LEESWIJZER:

Dit document is een concept van een hoofdstuk in de ministeriële regeling waarin een nadere uitwerking is opgenomen van de zorgplicht (hoofdstuk 4 van het concept-cyberbeveiligingsbesluit (Cbb). Om belanghebbenden in staat te stellen zich een volledig beeld te vormen van de technische, organisatorische en operationele maatregelen die essentiële en belangrijke entiteiten moeten nemen, wordt dit concepthoofdstuk nu reeds gedeeld en gelijktijdig met het concept-Cyberbeveiligingsbesluit (Cbb) ter consultatie voorgelegd.

Voor wie

De regels uit de concept-ministeriële regeling zullen **niet** van toepassing worden op overheids-organisaties (zie artikel 2 Reikwijdte) en de entiteiten zoals genoemd in artikel 4 van het Cyberbeveiligingsbesluit.

Dit concept geldt voor essentiële, belangrijke en kritieke entiteiten in de volgende sectoren en subsectoren.

Minister	**Sector**	**Subsector**
Onze Minister van Klimaat en Groene Groei	energie	elektriciteit
		stadsverwarming en -koeling
		aardolie
		aardgas
		waterstof
Onze Minister van Economische Zaken	digitale infrastructuur	Aanbieders van internetknooppunten
		Aanbieders van openbare elektronische communicatienetwerken
		Aanbieders van openbare elektronische communicatiediensten
	ruimtevaart	
	post- en koeriersdiensten	
	vervaardiging	vervaardiging van informaticaproducten en van elektronische en optische producten
		vervaardiging van elektrische apparatuur
		vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd

		vervaardiging van motorvoertuigen, aanhangers en opleggers
		vervaardiging van andere transportmiddelen
Onze Minister van Infrastructuur en Waterstaat	vervoer	lucht
		spoor
		water
		weg
	drinkwater	
	afvalwater	
	afvalstoffenbeheer	
	vervaardiging, productie en distributie van chemische stoffen	
Onze Minister van Landbouw, Visserij, Voedselzekerheid en Natuur	productie, verwerking en distributie van levensmiddelen	

Van wie

Deze concept ministeriële regeling is een gezamenlijk document van de ministeries van Economische Zaken (EZ), Klimaat en Groene Groei (KGG), Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN), en Infrastructuur en Waterstaat (IenW). Deze ministeries werken aan een (zoveel mogelijk) uniforme kader voor de zorgplicht voor de entiteiten in hun sectoren. Ieder van deze ministers zal een (eigen) ministeriële regeling vaststellen, waarin de zorgplicht opgenomen zal worden. In die ministeriële regelingen zullen daarnaast ook andere aspecten opgenomen worden, zoals de drempelwaarden voor significante incidenten, waarvoor de meldplicht geldt.

CONCEPT-artikelen

Grondslag: artikel 19 van het Cyberbeveiligingsbesluit

Artikel 1 (begripsbepalingen)

[PM begripsbepalingen]

Artikel 2 (reikwijdte)

Deze regeling is van toepassing op essentiële entiteiten en belangrijke entiteiten, die geen overheidsinstantie zijn, en die vallen onder een of meer van de volgende sectoren:

Minister	**Sector**	**Subsector**
Onze Minister van Klimaat en Groene Groei	energie	elektriciteit
		stadsverwarming en -koeling
		aardolie
		aardgas
		waterstof
Onze Minister van Economische Zaken	digitale infrastructuur	Aanbieders van internetknooppunten
		Aanbieders van openbare elektronische communicatienetwerken
		Aanbieders van openbare elektronische communicatiediensten
	ruimtevaart	
	post- en koeriersdiensten	
	vervaardiging	vervaardiging van informaticaproducten en van elektronische en optische producten
		vervaardiging van elektrische apparatuur
		vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd
		vervaardiging van motorvoertuigen, aanhangers en opleggers

		vervaardiging van andere transportmiddelen
Onze Minister van Infrastructuur en Waterstaat	vervoer	lucht
		spoor
		water
		weg
	drinkwater	
	afvalwater	
	afvalstoffenbeheer	
	vervaardiging, productie en distributie van chemische stoffen	
Onze Minister van Landbouw, Visserij, Voedselzekerheid en Natuur	productie, verwerking en distributie van levensmiddelen	

Paragraaf [PM]. Nadere invulling zorgplicht

Artikel 3 (Beleid over beveiliging van netwerk- en informatiesystemen - artikel 6 van het Cyberbeveiligingsbesluit)

1. Een essentiële entiteit of een belangrijke entiteit bewaakt de consistentie van beleid als bedoeld in hoofdstuk 4 van het Cyberbeveiligingsbesluit.

2. Het beleid over beveiliging van netwerk- en informatiesystemen, bedoeld in artikel 6, eerste lid, van het Cyberbeveiligingsbesluit, sluit aan bij de bredere bedrijfsstrategie en -doelstellingen van de essentiële entiteit of de belangrijke entiteit en omvat:

a. ten minste doelstellingen met betrekking tot de beveiliging van netwerk- en informatiesystemen die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt; en

b. een beschrijving van de passende en evenredige middelen die noodzakelijk zijn voor de uitvoering van de onder a genoemde doelstellingen.

3. De essentiële entiteit of de belangrijke entiteit stelt, als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het Cyberbeveiligingsbesluit, beleid vast voor het beoordelen van de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's. Dit beleid omvat ten minste het volgende:

a. de maatregelen, bedoeld in artikel 21, eerste lid, van de wet, voor het beheer van cyberbeveiligingsrisico's die de entiteit monitort en meet, analyseert en evalueert;

b. de methoden voor het monitoren, meten, analyseren en evalueren van de onder a bedoelde maatregelen;

c. de frequentie van de monitoring, de meting, de analyse en het evalueren van de onder a bedoelde maatregelen;

d. de voorwaarden voor het analyseren en evalueren van de resultaten van de monitoring en meting;

e. de verantwoordelijke voor het monitoren en meten van de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's.

