NOTA VAN TOELICHTING

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 Cyberbeveiligingsbesluit

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 ook wel 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 18 Cbb. Voor een toelichting op deze artikelen wordt verwezen naar de artikelsgewijze toelichting.

De artikelen 6 tot en met 16 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 waarop de Uitvoeringsverordening (EU) 2024/2690[2] 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 16 Cbb op een groot aantal entiteiten biedt een gemeenschappelijk basisniveau voor de digitale weerbaarheid van een groot aantal essentiële entiteiten en belangrijke entiteiten.

---

[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 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 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.

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 en soorten entiteiten, bijvoorbeeld vanwege de specifieke aard van een bepaalde sector, subsector of soort 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 20 tot en met 23 Cbb worden regels gesteld over de hiervoor bedoelde training. Deze regels zien onder meer op de eisen aan de training, de trainer 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 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. In artikel 2 Cbb wordt geregeld welke partij voor essentiële entiteiten en belangrijke entiteiten als CSIRT wordt of kan worden aangewezen. Voor een toelichting hierop wordt verwezen naar de artikelsgewijze toelichting op deze bepaling.

Daarnaast is in artikel 17, eerste lid, Cbw bepaald dat één van de als CSIRT aangewezen partijen bij algemene maatregel van bestuur 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.

3. Gevolgen

Aan de hand van interviews met het bedrijfsleven is een inschatting gemaakt van de regeldruk als gevolg van de Cbw en het Cbb.

Bedrijven geven aan al diverse maatregelen op het gebied van de beveiliging van hun netwerk- en informatiesystemen te hebben genomen. Het huidige wettelijke kader (Wet beveiliging netwerk- en informatiesystemen, hierna: Wbni) ligt hieraan ten grondslag, maar ook andere regelgeving zoals de Algemene verordening gegevensbescherming en sectorspecifieke wetgeving. Met het Cbb verwachten bedrijven zowel eenmalige als structurele kosten te maken, boven op de kosten die reeds worden uitgegeven ter beveiliging van de netwerk- en informatiesystemen.

Eenmalige regeldruk
De eenmalige regeldrukkosten voorvloeiend uit de zorgplicht bestaan voor de meeste bedrijven uit de voorbereidingen van de uit te voeren maatregelen en de eenmalige implementatiekosten van deze maatregelen. Het uitvoeren van een *gap assessment* vormt een belangrijk onderdeel van deze voorbereiding. Het aanpassen van bestaande en het invoeren van nieuwe werkprocessen vormen daarnaast een andere kostenpost. Een laatste eenmalige kostenpost betreft de aanschaf van soft- en hardware.

Tabel 1. Eenmalige regeldrukgevolgen Cbw & Cbb

Artikel	**Aantal personen**	**Kosten per persoon**	**Tijds-besteding in uren (totaal)**	**Uurtarief**	**Out-of-pocket (€)**	**Aantal**	**Kosten (P×Q)**
Artikel 21 Cbw (zorgplicht)	-	-	2.177	€ 54,00	€ 33.750	8.100	**€ 1.225.594.800**
Artikel 24 Cbw (governance)	6	€ 2.469	-	-	-	8.100	**€ 119.993.400**
Artikel 44 Cbw (informatie-verstrekking t.b.v. registratie in nationaal register)	-	-	5	€ 54,00	-	8.100	**€ 2.187.000**
Totaal							**€ 1.347.775.200**
Gemiddeld per bedrijf							**€ 166.392**

In het kader van de eisen omtrent de governance dient het bestuur van een bedrijf kennis te hebben van cyberbeveiliging en -hygiëne. Bedrijven geven aan dat dit veelal al het geval is omdat er al scholing, vaak intern, verzorgd wordt. De verwachte regeldruk is gelegen in dat de cursus of opleiding door een externe partij moet worden verzorgd en dat bij de huidige scholing geen certificaat wordt uitgereikt zoals dit verplicht wordt gesteld in het Cbb. Dit betekent dat bestuursleden opnieuw moeten worden geschoold.

Bedrijven verwachten dat de registratieplicht gepaard gaat met eenmalige tijdbesteding om het bedrijf te registreren bij het Nationaal Cyber Security Centrum. In tabel 1 worden per wetsartikel uit de Cbw de eenmalige regeldrukkosten weergegeven die bedrijven verwachten te maken om aan de Cbw en onderliggende regelgeving te voldoen.

