenten als gevolg waarvan back-ups, al dan niet door acties van kwaadwillende, onbruikbaar worden. Ook de betrouwbaarheid van back-ups dient gewaarborgd te worden, om zo ongeautoriseerde wijziging van gegevens te voorkomen. Een voorbeeld hiervan is een ransomware-aanval. De hiervoor bedoelde processen en procedures moeten aantoonbaar worden toegepast en periodiek worden getest.

Artikel 9, derde lid, Cbb schrijft voor dat essentiële entiteiten en belangrijke entiteiten een vastgesteld bedrijfscontinuïteitsplan met betrekking tot haar netwerk- en informatiesystemen moeten hebben. Dit plan moet schriftelijk zijn vastgesteld, aantoonbaar worden toegepast en periodiek worden getest. Op deze wijze kunnen zij controleren of het plan nog steeds werkt en actueel is. De entiteit bepaalt zelf de vorm van het testen. Te denken valt bijvoorbeeld aan een *tabletop exercise*. De periode hangt af van de uitkomsten van de risicoanalyse. Het bedrijfscontinuïteitsplan kan ook paragrafen bevatten die voortvloeien uit eisen die andere wet- en regelgeving naast de Cbw stellen aan bedrijfscontinuïteit.
Indien een incident zich voordoet die de bedrijfscontinuïteit in gevaar kan brengen moet het bedrijfscontinuïteitsplan door de entiteit worden toegepast. Dit plan richt zich op het minimaliseren van de impact van een incident op de dienstverlening en het zo spoedig mogelijk herstellen en hervatten van de dienstverlening. Bij het opstellen van het plan houdt de entiteit rekening met de geïdentificeerde risico's, bedoeld in artikel 7 Cbb.
Het is aan de entiteit zelf om een afweging te maken welke processen en procedures moeten worden beschreven in het bedrijfscontinuïteitsplan. Dit hangt af van meerdere factoren. Het is bijvoorbeeld denkbaar dat bij kleinere entiteiten een bellijst volstaat met IT-leveranciers en een overzicht van de met hen gemaakte afspraken over het herstellen van de netwerk- en informatiesystemen in geval van een incident. Bij grotere entiteiten of entiteiten met een complexe IT is een uitgebreider plan vereist, waarin een verdeling van rollen, verantwoordelijkheden en bevoegdheden van betrokkenen binnen en buiten de entiteit is opgenomen. Hierbij dient aansluiting gezocht te worden bij de specifieke inrichting van de netwerk- en informatiesystemen van de betreffende entiteit en de daaruit voorvloeiende risico's op het gebied van bedrijfscontinuïteit.

In artikel 9, vierde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten een herstelplan moeten hebben. Herstelplannen staan ook wel bekend als een "Disaster Recovery Plan" en maken in de regel onderdeel uit van een bedrijfscontinuïteitsplan. In het herstelplan is vastgelegd in welke gevallen dit plan moet worden toegepast. De entiteit legt dat plan schriftelijk vast, past dat plan toe in geval van een incident en test dit plan periodiek. Het doel van het herstelplan is dat de entiteit voorbereid is om specifieke netwerk- en informatiesystemen te kunnen herstellen na een incident en daarvoor alle benodigdheden in kaart heeft gebracht, evenals de stappen die doorlopen dienen te worden. In de praktijk kan de entiteit meerdere herstelplannen hebben en kunnen deze ook de vorm van een uitwijk- en herstelplan hebben, waarbij van een uitwijklocatie gebruik wordt gemaakt om de impact van een incident te beperken.

In artikel 9, vijfde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten een plan voor crisisbeheer moeten hebben. Een crisis is een buitengewone situatie die de voortzetting van de dienstverlening of werkzaamheden van een entiteit bedreigt dat niet kan worden opgelost binnen de bestaande structuren van een entiteit. Hierbij kan gedacht worden aan een plan dat voldoet aan de ISO22361. Daarin moeten in elk geval de rollen, verantwoordelijkheden en bevoegdheden ten tijde van een crisis voor het personeel en andere in de entiteit werkzame personen worden beschreven. Dit maakt de tijdige en adequate inzet in crisissituaties mogelijk. Het plan moet ook de communicatiemiddelen ten tijde van een crisis beschrijven. Wanneer passend moet het plan ook de beschikbare noodvoorzieningen beschrijven, waaronder het gebruik van beveiligde noodcommunicatiesystemen. Dit is bijvoorbeeld het geval wanneer een entiteit voor een goede crisisbeheersing ook bij uitval van algemene telecommunicatienetwerken moet kunnen communiceren met medewerkers op verschillende locaties. Noodvoorzieningen zijn voorzieningen die permanent aanwezig of beschikbaar zijn, maar slechts in noodsituaties gebruikt zal worden. Bij noodvoorzieningen kan gedacht worden aan uitwijklocaties, noodstroomvoorzieningen en dergelijke. Van belang is dat de entiteit het plan voor crisisbeheer periodiek test en beoefent,

zodat ten tijde van een crisis alle betrokkenen bekend zijn met hun rollen, verantwoordelijkheden en bevoegdheden.

Hierbij wordt opgemerkt dat het kan gaan om één gecombineerd plan met paragrafen over bedrijfscontinuïteit en noodvoorzieningen, maar dat het ook kan gaan om losstaande plannen. Het is van belang dat wanneer sprake is van verschillende plannen deze integraal op elkaar zijn afgestemd om tegenstrijdige procedures bij incidenten te voorkomen en als samenhangend worden toepast binnen het bedrijfscontinuïteitsmanagementsysteem. Het bedrijfscontinuïteitsplan beschrijft hoe de entiteit haar dienstverlening zo snel mogelijk kan hervatten bij verstoringen en de impact kan beperken. Het herstelplan bevat concrete maatregelen voor het herstel van systemen en gegevens. Het crisisplan regelt de inzet en coördinatie in geval van een crisis, waaronder de verantwoordelijkheden, communicatie en inzet van noodvoorzieningen.

Artikel 10 (beveiliging van de toeleveringsketen)

In artikel 21, derde lid, onderdeel d, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval de beveiliging van de toeleveringsketen moeten omvatten. In artikel 10 Cbb wordt deze verplichting verder uitgewerkt. Hierbij wordt opgemerkt dat de genoemde verplichtingen in artikel 10 Cbb uitsluitend zien op aspecten van de toeleveringsketen die relevant zijn voor de beveiliging van de netwerk- en informatiesystemen die de entiteit gebruikt voor haar werkzaamheden of die zij voor het verlenen van haar diensten gebruikt. De relatie met een leverancier van potloden zal bijvoorbeeld buiten de reikwijdte van de verplichtingen vallen, omdat het leveren van potloden geen verband houdt met de beveiliging van de eerdergenoemde netwerk- en informatiesystemen die de entiteit gebruikt voor haar werkzaamheden of het verlenen van haar diensten. De relatie met bijvoorbeeld een softwareleverancier of leverancier van hardware-onderdelen die relevant zijn voor het goed functioneren van de netwerk- en informatiesystemen, valt wel binnen de reikwijdte.

In artikel 10, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten vastgesteld beleid moeten hebben over de beveiliging van de toeleveringsketen. De entiteit moet in dat beleid haar omgang bepalen met afhankelijkheden van de producten en diensten van haar leveranciers en dienstverleners die invloed kunnen hebben op de beveiliging van haar netwerk- en informatiesystemen. Het beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast.

In artikel 10, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten toetsen of hun rechtstreekse leveranciers en rechtstreekse dienstverleners, bedoeld in artikel 10, eerste lid, Cbb voldoen aan hun beveiligingseisen, bedoeld in artikel 7, vijfde lid, Cbb. De entiteit kan dit bijvoorbeeld beoordelen door certificering van de toeleveranciers of clausules in leveringsovereenkomsten. De entiteit zal op basis van haar cyberbeveiligingseisen periodiek moeten beoordelen of haar rechtstreekse leverancier of haar rechtstreekse dienstverlener nog steeds voldoet aan de beveiligingseisen. Wanneer dit niet het geval is moet de entiteit beoordelen of er aanvullende maatregelen getroffen kunnen worden om de risico's te mitigeren. Gedacht kan worden aan het heronderhandelen van contracten, het afsluiten van een aanvullend contract of het overstappen naar een andere leverancier of dienstverlener.

Artikel 11 (beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen)

In artikel 21, derde lid, onderdeel e, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen moeten omvatten. In artikel 11 Cbb wordt deze verplichting verder uitgewerkt.

In artikel 11, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten op basis van de beveiligingseisen, bedoeld in artikel 7, vijfde lid, Cbb vastgesteld beleid moeten hebben voor het mitigeren en beheersen van risico's die voortvloeien uit het verwerven van software, hardware of diensten die betrekking hebben op hun netwerk- en informatiesystemen. Deze eisen gelden ook wanneer de entiteit de netwerk- en informatiesystemen zelf ontwikkelt. Het beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast.

In artikel 11, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten, indien van toepassing, processen en procedures moeten vaststellen voor de veilige ontwikkeling van hun

netwerk- en informatiesystemen. Deze bepaling is van toepassing indien de betreffende entiteit zelf netwerk- en informatiesystemen ontwikkelt of deze laat ontwikkelen. Deze processen en procedures moeten aantoonbaar worden toegepast. Deze processen en procedures hebben betrekking op alle ontwikkelingsfasen van de netwerk- en informatiesystemen. Die fasen betreffen in ieder geval specificatie, ontwerp, implementatie, en doorontwikkeling en testen. Het uitgangspunt is dat de entiteit de *security by design*- of *security by default*-principes hanteert bij de ontwikkeling en implementatie van software, hardware en diensten, zodat al tijdens deze fases rekening wordt gehouden met beveiligingsmaatregelen. Hierbij wordt tevens opgemerkt dat deze activiteiten extern kunnen worden uitbesteed. Hierbij gaat het om activiteiten die direct impact hebben op de netwerk- en informatiesystemen.

In artikel 11, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten processen en procedures moeten vaststellen voor het onderhoud en beheer van hun netwerk- en informatiesystemen. Het onderhoud en beheer kan worden uitbesteed. De hiervoor bedoelde processen en procedures moeten ten minste betrekking hebben op het configuratiebeheer. Configuratiebeheer is het beheer van de inrichting van software en hardware en hun onderlinge verbindingen. Daaronder valt in elk geval een veilige configuratie van software, hardware en diensten. De hiervoor bedoelde processen en procedures moeten ook ten minste betrekking hebben op het wijzigingsbeheer van de netwerk- en informatiesystemen, zodat de entiteit op gecontroleerde wijze wijzigingen in haar netwerk- en informatiesystemen doorvoert. Ook ten aanzien van deze processen en procedures geldt dat deze aantoonbaar moeten worden toegepast.

