STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 25478
23 juli 2026

Regeling van de Staatssecretaris van Landbouw, Visserij, Voedselzekerheid en Natuur van 16 juli 2026, nr. WJZ/107402891, houdende nadere regels over cyberbeveiliging voor essentiële en belangrijke entiteiten in de LVVN-sectoren (Regeling cyberbeveiliging LVVN) [KetenID WGK28488]

De Staatssecretaris van Landbouw, Visserij, Voedselzekerheid en Natuur, na overleg met de Minister van Justitie en Veiligheid;

Gelet op de artikelen 19, 23, eerste lid, en 28 van het Cyberbeveiligingsbesluit;

Besluit:

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:
– *besluit:* Cyberbeveiligingsbesluit;
– *levensmiddelenbedrijven:* levensmiddelenbedrijven als bedoeld in artikel 3, punt 2, van Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden (PbEG L 31) die zich bezighouden met groothandel en industriële productie en verwerking;
– *Minister:* minister van Landbouw, Visserij, Voedselzekerheid en Natuur;
– *zone:* een afgebakende groep van netwerk- en informatiesystemen.

Artikel 2. Reikwijdte

Deze regeling is van toepassing op essentiële en belangrijke entiteiten in de sectoren:
a. productie, verwerking en distributie van levensmiddelen, genoemd in bijlage 2 van de wet;
b. onderzoek, met als hoofddoel het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen, ten aanzien waarvan de minister ingevolge artikel 15, vierde lid, van de wet de bevoegde autoriteit is.

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen

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

Artikel 4. Bedrijfscontinuïteit

1. De processen en procedures voor het maken en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens, bedoeld in artikel 9, tweede lid, van het besluit, omschrijven van welke software en gegevens een back-up wordt gemaakt en bevatten ten aanzien van die software en gegevens:
   a. hersteltijden;
   b. herstelpunten;
   c. waarborgen voor de volledigheid en nauwkeurigheid van back-ups;
   d. waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
   e. waarborgen voor herstel van software en gegevens uit back-ups;
   f. bewaartermijnen.

2. Het bedrijfscontinuïteitsplan, bedoeld in artikel 9, derde lid, van het besluit, houdt rekening met de uitgevoerde beoordeling van risico's, bedoeld in artikel 7 van het besluit, en omvat in ieder geval:
   a. doel en reikwijdte;
   b. taken en verantwoordelijkheden;
   c. belangrijkste contacten en interne en externe communicatiekanalen;
   d. voorwaarden voor activering en de-activering van het bedrijfscontinuïteitsplan;
   e. vereiste middelen, met inbegrip van back-ups en redundanties;
   f. voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

Artikel 5. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

1. De processen en procedures, bedoeld in artikel 11, derde lid, van het besluit, hebben tevens betrekking op de processen en procedures inzake:
   a. beveiligingstesten;
   b. beveiligingspatchbeheer.

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

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

4. Ter uitvoering van artikel 21, derde lid, onderdeel g, van de wet segmenteert de essentiële entiteit of belangrijke entiteit:
   a. haar netwerk- en informatiesystemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het besluit bedoelde risicoanalyse;
   b. waar passend, haar netwerk- en informatiesystemen van de netwerk- en informatiesystemen van derden.

Artikel 6. Beveiligingsaspecten ten aanzien van toegangsbeleid

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

2. Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, zorgt ervoor dat:
   a. sterke identificatie-, authenticatie- en autorisatieprocedures voor bevoorrechte accounts en systeembeheeraccounts worden toegepast;
   b. voorrechten op het gebied van systeembeheer zoveel mogelijk geïndividualiseerd en beperkt worden toegekend;
   c. voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt.

Artikel 7. Criteria significant incident in de levensmiddelensector

1. Voor een essentiële entiteit of een belangrijke entiteit die levensmiddelenbedrijf is, is een operationele verstoring ernstig als bedoeld in artikel 25, tweede lid, onderdeel a, van de wet, indien deze voldoet aan een of meer van de volgende criteria:

a. de productie, verwerking of distributie van levensmiddelen gedurende ten minste 24 uur gedeeltelijk onderbroken is;
b. ten minste 50% van de productie, verwerking of distributie van levensmiddelen gedurende ten minste 12 uur onderbroken is; of
c. de productie, verwerking of distributie van levensmiddelen gedurende ten minste zes uur geheel onderbroken is.

2. In afwijking van het eerste lid is een geplande dienstonderbreking of een ander voorzien gevolg van onderhoudswerkzaamheden die door of namens een essentiële entiteit of een belangrijke entiteit worden uitgevoerd, geen ernstige operationele verstoring.

3. Voor een essentiële entiteit of een belangrijke entiteit die levensmiddelenbedrijf is, is materiële of immateriële schade aanzienlijk als bedoeld in artikel 25, tweede lid, onderdeel b, van de wet, indien deze voldoet aan een of meer van de volgende criteria:
   a. het incident heeft de dood van een of meer natuurlijke personen veroorzaakt of kan die veroorzaken;
   b. het incident heeft aanzienlijke schade aan de gezondheid van een of meer natuurlijke personen veroorzaakt of kan die veroorzaken;
   c. de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienst of levensmiddelen die de essentiële entiteit of belangrijke entiteit verleent of onderscheidenlijk produceert, verwerkt of distribueert, worden opgeslagen, verzonden of verwerkt, is aangetast; of
   d. sprake is van een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van de essentiële entiteit of belangrijke entiteit.

Artikel 8 Criteria significant incident in de sector onderzoek

Voor een essentiële entiteit of een belangrijke entiteit in de sector onderzoek als bedoeld in bijlage 2 bij de wet, ten aanzien waarvan de minister ingevolge artikel 15, vierde lid, van de wet de bevoegde autoriteit is, is een incident in ieder geval een significant incident als:
a. het incident heeft geleid of kan leiden tot de ongeoorloofde openbaarmaking van bedrijfsgeheimen als bedoeld in artikel 2, eerste lid, van Richtlijn (EU) 2016/943 van de essentiële entiteit of belangrijke entiteit; of
b. de integriteit, vertrouwelijkheid of authenticiteit van onderzoeksgegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast, waardoor aanzienlijke materiële of immateriële schade ontstaat bij andere entiteiten.

Artikel 9. Aanwijzing bevoegde autoriteiten

De volgende autoriteiten zijn aangewezen als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet:
a. de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur voor de taken uit hoofde van de Wet dieren;
b. de Minister van Volksgezondheid, Welzijn en Sport voor de taken uit hoofde van de Warenwet.

Artikel 10. Inwerkingtreding

Indien het bij koninklijke boodschap van 2 juni 2025 ingediende voorstel van wet houdende regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet) (Kamerstukken 36 764) tot wet is of wordt verheven en die wet in werking treedt, treedt deze regeling op hetzelfde tijdstip in werking.

Artikel 11. Citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging LVVN.

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

's-Gravenhage, 16 juli 2026

De Staatssecretaris van Landbouw, Visserij, Voedselzekerheid en Natuur,
S.P.A. Erkens

TOELICHTING

I. Algemeen

1. Inleiding

De Cyberbeveiligingswet implementeert de NIS2-richtlijn[1] en beoogt een hoger niveau van cyberweerbaarheid voor de onder haar werkingssfeer vallende essentiële en belangrijke entiteiten te bewerkstelligen. De Cyberbeveiligingswet verplicht deze entiteiten onder andere tot het treffen van passende technische en organisatorische maatregelen ter bevordering van de cyberweerbaarheid van hun netwerk- en informatiesystemen, alsmede tot het melden van significante incidenten die verband houden met de beveiliging daarvan.

In deze regeling worden de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) nader uitgewerkt voor de sector productie, verwerking en distributie van levensmiddelen.