Structurele regeldruk
De zorgplicht en de eisen op het gebied van governance die worden gesteld in de Cbw en het Cbb resulteren naar verwachting ook in structurele regeldrukkosten voor bedrijven. De structurele regeldrukgevolgen die voorvloeien uit de zorgplicht betreffen primair de aspecten die meer diepgang of een bredere scope van toepassing vereisen dan de maatregelen die bedrijven op dit moment al nemen. Bedrijven verwachten met name kosten te maken bij de beoordeling van risico's in de toeleveringsketen, omdat er verder gekeken moet worden in de keten dan alleen de directe leveranciers. Ook incidentenbehandeling en de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen worden genoemd als bron van regeldruk. Veel van de bedrijven geven aan het dat het moeilijk is om een precieze inschatting te geven van de regeldrukgevolgen van de zorgplicht omdat de tijdsbesteding of out-of-pocket kosten pas goed inzichtelijk worden wanneer de Cbw in werking is getreden. De berekende structurele regeldrukkosten die voortvloeien uit de zorgplicht dienen daarom als een voorlopige inschatting te worden beschouwd.
De verwachte regeldrukkosten die voortvloeien uit de verplichtingen op het gebied van governance betreffen de kosten die worden gemaakt om nieuwe bestuursleden te laten scholen op het gebied van netwerk- en informatiesystemen en het periodiek scholen van het zittende bestuur. Bedrijven verwachten vooral de regeldruk te ervaren ten gevolge van de verplichting dat een externe opleider de scholing moet verzorgen.

Tabel 2. Structurele regeldrukgevolgen Cbw & Cbb

Artikel	Aantal personen	Kosten per persoon	Tijds-besteding in uren (totaal)	Uurtarief	Out-of-pocket (€)	Aantal	Kosten (P×Q)
Artikel 21 Cbw (zorgplicht)	-	-	968	€ 77,00	€ 25.000	8.100	**€ 806.241.600**
Artikel 24 Cbw (governance)	0,3	2.469	-	-	-	8.100	**€ 5.999.700**
Totaal							**€ 812.241.300**
Gemiddeld per bedrijf							**€ 100.300**

Panel mkb
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, governance en registratieplicht.
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.
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.
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. Gepleit wordt voor het werken met doelvoorschriften, waarbij precieze invulling aan de ondernemers wordt gelaten. Faciliteer maatwerk, is hierbij de kernboodschap. Daarnaast wordt de suggestie gedaan om de ISO27001-standaard als kapstok te hanteren, omdat veel mkb'ers al bekend zijn met dit normenkader.
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.
Met betrekking tot de inwerkingtreding van de Cbw en het Cbb 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 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 gestelde eisen op het gebied van governance van de Cbw en het Cbb zijn behoorlijk uitgebreid, zo merken de deelnemers op. De eis dat een trainer een onafhankelijke partij, dat wil zeggen 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 er voor 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 een pleidooi voor proportionele en evenredige eisen.
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 Nationaal Cyber Security Centrum (NCSC) die namens de Minister van Justitie en Veiligheid, als centraal contactpunt zal fungeren en het nationaal register zal beheren. Ook met betrekking tot de registratieplicht zou het mkb-panel graag harmonisatie en afstemming tussen EU-lidstaten zien. Het is niet werkbaar wanneer sommige mkb'ers zich mogelijk 27 keer moeten registreren.

4. Advies en consultatie

PM

5. Overgangsrecht en inwerkingtreding

PM

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 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 Nationaal Cyber Security Centrum (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 én de omstandigheid dat het Ministerie van Justitie en Veiligheid, meer in het bijzonder het daarvan deel uitmakende NCSC, voldoet aan de eisen die krachtens artikel 11, eerste lid, NIS2-richtlijn aan een CSIRT worden gesteld. Van belang is hierbij bovendien dat deze aanwijzing in lijn ligt met de aanwijzing van de Minister van Justitie en Veiligheid als CSIRT voor de meeste aanbieders van essentiële diensten krachtens de huidige Wbni.

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 én 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).

Bij genoemde ministeriële regelingen kan de betrokken vakminister op grond van artikel 16, tweede lid, Cbw, na overleg met de Minister van Justitie en Veiligheid, ook nog regels stellen over onder meer de functionele en organisatorische vereisten waaraan het CSIRT zal moeten voldoen. 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 Nationaal Cyber Security Centrum. Voor deze aanwijzing is gekozen, niet alleen omdat de Minister van Justitie en Veiligheid zoals hierboven toegelicht 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.