Artikel 12 (basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging)

In artikel 21, derde lid, onderdeel g, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging moeten omvatten. In artikel 12 Cbb wordt deze verplichting verder uitgewerkt. Hierbij gaat het om al het personeel dus ook die worden ingehuurd.

In artikel 12, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten ervoor moeten zorgen dat hun personeel en andere binnen de entiteit werkzame personen, voor zover relevant voor hun functie, bewust zijn van risico's met betrekking tot de netwerk- en informatiesystemen van de entiteit, op de hoogte zijn van het belang van cyberbeveiliging en praktijken op het gebied van cyberhygiëne toepassen. Cyberhygiëne omvat een gemeenschappelijke basisreeks van praktijken, met inbegrip van software- en hardware-updates, het wijzigen van wachtwoorden, het beheer van nieuwe installaties, de beperking van toegangsaccounts op beheersniveau en het maken van back-ups van gegevens. Hierdoor is een proactief kader mogelijk met betrekking tot paraatheid, algemene veiligheid en beveiliging in geval van incidenten of cyberdreigingen. Om de cyberhygiëne bij haar personeel en andere binnen de entiteit werkzame personen te borgen kan de entiteit bijvoorbeeld denken aan het verzorgen van bewustwordings- en trainingsactiviteiten, voor zover relevant voor de functie.

In artikel 12, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten het personeel en andere binnen de entiteit werkzame personen waarvan de rollen, verantwoordelijkheden en bevoegdheden vaardigheden en deskundigheid vereisen op het gebied van de beveiliging van netwerk- en informatiesystemen, moeten aanwijzen. Zij dienen regelmatig opleiding te krijgen over de beveiliging van netwerk- en informatiesystemen, passend bij hun functie. Deze opleidingen kunnen bijvoorbeeld betrekking hebben op de werking en beveiliging van netwerk- en informatiesystemen, bekende dreigingen of werkwijzen van kwaadwillende en incidentbehandeling. Met die opleidingen wordt voor het betreffende personeel de benodigde kennis en kunde over de beveiliging van netwerk- en informatiesystemen ook steeds actueel gehouden. Afhankelijk van de functie zal er een zwaardere of minder zwaardere opleiding gevolgd moeten worden. Hierbij wordt opgemerkt dat met de term opleiding ook een training of cursus wordt bedoeld.

Artikel 13 (beleid over het gebruik van cryptografie)

In artikel 21, derde lid, onderdeel h, Cbw is bepaald dat essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht beleid en procedures moeten hebben over het gebruik van cryptografie. In artikel 13 Cbb wordt deze verplichting verder uitgewerkt.

In artikel 13, eerste lid, Cbb wordt bepaald dat essentiële entiteiten en belangrijke entiteiten vastgesteld beleid hebben over het gebruik van cryptografie. Dat beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast. Cryptografie is het geheel van methoden voor het versleutelen en beveiligen van gegevens. Het doel van cryptografie en bijbehorend beleid is om te voorkomen dat ongeautoriseerde gebruikers toegang hebben tot de data van de entiteit of dat de integriteit van de data wordt aangetast. Door middel van cryptografie kan de data voor ongeautoriseerde gebruikers onleesbaar gemaakt worden en kunnen ongeautoriseerde wijzigingen worden vastgesteld. De cryptografie kan door bijvoorbeeld zwaktes in algoritmes, implementatiefouten of de komst van quantumcomputers toch doorbroken worden. Daarom moeten cryptografische middelen met minimale inspanning gewijzigd kunnen worden (cryptografische behendigheid). De vereiste mate van cryptografische behendigheid is afhankelijk van de geïdentificeerde risico's, bedoeld in artikel 7 Cbb.

Artikel 13, tweede lid, Cbb, schrijft voor dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van het beleid, bedoeld in artikel 13, eerste lid, Cbb processen en procedures vaststellen over het gebruik van cryptografie. De entiteit past deze processen en procedures aantoonbaar toe.

In artikel 13, derde lid, Cbb is bepaald dat in het hiervoor bedoelde beleid en processen en procedures in ieder geval is uitgewerkt in welke gevallen cryptografie wordt ingezet en welke type encryptie in voorkomende gevallen worden gebruikt. Daarbij kan onderscheid per toepassingsgebied worden gemaakt, bijvoorbeeld voor opgeslagen gegevens en gegevens die worden verzonden, evenals per categorie van gegevens. Ook moet in het beleid inzichtelijk worden gemaakt wie verantwoordelijk is voor de implementatie van cryptografie en wie binnen de entiteit verantwoordelijk is voor het sleutelbeheer. Door deze rollen, verantwoordelijkheden en bevoegdheden inzichtelijk te maken bewerkstelligt de entiteit dat iedereen in de organisatie op de hoogte is van zijn of haar specifieke rollen, verantwoordelijkheden en bevoegdheden met betrekking tot encryptie. Hierdoor wordt de kans op misverstanden, misbruik en nalatigheid verminderd.

Artikel 14 (beveiligingsaspecten ten aanzien van personeel)

In artikel 21, derde lid, onderdeel i, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets moeten omvatten. In artikel 14 Cbb wordt deze verplichting verder uitgewerkt, specifiek over de beveiligingsaspecten ten aanzien van het personeel. Het gaat daarbij om personeel dat daadwerkelijk in verband met haar functie de beveiliging van de netwerk- en informatiesystemen kan beïnvloeden.

In artikel 14, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten het personeel en andere binnen de entiteit werkzame personen aanwijzen dat wordt belast met rollen, verantwoordelijkheden en bevoegdheden met betrekking tot de beveiliging van hun netwerk- en informatiesystemen. Dit artikel houdt verband met artikel 6, tweede lid, Cbb, waarin is bepaald dat de entiteit de rollen, verantwoordelijkheden en bevoegdheden in relatie tot de beveiliging van haar netwerk- en informatiesystemen heeft vastgelegd. Doordat de entiteit in artikel 14, eerste lid, Cbb bepaalt en vastlegt wie binnen de entiteit in relatie tot de beveiliging van de netwerk- en informatiesystemen verantwoordelijk is, is er altijd een eigenaar van het systeem en wordt voorkomen dat de netwerk- en informatiesystemen onvoldoende beveiligd worden.

De hiervoor bedoelde aanwijzing moet op grond van artikel 14, tweede lid, Cbb periodiek worden geëvalueerd en indien nodig bijgewerkt. Het doel van de evaluatie is om na te gaan of de aanwijzing nog passend is en in lijn is met de rollen, verantwoordelijkheden en bevoegdheden in de praktijk.

In artikel 14, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten indien dit blijkt uit de risicoanalyse, bedoeld in artikel 7 Cbb, betrouwbaarheidseisen moeten opstellen waaraan hun personeel en andere binnen of namens de entiteit werkzame personen moeten voldoen, voor zover deze passend en noodzakelijk zijn voor hun taakuitoefening met betrekking tot de beveiliging van de netwerk- en informatiesystemen van de entiteit. Voor bepaalde functionarissen kan dit betekenen dat er een screening plaatsvindt. Hierbij valt onder meer te denken aan functionarissen met hoge rechten in kritieke omgevingen van de netwerk- en informatiesystemen van de entiteit.

Artikel 15 (beveiligingsaspecten ten aanzien van toegangsbeleid)

In artikel 21, derde lid, onderdeel i, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets moeten omvatten. In artikel 15 Cbb wordt deze verplichting verder uitgewerkt, specifiek over de beveiligingsaspecten ten aanzien van toegangsbeleid.

In artikel 15, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten vastgesteld beleid moeten hebben over de logische en fysieke toegang (*access management*) tot hun netwerk- en informatiesystemen. Dat beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast. Logische toegang houdt het beheersen van de toegang tot de netwerk- en informatiesystemen in en vereist de authenticatie van de identiteit van een individu via een mechanisme, zoals een toegangspas, token of cijfercode. Met fysieke toegang wordt bedoeld: de directe fysieke toegang tot de netwerk- en informatiesystemen. Het doel van het genoemde beleid is om ongeautoriseerde logische en fysieke toegang tot de netwerk- en informatiesystemen van de entiteit te voorkomen. Het uitgangspunt is dat de entiteit daarbij de *need-to-know*- en *least-privilege*-principes hanteert. Dit betekent dat alleen toegang wordt verkregen tot informatie en ruimtes die passen bij de functie, ongeacht beveiligingsmachtiging of andere goedkeuringen.

Op grond van artikel 15, tweede lid, Cbb moet het beleid in elk geval omvatten: het uitgeven, monitoren, gebruiken, wijzigen en intrekken van identiteiten en autorisaties, en het beheer van identiteiten en autorisaties. Deze aspecten worden voorgeschreven, zodat ongeautoriseerde toegang tot en wijzigingen in de netwerk- en informatiesystemen kunnen worden gedetecteerd en waar mogelijk worden voorkomen. Hierbij wordt opgemerkt dat de toegang ook extern kan worden uitbesteed. Het is ook mogelijk dat de monitoring plaatsvindt door een andere vestiging van de entiteit die zich in het buitenland bevindt.

In artikel 15, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten identiteiten, authenticatiemiddelen en autorisaties periodiek moeten controleren op de noodzakelijkheid, juistheid en actualiteit. Indien nodig voert de entiteit wijzigingen door in die identiteiten, authenticatiemiddelen en autorisaties. Door deze periodieke toets kan de toekenning van een identiteit of autorisatie tijdig worden aangepast, bijvoorbeeld als deze niet langer noodzakelijk is of (gewijzigde) risico's voor de beveiliging van de netwerk- en informatiesystemen hiertoe aanleiding geeft.

Artikel 16 (beveiligingsaspecten ten aanzien van beheer van assets)

In artikel 21, derde lid, onderdeel i, Cbw is bepaald dat de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen in elk geval beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets moeten omvatten. In artikel 16 Cbb wordt deze verplichting verder uitgewerkt, specifiek over de beveiligingsaspecten ten aanzien van het beheer van assets, in het bijzonder de netwerk- en informatiesystemen die essentiële en belangrijke entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken.