2. Hoofdlijnen van de regeling

2.1 Algemeen

In deze regeling zijn verschillende verplichtingen uit de Cbw en het Cbb nader uitgewerkt ter bevordering van de beveiliging van de netwerk- en informatiesystemen. Verder omvat deze regeling een nadere invulling van de criteria voor de beoordeling of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, van de Cyberbeveiligingswet.
Daarnaast zijn in deze regeling autoriteiten aangewezen waarmee het CSIRT, de toezichthouder en het centrale contactpunt kan samenwerken en informatie uitwisselen.

2.2 Nadere regels zorgplicht

In deze regeling worden voor de in artikel 2 genoemde sectoren nadere regels gesteld ten aanzien van de zorgplicht, bedoeld in artikel 21 van de Cbw, zoals nader uitgewerkt in het Cbb. Het doel van deze nadere invulling is om de normen uit de wet en het besluit verder te concretiseren op onderdelen die worden gezien als van groot belang voor de beveiliging van netwerk- en informatiesystemen. Dit biedt duidelijkheid aan essentiële en belangrijke entiteiten en draagt bij aan een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen.
Bij het opstellen van deze nadere regels is aangesloten bij de systematiek van de Cbw, het Cbb en Uitvoeringsverordening (EU) 2024/2690. Daarmee is de regeling afgestemd op de systematiek van Uitvoeringsverordening (EU) 2024/2690, zodat entiteiten op wie die uitvoeringsverordening van toepassing is, beide kaders naast elkaar kunnen toepassen. Net zoals bij de uitwerking van de zorgplicht in de Cbw en het Cbb zijn bij het nader uitwerken van de zorgplicht in deze regeling bestaande normenkaders als uitgangspunt gehanteerd, zoals ISO 27001. Daarbij is gecontroleerd of de zorgplicht in deze regeling deze normenkaders niet doorkruist. In de toelichting wordt, waar van toepassing, naar bestaande normenkaders verwezen. Entiteiten behouden hiermee de ruimte om hun bestaande normenkader te blijven hanteren, mits zij ervoor zorgen dat de maatregelen die voortvloeien uit de in artikel 21 van de Cbw neergelegde zorgplicht en de uitwerking daarvan in het Cbb en deze regeling, zijn geborgd. Net zoals de Cbw en het Cbb gaat deze regeling uit van een risico gebaseerde aanpak en schrijft daarom niet in alle gevallen voor hoe invulling moet worden gegeven aan de maatregelen. Essentiële en belangrijke entiteiten dienen overeenkomstig de zorgplicht van artikel 21 van de Cbw deze maatregelen op passende en evenredige wijze in te vullen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken te beheersen en incidenten te voorkomen of de gevolgen ervan te beperken.

2.3 Nadere regels meldplicht

Deze regeling bevat nadere criteria voor de beoordeling of sprake is van een significant incident. Deze criteria zijn van toepassing op essentiële en belangrijke entiteiten binnen de sector productie, verwerking en distributie van levensmiddelen en de sector onderzoek waar de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur beleidsverantwoordelijkheid voor is.
De meldplicht geldt als zich een significant incident voordoet. Een incident is in artikel 1 van de Cbw

[1] 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 (NIS 2-richtlijn).

gedefinieerd als: '*een gebeurtenis die de beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit van netwerk- en informatiesystemen of diensten die worden aangeboden, in gevaar brengt*.' Op grond van artikel 25, tweede lid, Cbw is sprake van een significant incident als het incident een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of als het incident andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

In artikel 23, eerste lid, van het Cbb is bepaald dat de betrokken minister, na overleg met de Minister van Justitie en Veiligheid, bij regeling de criteria kan vaststellen op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, van de Cbw.

Bij de uitwerking van de nadere criteria is uitgegaan van het belang van de continuïteit van essentiële diensten en de leveringszekerheid van levensmiddelen.
Voor de beoordeling van de ernst van de operationele verstoring is gekeken naar de gevolgen voor de eigen essentiële dienst van de betrokken essentiële entiteit of belangrijke entiteit. De gevolgen voor derden zijn daarbij niet bepalend geweest.
Bij de uitwerking van de nadere criteria voor materiële en immateriële schade is rekening gehouden met de aard van de risico's die binnen de betrokken sectoren en met de doelstelling van de wet.

De in deze regeling opgenomen drempelwaarden bieden objectieve aanknopingspunten voor de beoordeling of sprake is van ernstige operationele verstoring of aanzienlijke materiële of immateriële schade.

Deze criteria vormen een gedeeltelijke nadere uitwerking van de wettelijke norm en beogen duidelijkheid te bieden over wanneer in ieder geval sprake is van een meldplichtig incident. Met het oog op de uitvoerbaarheid en de beperking van regeldruk voor entiteiten is ervoor gekozen om niet alle parameters uit artikel 25, tweede lid, van de Cbw nader uit te werken. Dit zou ertoe leiden dat entiteiten voor al die criteria specifieke processen zouden moeten inrichten om tijdig te kunnen vaststellen of zij aan die criteria voldoen, zoals het vaststellen van een meldcriterium voor financieel verlies. De meldplicht is in deze regeling dan ook niet uitputtend geregeld. Incidenten die voldoen aan de algemene criteria in de wet blijven in beginsel meldplichtig. De in de regeling opgenomen criteria zijn bedoeld als het primaire beoordelingskader voor entiteiten en voor het uitoefenen van toezicht en handhaving. De wettelijke criteria uit artikel 25, tweede lid, van de Cbw blijven onverkort van toepassing als vangnet voor gevallen die niet onder de in deze regeling opgenomen criteria vallen.

2.4 Aanwijzing autoriteiten

Een aantal wetten heeft nauwe raakvlakken met de Cbw. Het is daarom gewenst dat de bevoegde autoriteiten, CSIRT's en het centrale contactpunt onder de Cbw voor de doeltreffende en doelmatige uitvoering van hun taken samenwerken en informatie uitwisselen met de autoriteiten, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cbw.

3. Toezicht en handhaving

Met het toezicht op de naleving van deze regeling worden ambtenaren van de Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA) belast. De betreffende ambtenaren oefenen hun bevoegdheden uit met inachtneming van artikel 69 van de Cbw.

4. Notificatie

Deze regeling bevat geen technische voorschriften in de zin van richtlijn nr. 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PbEU 2015, L 241). Er is derhalve geen notificatie krachtens deze richtlijn nodig.

5. Regeldruk

Deze regeling veroorzaakt geen incidentele of structurele aanvullende regeldruk ten opzichte van de reeds berekende regeldruk voor essentiële en belangrijke entiteiten onder de Cbw en het Cbb. De meldplicht en de zorgplicht in deze regeling betreffen een nadere uitwerking van de Cbw en het Cbb en kunnen niet los worden gezien van het gehele pakket aan regels in de zorg- en meldplicht uit de NIS2-richtlijn, de Cbw en het Cbb.
Binnen de reikwijdte van deze regeling vallen naar schatting tussen de 800 en 1100 bedrijven.

6. Advies en consultatie

6.1 Internetconsultatie

Over een concept van deze regeling is een internetconsultatie gehouden via www.internetconsultatie.nl. De consultatie heeft 8 openbare reacties opgeleverd.

Algemeen

CBL en NZO hebben verzocht om een overgangsperiode. Een formele overgangsperiode is niet in deze regeling opgenomen omdat dit, indien dat wenselijk zou zijn, in bovenliggende wetgeving zou moeten worden geregeld.

Cyberveilig Nederland en NZO hebben verzocht om in de regeling het bevoegde CSIRT aan te wijzen, dan wel te verduidelijken hoe de samenwerking met het CSIRT is geregeld.
In artikel 2, eerste lid, van het Cbb is de Minister van Justitie en Veiligheid aangewezen als het CSIRT. De Minister van Justitie en Veiligheid zal dit uitvoeren voor de sectoren die onder de beleidsverantwoordelijkheid van de Minister van Landbouw Visserij, Voedselzekerheid en Natuur vallen. Omdat dit reeds in het Cyberbeveiligingsbesluit is geregeld, hoeft dit niet afzonderlijk in deze regeling te worden opgenomen.