Ter uitvoering van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn heeft de Europese Commissie de Uitvoeringsverordening (EU) 2024/2690[3] (hierna: de uitvoeringsverordening) vastgesteld. De uitvoeringsverordening is op grond van artikel 16 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 16 en 24 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 cloudcomputingdienst. 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 de 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 de Cbb in haar hoedanigheid van internetknooppunt.

Artikel 5 (uitvoering van artikel 21 van de wet)

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

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 18 Cbb, moeten nemen, waarmee zij uitvoering geven aan de zorgplicht uit artikel 21 Cbw.

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 Cbb wordt deze verplichting verder uitgewerkt.

In artikel 6, eerste lid, Cbb is opgenomen dat het hiervoor bedoelde beleid schriftelijk moet zijn vastgesteld en aantoonbaar moet worden toegepast. In artikel 6, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten in het kader van dat beleid de rollen, verantwoordelijkheden en bevoegdheden in relatie tot de beveiliging van hun netwerk- en informatiesystemen vaststellen. Hiermee bewerkstelligen entiteiten dat alle rollen, verantwoordelijkheden en bevoegdheden met betrekking tot de beveiliging van netwerk- en informatiesystemen kenbaar zijn.

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 de 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. Doordat het beleid daadwerkelijk wordt toegepast, kunnen de netwerk- en informatiesystemen op de juiste wijze beveiligd worden.

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. 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, zodat afgewogen besluiten kunnen worden genomen over de beveiliging van de netwerk- en informatiesystemen en het aantoonbaar is welke maatregelen er zijn genomen of welk beleid is vastgesteld. Voorbeelden hiervan zijn een Information Security Management Systeem (ISMS) zoals de ISO 27000-reeks of het Cyber Security Management System (CSMS) op basis van EIC 62443.

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 risicoanalyses. 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 en dat de entiteit op basis van dit beleid maatregelen neemt om op een structurele wijze tot een beveiligingsniveau te komen dat is afgestemd op de risico's. Met structureel wordt cyclisch bedoeld. Er is voor gekozen om risicomanagement als terminologie te hanteren, 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 beleidslijnen 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.

Bij het in kaart brengen van de dreigingen, kwetsbaarheden en afhankelijkheden hanteert de entiteit een *all hazard*-benadering. Een te beschermen belang is datgene wat belangrijk is voor 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 de mogelijkheid van compromittering, nadelige gevolgen, of een risico daarop, kunnen ontstaan voor het functioneren van de entiteit en haar dienstverlening. De risico's worden door het nemen van maatregelen op structurele wijze teruggebracht naar een acceptabel niveau aan de hand van de geïdentificeerde relevante risico's.

Hierbij 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. De maatregelen 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 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 netwerk- en informatiesystemen een onderdeel van het bredere risicobeheerproces van de entiteit te zijn.

Artikel 7, tweede lid, Cbb vereist onder meer dat essentiële entiteiten en belangrijke entiteiten ter uitvoering van het hiervoor bedoelde beleid een risicomanagementmethodiek vaststellen. Het doel van een risicomanagementmethodiek is op een gestandaardiseerde wijze risicoacceptatiecriteria vast te stellen en om risico's te identificeren, te beoordelen en om vervolgens maatregelen te nemen om de risico's weg te nemen of te beperken.

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 beleid moeten hebben over incidentenbehandeling waarin de rollen, verantwoordelijkheden, bevoegdheden en procedures voor het tijdig detecteren van, analyseren en beoordelen van, reageren op, herstellen van, documenteren van en rapporteren en leren van incidenten worden vastgelegd. Dat beleid moet schriftelijk zijn vastgesteld en aantoonbaar worden toegepast. Incidentenbehandeling heeft als doel de impact van incidenten op het functioneren van de entiteit te voorkomen of te beperken.

Artikel 8, tweede lid, Cbb schrijft voor dat essentiële entiteiten en belangrijke entiteiten, als onderdeel van het hiervoor bedoelde beleid, procedures moeten vaststellen om activiteiten in hun netwerk- en informatiesystemen te monitoren en te registreren. Die procedures zijn bedoeld om incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden te detecteren, analyseren en classificeren. Met activiteiten wordt tenminste gedoeld op alle activiteiten die de dienstverlening, voor zover daarvoor gebruik wordt gemaakt van netwerk- en informatiesystemen, 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, derde lid, Cbb schrijft voor dat essentiële entiteiten en belangrijke entiteiten procedures vast moet stellen om de gevolgen van een incident te mitigeren, de oorzaak van een incident weg te nemen en te herstellen van een incident. Deze procedures hebben als doel snel te kunnen handelen wanneer een incident zich voordoet zodat de impact zoveel mogelijk beperkt kan worden.