Artikel 4 (Beleid over risicomanagement - artikel 7 van het Cyberbeveiligingsbesluit)

1. In de procedures, bedoeld artikel 7, tweede lid, onderdeel b, van het Cyberbeveiligingsbesluit, wordt in ieder geval vastgesteld op welke wijze:

a. de risicocriteria voor de beveiliging van netwerk- en informatiesystemen worden vastgesteld en onderhouden, waaronder de risicoacceptatiecriteria en de criteria voor het uitvoeren van risicobeoordelingen;

b. de risico's voor de beveiliging van netwerk- en informatiesystemen en de risico-eigenaren worden geïdentificeerd;

c. de geïdentificeerde risico's op basis van de potentiële gevolgen en de waarschijnlijkheid dat de risico's zich voordoen worden geanalyseerd;

d. de vastgestelde risico's voor de beveiliging van netwerk- en informatiesystemen worden geëvalueerd;

e. passende en evenredige opties voor de behandeling van de risico's voor de beveiliging van netwerk- en informatiesystemen in kaart worden gebracht en beheersmaatregelen worden vastgesteld die nodig zijn om de gekozen opties voor de behandeling van de risico's voor de beveiliging van netwerk- en informatiesystemen te implementeren;

f. de risicobeheersmaatregelen worden geselecteerd en geformuleerd in een risicobehandelingsplan alsmede de goedkeuring van de risico-eigenaren voor het risicobehandelingsplan en hun acceptatie van de resterende risico's voor de beveiliging van netwerk- en informatiesystemen wordt verkregen.

2. De evaluatie, bedoeld in het eerste lid, onderdeel d, vindt plaats door de resultaten van de risicoanalyse te vergelijken met de vastgestelde risicocriteria, bedoeld in het eerste lid, onderdeel a, en deze te prioriteren voor risicobehandeling.

Artikel 5 (Bedrijfscontinuïteit - artikel 9 van het Cyberbeveiligingsbesluit)

1. Het bedrijfscontinuïteitplan, bedoeld in artikel 9, eerste lid, van het Cyberbeveiligingsbesluit, houdt rekening met de uitgevoerde beoordeling en herbeoordeling van risico's, bedoeld in artikel 7 van het Cyberbeveiligingsbesluit. Dit bedrijfscontinuïteitplan bevat, waar passend, in ieder geval:

a. doel en reikwijdte;

b. de verdeling van taken, verantwoordelijkheden, en bevoegdheden van betrokkenen;

c. belangrijkste contacten en (interne en externe) communicatiekanalen;

d. voorwaarden voor activering en deactivering van het plan;

e. herstelplannen voor activiteiten, met inbegrip van hersteldoelstellingen;

f. het beschrijven van de vereiste middelen, met inbegrip van back-ups en redundanties.

2. De procedures, bedoeld in artikel 9, tweede lid, van het Cyberbeveiligingsbesluit, omvatten in ieder geval:

a. gegevens waarvan back-ups worden gemaakt;

b. hersteltijden;

c. herstelpunten;

d. waarborgen van integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;

e. de wijze van herstel van gegevens uit back-ups;

f. bewaartermijnen.

Artikel 6 (Beveiliging van toeleveringsketen - artikel 10 van het Cyberbeveiligingsbesluit)

Waar passend, houden de afspraken, bedoeld in artikel 10, tweede lid, van het Cyberbeveiligingsbesluit, ten minste in:

a. een verplichting voor rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten om de essentiële entiteit of belangrijke entiteit onverwijld in kennis te stellen van incidenten die een risico vormen voor de beveiliging van de netwerk- en informatiesystemen van die entiteiten;

b. een verplichting voor rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten om kwetsbaarheden te verhelpen die een risico vormen voor de beveiliging van de netwerk- en informatiesystemen van de betrokken entiteit;

c. verplichtingen die rusten op de rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten bij beëindiging van de overeenkomst.

Artikel 7 (Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen - artikel 11 van het Cyberbeveiligingsbesluit)

1. De eisen, bedoeld in artikel 11, eerste lid, van het Cyberbeveiligingsbesluit omvatten ten minste:

a. de vereisten die worden gesteld aan de cyberbeveiliging van de ICT-diensten of ICT-producten en aan de configuratie die nodig is voor de veilige werking van ICT-producten;

b. vereisten inzake beveiligingsupdates gedurende de gehele levensduur van de ICT-diensten of ICT-producten, of vervanging na het einde van de ondersteuningsperiode;

c. de vereisten voor het bewijs door leveranciers van ICT-diensten of ICT-producten dat deze voldoen aan de vermelde beveiligingseisen, bedoeld in artikel 10, tweede lid, van het Cyberbeveiligingsbesluit, alsmede documentatie van de resultaten van de validering.

2. De procedures, bedoeld in artikel 11, derde lid, van het Cyberbeveiligingsbesluit, voor het onderhoud en beheer van haar netwerk- en informatiesystemen, hebben betrekking op ten minste de procedures inzake:

a. beveiligingspatches;

b. bescherming van netwerk- en informatiesystemen tegen kwaadaardige en ongeoorloofde software;

c. technische kwetsbaarheden;

d. netwerksegmentatie.