De NZO vraagt om een sectorale regeldrukanalyse volgens de Rijksbrede methodiek. Hiervoor wordt verwezen naar hoofdstuk 5 van deze toelichting waarin de regeldruk verder is toegelicht.

Reikwijdte

IKEA en de RND vragen om een duidelijkere afbakening van het begrip 'groothandel in levensmiddelen' (B2B Food Wholesaler), zodat bedrijven met slechts beperkte B2B-verkoop van levensmiddelen niet onbedoeld onder de reikwijdte van de regeling vallen. Naar aanleiding hiervan is de toelichting bij artikel 2 (reikwijdte) uitgebreid met een nadere duiding van de begrippen 'groothandel' en 'industriële productie en verwerking'.

NZO vraagt om verduidelijking van de reikwijdte met praktijkvoorbeelden. Hieraan is tegemoetgekomen door uitbreiding van de toelichting bij artikel 2.

Zorgplicht

Gelijktijdig met internetconsultatie over een concept van deze regeling vonden internetconsultaties plaats over de concepten van de Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector, de Cyberbeveiligingsregeling IenW, en de Regeling cyberbeveiliging EZK. In het kader daarvan zijn eveneens reacties ingediend. De reacties die met betrekking tot de zorgplicht op de hierboven genoemde concept-regelingen zijn binnengekomen, zijn door de betrokken ministeries gezamenlijk en integraal beoordeeld om zodoende tot een gelijkluidende uitwerking van de zorgplicht in de betreffende regelingen te komen.

BTG heeft in haar reactie verzocht een verwijzing naar bestaande normen, zoals ISO- en NEN-normen, op te nemen. Naar aanleiding van deze reactie en soortgelijke reacties op de concept-regelingen van de andere ministeries, is de algemene inleiding van de toelichting op de zorgplicht aangevuld.

NOREA stelt in haar reactie voor om netwerksegmentatie uit te breiden naar leveranciersscreening en ketenaudits. Dit voorstel is niet overgenomen. Een dergelijke verplichting zou leiden tot verhoogde regeldruk en aanzienlijk hogere kosten voor essentiële en belangrijke entiteiten, en is in sommige gevallen moeilijk uitvoerbaar.
Het Cyberbeveiligingsbesluit bevat al een artikel over beveiliging van de toeleveringsketen. Deze regeling werkt dat artikel bewust niet verder uit. De NIS2-richtlijn introduceert weliswaar nieuwe eisen op dit punt, maar de regels uit het Cyberbeveiligingsbesluit worden voor nu als toereikend worden beschouwd. Nadere uitwerking is daarom op dit moment niet nodig.

Daarnaast vragen meerdere partijen, waaronder Holland Solar en Energie Nederland, een duidelijker onderscheid aan te brengen tussen IT-systemen en OT-systemen, onder meer voor patchmanagement. Dit onderscheid is toegelicht in de toelichting op artikel 5 over beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen. Voor patchmanagement is in de toelichting op artikel 5, tweed lid, onderdeel c, bijvoorbeeld nader toegelicht dat bij het toepassen van beveiligingspatches op OT-systemen de noodzaak van continuïteit van dienstverlening en de verouderde aard van veel industriële componenten een rol kunnen spelen bij de afweging of de nadelen van toepassing zwaarder wegen dan de voordelen voor cyberbeveiliging.

RWE onderschrijft het belang van sterke identificatie- en authenticatieprocedures en een zorgvuldig gereguleerde autorisatie. RWE benadrukt in haar reactie dat niet alle OT-systemen technisch in staat zijn om deze functionaliteiten te ondersteunen, en adviseert een clausule op te nemen zoals 'waar mogelijk', dan wel een verplichting om voor systemen die deze functionaliteiten niet kunnen implementeren, alternatieve maatregelen te treffen.

CBL en NZO hebben gevraagd of het tijdelijk verhogen van bevoegdheden een volwaardig alternatief is voor vaste systeembeheeraccounts. Naar aanleiding hiervan is artikel 6 aangepast. De eis om specifieke systeembeheeraccounts op te zetten is vervallen. Het artikel laat daarmee toe dat bevoegdheden tijdelijk worden verhoogd, bijvoorbeeld via Privileged Identity Management, en ziet niet op de wijze waarop die voorrechten worden toegekend, tijdelijk of permanent.

Meldplicht

Het CBL en de NZO vragen of een verstoring die effectief wordt opgevangen via bijvoorbeeld redundantie of omleiding, als significant incident moet gelden. De meldcriteria in artikel 7 zijn hierop niet aangepast, omdat een effectief opgevangen verstoring de in dat artikel genoemde onderbrekingstermijnen in de praktijk niet haalt en daarmee de drempel niet wordt bereikt. Aan de overige punten van NZO is tegemoetgekomen door verduidelijking in de toelichting op artikel 7 over de rol van het NCSC en de doorzetting van een melding naar de NVWA. In de toelichting op artikel 7 zijn tevens twee voorbeeldsituaties genoemd. Deze voorbeelden zijn niet specifiek toegesneden op de zuivelketen, maar bieden algemene illustratie van de toepassing van de meldcriteria.

Het CBL merkt daarnaast op dat niet iedere ongeoorloofde toegang tot een significante impact leidt, bijvoorbeeld wanneer de toegang beperkt blijft en snel wordt geadresseerd, en vraagt zich af of artikel 7, derde lid, onder d, niet te ruim is. Dit onderdeel is niet aangepast. De vaststelling van een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang vormt op zichzelf een aanzienlijk risico, ongeacht of al feitelijke schade is opgetreden.

Naar aanleiding van de reactie van Cyberveilig Nederland is in de toelichting op artikel 7 bevestigd dat het NCSC fungeert als centraal meldportaal voor de levensmiddelensector, en dat een melding via dat portaal automatisch wordt doorgezet naar de NVWA als bevoegde autoriteit.

6.2 Advies Adviescollege toetsing regeldruk

Gelijktijdig met de internetconsultatie is het Adviescollege toetsing regeldruk (hierna: ATR) gevraagd om deze regeling te beoordelen op nut en noodzaak, minder belastende alternatieven, werkbaarheid van de regeling en de gevolgen voor de regeldruk. In deze paragraaf wordt nader ingegaan op het advies van het ATR en de wijze waarop de aanbevelingen zijn verwerkt. Op het onderdeel nut en noodzaak wordt niet nader ingegaan, omdat het ATR daarover geen advies heeft uitgebracht.
Het college adviseert om de regeldruk in kaart te brengen voor essentiële entiteiten en belangrijke entiteiten uit de levensmiddelsector, omdat dit mogelijk gaat om sectorspecifieke aanvullingen.

6.2.1 Totstandkoming meldcriteria en minder belastende alternatieven

Het college adviseert nader te onderbouwen hoe de uitwerking van de zorgplicht en hoe de criteria oor de meldplicht tot stand zijn gekomen, welke mogelijk minder belastende alternatieven zijn overwogen en waarom die alternatieven niet zijn gekozen.

Wat de zorgplicht betreft, worden in deze regeling enkele bepalingen uit de Cbw en Cbb verder geconcretiseerd. Behoudens de verplichting tot kwetsbaarheidsscans en segmentering, betreft deze concretisering vooral een verduidelijking van de verplichtingen uit het Cbb. De regeling onderkent dat een entiteit onder verschillende sectoren kan vallen. Om die reden is een uniform luidende zorgplicht opgenomen voor entiteiten in de sectoren die onder de verantwoordelijkheid vallen van de Minister van Economische Zaken en Klimaat, de Minister van Klimaat en Groene Groei, de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur en de Minister van Infrastructuur en Waterstaat.
Er is aansluiting gezocht bij internationaal gebruikelijke standaarden, zoals ISO 2700X, waarbij wordt opgemerkt dat deze standaarden voor bedrijven zijn niet voorgeschreven. Voorts is aansluiting gezocht bij de Uitvoeringsverordening 2024/2690.