Artikel 8, vierde lid, Cbb ziet op het loggen van activiteiten, handelingen en 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 zij opvolging kunnen geven aan de bevindingen die hieruit voortkomen. Entiteiten kunnen onder meer op basis van geïdentificeerde risico's als bedoeld in artikel 7 Cbb bepalen welke gegevens worden gelogd en welke loggegevens moeten worden beschermd tegen ongeautoriseerde toegang of wijzigingen.

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 moeten omvatten. In artikel 9 Cbb wordt deze verplichting verder uitgewerkt.

Artikel 9, eerste lid, Cbb bepaalt dat essentiële entiteiten en belangrijke entiteiten een bedrijfscontinuïteit- en noodvoorzieningenplan moeten hebben vaststellen. 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.

Indien een incident zich voordoet die de bedrijfscontinuïteit in gevaar kan brengen moet het bedrijfscontinuïteit- en noodvoorzieningenplan door de entiteit worden toegepast. Dit plan richt zich op het continueren van de dienstverlening tijdens de incident totdat deze kan worden hersteld en hervat. Bij het opstellen van het plan kunnen entiteiten rekening houden met de geïdentificeerde risico's als bedoeld in artikel 7 Cbb.

De afweging welke processen en procedures moeten worden beschreven in het plan, is aan de entiteit en 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-omgeving is het denkbaar dat dat niet zal volstaan. Bij hen is het denkbaar dat een uitgebreider plan met een verdeling van rollen, verantwoordelijkheden en bevoegdheden van betrokkenen binnen en buiten de entiteit nodig is.

Artikel 9, eerste lid, Cbb schrijft ook voor dat essentiële entiteiten belangrijke entiteiten het bedrijfscontinuïteits- en noodvoorzieningenplan periodiek moeten testen en beoefenen. Op deze wijze kunnen zij controleren of het plan nog steeds werkt en nog actueel is.

In artikel 9, tweede lid, Cbb is opgenomen dat essentiële entiteiten en belangrijke entiteiten procedures moeten vaststellen voor het vervangen van hardware en voor het maken, terugzetten en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens. Dit moeten zij doen om een passend niveau van beschikbaarheid en integriteit van de software en gegevens, en de continuïteit van netwerk- en informatiesystemen te borgen. Het doel van deze procedures is om zo snel mogelijk de dienstverlening te hervatten en de duur en de gevolgen van een incident te beperken. In het bijzonder is het hierbij van belang dat entiteiten waarborgen treffen tegen incidenten als gevolg waarvan back-ups, al dan niet door acties van kwaadwillenden, onbruikbaar worden. Ook de vertrouwelijkheid van back-ups dient gewaarborgd te worden, om zo ongeautoriseerde wijziging van gegevens te voorkomen.

In artikel 9, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten een crisisbeheersingsplan moeten hebben. Daarin moeten in elk geval de rollen, verantwoordelijkheden en bevoegdheden voor het personeel en andere in de entiteit werkzame personen ten tijde van een crisis worden beschreven. Dit maakt de tijdige en adequate inzet in crisissituaties mogelijk. Het plan moet ook de communicatiemiddelen tussen de entiteit, het CSIRT en de bevoegde autoriteit ten tijde van een crisis beschrijven. Waar passend moet het plan ook het gebruik van beveiligde noodcommunicatiesystemen beschrijven. Van belang is dat de entiteit het crisisbeheersingsplan periodiek test en beoefent, zodat ten tijde van een crisis alle betrokkenen bekend zijn met hun rol en verantwoordelijkheden.

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 eerder genoemde 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. Entiteiten moeten in dat beleid hun omgang bepalen met afhankelijkheden van de producten en diensten van hun leveranciers en dienstverleners die invloed kunnen hebben op de beveiliging van hun netwerk- en

informatiesystemen. Het hebben van dat beleid is nodig, omdat entiteiten veelal gebruik maken van geleverde producten en diensten die van belang zijn voor de beveiliging van de netwerk- en informatiesystemen die de entiteit voor haar werkzaamheden of dienstverlening gebruikt.