3. Ter uitvoering van artikel 21, derde lid, onderdeel e, van de wet:

a. controleert, waar passend, de essentiële entiteit of belangrijke entiteit de beveiligingspatches op integriteit en of beveiligingspatches afkomstig zijn van betrouwbare bronnen;

b. test, waar passend, de essentiële entiteit of belangrijke entiteit beveiligingspatches voordat zij in de productieomgeving worden toegepast;

c. past de essentiële entiteit of belangrijke entiteit beveiligingspatches toe binnen een redelijke termijn nadat zij beschikbaar zijn, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen. De entiteiten legt de onderbouwing van een dergelijk besluit vast.

d. implementeert de essentiële entiteit of belangrijke entiteit maatregelen om het gebruik van kwaadaardige en ongeoorloofde software te detecteren en te voorkomen;

e. evalueert de essentiële entiteit of belangrijke entiteit haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft;

f. voert de essentiële of belangrijke entiteit waar passend periodiek kwetsbaarheidsscans uit en legt zij de resultaten van de scans vast;

g. verhelpt de essentiële entiteit of belangrijke entiteit onverwijld kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen, of motiveert waarom de kwetsbaarheid niet of op een later moment verholpen wordt en documenteert dit.

h. gebruikt de essentiële entiteit of belangrijke entiteit segmentatie om te verhinderen dat een kwetsbaarheid of ongeautoriseerde toegang tot een netwerk- of informatiesysteem gebruikt kan worden om andere netwerk- of informatiesystemen te compromitteren en de entiteit houdt daarbij rekening met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen.

Artikel 8 (Beveiligingsaspecten ten aanzien van personeel - artikel 14 van het Cyberbeveiligingsbesluit)

1. De essentiële entiteit of belangrijke entiteit heeft, vastgesteld beleid over de beveiligingsaspecten ten aanzien van haar personeel en andere binnen de entiteit werkzame personen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Het beleid, bedoeld in het eerste lid, omvat in elk geval een procedure die waarborgt dat het personeel en andere binnen de entiteit werkzame personen op de hoogte zijn van en handelen in overeenstemming met hun taken, verantwoordelijkheden en bevoegdheden inzake beveiliging van netwerk- en informatiesystemen.

3. De essentiële entiteit of belangrijke entiteit waarborgt, waar passend, dat het personeel en andere binnen de entiteit werkzame personen de beveiliging van netwerk- en informatiesystemen toepassen overeenkomstig de in het Cyberbeveiligingsbesluit en deze regeling voorgeschreven procedures.

Artikel 9 (Beveiligingsaspecten ten aanzien van toegangsbeleid - artikel 15 van het Cyberbeveiligingsbesluit)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over het toewijzen en het gebruik van speciale toegangsrechten voor de logische en fysieke toegang tot netwerk- en informatiesystemen, welke op basis van de noodzaak en per gebeurtenis aan gebruikers worden toegekend, in overeenstemming met het beleid over de logische en fysieke toegang tot haar

netwerk- en informatiesystemen, bedoeld in artikel 15, eerste lid van het Cyberbeveiligingsbesluit. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over authenticatieprocedures en -mechanismen, waaronder multi-factor authenticatie, waarbij de sterkte van gebruikersauthenticatie in verhouding staat tot de risico's voor de beveiliging van de netwerk- en informatiesystemen waartoe toegang wordt verleend. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

Artikel 10 (Beveiligingsaspecten ten aanzien van beheer van assets - artikel 16 van het Cyberbeveiligingsbesluit)

De inventaris, bedoeld in artikel 16, derde lid, van het Cyberbeveiligingsbesluit, bevat ten minste:

a. het classificatieniveau van de asset op basis van vereisten inzake de beveiliging van netwerk- en informatiesystemen van alle assets;

b. de voor de beveiliging relevante kenmerken en eigenschappen van de asset; en

c. de voor de beveiliging relevante informatie over rechtstreekse leveranciers of rechtstreekse dienstverleners met betrekking tot de asset;

d. een aanduiding van de processen waarvoor de asset wordt gebruikt.

TOELICHTING

Artikelsgewijze toelichting

Artikel 3 - Beleid over beveiliging van netwerk- en informatiesystemen

Artikel 3 bevat aanvullende eisen ten opzichte van artikel 6 van het Cyberbeveiligingsbesluit (Cbb), ten aanzien van het beleid over de beveiliging van netwerk- en informatiesystemen en ten aanzien van de managementsystematiek.

Het eerste lid bepaalt dat het beleid inzake de beveiliging van netwerk- en informatiesystemen, zoals bedoeld in artikel 6 van het Cyberbeveiligingsbesluit en dit artikel, consistent dient te zijn met de andere thematische beleidsverplichtingen die in hoofdstuk 4 van het Cyberbeveiligingsbesluit zijn opgenomen, waaronder het beleid ten aanzien van de risicomanagement en het beleid inzake de beveiliging van de toeleveringsketen.

Aangezien de netwerk- en informatiesystemen diverse aspecten van de bedrijfsvoering van de entiteit beïnvloeden, dient de beveiliging van deze systemen een integraal onderdeel te vormen van het algemene organisatiebeleid van de entiteit. Dat betekent, zoals vermeld in artikel 3, tweede lid, dat de entiteit bij het opstellen van het beleid inzake de beveiliging van netwerk- en informatiesystemen ervoor moet zorgen dat het beleid zo goed mogelijk aansluit bij de bredere organisatiestrategie en -doelstellingen. Om er ook voor te zorgen dat het beleid ook daadwerkelijk uitgevoerd kan worden zal de entiteit hiervoor ook middelen moeten vrijmaken, zoals vermeld in artikel 3, tweede lid, onderdeel b. Financiële middelen zullen bijvoorbeeld nodig zijn voor onder andere het hebben van het benodigde personeel en aan het ontwikkelen of inkopen of uitbesteden van ICT-producten, -diensten of -processen.