In artikel 16, eerste lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten vastgesteld beleid moeten hebben voor het beheer van hun assets die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken. Dat beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast. Het is van belang dat zij een dergelijk beleid hebben, omdat zij door een goed inzicht in hun assets hun risico's beter kunnen inschatten en gerichter informatie over kwetsbaarheden kunnen vinden.

In artikel 16, tweede lid, Cbb is bepaald dat het hiervoor bedoelde beleid in elk geval een systeem moet omvatten om assets op verschillende niveaus te kunnen classificeren op basis van, indien van toepassing, de eisen voor vertrouwelijkheid, integriteit en beschikbaarheid. Het beleid moet ook regels omvatten die aangeven wat er wel en niet mag met de assets (aanvaardbaar gebruik) Door assets te classificeren kunnen essentiële entiteiten en belangrijke entiteiten vaststellen welk beveiligingsniveau ten aanzien van hun netwerk- en informatiesystemen passend is. Dit is mede relevant in de context van de bedrijfscontinuïteit, bedoeld in artikel 9 Cbb, het toetsen of rechtstreekse leveranciers en rechtstreekse dienstverleners voldoen aan de beveiligingseisen,

bedoeld in artikel 10 Cbb, en de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, bedoeld in artikel 11 Cbb. Onder assets kan ook cryptografie worden verstaan. Denk hierbij aan cryptografische sleutels.

Artikel 16, derde lid, Cbb, schrijft voor dat essentiële entiteiten en belangrijke entiteiten in het kader van de toepassing van het beleid, bedoeld in artikel 16, eerste lid, Cbb, processen en procedures vaststellen voor het beheer van hun assets. De entiteit past deze processen en procedures aantoonbaar toe.

In artikel 16, vierde lid, Cbb, is bepaald dat essentiële entiteiten en belangrijke entiteiten een volledige en actuele inventaris van hun assets moeten hebben en deze inventaris moeten bijhouden. Deze inventaris dient voor de beveiliging van de netwerk- en informatiesystemen relevante registraties te bevatten, zoals de assets waar de entiteit over beschikt, inclusief digitale gegevens en software, evenals de locatie hiervan. Het abstractieniveau en de mate van gedetailleerdheid dient passend te zijn om de risico's voor de beveiliging van de netwerk- en informatiesystemen te kunnen beheersen.

Artikel 17 (attenderingen, adviezen en informatie)

Artikel 17 Cbb gaat over attenderingen, adviezen en informatie over kwetsbaarheden of cyberdreigingen die relevant zijn voor de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten en belangrijke entiteiten. Wanneer de entiteit deze attenderingen, adviezen en informatie gericht ontvangen, moet zij beoordelen of op basis daarvan aanpassingen of aanvullingen nodig zijn van de maatregelen die nodig zijn ter uitvoering van de zorgplicht. Het gaat hierbij om attenderingen en adviezen die gericht zijn aan de ICT-contactpersoon en niet generieke berichtgeving waar de doelgroep van de berichtgeving breder is dan de ICT-contactpersoon en ook niet enkel gericht is aan de specifieke entiteit. Een voorbeeld van specifieke adviezen en attenderingen zijn *high-high*-attenderingen van een CSIRT. Het is denkbaar dat adviezen niet altijd (direct) overgenomen worden wanneer de gevolgen van het opvolgen schadelijker zijn dan de gevolgen van de kwetsbaarheid zelf.

Artikel 18 (weren producten en diensten van leveranciers)

Inleidende opmerkingen

Nederland wordt steeds vaker geconfronteerd met cyberaanvallen op (al dan niet vitale) processen door statelijke en criminele actoren.[10] Naar verwachting zal de cyberdreiging de komende jaren aanhouden, omdat het relatief makkelijk is om een digitaal aanvalsprogramma op te zetten. Dergelijke aanvallen zijn ook steeds moeilijker herleidbaar tot de aanvaller. De inlichtingen- en veiligheidsdiensten identificeren in hun meest recente jaarverslagen een sterke toename van het aantal landen dat offensieve cyberprogramma's ontwikkelt en inzet bij het nastreven van hun politieke doelstellingen. In het licht van de hiervoor bedoelde ontwikkelingen, aanvallen en dreigingen voorziet artikel 18, eerste lid, Cbb in de bevoegdheid van de betrokken vakminister om, in overeenstemming met de Minister van Justitie en Veiligheid, een essentiële entiteit of belangrijke entiteit de verplichting op te leggen om in onderdelen van haar netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren. Door de producten of diensten van specifieke leveranciers te weren kunnen de risico's, die voortvloeien uit de hiervoor bedoelde offensieve cyberprogramma's, worden beheerst.

Artikel 18, eerste lid, Cbb geeft een nadere uitwerking aan de algemene zorgplicht van artikel 21 Cbw en hiermee wordt onder meer geconcretiseerd dat deze zorgplicht in de in artikel 18, eerste lid, Cbb genoemde gevallen kan leiden tot eigendomsregulering.

Reikwijdte

De betrokken vakminister maakt gebruik van de in artikel 18, eerste lid, Cbb opgenomen bevoegdheid indien hij van oordeel is dat dit noodzakelijk is om risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen. Wat onder incident als bedoeld in artikel 18, eerste lid, Cbb wordt verstaan volgt uit artikel 1 Cbw. Hierin is bepaald dat een incident in de zin van de Cbw en onderliggende regelgeving een gebeurtenis is die de beschikbaarheid, authenticiteit,

[10] *Kamerstukken II* 2022/23, 26643, nr. 1007.

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.
Het zal bij het weren van de producten of diensten van specifieke leveranciers moeten gaan om leveranciers die zelf de intentie hebben om de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten en belangrijke entiteiten aan te tasten of om incidenten bij die entiteiten te veroorzaken, of leveranciers die nauwe banden hebben met of onder invloed van een dergelijke partij zijn. Van laatstbedoelde nauwe banden of invloed kan bijvoorbeeld sprake zijn indien de leverancier afkomstig is, of onder controle staat van een partij, uit een land met wetgeving die particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder staatsorganen die zijn belast met een inlichtingen- of militaire taak.

Ten aanzien van de entiteit zal moeten worden bepaald welke onderdelen van de netwerk- en informatiesystemen van de entiteit de verplichting zou moeten betreffen. Daarbij zal het gaan om onderdelen waarvoor geldt dat de toegang daartoe, vanwege de gevoeligheid van die onderdelen, in geval van misbruik een risico voor de nationale veiligheid oplevert.

De bevoegdheid uit artikel 18, eerste lid, Cbb kan niet worden toegepast op essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn. Dit is geregeld in artikel 18, derde lid, Cbb. De reden voor deze regeling is dat de Telecommunicatiewet en daaronder liggende regelgeving voor deze aanbieders al in een vergelijkbare regime voorziet.
Met artikel 18, derde lid, Cbb wordt voorkomen dat er een dubbele grondslag ontstaat ten aanzien van die aanbieders. Immers, op grond van artikel 11.a1, tweede lid, Telecommunicatiewet (zoals gewijzigd in artikel 99, onderdeel B, Cbw) is het al mogelijk om bij of krachtens amvb technische, operationele en organisatorische maatregelen vast te stellen, om de risico's voor de beveiliging van hun netwerken of diensten te beheersen, teneinde de gevolgen van beveiligingsincidenten op de nationale veiligheid of openbare orde te beperken. Met het oog op voortzetting van de huidige sectorale wetgeving bevat het nieuwe tweede lid van artikel 11a.1 Telecommunicatiewet een wettelijke grondslag die in materieel opzicht een ongewijzigde basis biedt voor het Besluit veiligheid en integriteit telecommunicatie (hierna: Bvit). De delegatiegrondslag voor het Bvit in artikel 11a.1, tweede lid, Telecommunicatiewet is net zoals voorheen – met artikel 11a.1, vierde lid, Telecommunicatiewet (oud) – gebaseerd op een benadering die alle gevaren omvat. De maatregelen kunnen dus onverminderd bijdragen aan de bescherming van veiligheidsbelangen in brede zin, waaronder risico's voor de nationale veiligheid. Daarbij kan worden gedacht aan sabotage of spionage van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten.
Het Bvit kent in artikel 2, tweede en derde lid, vergelijkbare bepalingen als artikel 18, eerste en tweede lid, Cbb. Op grond van het Bvit heeft de Minister van Economische Zaken onder meer maatregelen getroffen met betrekking tot de bescherming van de toeleveringsketen van de mobiele telecommunicatienetwerken. Dit zijn reeds langere tijd geldende maatregelen op grond van nationaal beleid dat ongewijzigd wordt voortgezet. Zowel met betrekking tot de grondslag als de maatregelen die op grond van het Bvit zijn genomen doen er zich in materiële zin geen wijzigingen voor.

Beoordeling

De bovengenoemde maatregel wordt opgelegd door de vakminister, in overeenstemming met de Minister van Justitie en Veiligheid, als naar zijn oordeel de maatregel noodzakelijk is om risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen. Bij die beoordeling wordt als uitgangspunt genomen: de beoordeling van de risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij producten en diensten. Die beoordeling staat vermeld in een brief van de Minister van Justitie en Veiligheid aan de Tweede Kamer over C2000.[11] Deze beoordeling wordt ook gehanteerd in het Bvit, waarin een soortgelijke bevoegdheid is opgenomen.

De beoordeling is nader gespecificeerd naar het doel van de Cbw, te weten het in stand houden van kritieke maatschappelijke of economisch belangrijke functies of activiteiten, gericht op het verhogen van de cyberbeveiliging, bedoeld in artikel 2 Cbw. Dit past in de Nederlandse Cybersecuritystrategie (2022-2028) waarin een digitaal veilig Nederland het uitgangspunt is.

[11] *Kamerstukken II* 2018/19, 25124, nr. 96.

Bij de beoordeling of van de bevoegdheid uit artikel 18, eerste lid, Cbb gebruik moet worden gemaakt, zal de vakminister het volgende in ogenschouw nemen:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of afkomstig uit een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

Indien het antwoord op de bovenstaande vragen positief is, zal er sprake zijn van een partij die nauwe banden heeft met of onder invloed staat van een staat of entiteit die de intentie heeft een in Nederland aangeboden netwerk of -informatiesysteem te misbruiken of uit te laten vallen of om incidenten die de nationale veiligheid raken te veroorzaken, of waarvoor gronden zijn om dergelijke banden of invloed te vermoeden. Dan komen de volgende vragen aan de orde:

3A. Krijgt de partij die de dienst of product levert uitgebreide toegang tot netwerk- en informatiesystemen, waarbij misbruik kan leiden tot risico's voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken of een incident die de nationale veiligheid raakt?
3B. Zijn er maatregelen mogelijk en realiseerbaar die het risico op misbruik dat kan leiden tot risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken of dat kan leiden tot een incident bij de entiteit die de nationale veiligheid raakt, voldoende beheersen?