In artikel 10, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten indien mogelijk schriftelijke afspraken moeten maken met hun rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten van hun leveranciers en dienstverleners die invloed kunnen hebben op de beveiliging van de netwerk- en informatiesystemen van die essentiële entiteiten en belangrijke entiteiten. Die schriftelijke afspraken moeten zien op de aan die rechtstreekse leveranciers en rechtstreekse dienstverleners te stellen cyberbeveiligingseisen. Entiteiten zijn, in het bijzonder waar het grote leveranciers of dienstverleners betreffen, niet altijd in de positie om over cyberbeveiligingseisen te onderhandelen. In dat geval zal de entiteit op basis van haar cyberbeveiligingseisen moeten beoordelen of het cyberbeveiligingsniveau dat de betreffende leverancier aanbiedt passend is gezien de risico's. De entiteit moet ook beoordelen of er aanvullende maatregelen getroffen moeten worden of dat er voor een andere leverancier moet worden gekozen.
Ook moet deze entiteiten borgen dat deze afspraken worden nagekomen en dat deze actueel worden gehouden. Bij het maken van deze afspraken kunnen entiteiten onder meer rekening houden met de geïdentificeerde risico's, bedoeld in artikel 7 Cbb. Dit betekent dat de gemaakte afspraken kunnen variëren per rechtstreekse leverancier of dienstverlener.

In artikel 10, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten een actueel overzicht moeten bijhouden van de hiervoor bedoelde rechtstreekse leveranciers en rechtstreekse dienstverleners. Ook moeten zij bijhouden welke diensten of producten, zoals hiervoor bedoeld, worden geleverd en welke afspraken, zoals hiervoor bedoeld, zij met hun rechtstreekse leveranciers en rechtstreekse dienstverleners hebben gemaakt. Dit overzicht stelt entiteiten in staat om bijvoorbeeld in het geval van een incident snel te kunnen schakelen met de juiste 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 analyses in het kader van het uitvoeren van het beleid over risicomanagement, bedoeld in artikel 7 Cbb, eisen moeten vaststellen over de beveiliging van hun netwerk- en informatiesystemen. Deze eisen maken indien mogelijk deel uit van de overeenkomsten bij de verwerving van software, hardware of diensten die betrekking hebben op de netwerk- en informatiesystemen. De reden hiervoor is dat hiermee wordt bereikt dat alleen verwerving van producten of diensten plaatsvindt als dat voldoet aan de beveiligingseisen én zo de beveiligingsrisico's met betrekking tot de netwerk- en informatiesystemen kunnen worden beheerst.

In artikel 11, tweede lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten indien van toepassing procedures moeten opstellen voor de veilige ontwikkeling van hun netwerk- en informatiesystemen. Deze procedures hebben betrekking op alle ontwikkelingsfasen van de netwerk- en informatiesystemen. Die fasen betreffen in ieder geval specificatie, ontwerp, implementatie, onderhoud, beheer, beëindiging en vernietiging. Het is denkbaar dat entiteiten daarbij *security by design* of *security by default* als uitgangspunt hanteren 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 de ontwikkeling extern kan worden uitbesteed. Het uitbesteden ontslaat de entiteit niet van de verplichting om te zorgen dat de ontwikkeling van haar netwerk- en informatiesystemen op een veilige manier gebeurt.

In artikel 11, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten procedures moeten opstellen voor het onderhoud en beheer van hun netwerk- en informatiesystemen. Het onderhoud en beheer kan worden uitbesteed. De hiervoor bedoelde 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 procedures moeten ook ten minste betrekking hebben op het veranderingsbeheer van de netwerk- en informatiesystemen, zodat entiteiten op gecontroleerde wijze wijzigingen in de netwerk- en informatiesystemen doorvoeren.

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.

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 met betrekking tot hun netwerk- en informatiesystemen 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. Dit voor zover dat relevant is voor de functie. 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. Ook moeten zij ervoor zorgen dat dat personeel en andere binnen de entiteit werkzame personen regelmatig opleiding krijgen over de beveiliging van de netwerk- en informatiesystemen. Deze opleidingen kunnen bijvoorbeeld betrekking hebben op de werking en beveiliging van de netwerk- en informatiesystemen, bekende dreigingen of werkwijzen van kwaadwillenden en incidentbehandeling. Met die opleidingen wordt voor het betrokken personeel en andere binnen de entiteit werkzame personen de voor hun rollen, verantwoordelijkheden en bevoegdheden benodigde kennis en kunde over de beveiliging van de netwerk- en informatiesystemen ook steeds actueel gehouden.