Artikel 3, derde lid, stelt dat er beleid nodig is voor het beoordelen van de effectiviteit van de maatregelen voor het beheer de cyberbeveiligingsrisico's en dat dit beleid onderdeel dient te zijn van de managementsystematiek van de essentiële en de belangrijke entiteit. Het doel van een managementsystematiek is ervoor te zorgen dat de netwerk- en informatiebeveiligingsrisico's van de organisatie inzichtelijk zijn, om maatregelen te nemen om de risico's te beheersen en waar nodig bij te stellen om op een structurele wijze risico's terug te brengen tot een acceptabel niveau. Om dit te kunnen doen, dient de essentiële entiteit en belangrijke entiteit beleid te hebben op het monitoren, meten, analyseren en evalueren van de maatregelen. Het beleid omvat daarbij ten minste een methode hoe dit wordt gedaan, de frequentie daarvan en de aangestelde verantwoordelijke om dit beleid uit te voeren.

Artikel 4 – Beleid over risicomanagement

In artikel 4 is opgenomen dat de genoemde procedures uit artikel 7, tweede lid, onderdeel b, van Cyberbeveiligingsbesluit (Cbb), ten minste de wijze vaststelt: waarop de risicocriteria worden vastgesteld, de risico's worden geïdentificeerd, deze risico's worden geanalyseerd, deze risico's worden geëvalueerd, de risicobehandeling in kaart wordt gebracht en risicobeheersmaatregelen worden vastgesteld. De uitkomsten van deze procedures vormen een belangrijk fundament voor de andere maatregelen die de belangrijke of essentiële entiteit dient te nemen voor de bescherming van haar netwerk- en informatiesystemen.

In onderdeel a is opgenomen dat de procedure in het artikel 4 moet vastleggen op welk wijze risicocriteria voor de beveiliging van de netwerk- en informatiesystemen worden vastgesteld en onderhouden.
Onder risicocriteria wordt verstaan criteria voor risicoacceptatie en criteria voor het uitvoeren van risicobeoordelingen. Risicoacceptatie criteria kunnen worden gebruikt voor het beoordelen van risico's waarbij de entiteit bepaalt wanneer zij een risico acceptabel vindt of niet. Bovendien kunnen de risicoacceptatie criteria worden gebruikt om te bepalen of een risicobeheersmaatregel voldoende is om tot een acceptabel risiconiveau te komen of dat verdere risicobehandeling nodig is. Voor het bepalen van de risicoacceptatiecriteria dient rekening te worden gehouden met de bredere context van de entiteit en verschillende beïnvloedende

factoren, zoals: organisatiedoelen, operationele activiteiten, technische- of financiële beperkingen of relaties met leveranciers of dienstverleners. Vaak zijn waarschijnlijkheid en impact bepalende criteria bij de acceptatie van een risico. Zo kan een bepaald risico grote impact hebben (bijvoorbeeld in termen van financiële gevolgen, verstoring van de dienstverlening of reputatieschade) waardoor het ondanks een mogelijk lage waarschijnlijkheid niet wordt geaccepteerd. De grens voor risicoacceptatie hangt af van de risicobereidheid van de essentiële entiteit of belangrijke entiteit.
Criteria voor het uitvoeren van risicobeoordelingen gaat over de betekenis die aan een risico wordt gegeven door bijvoorbeeld te kijken naar de mogelijke gevolgen en de waarschijnlijkheid die gezamenlijk het risiconiveau bepalen (bijvoorbeeld: heel laag, laag, medium, hoog, heel hoog). De criteria die de entiteit heeft vastgesteld dienen als basis voor het analyseren van de risico's.

Onderdeel b stelt dat de procedure moet vastleggen op welke wijze risico's en risico-eigenaren worden geïdentificeerd. Voor het identificeren van risico's dient gekeken te worden naar risico's waarmee entiteiten mogelijk geconfronteerd kunnen worden die impact kunnen hebben op de organisatiedoelen ten aanzien van de beveiliging van netwerk- en informatiesystemen. Hierbij kan bijvoorbeeld gedacht worden aan het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatie- en netwerkbeveiliging. Zoals toegelicht in de nota van toelichting bij het Cyberbeveiligingsbesluit, houdt de essentiële entiteit of belangrijke entiteit hierbij rekening met de te beschermen belangen, dreigingen, kwetsbaarheden en afhankelijkheden. 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. Ook dienen de risico-eigenaren in kaart gebracht te worden bij de geïdentificeerde risico's. Hierbij kan gedacht worden aan het bestuur, managers van verschillende afdelingen, proceseigenaren of asset eigenaren. Het gaat er in ieder geval om dat de risico-eigenaren verantwoordelijkheid hebben voor het behandelen van de risico's en in de positie zijn om hierop besluiten te nemen. De acceptatie van rest-risico's wordt schriftelijk vastgelegd. Gebruikelijk is dat dit in een risico-register gebeurt.

In onderdeel c wordt geregeld dat de procedure moet vastleggen op welke wijze de geïdentificeerde risico's en de waarschijnlijkheid dat deze zich voordoen worden geanalyseerd . Met het analyseren van de risico's wordt bedoeld dat per risico de potentiële gevolgen van risico's (impact) in kaart worden gebracht en de waarschijnlijkheid dat dit risico zich voordoet. Hierbij kan gebruik worden gemaakt van verschillende methodieken, zoals kwantitatief, kwalitatief of beiden om waardes aan de waarschijnlijkheid en impact te hangen. Hierbij wordt gebruik gemaakt van de vastgestelde risicocriteria, bedoeld in onderdeel a. Het gezamenlijke niveau van de waarschijnlijkheid en impact vormen samen het risiconiveau.