De reikwijdte van de bevoegdheid is beperkt tot die onderdelen die in de beschikking worden aangewezen. Bij de afweging welke onderdelen in de beschikking worden aangewezen, komen bovenstaande overwegingen als volgt aan bod. Eerst worden de kritieke onderdelen in kaart gebracht. Dit zijn de onderdelen waarvoor geldt dat de leverancier uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen, vitale infrastructurele installaties of werken krijgt, waarbij misbruik een nationaal veiligheidsrisico kan vormen (overweging 3A). Vervolgens wordt beoordeeld of het opleggen van onderhavige maatregel in relatie tot die onderdelen noodzakelijk is om risico's die de nationale veiligheid raken te beheersen. Dit houdt in dat er geen beheersmaatregelen, met name de overige in het Cbb voorgeschreven maatregelen, mogelijk en realiseerbaar zijn om deze risico's voldoende te beheersen (overweging 3B). De kritieke onderdelen waar dit voor geldt worden vervolgens aangewezen in de beschikking, waarmee de reikwijdte van de verplichting om uitsluitend gebruik te maken van vertrouwde leveranciers tot die aangewezen onderdelen is beperkt.

Bij risico voor de nationale veiligheid kan gedacht worden aan sabotage, beïnvloeding of spionage door statelijke actoren of andere derde partijen van netwerk- en informatiesystemen. Ook de inzet van ransomware kan een risico vormen voor de nationale veiligheid als het gaat om de continuïteit van (vitale) processen, het weglekken en/of publiceren van vertrouwelijke of gevoelige informatie en de aantasting van de integriteit van de digitale ruimte.[12]

Termijn

Het zal voor een essentiële entiteit of belangrijke entiteit niet altijd mogelijk zijn om per direct gevolg te geven aan de op grond van artikel 18, eerste lid, Cbb genomen beschikking, zonder hiermee de continuïteit van de dienstverlening in gevaar te brengen. In zo'n geval zal de vakminister op grond van artikel 18, tweede lid, Cbb, in het belang van de hiervoor bedoelde continuïteit, in de beschikking een termijn opnemen waarbinnen de reeds in gebruik zijnde producten of diensten dienen te worden vervangen of beëindigd.

Eigendomsregulering

Het Cbb biedt met artikel 18, eerste lid, de grondslag om een beschikking op te leggen die kan leiden tot eigendomsregulering van essentiële entiteiten en belangrijke entiteiten. Van

[12] Cybersecuritybeeld Nederland 2024.

eigendomsregulering is sprake wanneer de gebruiksmogelijkheden van de eigendom worden beperkt, zonder dat de beschikking over het eigendom verloren gaat. Bij een beschikking op basis van artikel 18, eerste lid, Cbb is sprake van regulering van eigendom en geen (de facto) onteigening: het leidt immers niet tot verlies van eigendom dan wel dat de beschikking over het eigendom verloren gaat. De producten en diensten waarop de beschikking betrekking heeft behouden waarde, blijven eigendom van de entiteit en kunnen door haar te gelde worden gemaakt.

Artikel 1 van het Eerste Protocol bij het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EP EVRM) beschermt het recht op eigendom. Een beschikking op grond van artikel 18, eerste lid, Cbb vormt een inmenging in het in artikel 1 EP EVRM vervatte eigendomsrecht van essentiële entiteiten en belangrijke entiteiten. Van belang is dat het begrip "eigendom" in de zin van artikel 1 EP EVRM een autonome betekenis heeft. Dat betekent dat dit begrip een eigen betekenis heeft die losstaat van de betekenis die in de rechtstelsels van de verdragsstaten aan het begrip "eigendom" wordt gegeven. Bij de vraag of sprake is van eigendom in de zin van artikel 1 EP EVRM gaat het er volgens het Europees Hof voor de Rechten van de Mens (hierna: EHRM) uiteindelijk om dat in de omstandigheden van het geval sprake is van een *"title to a substantive interest"*. Uit jurisprudentie valt af te leiden dat het in algemene zin dient te gaan om op economische, op geld waardeerbare aanspraken en belangen.[13] Toekomstige inkomsten die nog niet betaald zijn en waarop naar nationaal recht ook nog geen vaststaand recht bestaat, kwalificeren volgens het EHRM bijvoorbeeld niet als eigendom in de zin van artikel 1 EP EVRM.

Het EHRM erkent dat een staat ter borging van het algemeen belang (het gebruik van) eigendom mag reguleren en aan beperkingen mag onderwerpen als aan een aantal voorwaarden wordt voldaan. Een inbreuk op het eigendomsrecht is gerechtvaardigd wanneer er sprake is van regulering van eigendom en deze aan de legaliteitstoets, de legitimiteitstoets en de evenredigheidstoets (*"fair balance"*) voldoet.

De legaliteitstoets houdt in dat de inmenging in het eigendomsrecht voorzien moet zijn bij wet of daarop gebaseerde regelgeving. De toepasselijke nationale regeling moet voldoende toegankelijk, precies en voorzienbaar zijn. Artikel 18, eerste lid, Cbb voldoet aan deze vereisten.

De legitimiteitstoets houdt in dat de inmenging enkel mag plaatsvinden in het algemeen belang en dat deze een legitiem doel dient. Het EHRM laat staten een ruime beoordelingsmarge bij het vaststellen van wat als een legitieme doelstelling in het kader van het algemeen belang kan gelden; nationale veiligheid kan daar ook onder geschaard worden. Hierbij is wel van belang dat wordt overwogen of de ingrijpendheid van de maatregel in redelijke verhouding staat tot het ermee beoogde legitieme doel (proportionaliteit) en of er geen andere, minder ingrijpende maatregelen mogelijk zijn om ditzelfde doel te bereiken (subsidiariteit). Bij de beschikking op grond van artikel 18, eerste lid, Cbb zal de vakminister aandacht moeten besteden aan de proportionaliteit en de subsidiariteit van dat besluit. Dat betekent dat de vakminister bij de beschikking zal moeten beoordelen of kan worden volstaan met de maatregelen die de betrokken entiteit in het kader van de zorgplicht reeds heeft genomen of nog kan nemen. Indien dat niet het geval is, moet de vakminister beoordelen tot welke onderdelen van de netwerk- en informatiesystemen het weren van producten en diensten van specifieke leveranciers zou moeten uitstrekken.

De evenredigheidstoets vraagt om een beoordeling of met de beschikking op grond van artikel 18, eerste lid, Cbb sprake is van een rechtvaardig en evenwichtig resultaat, oftewel *"fair balance"*, tussen het algemeen belang en de belangen van – in dit geval – de entiteit die wordt geraakt door de inmenging in haar eigendomsrecht. Bij de beoordeling of sprake is van een *"fair balance"* dienen verschillende aspecten in ogenschouw te worden genomen. De toepassing van de in artikel 18, eerste lid, Cbb opgenomen bevoegdheid mag niet leiden tot een individuele en buitensporige last voor de betrokken entiteit. Er moet bovendien een redelijke mate van evenredigheid bestaan tussen de gebruikte middelen en het nagestreefde doel. Een van de aspecten die een belangrijke rol speelt in het kader van de *"fair balance"* is de voorzienbaarheid van de maatregel (in casu de toepassing van de in artikel 18, eerste lid, Cbb opgenomen bevoegdheid). Hiermee wordt bedoeld of de maatregel in de lijn der verwachting ligt, ook al bestond er nog geen concreet zicht op de

[13] EHRM 30 november 2004, ECLI:CE:ECHR:2004:1130JUD004893999 (*Öneryıldız/Turkije*), rechtsoverweging 124; EHRM 11 januari 2007, ECLI:CE:ECHR:2007:0111JUD007304901 (*Anheuser-Busch Inc./Portugal*), rechtsoverwegingen 75 tot en met 78; EHRM 23 maart 2010, ECLI:CE:ECHR:2011:1018JUD000907407 (*Mullai e.a./Albanië*), rechtsoverweging 97.

omvang waarin, de plaats waar en het moment waarop de ontwikkeling zich zou voordoen. Essentiële entiteiten en belangrijke entiteiten zijn op grond van artikel 21 Cbw verplicht om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruiken, te beheersen. Ook moeten zij deze maatregelen nemen om incidenten te voorkomen. Daarmee is echter niet altijd op voorhand te zeggen dat die risico's voldoende kunnen worden beheerst wanneer in specifiek aan te wijzen onderdelen van de netwerk- en informatiesystemen niet uitsluitend producten of diensten van vertrouwde leveranciers worden gebruikt (en welke leveranciers als vertrouwd worden gezien). In sommige gevallen kan er sprake zijn van schade die voortvloeit uit het (vroegtijdig, voor afloop van de afschrijvingstermijn) moeten vervangen van producten, hetgeen op het moment van aanschaf niet voorzienbaar was. In zulke gevallen kan het noodzakelijk zijn nadeelcompensatie te bieden, om de vereiste *"fair balance"* te bereiken.

Nadeelcompensatie

Titel 4.5 van de Algemene wet bestuursrecht (hierna: Awb) behelst een codificatie van het égalitébeginsel en geeft de belangrijkste materiële en procedurele regels voor de toekenning van nadeelcompensatie. In artikel 4:126, eerste lid, Awb is bepaald dat indien een bestuursorgaan in de rechtmatige uitoefening van zijn publiekrechtelijke bevoegdheid of taak schade veroorzaakt die uitgaat boven het normale maatschappelijke risico en die een benadeelde in vergelijking met anderen onevenredig zwaar treft, het bestuursorgaan de benadeelde desgevraagd een vergoeding toekent. De op grond van de onderhavige bevoegdheid op te leggen beschikkingen vallen onder de reikwijdte van deze bepaling en meer algemeen titel 4.5 Awb.