De criteria van de meldplicht in deze regeling zijn in nauwe afstemming met diverse brancheverenigingen, sectorpartijen en betrokken toezichthouders opgesteld. Uitgangspunt was dat de criteria voor de meldplicht goed handhaafbaar en uitvoerbaar zouden zijn. Zo is eerder een alternatief overwogen om de criteria te koppelen aan het aantal afnemers dat door het significante incident geen toegang heeft tot de geleverde goederen of dienst. Dit bleek een moeilijk te handhaven en uit te voeren optie. Daarom is gekozen voor criteria die enkel zien op een verstoring van de productie, verwerking of

distributie van levensmiddelen. Uit de gesprekken met brancheverenigingen, sectorpartijen en de toezichthouder is gebleken dat dit een werkbare optie is, en dat hiermee de regeldruk wordt beperkt.

6.2.2 Werkbaarheid

Het college adviseert om in de toelichting nader in te gaan op de gehanteerde definities van de reikwijdte van de regeling en steeds aanvullend een meer algemene omschrijving van deze reikwijdte op te nemen. Naar aanleiding van dit advies is de reikwijdte van deze regeling nader toegelicht in artikel 2 van de artikelsgewijze toelichting. In gesprekken met diverse partijen uit de sector is gebleken waar de pijnpunten precies zitten over de reikwijdte van de regeling. Deze punten zijn in de toelichting verduidelijkt, waarbij aansluiting is gezocht bij de definities uit de Europese levensmiddelenverordening.

Het college adviseert aan de hand van scenario's inzichtelijk te maken welke organisatie(s) wanneer en waarover verantwoordelijk zijn voor meldingen. Naar aanleiding van dit adviespunt is de artikelsgewijze toelichting op artikel 7 aangevuld met twee uitgewerkte voorbeeldsituaties, waarin wordt geïllustreerd hoe de meldcriteria in onderlinge samenhang worden toegepast en vanaf welk moment de meldtermijnen op grond van de artikelen 26 en 27 van de wet aanvangen.

6.2.3 Invoeringstoets

Het ATR adviseert een jaar na inwerkingtreding van de materiële verplichtingen voor de entiteiten een invoeringstoets uit te voeren om tijdig vast te stellen of de uitwerking van de zorgplicht en de meldcriteria voor incidenten passend en werkbaar zijn voor de sectoren en entiteiten. Naar aanleiding van een aangenomen amendement door de Tweede Kamer is in artikel 94, eerste lid, Cbw geregeld dat een invoeringstoets plaatsvindt 18 maanden na inwerkingtreding van de wet. Hiermee wordt gehoor gegeven aan dit advies van het ATR.

6.2.4 Gevolgen regeldruk

Het college adviseert om de regeldruk in kaart te brengen voor essentiële entiteiten en belangrijke entiteiten uit de levensmiddelsector, conform de Rijksbrede methodiek, en daarbij opvolging te geven aan de genoemde aandachtspunten. Zie voor het antwoord hierop hoofdstuk 4 van de toelichting.

6.3 Uitvoerbaarheids- en handhaafbaarheidstoets

De NVWA heeft een uitvoerbaarheids- en handhaafbaarheidstoets (UHT) uitgevoerd. De NVWA acht de regeling uitvoerbaar, handhaafbaar en fraudebestendig, mits er rekening gehouden wordt met een aantal aandachtspunten en de NVWA de benodigde capaciteit voor het toezicht ter beschikking krijgt. In deze paragraaf worden deze aandachtspunten geadresseerd.

Naar aanleiding van de toets is de regelingstekst op een aantal punten aangepast Het betreft voornamelijk redactionele verduidelijkingen en het wegnemen van overlap tussen enkele bepalingen, evenals het schrappen van een overbodige definitie en een dubbele weergave van regelingstekst. Daarnaast is de toelichting op enkele punten aangepast. In paragraaf 3 is per subparagraaf aangegeven op welke artikelen van de regeling deze betrekking heeft. In de toelichting op artikel 5, derde lid, onderdeel d, zijn de begrippen ″verhelpen″ en ″onverwijld″ overgenomen in lijn met de artikeltekst. In de toelichting op artikel 6 is de bewoording van het artikel aangehouden, zodat tot uitdrukking komt dat niet alleen het bestaan maar ook de werking van het beleid aantoonbaar moet zijn. In de toelichting op artikel 7, eerste lid, is het woord ″essentieel″ vervangen door ″cruciaal″, omdat alleen de op grond van de Wet weerbaarheid kritieke entiteiten aangewezen levensmiddelenbedrijven essentieel zijn en de op grond van de Cbw geregistreerde bedrijven belangrijk.Ttevens is verduidelijkt dat met ″traceerbaarheid″ wordt gedoeld op de traceerbaarheid als bedoeld in artikel 3, punt 15, en artikel 18 van Verordening (EG) nr. 178/2002.

Niet alle opmerkingen hebben tot aanpassing geleid. De aanbeveling om in artikel 4, tweede lid, de frequentie van het testen van het herstel van back-ups op te nemen, is niet overgenomen, omdat dit reeds in artikel 9, tweede lid, van het Cyberbeveiligingsbesluit is geregeld. Het verzoek om artikel 7, derde lid (overlijden of gezondheidsschade), te herschrijven wegens een ontbrekend causaal verband is evenmin overgenomen: een significant incident kan ook rechtstreeks de dood of gezondheidsschade veroorzaken, bijvoorbeeld wanneer een aangetast besturingssysteem een machine ongecontroleerd laat functioneren.

7. Inwerkingtreding

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

afgeweken van het systeem van vaste verandermomenten omdat deze regeling samenhangt met de implementatie van bindende Europese regelgeving in de Cyberbeveiligingswet.

II. Artikelsgewijze toelichting

Artikel 1 – Begripsbepalingen

Dit artikel bevat de begripsbepalingen die in deze regeling worden gebruikt. Voor zover begrippen reeds zijn gedefinieerd in de Cbw of het Cbb, sluiten de definities in deze regeling daarbij aan. Een aantal definities is uitgewerkt in andere wet- en regelgeving. Voor de uitleg van die begrippen wordt verwezen naar de desbetreffende wet- en regelgeving.

Artikel 2 – Reikwijdte

Dit artikel benoemt de reikwijdte van de sectoren waarop deze regeling van toepassing is.
De Cyberbeveiligingswet definieert de sector als 'Productie, verwerking en distributie van levensmiddelen'. De entiteiten die hieronder vallen zijn volgens de wet 'Levensmiddelenbedrijven als bedoeld in artikel 3, onderdeel 2, Verordening (EG) nr. 178/2002 die zich bezighouden met groothandel en industriële productie en verwerking.' Hieronder wordt verder toegelicht wat onder levensmiddelen en groothandel en industriële productie en verwerking wordt verstaan. Hierbij is het van belang om te benadrukken dat het uiteindelijk aan het Europese Hof van Justitie is om definitief te bepalen wat onder begrippen uit Europese regelgeving wordt verstaan.

Levensmiddelen

Levensmiddelen zijn op grond van artikel 2 van Verordening 178/2002 alle stoffen en producten, verwerkt, gedeeltelijk verwerkt of onverwerkt, die bestemd zijn om door de mens te worden geconsumeerd of waarvan redelijkerwijs kan worden verwacht dat zij door de mens worden geconsumeerd. Dit begrip omvat tevens drank, kauwgom alsmede iedere stof, daaronder begrepen water, die opzettelijk tijdens de vervaardiging, de bereiding of de behandeling aan het levensmiddel wordt toegevoegd.