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 beleid hebben over het gebruik van cryptografie. Het doel van cryptografie en bijbehorend beleid is om te voorkomen dat ongeautoriseerde gebruikers toegang hebben tot de data van de entiteit. Door middel van cryptografie is de data voor ongeautoriseerde gebruikers onleesbaar. 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.

In artikel 13, tweede lid, Cbb is bepaald dat het hiervoor bedoelde beleid in ieder geval is uitgewerkt in welke gevallen cryptografie wordt ingezet en welke type encryptie worden gebruikt. Door dit inzichtelijk te maken past de entiteit cryptografie op een consistente en juiste wijze toe. 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 en verantwoordelijkheden 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 assetsmoeten omvatten. In artikel 14 Cbb wordt deze verplichting verder uitgewerkt, specifiek over de beveiligingsaspecten ten aanzien van het personeel.

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. Doordat de entiteit 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 netwerk- en informatiesystemen onvoldoende beveiligd worden. De hiervoor bedoelde aanwijzing moeten zij op grond van artikel 14, tweede lid, Cbb periodiek evalueren en indien nodig bijwerken. 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 betrouwbaarheidseisen moeten opstellen waaraan hun personeel en andere binnen 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 tot hun netwerk- en informatiesystemen. Logische toegang houdt het beheersen van de toegang tot netwerk- en informatiesystemen in en vereist de authenticatie van de identiteit van een individu via een mechanisme, zoals een toegangspas, token of cijfercode. Het doel van dat beleid is om ongeautoriseerde logische en fysieke toegang tot hun netwerk- en informatiesystemen te voorkomen. Het is denkbaar dat de entiteit daarbij het need-to-know-principe 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 dat beleid in elk geval omvatten: het uitgeven, monitoren, gebruiken en intrekken van identiteiten, authenticaties en autorisaties, en het beheer van logbestanden van toegang, identiteiten, authenticaties en autorisaties. Deze aspecten worden voorgeschreven, zodat ongeautoriseerde toegang tot en wijzigingen in de netwerk- en informatiesystemen kan worden gedetecteerd en waar mogelijk worden voorkomen.

In artikel 15, derde lid, Cbb is bepaald dat essentiële entiteiten en belangrijke entiteiten identiteiten, authenticaties en autorisaties periodiek moeten beoordelen op de noodzakelijkheid, juistheid en actualiteit. Zo nodig moeten zij de toekenning daarvan wijzigen. Door deze periodieke toets op noodzakelijkheid en juistheid kan de toekenning van een identiteit, authenticatie of autorisatie tijdig worden aangepast, bijvoorbeeld als (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 en de werking van de netwerk- en informatiesystemen die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken. Het is van belang dat zij een dergelijk beleid hebben, omdat de entiteit door een goed inzicht in haar netwerk- en informatiesystemen haar risico's beter kan inschatten en gerichter informatie over kwetsbaarheden kan vinden.

In artikel 16, tweede lid, Cbb is bepaald dat het hiervoor bedoelde beleid in elk geval een systeem moet omvatten om netwerk- en informatiesystemen 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 voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en gerelateerde netwerk- en informatiesystemen. Door netwerk- en informatiesystemen te classificeren kan de entiteit vaststellen welk beveiligingsniveau ten aanzien van de netwerk- en informatiesystemen passend is. Dit is mede relevant in de context van de continuïteit van de dienstverlening, bedoeld in artikel 9 Cbb.

In artikel 16, derde lid, Cbb, is bepaald dat essentiële entiteiten en belangrijke entiteiten een volledige en actuele inventaris van informatie en andere gerelateerde netwerk- en informatiesystemen moeten hebben en deze inventaris moeten bijhouden. Deze inventaris dient voor de beveiliging van de netwerk- en informatiesystemen relevante registraties te bevatten, zoals de netwerk- en informatiesystemen 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 entiteiten deze attenderingen, adviezen en informatie ontvangen moeten zij beoordelen of op basis daarvan aanpassingen of aanvullingen nodig zijn van de maatregelen die nodig zijn ter uitvoering van de zorgplicht. Zij moeten de uitkomsten van die beoordeling schriftelijk vastleggen. Het is denkbaar dat adviezen niet altijd (direct) opgevolgd worden wanneer de gevolgen van het opvolgen schadelijker zijn dan de gevolgen van de kwetsbaarheid zelf.