Schade op grond van het égalitébeginsel komt alleen voor vergoeding in aanmerking voor zover de schade onevenredig is en in rechtstreeks verband staat tot het genomen besluit. Van onevenredige schade is sprake indien de schade op een beperkte groep burgers of bedrijven drukt (speciale last) en de schade boven het normaal maatschappelijke of ondernemersrisico uitstijgt (abnormale last).[14]

Voor de volledigheid wordt opgemerkt dat bij de beantwoording van de vraag of er een redelijk evenwicht bestaat tussen de eisen van het algemeen belang van de samenleving en de bescherming van de fundamentele rechten van het individu in het licht van artikel 1 EVRM EP, zoals hierboven is toegelicht, betrekt het EHRM de vraag of er een schadevergoeding is toegekend, alsmede de omvang daarvan. Op grond van de regeling in titel 4.5 Awb wordt de vraag naar de vergoedbaarheid van de schade en de omvang van de schadevergoeding los behandeld van de vraag naar de rechtmatigheid van het schadeveroorzakend overheidshandelen. Dit komt niet in strijd met de bescherming die artikel 1 EVRM EP beoogt te bieden, mits bestuursorganen zich er bij het nemen van een schadeveroorzakend besluit al rekenschap van geven dat het besluit aanleiding kan vormen voor aanspraken op nadeelcompensatie. In verband daarmee dient bij het nemen van het besluit tevens te worden bezien of er voor de afhandeling van een verzoek om nadeelcompensatie een met voldoende waarborgen omklede rechtsgang openstaat.[15] Dit is het geval nu een entiteit op grond van artikel 4:126, eerste lid, Awb een aanvraag voor nadeelcompensatie kan indienen.

Vrij verkeer van goederen

Een op grond van artikel 18, eerste lid, Cbb genomen beschikking is een kwantitatieve invoerbeperking (of maatregel van gelijke werking) in de zin van artikel 34 Verdrag betreffende de werking van de Europese Unie (hierna: VWEU). Een beperking in het vrije verkeer van goederen is slechts toegestaan indien dit gerechtvaardigd kan worden wegens een dwingende reden van algemeen belang, of in geval van discriminatoire maatregelen: een van de belangen opgesomd in artikel 36 VWEU, waaronder de bescherming van de openbare orde en openbare veiligheid, hetgeen ook de nationale veiligheid omvat. Een maatregel die leidt tot een beperking in het vrije verkeer van goederen moet voorts geschikt zijn om het beoogde doel te bereiken en niet verder gaan dan noodzakelijk is.

[14] Zie onder meer ABRvS 15 juli 2015, ECLI:NL:RVS:2015:2195 en ABRvS 30 mei 2012, ECLI:NL:RVS:2012:BW6926. Zie ook hoofdstuk 4.1 in het algemeen deel van de memorie van toelichting bij de wijziging van de Awb en enkele andere wetten in verband met het nieuwe omgevingsrecht en nadeelcompensatierecht (*Kamerstukken II* 2018/19, 35256, nr. 3).
[15] ABRvS 16 april 2003, ECLI:NL:RVS:2003:AF7355 en ABRvS 9 juli 2003, ECLI:NL:RVS:2003:AH9396.

Zoals hierboven toegelicht vindt een op grond van artikel 18, eerste lid, Cbb opgelegde maatregel (in casu de verplichting tot het weren van bepaalde diensten of producten van bepaalde leveranciers) zijn rechtvaardiging in het beschermen van de nationale veiligheid. Het opleggen van een dergelijke maatregel is enkel aan de orde als de maatregel geschikt is om het nagestreefde belang te beschermen en als – gelet op de geconstateerde risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken – die risico's niet afdoende te ondervangen zijn met de maatregelen die de betrokken entiteit in het kader van de zorgplicht reeds heeft genomen. De maatregel zal in dat geval niet verder gaan dan nodig voor het beoogde doel en geschikt zijn om het beoogde doel te bereiken.

Internationale handels- en investeringsafspraken

Bij een beschikking op basis van artikel 18, eerste lid, Cbb, die betrekking heeft op reeds in gebruik zijnde producten of diensten in de daarbij aangewezen onderdelen van de netwerk- en informatiesystemen van de betrokken entiteit, is tevens van belang dat de internationale afspraken tussen het Koninkrijk der Nederlanden en derde landen over investeringsbescherming in acht worden genomen. Onder deze afspraken wordt een buitenlandse investeerder in Nederland (en worden Nederlandse investeerders in het betreffende derde land) beschermd tegen onder meer onredelijk en/of discriminatoir handelen van de overheid. Daarnaast bieden deze afspraken voorwaarden op basis waarvan onteigend mag worden, namelijk indien de maatregel die tot (de facto) onteigening leidt non-discriminatoir is, in het publiek belang is en waartegenover een gepaste schadevergoeding wordt geboden. Indien een overheid jegens die investeerder niet redelijk heeft gehandeld of de voorwaarden voor onteigening heeft geschonden, kan de investeerder daartegen compensatie eisen. Dit is alleen van belang waar het gaat om een reeds bestaande investering.

Uit hetgeen hiervoor ten aanzien van de eigendomsregulering en nadeelcompensatie is besproken (vraagstukken waarvoor de toetsing dezelfde beginselen volgt), kan worden geconcludeerd dat beschikkingen op grond van artikel 18, eerste lid, Cbb in beginsel geen schending opleveren van de internationale investeringsbeschermingsafspraken op dit terrein. De vakminister zal bij het opleggen van beschikkingen op grond van artikel 18, eerste lid, Cbb steeds per geval toetsen aan de genoemde specifieke vereisten.

Verder is van belang dat een dergelijke beschikking geen afbreuk doet aan de handelsafspraken over diensten en goederen aangegaan onder de Wereldhandelsorganisatie (*World Trade Organization*) en bilaterale en regionale handelsakkoorden van de Europese Unie met derde landen. Deze akkoorden voorzien onder bepaalde voorwaarden in een uitzondering op de regels van markttoegang en non-discriminatoire behandeling. Zo kan een dergelijke beschikking gezien het doel van de maatregel gerechtvaardigd worden met een beroep op de algemene uitzondering voor de bescherming van de nationale veiligheid. Bij het nemen van de beschikking op grond van artikel 18, eerste lid, Cbb zal de vakminister moeten toetsen of dergelijke beperkende maatregelen noodzakelijk zijn om deze doelstelling te verwezenlijken, en er dus geen alternatieve maatregel bestaat die de handel minder beperkt en waarvan redelijkerwijs geacht wordt dat een staat die maatregel neemt. Uit artikel 18, eerste lid, Cbb blijkt dat de beschikking uitsluitend wordt opgelegd indien het opleggen van de verplichting om in onderdelen van de netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren noodzakelijk is om risico's die de nationale veiligheid raken te beheersen. Hieruit volgt tevens dat een dergelijke maatregel alleen wordt opgelegd indien andere maatregelen, meer in het bijzonder de maatregelen die de betrokken entiteit in het kader van de wettelijke zorgplicht al heeft genomen, onvoldoende zijn om de risico's voor de nationale veiligheid te beheersen.

Wat betreft een beroep op de uitzonderingen ter bescherming van de nationale veiligheid geldt nog specifiek dat een staat maatregelen kan nemen die het nodig acht ter bescherming van het wezenlijke belang van haar veiligheid en die (voor zover hier relevant) enkel worden toegepast in tijd van oorlog of van gevaarlijke internationale spanningen. Daarnaast kan een staat maatregelen nemen tot handhaving van de internationale vrede en veiligheid ingevolge haar verplichtingen krachtens het Handvest van de Verenigde Naties.

Gezien het doel van en de vereiste onderbouwing van de verplichting, bedoeld in artikel 18, eerste lid, Cbb, namelijk de bescherming van de nationale veiligheid, is een beschikking op grond van artikel 18, eerste lid, Cbb – afhankelijk van de specifieke situatie – in beginsel te rechtvaardigen onder de geldende uitzonderingsgronden van de handelsafspraken. De vakminister zal bij het

opleggen van een beschikking op grond van artikel 18, eerste lid, Cbb steeds per geval toetsen aan de genoemde specifieke vereisten.

Rechtsbescherming

De aan een essentiële entiteit of belangrijke entiteit op te leggen verplichting, bedoeld in artikel 18, eerste lid, Cbb, is een besluit in de zin van de Awb. Tegen het besluit staan rechtsmiddelen (bezwaar, beroep en hoger beroep) open.

Artikel 19 (evaluatie)

In artikel 19 Cbb is geregeld dat essentiële entiteiten en belangrijke entiteiten de maatregelen die zij hebben genomen in het kader van de zorgplicht periodiek moeten evalueren op de doeltreffendheid en de effecten daarvan in de praktijk, en de resultaten van deze evaluatie schriftelijk moeten vastleggen. Deze evaluaties hebben tot doel om op basis daarvan te beoordelen of de maatregelen aangepast moeten worden.

Het is aan entiteiten zelf om in te schatten welke periode tussen de evaluaties passend is. Wanneer het weer tijd is voor een entiteit om te evalueren kan afhankelijk zijn van bijvoorbeeld technologische ontwikkelingen, veranderingen in de sector of binnen de entiteit, of veranderingen in risico's en dreigingen waarmee de entiteit geconfronteerd wordt en die invloed hebben op de beveiliging van de netwerk- en informatiesystemen van de entiteit.

In het kader van de door artikel 19 Cbb voorgeschreven evaluaties wordt opgemerkt dat deze evaluaties ook onderdeel kunnen zijn van andere periodieke evaluaties, zoals evaluaties van de leveringsplannen.

Artikel 20 (nadere regels)

In artikel 20 Cbb is een grondslag opgenomen om bij ministeriële regelingen van de vakministers, na overleg met de Minister van Justitie en Veiligheid, nadere regels te stellen over de maatregelen die essentiële entiteiten en belangrijke entiteiten moeten nemen in het kader van de zorgplicht. Hierbij kan onderscheid worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten. Het maken van onderscheid kan in sommige gevallen nodig zijn, bijvoorbeeld vanwege de (afwijkende) aard van een bepaalde sector ten opzichte van andere sectoren.

De grondslag in artikel 20 Cbb is niet enkel beperkt tot de maatregelen die worden genoemd in artikel 21, derde lid, Cbw en die zijn uitgewerkt in het Cbb. De grondslag biedt de mogelijkheid om regels te stellen over de maatregelen, bedoeld in artikel 21, eerste lid, Cbw.