In artikel 2 van verordening 178/2002 wordt ook benoemd wat niet als levensmiddel wordt beschouwd:
- diervoeder;
- levende dieren, tenzij bereid om in de handel te worden gebracht voor menselijke consumptie;
- planten vóór de oogst;
- geneesmiddelen;
- cosmetische producten;
- tabak en tabaksproducten;
- verdovende middelen en psychotrope stoffen;
- residuen en contaminanten.

Groothandel en Industriële productie en verwerking

De begrippen "groothandel" en "industriële productie en verwerking" worden in de Algemene levensmiddelenverordening en in de Cbw niet gedefinieerd. Voor de toepassing van deze regeling wordt hieronder verstaan alle activiteiten van exploitanten van levensmiddelenbedrijven als bedoeld in artikel 3, onder 2, van die verordening, met uitzondering van (a) de primaire productie in de zin van artikel 3, onder 17, van die verordening, en (b) de verkoop of levering van levensmiddelen aan de eindverbruiker. De eindverbruiker is volgens die verordening de laatste verbruiker van een levensmiddel die het niet als deel van een levensmiddelenexploitatie of -activiteit zal gebruiken.
Hieronder vallen zowel natuurlijke personen die het levensmiddel voor persoonlijk gebruik aanschaffen, als ondernemingen die het levensmiddel afnemen voor eigen consumptie binnen hun organisatie. Leveringen aan exploitanten van levensmiddelenbedrijven die het geleverde levensmiddel doorverkopen of in hun eigen levensmiddelenactiviteit verwerken, vallen niet onder uitzondering (b). Hiermee wordt aangesloten bij de reikwijdte van bijlage II bij de NIS2- richtlijn.

Op de entiteiten in de sector onderzoek is deze regeling van toepassing voor zover de betrokken belangrijke of essentiële entiteit onderzoeksactiviteiten verricht binnen een sector die onder de verantwoordelijkheid van de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur valt.

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen

Dit artikel geeft nadere invulling aan artikel 6 van het Cbb ten aanzien van het beleid over beveiliging van netwerk- en informatiesystemen.
Dit artikel regelt dat essentiële en belangrijke entiteit, als onderdeel van de managementsystematiek, de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's toetst door vast te leggen welke maatregelen worden gemonitord, gemeten, geanalyseerd en geëvalueerd, hoe dit gebeurt, wanneer dit plaatsvindt en wie daarmee belast is. Dit is een doorlopend proces.
Het doel van de managementsystematiek is te waarborgen dat de netwerk- en informatiebeveiligingsrisico's van de entiteit inzichtelijk zijn, dat passende en evenredige maatregelen worden genomen om de risico's te beheersen en dat deze maatregelen structureel worden beoordeeld en waar nodig bijgesteld. Door vast te leggen welke maatregelen worden gemonitord, met welke methoden, met welke frequentie en door wie, ontstaat een sluitende cyclus van plannen, uitvoeren, toetsen en bijsturen.
Opvolging van deze evaluatie en beoordeling dient plaats te vinden. Deze verplichting is niet in dit artikel opgenomen, aangezien zij al volgt uit artikel 6, vierde lid, en artikel 18 van het Cbb. Daarmee wordt geborgd dat het inzicht in de effectiviteit van de maatregelen actueel blijft en dat de resultaten van deze cyclus leiden tot verdere verbetering van de beveiliging. Deze elementen sluiten aan bij de werkwijze die in de praktijk gebruikelijk is in managementsystemen voor informatiebeveiliging en bij internationale normen, zoals ISO-normen.

Artikel 4 – Bedrijfscontinuïteit

Op grond van artikel 9, tweede lid, van het Cbb stelt de belangrijke entiteit of essentiële entiteit processen en procedures vast voor back-ups van software en gegevens en past die toe. De risicobeoordelingen op grond van artikel 7 van het Cbb zijn derhalve relevant voor zowel het bepalen van welke software en gegevens in back-ups dienen te worden opgenomen, als voor de hierna genoemde waarborgen.

De onderdelen van het eerste lid omschrijven welke aspecten in de processen en procedures voor back-ups van software en gegevens moeten worden opgenomen. Het bepalen van hersteltijden, in het Engels ook wel aangeduid als *recovery time objective (RTO),* heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. De term herstelpunten, in het Engels ook wel aangeduid als *recovery point objective (RPO),* heeft betrekking op de frequentie van de back-ups. Het voorschrift dat de processen en procedures waarborgen dat back-ups volledig zijn, ziet erop dat alle gegevens die nodig zijn voor het herstellen van de betreffende netwerk- en informatiesystemen zijn opgenomen, waaronder configuratiegegevens en gegevens die in cloudcomputingdiensten zijn opgeslagen. Dit is noodzakelijk om te waarborgen dat systemen en processen bij een herstel weer volledig functioneren. Daarnaast dienen de processen en procedures te waarborgen dat de back-ups nauwkeurig zijn. Hiermee wordt bedoeld dat de informatie in geval van herstel succesvol kan worden gebruikt, bijvoorbeeld door ervoor te zorgen dat de gegevens in de back-up zich in een staat bevinden die een succesvol herstel mogelijk maakt.

Daarnaast dienen de processen en procedures de beschikbaarheid, integriteit en vertrouwelijkheid van back-ups te waarborgen, zodat de back-ups daadwerkelijk ingezet kunnen worden. Met integriteit wordt bedoeld dat de entiteit borgt dat de back-ups niet zijn gemanipuleerd of beschadigd, bijvoorbeeld door derden. Dit voorkomt dat de geback-upte gegevens zijn gewijzigd, beschadigd of aangetast tijdens het back-upproces, de opslag of het herstel. Voor de beschikbaarheid is het van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet door toedoen van kwaadwillenden, zoals bij ransomware-aanvallen, onbruikbaar kunnen worden. Ook de vertrouwelijkheid van back-ups dient te worden gewaarborgd, om ongeautoriseerde toegang tot gegevens te voorkomen. Daarnaast dienen de processen en procedures waarborgen te bevatten voor het herstellen van software en gegevens. Dit omvat zowel de wijze waarop back-ups hersteld kunnen worden als de waarborg dat back-ups zo nodig daadwerkelijk teruggezet kunnen worden. Een gangbare praktijk hierbij is het periodiek testen van het terugzetten van back-ups, om de werking van back-ups in de praktijk te verifiëren. Ten slotte dienen de processen en procedures te omschrijven hoe lang de betreffende back-ups bewaard moeten worden.

Bedrijfscontinuïteitsplan

De essentiële entiteit of belangrijke entiteit stelt op grond van artikel 9, derde lid, Cbb een bedrijfscontinuïteitsplan op. Daarmee kan zij zich voorbereiden op incidenten die de bedrijfscontinuïteit in gevaar kunnen brengen, hierop doeltreffend en tijdig reageren en de duur en gevolgen van dergelijke incidenten beperken. Op grond van het tweede lid van dit artikel dient de entiteit bij het opstellen van het bedrijfscontinuïteitsplan rekening te houden met de risicobeoordelingen op grond van artikel 7

van het Cbb, zodat zij alle relevante risico's en risicoscenario's meeneemt bij het formuleren van deze plannen.

De onderdelen van het tweede lid omschrijven de elementen die het bedrijfscontinuïteitsplan moet bevatten. Allereerst dient het plan het doel en de reikwijdte ervan te omschrijven, zodat de context en het toepassingsbereik van het bedrijfscontinuïteitsplan op voorhand duidelijk zijn. Daarbij ligt het voor de hand dat de entiteit bij het opstellen van het bedrijfscontinuïteitsplan prioriteit geeft aan haar kritieke processen. Dit laat onverlet dat de zorgplicht van artikel 21 van de wet van toepassing blijft op alle netwerk- en informatiesystemen van de entiteit.