Artikel 18 (evaluatie)

In artikel 18 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 daarvan 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 deze maatregelen moeten worden geëvalueerd. De periode tussen de evaluaties kan afhankelijk zijn van technologische ontwikkelingen, veranderingen in de sector of binnen de entiteit, en veranderingen in risico's en dreigingen waarmee de entiteit geconfronteerd wordt en die invloed hebben op de beveiliging van netwerk- en informatiesystemen. Door in de evaluatie te motiveren waarom bepaalde keuzes worden gemaakt, kan worden vastgesteld of voldaan wordt aan de zorgplicht.

Artikel 19 (nadere regels)

In artikel 19 Cbb is een grondslag opgenomen om bij ministeriële regelingen van de vakministers 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 en soorten 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 19 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, en is dus niet enkel beperkt tot de maatregelen die in artikel 21, derde lid, Cbw worden genoemd en die zijn uitgewerkt in het Cbb.

Artikel 20 (doel van de training)

Artikel 24, tweede lid, Cbw bepaalt dat ieder lid van het bestuur van de essentiële entiteit of belangrijke entiteit 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 essentiële entiteit of belangrijke 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 20 Cbb wordt het doel van de training bepaald. De training moet bestuursleden in staat stellen om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren 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 21 (eisen aan de training)

In artikel 21 Cbb wordt geregeld waar de training (te volgen door ieder lid van het bestuur van een essentiële entiteit en belangrijke entiteit), 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.

Artikel 21, 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 21, 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 22 (eisen aan de trainer)

In artikel 22 Cbb worden eisen gesteld aan de trainer van de training, bedoeld in artikel 24, vijfde lid, Cbw.

In artikel 22, eerste lid, Cbb, is bepaald dat de trainer onafhankelijk en gekwalificeerd moet zijn. De vereiste onafhankelijkheid houdt in dat de training niet gegeven kan worden door een persoon die verantwoordelijk is voor de beveiliging van netwerk- en informatiesystemen binnen de betreffende essentiële entiteit of belangrijke entiteit. Uiteraard is het wel mogelijk dat een persoon met dergelijke verantwoordelijkheden, zoals een *chief information security officer* (CISO), wel aanwezig is bij een training om waar nodig toelichting te geven over specifieke context van de essentiële entiteit of belangrijke entiteit.

Artikel 22, tweede lid, Cbb ziet op de vereiste specifieke kennis en kunde van de trainer, zodat de trainer in staat is om de kennis en vaardigheden waar bestuursleden over moeten beschikken, over te dragen.

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 minstens 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.

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 algemene maatregel van bestuur 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 entiteit. 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. 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 sectorbreed en dus op alle entiteiten uit alle sectoren van toepassing kunnen zijn. Door subdelegatie kunnen die 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. 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 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, (zo mogelijk) een prognose van de hersteltijd en (zo mogelijk) de door de essentiële entiteit of belangrijke entiteit genomen maatregelen om de gevolgen van het significante incident te beperken of herhaling hiervan te voorkomen. Hiermee kan onder meer beter worden ingeschat of en hoe respons mogelijk is, en kan ook beter worden ingeschat wat mogelijke cascade-effecten zijn op bijvoorbeeld andere entiteiten. In het verlengde hiervan is het ook relevant dat de entiteit, zo mogelijk, melding maakt van de door haar genomen of te nemen maatregelen om de gevolgen van het significante incident te beperken of herhaling hiervan te voorkomen.

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 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 (verstrekking overige informatie)

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, indien van toepassing, 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 entiteiten. 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 Wbni, 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. 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 entiteiten 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 er aan 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 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 bevoegde autoriteiten)

Artikel 51, tweede lid, onderdeel h, Cbw biedt de mogelijkheid om bij of krachtens amvb bevoegde 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 daartoe onderling alle daarvoor noodzakelijke gegevens uitwisselen.

In artikel 29 Cbb is een delegatiegrondslag opgenomen op grond waarvan de vakminister de hiervoor bedoelde (eerstgenoemde) bevoegde autoriteiten bij regeling kan aanwijzen. De reden voor het doordelegeren is dat naar verwachting vooral bevoegde autoriteiten zullen worden aangewezen die uit hoofde van sectorale regelgeving een rol hebben in het toezicht op entiteiten die ook onder toepassing van de Cbw vallen. Door dit bij regeling te regelen kan door de vakminister vanuit diens verantwoordelijkheid voor sectoren hier een passende invulling aan gegeven worden en waar nodig worden bijgesteld. De aanwijzing maakt het in het bijzonder voor bevoegde autoriteiten mogelijk om in het geval van overlappend toezicht nauwer samen te werken, informatie uit te wisselen en op die wijze doelmatig en doeltreffend toezicht te bevorderen en daarmee ook onnodige toezichtslasten voor entiteiten te beperken.