Artikel 21 (doel van de training)

Artikel 24, tweede lid, Cbw bepaalt dat ieder lid van het bestuur van essentiële entiteiten en belangrijke entiteiten moet beschikken over kennis en vaardigheden om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren, risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen en de gevolgen van de risico's en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend, te kunnen beoordelen. Artikel 24, vijfde lid, Cbw bepaalt dat al die bestuursleden over een certificaat moeten beschikken waaruit de deelname blijkt aan een training die de onderwerpen, bedoeld in artikel 24, tweede lid, Cbw, behandelt. In artikel 21 Cbb wordt het doel van de training bepaald. De training moet bestuursleden in staat stellen om het proces voor het identificeren van risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen begrijpen en de maatregelen inclusief gevolgen te beoordelen, om zo tot een goede afweging en afgewogen besluitvorming rondom de beveiliging van netwerk- en informatiesystemen te komen.

Artikel 22 (eisen aan de training)

In artikel 22 Cbb wordt geregeld waar de training (te volgen door ieder lid van het bestuur van essentiële entiteiten en belangrijke entiteiten), bedoeld in artikel 24, vijfde lid, Cbw, inhoudelijk aan moet voldoen. Hierbij wordt aangesloten bij de kennis- en vaardighedenvereisten uit artikel 24, tweede lid, Cbw. Hierbij wordt opgemerkt dat het uitdrukkelijk geen opleiding betreft waarin van de bestuurder wordt verwacht technische kennis te bezitten en de werking van netwerk- en informatiesystemen te kunnen uitleggen. Wel wordt van de bestuurder op strategisch niveau

kennis verwacht op de genoemde onderwerpen, zodat de bestuurder in staat is de maatregelen te beoordelen en de risico's te (laten) beheersen. Hiervoor is een bepaalde basiskennis vereist.

Artikel 22, eerste lid, Cbb ziet op de kennis en vaardigheden om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en de gevolgen van deze risico's te kunnen beoordelen. Voor een goede identificatie van risico's is kennis over de verschillende soorten risico's nodig die spelen bij netwerk- en informatiesystemen, zoals de dreiging van malware, *insiders threat* en DDoS-aanvallen die een risico vormen voor de integriteit en beschikbaarheid. Daarnaast is inzicht in hoe het risicomanagementproces in elkaar zit en de risicomanagementmethodiek relevant om te weten op welke wijze risico's systematisch geïdentificeerd, beoordeeld en behandeld kunnen worden.

Artikel 22, tweede lid, Cbb ziet op de kennis en vaardigheden om risicobeheersmaatregelen op het gebied van cyberbeveiliging en de gevolgen van die maatregelen te kunnen beoordelen. In deze bepaling is geregeld dat de training in elk geval moet zien op de onderwerpen die in artikel 21, derde lid, onderdelen a tot en met j, Cbw worden genoemd. Dit artikel ziet op de maatregelen die in elk geval moeten worden genomen in het kader van de zorgplicht. Globale kennis van dergelijke maatregelen is van belang voor een goede beoordeling van de maatregelen.

Artikel 23 (eisen aan het certificaat)

In artikel 23 Cbb worden eisen gesteld aan de inhoud van het certificaat van de training, bedoeld in artikel 24, vijfde lid, Cbw.

In artikel 23, eerste lid, Cbb is bepaald welke informatie het certificaat ten minste moet bevatten. Die eisen, waaronder de eis dat uit het certificaat moet blijken welke onderwerpen zijn behandeld, zijn nodig om na te kunnen gaan of de training voldoet aan de eisen die aan de training worden gesteld in de Cbw en het Cbb. Hierbij dient te worden opgemerkt dat dit certificaat uitsluitend verplicht is in het kader van de verplichte training van artikel 24, vijfde lid, Cbw. Een certificaat met de in het Cbb opgenomen vereisten is niet verplicht voor het aantoonbaar actueel houden van de kennis en vaardigheden als bedoeld in artikel 24, vierde lid, Cbw. Leden van bestuur kunnen dat ook op andere wijze aantonen.

Artikel 23, tweede lid, Cbb bevat het vereiste dat het certificaat is opgesteld in de Nederlandse of Engelse taal. Dit vereiste is noodzakelijk voor efficiënt en effectief toezicht op de verplichting voor bestuursleden om de training te volgen. Dit vereiste geldt alleen voor het certificaat en niet voor de taal van de training. De training mag in iedere taal worden gegeven.

Artikel 24 (significante incidenten)

Artikel 25, derde lid, Cbw regelt dat bij of krachtens amvb de criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, Cbw, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en soorten entiteiten. Die criteria staan ook bekend als drempelwaarden. In artikel 24, eerste lid, Cbb is geregeld dat de hiervoor bedoelde criteria worden vastgesteld bij ministeriële regeling van de vakminister en na overleg met de Minister van Justitie en Veiligheid.
Er is gekozen voor subdelegatie, omdat het vanwege de verschillen tussen sectoren en subsectoren en in sommige gevallen zelfs tussen soorten entiteiten binnen die (sub)sectoren niet mogelijk is om de bedoelde criteria vast te stellen die op alle entiteiten uit alle sectoren van toepassing kunnen zijn. Door subdelegatie kunnen de vakministers bij ministeriële regelingen voor de sectoren waar zij beleidsverantwoordelijk voor zijn, criteria vaststellen, aan de hand van de kennis die zij hebben over de sectoren en met consultatie van de betrokkenen binnen die sectoren. Door het overleg met de betrokken sector kan zoveel mogelijk maatwerk worden geleverd per sector, subsector of soort entiteit. Indien relevant kan zodoende ook rekening worden gehouden met andere sectorale meldplichten en de daarvoor geldende criteria.

Artikel 24, tweede lid, Cbb bepaalt dat de hiervoor bedoelde criteria ten minste elke vier jaar moeten worden geëvalueerd door de betrokken vakminister. Indien nodig past hij, na overleg met de Minister van Justitie en Veiligheid, de criteria aan. Met het evalueren kan worden bewerkstelligd dat de criteria actueel blijven en aansluiten op de gevaren en dreigingen die voor een sector relevant zijn. Denk daarbij bijvoorbeeld aan zeer snelle technologische ontwikkelingen.

Artikel 24, derde lid, Cbb regelt dat met de delegatiegrondslag van artikel 24, eerste lid, Cbb geen regels kunnen worden gesteld over in welke gevallen een incident als significant incident wordt beschouwd ten aanzien van de entiteiten waarvoor in uitvoeringshandelingen op grond van artikel 23, elfde lid, NIS2-richtlijn nader is gespecificeerd in welke gevallen een incident bij die entiteiten als significant wordt beschouwd. De Europese Commissie kan die uitvoeringshandelingen vaststellen ten aanzien van alle essentiële entiteiten en belangrijke entiteiten.
De uitvoeringsverordening is een uitvoeringshandeling die zijn grondslag vindt in onder meer artikel 23, elfde lid, NIS2-richtlijn. Met de uitvoeringsverordening heeft de Europese Commissie met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, aanbieders van onlinezoekmachines en aanbieders van platforms voor socialenetwerkdiensten, uitvoeringshandelingen vastgesteld waarin nader wordt gespecificeerd in welke gevallen een incident als significant wordt beschouwd als bedoeld in artikel 24, derde lid, NIS2-richtlijn. Dit betekent dus dat de betrokken vakministers ten aanzien van de hiervoor genoemde entiteiten geen drempelwaarden kunnen vaststellen in het kader van de meldplicht.

Artikel 25 (gegevens waar een vroegtijdige waarschuwing uit moet bestaan)

Artikel 35 Cbw biedt de grondslag om bij of krachtens amvb regels te stellen over onder meer de gegevens waar de vroegtijdige waarschuwing, bedoeld in artikel 26, eerste lid, Cbw, uit moet bestaan. Op grond van artikel 35 Cbw is in artikel 25 Cbb bepaald dat de vroegtijdige waarschuwing ook moet bestaan uit het vermoedelijke tijdstip van aanvang van het significante incident, een beschrijving van de aard en gevolgen van het incident, (zo mogelijk) een prognose van de hersteltijd en (zo mogelijk) de door essentiële entiteiten en belangrijke entiteiten genomen of voorgenomen maatregelen om de gevolgen van het significante incident te beperken of herhaling hiervan te voorkomen. Met deze informatie kan door het CSIRT en de bevoegde autoriteit beter worden ingeschat of zij willen reageren en hoe respons mogelijk is. Daarnaast kan door deze informatie beter worden ingeschat wat mogelijke cascade-effecten zijn op bijvoorbeeld andere entiteiten.

Artikel 26 (wijze waarop een melding geschiedt)

Artikel 26 Cbb verplicht essentiële entiteiten en belangrijke entiteiten om meldingen van significante incidenten te doen bij een hiervoor door de Minister van Justitie en Veiligheid ingericht meldpunt.

Artikel 27 (nadere regels over meldingen)

Artikel 27 Cbb biedt de betrokken vakminister, na overleg met de Minister van Justitie en Veiligheid, de grondslag om bij ministeriële regeling regels te stellen ter uitwerking van de artikelen 26 tot en met 30, 33 en 34 Cbw. Deze grondslag biedt de mogelijkheid om met regels te komen die zijn toegespitst op een specifieke sector, subsector of soort entiteit.

Artikel 28 (informatieverstrekking ten behoeve van nationaal register)

In artikel 44, eerste lid, Cbw is geregeld dat essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen bepaalde informatie moeten verstrekken aan de Minister van Justitie en Veiligheid voor de registratie in het nationaal register, bedoeld in artikel 43 Cbw. Op grond van artikel 44, eerste lid, onderdeel f, Cbw kan aanvullende informatie worden verlangd voor de registratie in het nationaal register. In artikel 28 Cbb is gebruik gemaakt van deze mogelijkheid.

Artikel 28, eerste lid, Cbb is van toepassing op essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Zij moeten op grond van artikel 28, eerste lid, onderdeel a, Cbb voor hun registratie in het nationaal register aangeven of zij dit doen als essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent. Aan de hand van die opgegeven informatie kan de bevoegde autoriteit bepalen onder welk toezichts- en handhavingsregime de entiteit valt. Daarnaast wordt deze informatie door het CSIRT gebruikt voor de triage in geval van incidenten.
Op grond van artikel 28, eerste lid, onderdeel b, Cbb moeten zij ook het nummer verstrekken waarmee zij in het handelsregister, bedoeld in artikel 2 Handelsregisterwet 2007, staan

ingeschreven. Dit nummer staat ook bekend als het Kamer van Koophandel-nummer. Op deze wijze wordt met de registratie aangesloten bij het Nederlandse beleid en stelsel van basisregistraties, inclusief bijhorende unieke identificatie van entiteiten. Het stelt bovendien de bevoegde autoriteiten en CSIRT's in staat om op uitvoerbare wijze relaties tussen verschillende entiteiten in kaart te brengen, zoals moeder-dochter-relaties.