Het vastleggen van de belangrijkste contacten en interne en externe communicatiekanalen in een bedrijfscontinuïteitsplan is van belang voor snelle, gecoördineerde actie en communicatie tijdens incidenten of crises. Hierbij kan worden gedacht aan contacten voor directe actie, zoals noodnummers van hulpdiensten, sleutelpersoneel in de organisatie zoals crisisteams, IT/OT-specialisten, directie, evenals externe partners als leveranciers, klanten of overheidsorganisaties. Wat betreft overheidsorganisaties kan in ieder geval worden gedacht aan de bevoegde autoriteit en het CSIRT waar significante incidenten gemeld dienen te worden.
De voorwaarden voor activering en de-activering beschrijven in welke gevallen of onder welke omstandigheden het bedrijfscontinuïteitsplan of onderdelen ervan in werking treden dan wel worden beëindigd.
De vereiste middelen, met inbegrip van back-ups en redundanties, beschrijven welke middelen nodig zijn voor een goede uitvoering van het bedrijfscontinuïteitsplan.
Ten slotte dient het bedrijfscontinuïteitsplan de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen te bevatten, zodat de overgang naar een normale bedrijfsvoering wordt gewaarborgd.

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

Artikel 5 – Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Eerste lid

Artikel 11, derde lid, van het Cbb verplicht essentiële en belangrijke entiteiten om processen en procedures vast te stellen voor het onderhoud en beheer van haar netwerk- en informatiesystemen. Deze processen en procedures hebben ten minste betrekking op het configuratiebeheer en het wijzigingsbeheer van de netwerk- en informatiesystemen van de entiteit, alsmede, op grond van het eerste lid, op beveiligingstesten en beveiligingspatchbeheer. Beveiligingstesten zijn noodzakelijk om vast te stellen of de getroffen maatregelen in de praktijk doeltreffend functioneren en of kwetsbaarheden tijdig aan het licht komen. Door structureel processen en procedures voor beveiligingstesten vast te leggen, wordt geborgd dat testen systematisch, herhaalbaar en volgens vooraf bepaalde criteria plaatsvinden. Dit voorkomt dat testen ad hoc of onvolledig worden uitgevoerd en draagt eraan bij dat tekortkomingen tijdig kunnen worden verholpen voordat deze tot incidenten leiden.

Tweede lid

Om potentiële risico's voor de beveiliging van netwerk- en informatiesystemen weg te nemen, stelt de essentiële entiteit of belangrijke entiteit processen en procedures vast voor het toepassen van beveiligingspatches. Beveiligingspatchbeheer is van belang om bekende kwetsbaarheden in software en systemen tijdig te verhelpen en misbruik daarvan te voorkomen.
Op grond van onderdeel a geldt dat, waar passend, gecontroleerd moet worden of beveiligingspatches afkomstig zijn van betrouwbare bronnen en of de integriteit van deze patches gewaarborgd is. Dit vergt niet in alle gevallen handmatige actie van de essentiële entiteit of belangrijke entiteit. Zo is bij reguliere systeemupdates van besturingssystemen doorgaans al sprake van ingebouwde technische controles op herkomst en integriteit van beveiligingspatches. De essentiële of belangrijke entiteit dient zich hiervan echter wel te vergewissen.
Op grond van onderdeel b geldt dat beveiligingspatches, waar passend, getest moeten worden voordat zij in de productieomgeving worden toegepast. De noodzaak van een dergelijke test is afhankelijk van de risico's die het installeren van de patch met zich meebrengt. Voornoemde stappen dragen ertoe bij dat de toepassing van patches geen nieuwe kwetsbaarheden of verstoringen veroorzaakt. Onderdeel c bepaalt dat beveiligingspatches binnen een redelijke termijn nadat zij beschikbaar zijn moeten worden toegepast, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen. Dit kan bijvoorbeeld het geval zijn voor het toepassen van

beveiligingspatches op OT-systemen, waarbij het belang van continuïteit van de dienstverlening en de verouderde aard van veel industriële componenten een rol spelen. Hierbij kan gedacht worden aan het ongepland stilzetten van kritieke bedrijfsprocessen van een entiteit ter uitvoering van de patch, terwijl de patch ook uitgevoerd kan worden op een al ingepland moment van breder onderhoud aan de netwerk- en informatiesystemen. Indien een essentiële of belangrijke entiteit hiervoor kiest, dient de motivatie voor het niet of niet tijdig toepassen van de beveiligingspatch gedocumenteerd te worden.

Derde lid

Onderdeel a

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

Onderdeel b

Op grond van dit onderdeel voert de essentiële of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit op haar netwerk- en informatiesystemen en legt zij de resultaten daarvan vast. Deze scans maken het mogelijk om inzicht te krijgen in bekende kwetsbaarheden in systemen en applicaties en vormen daarmee een belangrijk hulpmiddel om risico's tijdig te onderkennen. De entiteit voert de scans, waar passend, uit waarbij rekening wordt gehouden met de blootstelling van systemen aan dreigingen en de netwerktoegankelijkheid van die systemen?, alsmede met de criticaliteit van die systemen voor de continuïteit van de dienstverlening en de potentiële gevolgen van uitval of misbruik.
Kwetsbaarheidsscans van OT-systemen vereisen vaak een andere aanpak dan die van IT-systemen, vanwege het belang van de continuïteit van de operationele diensten of de aanwezigheid van verouderde apparatuur. Het is daarom aan de essentiële of belangrijke entiteit om een passende vorm van kwetsbaarheidsscan in te zetten, gegeven de omgeving van haar netwerk- en informatiesystemen en de mogelijke risico's die zich daarin kunnen voordoen. Zo kan het in OT-omgevingen noodzakelijk zijn om dit op een passieve wijze vorm te geven, om zo verstoring van processen te voorkomen. Door de resultaten te documenteren kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.

Onderdeel c

Op grond van dit onderdeel evalueert de essentiële of belangrijke entiteit structureel haar blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van heeft ten aanzien van haar netwerk- en informatiesystemen, voor zover artikel 17 van het Cbb daar niet reeds toe verplicht. Dit onderdeel regelt daarmee aanvullend dat kwetsbaarheden uit de uitgevoerde kwetsbaarheidsscans van de essentiële of belangrijke entiteit of meldingen van interne werknemers worden geëvalueerd en verholpen. Door deze evaluatie structureel uit te voeren, ontstaat een actueel beeld van het risicolandschap en kan tijdig worden bepaald welke aanvullende maatregelen nodig zijn om de weerbaarheid te vergroten.

Onderdeel d

Op grond van dit onderdeel verhelpt de essentiële entiteit of belangrijke entiteit onverwijld kwetsbaarheden die een risico vormen voor de beveiliging van haar netwerk- en informatiesystemen. Indien een kwetsbaarheid niet of op een later moment verholpen wordt, dient de essentiële entiteit of belangrijke entiteit dit te motiveren en te documenteren. Evenals bij het niet toepassen van een beveiligingspatch (zie het tweede lid) wordt voor de toezichtspraktijk daarmee duidelijk waarom wordt afgeweken en kan de bevoegde autoriteit oordelen of deze keuze terecht is gemaakt.

Vierde lid

Onderdeel a

De essentiële entiteit of belangrijke entiteit waarborgt dat bij incidenten met betrekking tot de beveiliging van een netwerk- en informatiesysteem de gevolgen voor andere netwerk- en informatiesystemen worden beperkt. Op grond van onderdeel a segmenteert de essentiële entiteit of belangrijke entiteit haar netwerken overeenkomstig de resultaten van de in artikel 7, derde lid, van het Cbb bedoelde risicobeoordeling. De entiteit bepaalt zelf op welke wijze zij de netwerksegmentatie toepast. Netwerksegmentatie betreft het onderverdelen van systemen en netwerken in verschillende, van

elkaar gescheiden segmenten, waardoor er geen automatische toegang is tussen systemen en netwerken. Daarbij wordt rekening gehouden wordt met de functionele, logische en fysieke relatie, met inbegrip van de locatie, tussen betrouwbare netwerken- en informatiesystemen. De essentiële entiteit of belangrijke entiteit doet er verstandig aan bij de netwerksegmentatie nadrukkelijk te betrekken of er sprake is van Informatie Technologie (IT)- en Operationele Technologie (OT)-systemen en deze waar mogelijk van elkaar te scheiden.
Als goede praktijken kunnen worden genoemd- toegang tot een netwerk of zone te verlenen 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 te houden, en een gedemilitariseerde zone in communicatiekanalen uit te rollen om te waarborgen dat communicatie die afkomstig is van of bestemd is voor haar netwerken beveiligd is.
Andere goede praktijken zijn het specifieke netwerk voor het beheer van netwerk- en informatiesystemen te scheiden van het operationele netwerk van de entiteit, de kanalen voor netwerkbeheer te scheiden van ander netwerkverkeer, en de productiesystemen voor de diensten van de entiteit te scheiden van de systemen die worden gebruikt voor de ontwikkeling en tests, met inbegrip van back-ups.