Onderdeel van het proces voor het beheer van risico's ten aanzien van de netwerk- en informatiesystemen is het evalueren van risicoanalyses. Dit is geregeld in onderdeel d. Hierdoor kunnen nieuwe inzichten en eventuele nieuwe risico's worden meegenomen waarop de maatregelen worden aangepast. Door te motiveren waarom bepaalde keuzes worden gemaakt, kan worden vastgesteld in hoeverre voldaan wordt aan de zorgplicht. Doel van het opnemen van de verschillende elementen in de motivering, is dat alle aspecten worden meegewogen in het vaststellen en nemen van passende en evenredige maatregelen.

Onderdeel d stelt dat de procedure moet vastleggen op welke wijze uit het de risico worden geëvalueerd. In het tweede lid van artikel 4 is daar nadere invulling aan gegeven. De uitkomsten van de risicoanalyse worden naast de risicoacceptatie criteria gelegd om te bepalen welke risico's worden geaccepteerd en welke risico's behandeling vergen waarbij een prioritering wordt gemaakt aan de hand van het risiconiveau dat is vastgesteld bij de risicoanalyse.

Onderdeel e stelt dat de procedure moet vastleggen op welke wijze opties in kaart worden gebracht om de risico's wel of niet te mitigeren en op welke wijze beheersmaatregelen worden vastgesteld. Opties voor risicobehandeling kunnen zijn: risico acceptatie, risicovermijding, risico preventie, risico repressie waarbij de gevolgen van een risico worden verkleind mocht het risico zich toch voordoen, het behouden van een risico of het delen van een risico waarbij de

verantwoordelijkheid wordt gedeeld met interne of externe partijen (bijvoorbeeld via verzekeringen). Bij het vaststellen en prioriteren van passende en evenredige opties voor risicobehandelingen risicobeheermaatregelen houdt de essentiële entiteit of belangrijke entiteit rekening met de resultaten van de risicobeoordeling, de resultaten van de procedure om de doeltreffendheid van risicobeheersmaatregelen op het gebied van cyberbeveiliging te beoordelen, en met de uitvoeringskosten in verhouding tot het verwachte voordeel.

De maatregelen voor het beheer van cyberbeveiligingsrisico's, bedoeld in onderdeel e, moeten gebaseerd zijn op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen te beschermen tegen gebeurtenissen die de beschikbaarheid, de authenticiteit, de integriteit of de vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via netwerk- en informatiesystemen worden aangeboden, in gevaar kunnen brengen, zoals diefstal, brand, overstromingen en telecommunicatie- en stroomstoringen of ongeoorloofde fysieke toegang tot, beschadiging van of interferentie met de informatie- en informatieverwerkingsfaciliteiten van een entiteit. Bij de vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's moet daarom ook aandacht worden besteed aan de fysieke en omgevingsbeveiliging van netwerk- en informatiesystemen door maatregelen op te nemen om dergelijke systemen te beschermen tegen systeemstoringen, menselijke fouten, kwaadaardige handelingen of natuurverschijnselen.

Onderdeel f schrijft voor dat de procedure de wijze moet vastleggen wijze waarop risicobeheersmaatregelen worden geselecteerd en geformuleerd in een risicobehandelingsplan, alsmede de goedkeuring van de risico-eigenaren voor het risicobehandelingsplan en hun acceptatie van de resterende risico's voor de beveiliging van netwerk- en informatiesystemen wordt verkregen. Het kan zijn dat een essentiële entiteit of belangrijke entiteit na een expliciete risico evaluatie bepaalde risico's accepteert waarvoor goedkeuring nodig is.

Artikel 5 - Bedrijfscontinuïteit

Artikel 5 beschrijft de nadere maatregelen die de belangrijke entiteit of essentiële entiteit moet nemen op het vlak van bedrijfscontinuïteitplan, bedoeld in artikel 9 van het Cyberbeveiligingsbesluit.

Bedrijfscontinuïteitsplan

De belangrijke entiteit of essentiële entiteit dient een bedrijfscontinuïteitsplan op te stellen, om zo voorbereid te zijn op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen en om op dergelijke incidenten goed en tijdig te kunnen reageren, om zo de duur en gevolgen van dergelijke incidenten te beperken. Bij het opstellen daarvan moet zij rekening houden met de risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit, zodat zij alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen. De onderdelen van het eerste lid omschrijven de onderdelen die normaliter geadresseerd zouden moeten worden in het plan. Met de zinssnede "waar passend" wordt tot uitdrukking gebracht dat de invulling van het bedrijfscontinuïteitsplan dient aan te sluiten bij de bedrijfsvoeringscontext van de betreffende belangrijke entiteit of essentiële entiteit. In de praktijk kan het bedrijfscontinuïteitsplan zoals hier bedoeld deel uitmaken van een algemeen bedrijfs- en continuïteitsplan van de belangrijke en essentiële entiteit.

Door te zorgen voor ten minste gedeeltelijke redundantie van netwerk- en informatiesystemen, assets (met inbegrip van faciliteiten, uitrusting en benodigdheden), personeel met de nodige verantwoordelijkheid, bevoegdheid en bekwaamheid en passende communicatiekanalen zorgen de essentiële entiteit en belangrijke entiteit ervoor dat er voldoende middelen beschikbaar zijn om de primaire processen doorgang te laten vinden.