In artikel 28, tweede lid, Cbb is geregeld dat overheidsinstanties de identificatiecode moeten verstrekken waarmee zij geregistreerd staan in het Register voor Overheidsorganisaties.
Niet alle overheidsinstanties beschikken over een Kamer van Koophandel-nummer, terwijl zij over het algemeen wel geregistreerd staan in het Register voor Overheidsorganisaties. Het Register voor Overheidsorganisaties is daarom een betere basis voor het identificeren van overheidsinstanties. Mocht de onvoorziene situatie zich voordoen dat een overheidsinstantie niet ingeschreven staat in het Register van Overheidsorganisaties, dan geeft deze bepaling de mogelijkheid om ook het Kamer van Koophandel-nummer te overleggen. Daarnaast kan de betreffende overheidsinstantie zich ook registeren in het Register van Overheidsorganisaties.

Artikel 28, derde lid, Cbb is van toepassing op essentiële entiteiten en belangrijke entiteiten. In artikel 28, derde lid, onderdeel a, Cbb is bepaald dat zij voor hun registratie in het nationaal register moeten aangeven van welk soort zij zijn. Aan de hand van die opgegeven informatie hebben de bevoegde autoriteit en de CSIRT een beter inzicht in de bedrijfsactiviteiten van de betreffende entiteit, wat door de bevoegde autoriteit gebruikt kan worden voor meer gericht toezicht en door het CSIRT voor beter gerichte ondersteuning aan de betreffende entiteit. Dit sluit ook aan bij de systematiek die geldt voor de soorten entiteiten die zich dienen te registreren in het Enisa-register op basis van artikel 47 Cbw, waarbij eveneens de soort geregistreerd dient te worden. Ook sluit het aan bij de huidige praktijk onder de Wet beveiliging netwerk- en informatiesystemen, waarbij van entiteiten duidelijk is van welk soort zij zijn.
In artikel 28, derde lid, onderdeel b, Cbb is bepaald dat zij ook hun domeinnamen moeten aanleveren. Het gaat daarbij om de publieke domeinnamen die eigendom zijn van de entiteit. Deze informatie is noodzakelijk voor CSIRT's om hun wettelijke taken richting deze entiteiten, bevoegde autoriteiten en andere relevante partijen effectief uit te kunnen voeren. In sommige gevallen beschikt een CSIRT alleen over domeinnamen van een potentieel doelwit of slachtoffer (zoals bij gelekte inloggegevens), en niet over een IP-adres. Om in die gevallen de entiteit te kunnen informeren over een dreiging of kwetsbaarheid, is het van belang dat het CSIRT ook beschikt over de domeinnamen van de entiteit.

Over het nationaal register, bedoeld in artikel 43 Cbw, wordt ten slotte nog het volgende toegelicht. De bevoegde autoriteiten en CSIRT's maken gebruik van de registratie-informatie voor het uitoefenen van hun taken op grond van de Cbw. In het registratieproces worden daarom maatregelen ingebouwd die eraan bijdragen dat de opgegeven informatie juist en volledig is en de entiteiten niet te veel worden belast. Dit gebeurt doordat vanuit het authenticatiemiddel (zoals SSO-rijk of eHerkenning) dat bij registratie wordt gebruikt, automatisch onder meer het Kamer van Koophandel-nummer van een entiteit wordt verkregen. Hierdoor kan het nationaal register worden gekoppeld aan het handelsregister of andere registers, zoals het Register van Overheidsorganisaties, om bekende gegevens van de entiteit op te halen. Dit is informatie die bij registratie door de entiteit moet worden gecontroleerd. Dit betreffen gegevens die de entiteit ook verplicht is om aan te leveren op grond van artikel 44 Cbw, namelijk de naam en het adres van de entiteit. Daarnaast geldt dat deze werkwijze kan valideren dat een persoon gerechtigd is om namens een entiteit het registratieproces te doorlopen. Dit biedt extra zekerheid voor de juistheid van deze gegevens en hiermee worden dus de administratieve lasten verminderd voor entiteiten die onder het toepassingsbereik van de Cbw vallen.

Artikel 29 (aanwijzing autoriteiten)

Artikel 51, tweede lid, onderdeel i, Cbw biedt de betrokken vakminister, na overleg met de Minister van Justitie en Veiligheid, de mogelijkheid om bij of krachtens amvb autoriteiten aan te wijzen waar de bevoegde autoriteiten in de zin van de Cbw, de CSIRT's en het centrale contactpunt mee samenwerken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van de Cbw en in het kader van die samenwerking alle daarvoor noodzakelijke gegevens uitwisselen.

In artikel 29 Cbb is een delegatiegrondslag opgenomen op grond waarvan de vakminister de hiervoor bedoelde autoriteiten bij regeling kan aanwijzen. De reden voor het doordelegeren is dat naar verwachting vooral autoriteiten zullen worden aangewezen die uit hoofde van sectorale regelgeving een rol hebben in het toezicht op entiteiten die ook onder toepassing van de Cbw

vallen. Door dit bij regeling te regelen kan door de vakminister vanuit diens verantwoordelijkheid voor sectoren hier een passende invulling aan gegeven worden en waar nodig worden bijgesteld. De aanwijzing maakt het in het bijzonder voor autoriteiten mogelijk om in het geval van overlappend toezicht nauwer samen te werken, informatie uit te wisselen en op die wijze doelmatig en doeltreffend toezicht te bevorderen en daarmee ook onnodige toezichtslasten voor entiteiten te beperken.

Artikel 30 (bewaring van persoonsgegevens)

In artikel 30, eerste lid, Cbb is bepaald dat de persoonsgegevens die door het CSIRT, het centrale contactpunt en de Minister van Justitie en Veiligheid bij of krachtens de Cbw worden verwerkt, niet zijnde de persoonsgegevens, bedoeld in artikel 64, tweede lid, Cbw, maximaal 60 maanden, gerekend vanaf de eerste verwerking, worden bewaard.

Het CSIRT verwerkt in het kader van de uitoefening van haar taken allerlei soorten gegevens, waaronder persoonsgegevens. Het gedurende een periode bewaren van deze gegevens kan in het belang zijn de uitoefening van die taken. Zo kan het bewaren nodig zijn om te voorzien in de gevallen dat een bepaald IP-adres opnieuw geraakt wordt, als een digitale aanval steeds vanuit dezelfde hoek komt of wanneer een serie IP-adressen gebruikt is in bijvoorbeeld een botnet. Dit kan voor het CSIRT aanleiding zijn om onderzoek te doen naar de relevantie voor andere recent getroffen IP-adressen. Ook kan uit nader onderzoek van een afgehandeld incident blijken dat relevante informatie, zoals een kwetsbaarheid van bepaalde IP-adressen of bepaalde gebruikte aanvalstechnieken, door kwaadwillende actoren opnieuw worden gebruikt tegen andere partijen. Voor een gedegen onderzoek van afgehandelde incidenten is het noodzakelijk dat deze gegevens niet te snel worden vernietigd. Een maximale bewaartermijn van 60 maanden wordt passend geacht voor de taken van het CSIRT, zoals het monitoren en analyseren van cyberdreigingen waarbij onderzoek over een langere periode noodzakelijk is om goed te kunnen kijken naar trends.

Ook voor het centrale contactpunt is het wenselijk dat persoonsgegevens zoals e-mailadressen en contactgegevens langere tijd kunnen worden bewaard, om zo een goede samenwerking mogelijk te maken. Het is daarbij een te grote administratieve last om de contactgegevens en e-mailadressen telkens opnieuw te moeten verzamelen. Daarom is er ook ten aanzien van het centrale contactpunt gekozen voor een maximale bewaartermijn van 60 maanden.

Artikel 30, tweede lid, Cbb bevat een uitzondering op het bepaalde in artikel 30, eerste lid, Cbb voor de persoonsgegevens die worden verwerkt in het kader van het nationale register, bedoeld in artikel 43 Cbw. Voor deze persoonsgegevens geldt een maximale bewaartermijn van 60 maanden na de laatste bevestiging van de juistheid van de betreffende persoonsgegevens. Het regelen van deze uitzondering is nodig omdat het niet wenselijk is dat deze gegevens, die door entiteiten zijn aangeleverd, zonder meer na vijf jaar moeten worden verwijderd, terwijl deze gegevens nog steeds relevant zijn voor de wettelijke taken van de Minister van Justitie en Veiligheid. De verwachting is dat de bedoelde gegevens binnen die vijf jaar telkens zullen worden gewijzigd of geactualiseerd. Daarom wordt de maximale bewaartermijn van vijf jaar gekoppeld aan de laatste bevestiging van de juistheid van de gegevens. Indien de termijn van vijf jaar dreigt te verlopen kan de Minister van Justitie en Veiligheid de entiteit al dan niet geautomatiseerd vragen om de actualiteit en juistheid van de gegevens te bevestigen. Indien de entiteit deze actualiteit en juistheid bevestigt begint het termijn van vijf jaar opnieuw te lopen.

Voor toezicht op en het handhavend kunnen optreden tegen bijvoorbeeld een entiteit of eventueel een bestuurder van de entiteit moet er een dossier worden opgebouwd. Voor de opbouw van een doorlopend toezichtdossier en in het kader daarvan genomen besluiten en de afhandeling van eventuele bestuursrechtelijke procedures kan het nodig zijn om toezichtinformatie lang te bewaren. Persoonsgegevens kunnen daar een onlosmakelijk onderdeel van zijn, bijvoorbeeld als onderdeel van besluiten, gespreksverslagen of opgevraagde documentatie. Het gaat daarbij met name om namen, e-mailadressen en telefoonnummers van werknemers en bestuurders van entiteiten. Artikel 30, derde lid, Cbb bepaalt daarom dat een uiterlijke bewaartermijn voor persoonsgegevens van 120 maanden wordt aangehouden ten aanzien van de persoonsgegevens die door de bevoegde autoriteit bij of krachtens de Cbw worden verwerkt. Dit zorgt voor een uitvoerbare praktijk en zorgt tegelijkertijd voor rechtszekerheid dat persoonsgegevens uiterlijk na 120 maanden verwijderd worden.