Onderdeel b

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

Artikel 6 – Beveiligingsaspecten ten aanzien van toegangsbeleid

Het beleid, bedoeld in artikel 15, eerste lid, van het besluit, dient ook beleid te omvatten over bevoorrechte accounts en systeembeheeraccounts. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Systeembeheeraccounts zijn een specifieke categorie bevoorrechte accounts die worden gebruikt voor het beheer van systemen, zoals het uitvoeren van updates, het wijzigen van configuraties of het beheren van gebruikersrechten.
Het tweede lid geeft nadere invulling aan het beleid voor bevoorrechte accounts en systeembeheeraccounts door te specificeren welke maatregelen en procedures moeten worden toegepast. Het beleid waarborgt dat bij bevoorrechte accounts en systeembeheeraccounts sterke identificatie-, authenticatie- en autorisatieprocedures worden toegepast. Bij sterke identificatie kan gedacht worden aan het vooraf betrouwbaar vaststellen van de identiteit van de gebruiker voordat accounts worden uitgegeven. Bij sterke authenticatie kan worden gedacht aan phishing-bestendige multifactorauthenticatie, waarmee de dreiging van phishing en ander misbruik van dergelijke accounts zoveel mogelijk wordt tegengegaan. Bij sterke autorisatie kan worden gedacht aan een strikte scheiding van rollen en bevoegdheden. Daarnaast waarborgt het beleid dat de voorrechten van deze accounts zoveel mogelijk geïndividualiseerd en beperkt worden toegekend. Dit zorgt ervoor dat misbruik beter te herleiden is tot specifieke accounts. Tevens waarborgt het beleid dat voorrechten op het gebied van systeembeheer uitsluitend voor systeembeheer worden gebruikt. Deze maatregelen verkleinen tezamen het risico op misbruik of onbedoelde gevolgen van het inzetten van deze voorrechten.

Artikel 7 – Criteria significant incident levensmiddelensector

Dit artikel bevat nadere criteria op grond waarvan incidenten als significant worden aangemerkt. De criteria gelden voor essentiële en belangrijke entiteiten in de levensmiddelensector. Een incident is significant indien het voldoet aan een of meer van de in dit artikel opgenomen drempelwaarden.

Eerste lid – ernstige operationele verstoring

Levensmiddelenbedrijven die zich bezighouden met de groothandel of industriële productie of verwerking van levensmiddelen zijn van cruciaal belang voor het in stand houden van de levensmiddelensector. Voor de goede functionering en continuering van levensmiddelensector is het noodzakelijk dat essentiële en belangrijke entiteiten binnen deze sector significante incidenten melden bij het

centrale meldportaal van de NCSC. Via dit meldportaal wordt de melding ook doorgezet naar de toezichthouder, de NVWA.
Er is sprake van een significant incident wanneer een ernstige verstoring van de productie, verwerking of distributie van levensmiddelen plaatsvindt waardoor de leveringszekerheid in het gedrang komt. Dit kan zich bijvoorbeeld voordoen bij uitval van koelinstallaties, productiebanden, planningssystemen of voorraadbeheer.
Om vast te stellen of sprake is van een ernstige operationele verstoring, zijn in dit lid drie drempelwaarden vastgesteld. Onderdeel a ziet op situaties waarin de productie, verwerking of distributie van levensmiddelen gedurende ten minste 24 uur is onderbroken. Daarbij wordt geen onderscheid gemaakt in de omvang van de onderbreking, zowel gedeeltelijke als volledige uitval van de operationele capaciteit van een essentiële of belangrijke entiteit geldt als een onderbreking.
Onder distributie wordt mede verstaan de uitlevering van levensmiddelen aan directe afnemers van de entiteit, waaronder worden begrepen andere schakels binnen de voedselketen zoals verwerkingsbedrijven, groothandel, detailhandel, horeca en andere partijen die afhankelijk zijn van de continuïteit van de levering.

De keuze voor een uniforme drempelwaarde is gebaseerd op de onderlinge verwevenheid van de levensmiddelensector, waarin zelfs kortdurende verstoringen aanzienlijke keteneffecten kunnen veroorzaken. Door onderscheid te maken tussen gedeeltelijke of volledige uitval wordt gewaarborgd dat ook situaties met substantiële capaciteitsbeperkingen tijdig worden gemeld.
In de praktijk betekent dit dat zowel een onderbreking van een productielijn als een grootschalige ICT-storing binnen distributie, opslag of traceerbaarheid (als bedoeld in artikel 3, punt 15, en artikel 18 van Verordening (EG) nr. 178/2002) onder deze drempel valt, indien de continuïteit van de levering aan directe afnemers gedurende 24 uur of langer niet is gewaarborgd.
Onderdeel b en onderdeel c onderscheiden zich door de verhouding tussen de omvang van de onderbreking en de duur van de onderbreking. Indien een entiteit niet in staat is om het percentage van de geraakte operationele capaciteit exact te berekenen, kan zij zich baseren op een redelijke schatting van de maximale onderbreking van de totale operationele capaciteit, op basis van de beschikbare operationele gegevens.

Tweede lid -onderhoudswerkzaamheden

Beperkte beschikbaarheid of niet-beschikbaarheid van diensten als gevolg van geplande onderhoudswerkzaamheden wordt niet als significant incident beschouwd, voor zover de gevolgen daarvan voorzien waren. Evenmin worden geplande onderbrekingen van de dienstverlening op basis van een vooraf bepaalde contractuele afspraken als significante incidenten beschouwd.

Derde lid – materiële en immateriële schade

Een incident is, op grond van artikel 25, tweede lid, onderdeel b, van de wet, eveneens significant wanneer het aanzienlijke materiële of immateriële schade veroorzaakt of kan veroorzaken.

Onderdelen a en b

Deze onderdelen hebben betrekking op situaties waarin het incident de dood van een natuurlijk persoon of aanzienlijke gezondheidsschade aan een natuurlijk persoon heeft veroorzaakt of kan veroorzaken. Deze incidenten dienen altijd te worden gemeld, omdat dergelijke gevolgen directe risico's vormen voor de volksgezondheid en de voedselveiligheid. Als voorbeeld kan worden gedacht aan levensmiddelen die als onveilig worden beschouwd, doordat zij schadelijk zijn voor de gezondheid of ongeschikt zijn voor menselijke consumptie in de zin van artikel 14, tweede lid, van Verordening (EG) No 178/2002.
Bij de beoordeling of een incident aanzienlijke schade aan de gezondheid van een natuurlijke persoon heeft veroorzaakt of kan veroorzaken, dienen entiteiten rekening te houden met de ernst van de verwondingen of gezondheidsproblemen die zich voordoen of kunnen voordoen. Daarbij hoeft geen aanvullende informatie te worden verzameld waartoe de entiteit redelijkerwijs geen toegang heeft.