Back-upplannen

Op basis van de risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit en het bedrijfscontinuïteitsplan dient de belangrijke entiteit of essentiële entiteit back-upplannen vast te stellen. De onderdelen artikel 5, tweede lid, omschrijven welke aspecten in de back-upplannen terug dienen te komen. Het back-up plan beschrijft allereerst van welke gegevens back-ups gemaakt dienen worden. Het bepalen van hersteltijden, in het Engels ook wel bekend als *recovery time objective (RTO),* ziet op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. Herstelpunten, in het Engels ook wel bekend als *recovery point objective (RPO),* ziet op de frequentie van de back-ups. Daarnaast dient de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups gewaarborgd te worden, zodat de back-ups ook daadwerkelijk ingezet kunnen worden. In het bijzonder is hierbij van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door acties van kwaadwillenden zoals ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups dient gewaarborgd te worden, om zo ongeautoriseerde toegang tot gegevens te voorkomen. De risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit zijn derhalve zowel relevant voor het bepalen van welke gegevens in back-ups dienen te worden opgenomen, als het bepalen van de eerdergenoemde waarborgen. Het is tevens van belang dat de vertrouwelijkheid, integriteit en beschikbaarheid van de back-ups doorlopend gemonitord wordt, zodat de belangrijke en essentiële entiteit tijdig wordt geïnformeerd over tekortkomingen. Het plan dient tevens te omschrijven op welke wijze de gegevens hersteld kunnen worden. Ook dienen de back-upplannen te omschrijven hoe lang de betreffende back-ups bewaard moeten worden. Ten slotte dient de belangrijke entiteit en essentiële entiteit, waar mogelijk, periodiek het terugzetten van back-ups te testen, om zo de werking van back-ups in de praktijk te testen. Enerzijds beoefenen belangrijke entiteiten en essentiële entiteiten op deze wijze het terugzetten van back-ups, zodat zij bij incidenten over de kennis en vaardigheden beschikken om dit uit te voeren. Anderzijds biedt het testen meer zekerheid dat er geen technische belemmeringen zijn om de back-ups daadwerkelijk terug te zetten.

Artikel 6 - Beveiliging van de toeleveringsketen

Dit artikel werkt artikel 10, tweede lid, van het Cyberbeveiligingsbesluit nader uit. Het gaat hierom afspraken die de essentiële entiteit en belangrijke entiteit dienen te maken met haar rechtstreekse leveranciers en dienstverleners. Dit artikel stelt nadere criteria over wat deze afspraken, waar passend, ten minste moeten bevatten.

Wanneer er een cyberincident bij een rechtstreekse leverancier of dienstverlener plaatsvindt of wanneer er een kwetsbaarheid is gedetecteerd, is het van belang dat een essentiële entiteit en belangrijke entiteit zo snel mogelijk op de hoogte worden gesteld in het geval dit een risico kan vormen voor de beveiliging van haar netwerk- en informatiesystemen. Afspraken maken over de aanpak van kwetsbaarheden en wanneer en hoe dit wordt gemeld is daarbij van belang. Tevens is ook van belang om afspraken te maken over verplichtingen die rusten op de rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten bij beëindiging van de overeenkomst. Met het treffen van deze afspraken wordt de beveiliging en digitale weerbaarheid van de toeleveringsketen verhoogd. Hiermee wordt de kans verkleind dat er een cyberincident in de toeleveringsketen plaatsvindt of dat de cascade effecten van zo'n incident worden beperkt. Bij het maken van de afspraken, houdt de essentiële entiteit of belangrijke entiteit rekening met haar risicoanalyses waarbij de te maken afspraken in verhouding dienen te staan tot het te beheersen risico.

Artikel 7 - Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Artikel 7, eerste en tweede lid, zijn een uitwerking van artikel 11 van het Cyberbeveiligingsbesluit. De essentiële entiteit en belangrijke entiteit hebben, op basis van artikel 11, eerste lid van het Cyberbeveiligingsbesluit, beleid met betrekking tot alle ontwikkelingsfasen van haar netwerk- en informatiesystemen. In het eerste lid is omschreven dat dit beleid in elk geval vereisten bevatten voor de cyberbeveiliging van de ICT-diensten of producten en de configuratie die nodig is voor de veilige werking ervan, vereisten voor beveiligingsupdates gedurende de gehele levensduur van ICT-producten of diensten, en vereisten voor het vanuit leveranciers laten leveren van bewijs dat de geleverde ICT-diensten of ICT-producten aan de vermelde beveiligingseisen voldoen. ICT-producten en ICT-diensten omvat zowel informatietechnologie als operationele technologie. Hierbij kan Security by design of zero trust architectuur als uitgangspunt voor de inrichting en ontwikkelingen van software, hardware en diensten worden gebruikt. Hierdoor wordt er al tijdens het ontwerp rekening gehouden met beveiligingsmaatregelen. De essentiële en belangrijke entiteit kan beveiligingsvoorschriften vaststellen met betrekking tot de ontwikkelingsomgevingen, beveiligingstestprocessen vaststellen en toepassen in de omgevingscyclus, gegevens over beveiligingstests op passende wijze selecteren, beschermen, en beheren, en testgegevens saneren en anonimiseren. Hierdoor kan de essentiële entiteit en belangrijke entiteit zich beter beschermen tegen cyberdreigingen, zoals ransomware, insider threat en hacking. Hiermee wordt er afstand genomen van security achteraf, waarbij de beveiligingsaanpak pas in gang wordt gezet wanneer zich problemen voordoen en als er iets misgaat.