Artikel 31 (wijziging Besluit EU-verordeningen Wft)

Gelijktijdig met de NIS2-richtlijn is de zogeheten *Digital Operational Resilience Act* (hierna: DORA) vastgesteld.[16] Deze verordening is van toepassing op de financiële sector.

Banken, exploitanten van handelsplatformen en centrale tegenpartijen vallen zowel onder het toepassingsbereik van de DORA, als onder het toepassingsbereik van de NIS2-richtlijn. De bepalingen uit de verordening over het melden van grote ICT-gerelateerde incidenten zijn op hen van toepassing, in plaats van de bepalingen hierover uit de NIS2-richtlijn. Dit volgt uit artikel 1, tweede lid, DORA jo. artikel 4 NIS2-richtlijn. De bepalingen uit de Cbw over de meldplicht zijn dan ook niet op hen van toepassing, waaronder de verplichting om melding te doen bij het CSIRT.

De DORA biedt in artikel 19, eerste lid, zesde alinea, lidstaten de mogelijkheid om financiële entiteiten te verplichten om de melding, bedoeld in artikel 19, vierde lid, van de verordening ook te melden bij het CSIRT. Nederland maakt met artikel 31 Cbb gebruik van deze mogelijkheid. Hierdoor moeten banken, exploitanten van handelsplatformen, centrale tegenpartijen en centrale effectenbewaarinstellingen de melding zowel bij de financiële toezichthouder (de Autoriteit Financiële Markten, hierna: AFM, of De Nederlandsche Bank, hierna: DNB), als bij het CSIRT doen. Voor hen geldt dus een dubbele meldplicht. Het gebruiken van deze lidstaatoptie behelst voor hen geen nieuwe verplichting, maar een bestendiging van de meldplicht die thans voor hen geldt. Voor de hiervoor genoemde financiële entiteiten geldt immers op grond van artikel 10, eerste lid, Wbni al de verplichting om ernstige cyberincidenten te melden bij de Minister van Justitie en Veiligheid, die op grond van artikel 2 Wbni het CSIRT is voor deze aanbieders. De Wbni wordt met de komst van de NIS2-richtlijn ingetrokken.

Door het benutten van de in de DORA geboden lidstaatoptie hebben banken, exploitanten van handelsplatformen, centrale tegenpartijen en centrale effectenbewaarinstellingen een dubbele meldplicht. Het belang van deze dubbele meldplicht is dat het CSIRT een andere rol vervult en een ander doel heeft met het ontvangen van meldingen dan DNB of AFM. Het CSIRT is er om indien nodig bijstand te verlenen, overloopeffecten te identificeren, andere entiteiten te waarschuwen en trends te analyseren. DNB en AFM gebruiken de meldingen om de toezichtspraktijk te verbeteren en de financiële stabiliteit te waarborgen.

Artikel 19, tweede lid, DORA biedt lidstaten de mogelijkheid om te regelen dat financiële entiteiten *significante* cyberdreigingen op vrijwillige basis kunnen melden bij het CSIRT. Er wordt gebruik gemaakt van deze mogelijkheid, omdat het CSIRT naar aanleiding van vrijwillige meldingen kan overgaan op het identificeren van overloopeffecten, het waarschuwen van andere entiteiten en het analyseren van trends.

Artikel 32 (wijziging Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten)

De implementatie van de NIS2-richtlijn leidt tot wijzigingen van het Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten. De wijzigingen zijn van een technische aard en beogen geen beleidswijziging.

De zorgplicht met betrekking tot de beveiliging van openbare elektronische communicatienetwerken en -diensten wordt grotendeels in de Cbw geregeld. Met betrekking tot de beveiliging van diensten geldt dat alleen de beveiliging van de netwerk- en informatiesystemen die worden gebruikt voor het verlenen van diensten of verrichten van activiteiten onder de Cbw komen te vallen. Om er toch voor te zorgen dat beveiliging van diensten volledig onder de regelgeving blijft vallen, is bij de implementatie van de NIS2-richtlijn in artikel 11.a, eerste lid, Telecommunicatiewet (hierna: Tw) de zorgplicht voor de beveiliging van diensten gecontinueerd. In de memorie van toelichting bij artikel 98 Cbw is dit nader toegelicht.

De maatregelen in het Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten waarmee een nadere invulling werd gegeven aan de zorgplicht uit artikel 11.a1, eerste lid, Tw zijn geschrapt, omdat deze onder de Cbw verder zijn uitgewerkt. De delegatiegrondslag is behouden gebleven (onderdeel B). De meldplicht van incidenten voor de aanbieders van openbare elektronische communicatienetwerken en -diensten valt thans volledig onder de Cbw. De betreffende bepalingen inzake de meldplicht zijn derhalve uit

[16] Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (*PbEU* 2022, L 333).

het Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten geschrapt (onderdelen D en F).

De maatregelen die zien op de beveiliging van de antenne-opstelpunten met een hoofdzender voor het verspreiden van programma's voor het omroepnet voor radio van regionale media-instellingen (zie artikel 3.7, onderdelen b en c, Tw) zijn een continuering van het nationaal beleid. Het gaat hierbij om het treffen van beveiligingsmaatregelen zodat de continuïteit van radio-uitzendingen die onder meer in het bijzonder van belang is bij radiokanalen met de functie van calamiteitenzender zo goed mogelijk wordt geborgd. Dit nationale beleid wordt voortgezet (onderdelen C en D).

Na artikel 5b Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten wordt een omhangbepaling ingevoegd, als gevolg van de wijziging van de grondslag in de Tw.

Artikel 33 (wijziging Besluit veiligheid en integriteit telecommunicatie)

Na artikel 2 Bvit wordt een omhangbepaling ingevoegd, als gevolg van de wijziging van de grondslag in de Tw (artikel 11.a1, tweede lid), ter uitvoering van de NIS2-richtlijn.

Artikel 34 (wijziging Drinkwaterbesluit)

De wijzigingen van het Drinkwaterbesluit (hierna: Dwb) beogen een samenhangende uitvoering te faciliteren van enerzijds de verplichtingen die voortvloeien uit de Cbw (en overigens ook van de Wwke) en anderzijds de bestaande verplichtingen inzake risicobeoordeling en risicobeheer in het Dwb, die onder meer voortvloeien uit de zogeheten Drinkwaterrichtlijn.[17]

Wijziging artikel 15 Dwb
De wijzigingen van artikel 15 Dwb zijn van redactionele aard; er is geen inhoudelijke wijziging van verplichtingen. De wijzigingen ondersteunen in samenhang met die van de artikelen 46a en 47 Dwb een samenhangende uitvoering van (reeds geïmplementeerde) verplichtingen op grond van de Drinkwaterrichtlijn en de verplichtingen op grond van de Cbw (en overigens ook van de Wwke).

Wijziging artikel 46a Dwb
De wijziging betreft een technische correctie. Het opschrift is gewijzigd in verband met de verplichting tot beheer, opgenomen in het vijfde lid van artikel 46a Dwb.

Wijziging artikel 47 Dwb
De uitvoering van de verplichte risicobeoordeling op grond van de Wwke wordt geïntegreerd in de bestaande systematiek van de verstoringsrisicoanalyse (VRA), bedoeld in artikel 47 Dwb, en de verstoringsparagraaf die op grond van artikel 47 Dwb onderdeel moet zijn van het leveringsplan, bedoeld in artikel 37 Drinkwaterwet. De VRA gaat dan omvatten:
a. de risicobeoordeling, bedoeld in artikel 14 Wwke;
b. de benadering, bedoeld in artikel 21, derde lid, Cbw (*all hazard*);
c. nationale dreigingen en scenario's, zoals reeds opgenomen in het tweede lid van artikel 47 Dwb.

Omdat de VRA tevens onderdeel is van de risicobeoordeling van het watervoorzieningssysteem, bedoeld in artikel 46a Dwb, is daarmee ook integratie in het bredere systeem van risicobeoordeling ingevolge de Drinkwaterrichtlijn geborgd.

Het nieuwe zesde lid van artikel 47 Dwb regelt welke maatregelen op grond van het voorgaande moeten worden opgenomen in de verstoringsparagraaf van het leveringsplan. Omwille van de leesbaarheid wordt de bestaande bepaling dat de vereisten uit bijlage B, onderdeel 3, van het Dwb van toepassing zijn op de verstoringsparagraaf, in een separaat zevende lid opgenomen.

Nieuw artikel 47a Dwb
Het nieuwe artikel 47a Dwb maakt het, met het oog op een doelmatige uitvoering, expliciet mogelijk voor het drinkwaterbedrijf om de risicobeoordeling van het watervoorzieningssysteem en de VRA in samenhang voor te bereiden en uit te voeren, zodat een geïntegreerde risicobeoordeling en een geïntegreerd proces van totstandkoming en beoordeling door de Inspectie Leefomgeving en Transport (ILT) mogelijk wordt.

[17] Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water (herschikking) (*PbEU* 2020, L 435).

Artikel 35 (intrekking Besluit beveiliging netwerk- en informatiesystemen)

Artikel 103 Cbw regelt de intrekking van de Wbni. Het Besluit beveiliging netwerk- en informatiesystemen (hierna: Bbni) vindt zijn grondslag in de Wbni. Met de intrekking van de Wbni is er geen grond meer voor het Bbni en het Bbni moet dan ook worden ingetrokken. Dit wordt geregeld in artikel 35 Cbb.

Artikel 36 (inwerkingtreding)

Artikel 36 Cbb bepaalt dat het Cbb in werking treedt op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld. Op grond van dit artikel kan worden gekozen voor een gefaseerde inwerkingtreding. Dit is denkbaar in het geval dat bepaalde onderdelen van het Cbb nog niet in werking kunnen treden, terwijl dat bij andere onderdelen van het Cbb wel het geval is. De verwachting is dat bij de inwerkingtreding van (onderdelen van) het Cbb een uitzondering wordt gemaakt op de vaste verandermomenten en de minimuminvoeringstermijn, omdat het Cbb strekt ter uitvoering van de Cbw, en die wet ziet op de implementatie van een bindende EU-rechtshandeling.

Artikel 37 (citeertitel)

Artikel 37 Cbb bepaalt dat de citeertitel van dit besluit luidt: Cyberbeveiligingsbesluit.

De Minister van Justitie en Veiligheid,