Onderdeel c

Dit onderdeel ziet op aantasting van de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met de dienstverlening worden opgeslagen, verzonden of verwerkt. Hierbij kan worden gedacht aan het weglekken van hoogwaardige kennis of technologie. Deze gegevens kunnen in potentie van vertrouwelijke aard zijn, waardoor deze ook blootgesteld kunnen worden aan het risico van onbedoelde openbaarmaking of verlies. De vertrouwelijkheid van gegevens kan bijvoorbeeld zijn aangetast wanneer er sprake is geweest van ongeoorloofde toegang waardoor de kwaadwillende gegevens van de entiteit hebben ontvreemd. Ook kan sprake zijn van een aantasting van de integriteit van de dienstverlening. Dit kan zich bijvoorbeeld voordoen bij een verstoring in voorraadbeheersyste-

men, planningssoftware of koelfaciliteiten, waardoor de juistheid en volledigheid van deze gegevens niet langer kunnen worden gegarandeerd. Een dergelijke verstoring kan directe gevolgen hebben voor de betrouwbaarheid van de productie- en distributieprocessen en in sommige gevallen risico's opleveren voor de voedselveiligheid en leveringszekerheid. Bij kwaadwillige toegang kunnen gegevens aangetast worden die noodzakelijk zijn voor de correcte werking van de netwerk- en informatiesystemen van de essentiële of belangrijke entiteit, of gevolgen kunnen hebben voor derden. Tot slot wordt de authenticiteit meegenomen in dit meldcriterium, omdat dit een belangrijk aspect is om vertrouwelijkheid en integriteit te waarborgen.
De meldplicht is niet beperkt tot incidenten als gevolg van ongeoorloofde toegang. Ook menselijke fouten vallen hieronder. Daarbij kan worden gedacht aan het onbedoeld openbaar maken van vertrouwelijke gegevens of het onjuist uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Onderdeel d

Er is tevens sprake van een significant incident als er een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen heeft plaatsgevonden. Bij dergelijke incidenten hoeft nog geen sprake te zijn van feitelijke schade of directe gevolgen. De enkele vaststelling dat een kwaadwillige actor die zich ongeoorloofd toegang heeft verschaft tot de netwerk- en informatiesystemen van de entiteit, brengt reeds een aanzienlijk risico net zich mee voor de betrokken entiteit en mogelijk ook voor andere partijen. Daarbij kan worden gedacht aan de afnemers van een product of dienst waarin een kwetsbaarheid aanwezig is die door een actor kan worden misbruikt. Een actor kan zich bijvoorbeeld in de netwerk- en informatiesystemen van een essentiële of belangrijke entiteit nestelen met de bedoeling om op een later moment een verstoring van de dienstverlening te veroorzaken of anderszins schade toe te brengen. Voor het CSIRT en de toezichthoudende instantie is het van belang dat dergelijke incidenten worden gemeld, omdat het ook een risico kan vormen voor andere partijen. Tevens kan het CSIRT ook technische bijstand bieden.

Voorbeelden

Ter illustratie van de toepassing van dit artikel zijn hieronder twee voorbeeldsituaties uitgewerkt. Deze voorbeelden zijn niet uitputtend, zij dienen ter ondersteuning van de afweging of een incident voldoet aan de criteria voor significantie.
Voorbeeld 1: Een groothandel in levensmiddelen verzorgt de distributie naar afnemers vanuit zes distributievestigingen, waarbij de drie getroffen vestigingen tezamen circa de helft van de totale uitleveringscapaciteit verzorgen. Door een cyberaanval in het centrale orderverwerkingssysteem kunnen die drie vestigingen geen orders verwerken; de overige drie blijven volledig operationeel. Veertien uur na het optreden van de verstoring is het systeem hersteld.
Voor de beoordeling of sprake is van een significant incident toetst de entiteit aan de meldcriteria van het eerste lid. De meldcriteria uit onderdeel b wordt in dit voorbeeld wél bereikt: ten minste vijftig procent van de totale distributiecapaciteit was gedurende meer dan twaalf uur onderbroken. Onderdeel c, dat ziet op een volledige onderbreking van ten minste zes uur, is niet aan de orde. Het incident is daarmee een significant incident.
De termijnen voor de vroegtijdige waarschuwing en de melding vangen aan op het moment waarop de entiteit redelijkerwijs kan vermoeden dat het incident significant is. Indien op grond van een eerste technische analyse reeds in een vroeg stadium voorzienbaar is dat aan een meldcriterium zal worden voldaan kan de termijn voor de vroegtijdige waarschuwing op dat eerdere moment aanvangen.
Voorbeeld 2: Een industriële verwerker van levensmiddelen ontdekt naar aanleiding van een interne controle dat een externe actor enige tijd eerder ongeoorloofd toegang heeft gehad tot de netwerk- en informatiesystemen die worden gebruikt voor productieplanning. Onderzoek wijst uit dat gegevens zijn ingezien, dat geen wijzigingen zijn aangebracht en dat de productie en distributie ongestoord zijn doorgelopen.
Onderdeel d is in deze situatie van toepassing: er is sprake van een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van de entiteit. Daarnaast kan, afhankelijk van de aard van de ingeziene gegevens, de vertrouwelijkheid daarvan zijn aangetast in de zin van onderdeel c. Beide gronden zijn zelfstandig voldoende voor de kwalificatie als significant incident en brengen daarmee een meldplicht met zich mee, ook indien geen schade is geleden en geen operationele verstoring is opgetreden.
Voor de aanvang van de meldtermijnen is bepalend het moment waarop de entiteit kennis krijgt van de ongeoorloofde toegang.

Artikel 8 – Criteria significant incident in de sector onderzoek

Dit artikel ziet op situaties waarin een incident in de sector onderzoek als significant wordt aangemerkt. Een incident is significant indien de integriteit, vertrouwelijkheid of authenticiteit van gegevens die in verband met het verrichte onderzoek worden opgeslagen, verzonden of verwerkt, is aangetast.

Gegevens die noodzakelijk zijn voor de uitvoering van toegepast onderzoek met het oog op een commerciële toepassing zijn door de aard van het onderzoek doorgaans vertrouwelijk en lopen daardoor risico op onbedoelde openbaarmaking of verlies. De vertrouwelijkheid van gegevens kan bijvoorbeeld worden aangetast wanneer de encryptie van een dienst niet correct heeft gewerkt, of wanneer sprake is geweest van ongeoorloofde toegang waarbij gegevens van de entiteit zijn ontvreemd. Ook de integriteit van de gegevens kan worden aangetast. Bij ongeoorloofde toegang kunnen onderzoeksgegevens gecorrumpeerd worden, wat gevolgen kan hebben voor de betrouwbaarheid of juistheid van onderzoeksresultaten.
De meldplicht is niet beperkt tot kwaadwillige toegang. Ook menselijke fouten vallen hieronder. Hierbij kan worden gedacht aan het onbedoeld openbaar maken van vertrouwelijke gegevens of het onjuist uitvoeren van een systeemupdate waardoor de netwerk- en informatiesystemen niet meer naar behoren functioneren.

Artikel 9 – Aanwijzing bevoegde autoriteiten

Dit artikel geeft uitvoering aan de bevoegdheid van de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur om op grond van artikel 51, tweede lid, onderdeel i, van de Cbw autoriteiten aan te wijzen waarmee de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt als bedoeld in de wet (de zogenoemde Cbw-instanties) samenwerken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van de wet.
In dit artikel is de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur, uit hoofde van de Wet dieren, en de Minister van Volksgezondheid, Welzijn en Sport voor de taken uit hoofde van de Warenwet, aangewezen als autoriteit als bedoeld in artikel 1, tweede lid, onderdeel i, van de wet. De Nederlandse Voedsel- en Warenautoriteit houdt namens beide ministers toezicht op de naleving van de Wet dieren en de Warenwet. Dit toezicht betreft mede entiteiten die ook onder de reikwijdte van de Cbw vallen.

De Staatssecretaris van Landbouw, Visserij, Voedselzekerheid en Natuur,
S.P.A. Erkens