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, maximaal 60 maanden worden bewaard.

Een CSIRT verwerkt persoonsgegevens, slechts voor zover dat noodzakelijk is voor het uitvoeren van haar taken. Persoonsgegevens die het CSIRT verwerkt ten behoeve van zijn taken worden bovendien niet langer bewaard dan noodzakelijk. De maximale bewaartermijn is 60 maanden. Mailadressen en andere contactgegevens worden door het CSIRT verwerkt om entiteiten te kunnen informeren, bijstand te kunnen verlenen en te kunnen samenwerken met bijvoorbeeld andere CSIRT's. Voor de wettelijke taken zoals het monitoren en analyseren van cyberdreigingen kunnen allerlei soorten persoonsgegevens worden verwerkt. Dit komt voornamelijk doordat het bij deze wettelijke taken gaat over het verwerken van incidentinformatie. In incidentinformatie kunnen mogelijk ook persoonsgegevens zitten. Denk daarbij aan IP-adressen van slachtoffers, inloggegevens en dergelijke. Dergelijke gegevens die soms ook persoonsgegevens zijn, moeten langer worden bewaard dan het afhandelen van het incident bijvoorbeeld ten behoeve van analyse wanneer blijkt 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. Dat is de reden dat deze informatie maximaal 60 maanden bewaard dient te worden. De in de memorie van toelichting van de Wet beveiliging netwerk- en informatiesystemen benoemde bewaartermijnen voor persoonsgegevens vanwege bijvoorbeeld de benodigde analyse in de praktijk te kort gebleken om haar taken uit te voeren en persoonsgegevens te verwerken zoals voor 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 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 gekozen voor een termijn van 60 maanden.

Artikel 30, tweede lid, Cbb bevat een uitzondering op het eerste lid voor de persoonsgegevens die worden verwerkt in het kader van het nationaal register, bedoeld in artikel 43 Cbw. Voor deze persoonsgegevens geldt een maximale bewaartermijn van 60 maanden na de laatste wijziging van de betreffende persoonsgegevens. Het bepalen 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 wijziging van de contactgegevens.

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 toezichtsdossier 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. Daarom is ervoor gekozen om een uiterlijke bewaartermijn voor persoonsgegevens van 120 maanden aan te houden. 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 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 vastgesteld.[4] Deze verordening, die op een groot deel van de financiële sector van toepassing is, wordt hierna aangeduid als de Verordening digitale operationele weerbaarheid.

Banken, exploitanten van handelsplatformen en centrale tegenpartijen vallen zowel onder het toepassingsbereik van de Verordening digitale operationele weerbaarheid, 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, Verordening digitale operationele weerbaarheid 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 Verordening digitale operationele weerbaarheid 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 (AFM of 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 Verordening digitale operationele weerbaarheid 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.

[4] *PbEU* 2022, L 333.

Artikel 19, tweede lid, Verordening digitale operationele weerbaarheid 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 hebben doorgaans 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. Behoudens de maatregelen op grond van de Telecommunicatiewet komt de beveiliging van elektronische communicatienetwerken onder de Cbw te vallen. 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 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 wordt gegeven aan de zorgplicht die thans onder de Cbw valt, zijn geschrapt. 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 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, onderdeel b, Telecommunicatiewet) zijn een invulling van het nationaal beleid. Het gaat hierbij om het treffen van beveiligingsmaatregelen zodat de continuïteit van radio-uitzendingen die in het bijzonder van belang is bij radiokanalen met de functie van calamiteitenzender zo goed mogelijk wordt geborgd. Dit nationale beleid wordt voortgezet (onderdeel E). De implementatie van de NIS2-richtlijn doorkruist dit ook grotendeels niet.

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 Telecommunicatiewet ter uitvoering van de NIS2-richtlijn.

Artikel 33 (wijziging Besluit veiligheid en integriteit telecommunicatie)

Na artikel 2 Besluit veiligheid en integriteit telecommunicatie wordt een omhangbepaling ingevoegd, als gevolg van de wijziging van de grondslag in de Telecommunicatiewet 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[5].

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

[5] 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).

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.

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,