Artikel 11, derde lid, van het Cyberbeveiligingsbesluit stelt essentiële en belangrijke entiteiten verplicht om procedures te hebben voor het onderhoud en beheer van haar netwerk- en informatiesystemen. In dit artikel is gespecificeerd dat deze procedures ten minste betrekking dienen te hebben op beveiligingspatches, bescherming van netwerk- en informatiesystemen tegen kwaadaardige en ongeoorloofde software, technische kwetsbaarheden, en netwerksegmentatie.

Om potentiële risico's voor de beveiliging van netwerk- en informatiesystemen weg te nemen dienen essentiële en belangrijke entiteiten, op grond van artikel 7, derde lid, onderdeel c beveiligingspatches toe te passen binnen een redelijk termijn nadat deze beschikbaar zijn. Voorafgaand aan het toepassen van de patches binnen de productieomgeving dienen deze patches op grond van artikel 7, derde lid, onderdeel a, waar passend gecontroleerd te worden of ze afkomstig zijn van betrouwbare bronnen en integriteit, en op grond van het derde lid, onderdeel b, dienen waar passend de patches getest te worden voor deze in de productieomgeving worden toegepast. Op grond van artikel 7, derde lid, onderdeel c, worden essentiële entiteiten en belangrijke entiteiten echter ook de ruimte geboden om beveiligingspatches niet toe te passen als de nadelen van de toepassing van beveiligingspatches zwaarder wegen dan de voordelen op het gebied van cyberbeveiliging. Hierbij kan gedacht worden aan het ongepland stilzetten van kritieke bedrijfsprocessen van een entiteit ter uitvoering van de patch, terwijl de patch ook uitgevoerd kan worden op een al ingepland moment van breder onderhoud aan de netwerk- en informatiesystemen. Indien een essentiële of belangrijke entiteit hiervoor kiest, dient de motivatie voor het niet of niet direct toepassen van de beveiligingspatch gedocumenteerd te worden zodat voor de toezichtspraktijk ook duidelijk is waarom er van een wettelijke vereiste wordt afgeweken, en of dit een terechte keuze was.

Ter bescherming van diens netwerk- en informatiesystemen dienen essentiële entiteiten en belangrijke entiteiten op grond van artikel 7, derde lid, onderdeel d, ook maatregelen te nemen tegen kwaadaardige en ongeoorloofde software. Typische oplossingen voor netwerkbeveiliging omvatten het gebruik van firewalls om de interne netwerken van de relevante entiteiten te beschermen, alsmede het gebruik van antivirus software om potentiële kwaadaardige software op te kunnen sporen.

Om risico's op incidenten te verminderen als gevolg van technische kwetsbaarheden dienen essentiële entiteiten en belangrijke entiteiten, op grond van artikel 7, derde lid, onderdeel e, haar blootstelling aan kwetsbaarheden en relevante dreigingen waar zij kennis van hebben te evalueren. Omdat kwetsbaarheden risico's met zich meebrengen voor het functioneren van een

entiteit haar netwerk- en informatiesystemen dienen entiteiten ook zelf waar passend periodiek kwetsbaarheidsscans uit te voeren en het resultaat hiervan vast te leggen, op grond van artikel 7, derde lid, onderdeel f.

Op grond van artikel 7, derde lid, onderdeel g nemen essentiële entiteiten en belangrijke entiteiten maatregelen om deze potentiële kwetsbaarheden te adresseren. Het kan ook voorkomen dat een kwetsbaarheid niet in volledigheid gemitigeerd kan worden. Indien potentiële gevolgen van kwetsbaarheden het rechtvaardigen, kunnen essentiële en belangrijke entiteiten een plan op te stellen en uit te voeren om de desbetreffende kwetsbaarheden te beperken. In alle overige gevallen dient het niet nemen van maatregelen tegen kwetsbaarheden op grond van artikel 7, derde lid, onderdeel g, naar behoren te worden gemotiveerd en gedocumenteerd. Evenals bij het niet toepassen van een beveiligingspatch wordt voor de toezichtspraktijk dan duidelijk waarom er van een wettelijke verplichting wordt afgeweken, en kan de toezichthouder oordelen of deze beslissing terecht is genomen.

Essentiële entiteiten en belangrijke entiteiten dienen ook te waarborgen dat bij incidenten niet alle onderdelen van netwerk- en informatiesystemen niet kunnen functioneren. Op grond van het derde lid, onderdeel h, dienen essentiële entiteiten en belangrijke entiteiten diens netwerken te segmenteren. Hierbij kunnen entiteiten zelf in acht nemen op welke wijze ze de netwerksegmentatie wordt toegepast, waarbij rekening gehouden wordt met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen. Een essentiële entiteit of een belangrijke entiteit doet er verstandig aan bij de netwerksegmentatie nadrukkelijk te betrekken of er sprake is van IT- en OT-systemen en deze zo mogelijk van elkaar te scheiden. Essentiële entiteiten en belangrijke entiteiten kunnen toegang verlenen tot een netwerk of zone op basis van een beoordeling van de beveiligingsvoorschriften, systemen die van cruciaal belang zijn voor de werking van de entiteit of voor de veiligheid in beveiligde zones houden, en een gedemilitariseerde zone in haar communicatiekanalen uitrollen om te waarborgen dat communicatie die afkomstig is van of bestemd is voor haar netwerken beveiligd is. Essentiële entiteiten en belangrijke entiteiten kunnen ook het specifieke netwerk voor het beheer van netwerk- en informatiesystemen scheiden van het operationele netwerk van de entiteit, de kanalen voor netwerkbeheer scheiden van ander netwerkverkeer, en de productiesystemen voor de diensten van de entiteit scheiden van de systemen die worden gebruikt voor de ontwikkeling en tests, met inbegrip van back-ups.

Artikel 8 - Beveiligingsaspecten ten aanzien van personeel

Artikel 8 is een uitwerking van artikel 14 van het Cyberbeveiligingsbesluit. Op zijn minst zorgen de essentiële entiteit en belangrijke entiteit ervoor dat haar personeel en overige bij de essentiële of belangrijke entiteit werkzame personen het beleid van de essentiële entiteit of belangrijke entiteit inzake de beveiliging van netwerk- en informatiesystemen kennen, begrijpen en toepassen. Dit is noodzakelijk om te waarborgen dat het personeel en andere werkzame personen van en bij de essentiële entiteit en belangrijke entiteit zich bewust zijn van de risico’s op het gebied van cyberbeveiliging, en als gevolg hiervan ook in staat zijn om risico’s te herkennen en juist op te reageren.

Het tweede lid schrijft voor dat essentiële entiteiten en belangrijke entiteiten een procedure hebben die waarborgt dat het personeel en andere binnen de entiteit werkzame personen op de hoogte zijn van en handelt in overeenstemming met diens taken, verantwoordelijkheden en bevoegdheden inzake beveiliging van netwerk- en informatiesystemen. Entiteiten kunnen deze verantwoordelijkheden vastleggen in arbeidsovereenkomsten of interne richtlijnen. Trainingen kunnen ook bijdragen aan het actueel houden van kennis bij het personeel.

Artikel 9 - Beveiligingsaspecten ten aanzien van toegangsbeleid

Artikel 9 is een uitwerking van artikel 15 van het Cyberbeveiligingsbesluit. De essentiële entiteit of belangrijke entiteit dient ook een vastgesteld beleid te hebben voor het toewijzen aan en

gebruik van speciale toegangsrechten door gebruikers waarbij speciale toegangsrechten op basis van noodzaak tot gebruik en per gebeurtenis aan gebruikers worden toegekend. Met gebruikers wordt bedoeld degene aan wie bepaalde toegangsrechten zijn verleend tot bepaalde fysieke ruimtes, digitale systemen en eventuele vertrouwelijke informatie, en dus ook toegang kunnen krijgen tot deze ruimtes, systemen, en informatie.

Het is hierbij ook van belang dat er is nagedacht over welke risico's er geaccepteerd worden bij het verlenen van toegang aan fysieke ruimtes, digitale systemen en eventuele vertrouwelijke informatie die belangrijk kunnen zijn voor de netwerk- en informatiebeveiliging.

Voor de toepassing van de verplichtingen inzake toegangsbeleid kunnen essentiële entiteiten en belangrijke entiteiten verder denken aan het toewijzen en intrekken van toegangsrechten op basis van de beginselen "need-to-know", "least privilege" en scheiding van functies. Verder kunnen essentiële en belangrijke entiteiten toegangsrechten bij beëindiging of verandering van baan dienovereenkomstig wijzigen, toegang toestaan tot netwerk- en informatiesystemen door relevante personen, en ervoor zorgen dat toegangsrechten op passende wijze betrekking hebben op toegang van derden, zoals bezoekers, leveranciers en dienstverleners, met name door de toegangsrechten te beperken in reikwijdte en duur. Essentiële entiteiten en belangrijke entiteiten kunnen tevens een register bijhouden van de verleende toegangsrechten, en het beheer van toegangsrechten loggen.

Artikel 10 - Beveiligingsaspecten ten aanzien van beheer van assets

Artikel 10 is een uitwerking van artikel 16 van het Cyberbeveiligingsbesluit. In dat artikel gaat het over 'beleid voor het beheer en de werking van netwerk- en informatiesystemen'. Om de risico's van de beveiliging van netwerk- en informatiesystemen te kunnen bepalen dienen de essentiële entiteit en belangrijke entiteit te weten welke netwerk- en informatiesystemen zij heeft en hoe deze zich verhouden tot de eigen activiteiten en dienstverlening. In ISO 27002 wordt dit aangeduid met 'informatie en andere gerelateerde bedrijfsmiddelen', waarbij onder bedrijfsmiddelen wordt verstaan: alles wat van waarde is voor het bedrijf. In deze regeling wordt het begrip asset gebruikt. Daaronder wordt niet verstaan 'personeel of medewerkers' en evenmin 'financiële middelen'. Wel kan bijvoorbeeld een specifieke licentie een onderdeel vormen van de assets.

Voor een goede bescherming van deze assets is het noodzakelijk om een actuele inventaris te hebben van de assets. Deze inventaris dient ook een classificatie, als bedoeld in artikel 16, tweede lid, van het Cyberbeveiligingsbesluit van assets te omvatten, de relevante kenmerken en eigenschappen voor de beveiliging van de assets, en voor de beveiliging relevante informatie over rechtstreekse leveranciers en dienstverleners met betrekking tot de assets. Bij relevante kenmerken kan onder meer gedacht worden aan waar onderdelen van die asset nog leverbaar zijn, of wanneer de asset vervangen wordt. Doel van de classificatie is om vast te stellen welk beveiligingsniveau passend is. Gebruikelijk is dat de classificatie plaatsvindt in termen van impact op de bedrijfsvoering, dit is onder meer in ISO 27002 de standaard. Uit de inventaris moet ook duidelijk worden voor welke processen de asset wordt gebruikt. De koppeling met het bedrijfscontinuïteitsplan is van belang omdat de classificatie van de assets en hun impact van hun uitval op de continuïteit betrokken moet worden bij het bedrijfscontinuiteitsplan.