CONSULTATIEVERSIE

Regeling van de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur, van [PM datum], nr. WJZ/[PM nummer], houdende nadere regels over cyberbeveiliging voor essentiële en belangrijke entiteiten in de levensmiddelensector (Regeling cyberbeveiliging levensmiddelensector)

(KetenID WGK 28488)

De Minister van Landbouw, Visserij, Voedselzekerheid en Natuur,

Gelet op de artikelen 20, 24, eerste lid, en 29 van het Cyberbeveiligingsbesluit;

Besluit:

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:
- *besluit:* Cyberbeveiligingsbesluit;
- *criteria:* de drempelwaarden die bepalen wanneer een incident significant is, binnen de parameters van artikel 25, tweede lid, van de wet;
-*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.

Artikel 2. Reikwijdte

Deze regeling is van toepassing op essentiële entiteiten en belangrijke entiteiten in de sector productie, verwerking en distributie van levensmiddelen, genoemd in bijlage 2 van de wet.

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen

Als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het besluit, en ter uitvoering van artikel 19, van het besluit, bepaalt de essentiële entiteit of de belangrijke entiteit:

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

Artikel 4. Bedrijfscontinuïteit

1. Het bedrijfscontinuïteitplan, bedoeld in artikel 9, derde lid, van het besluit, houdt rekening met de uitgevoerde beoordeling en herbeoordeling 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 plan;
e. vereiste middelen, met inbegrip van back-ups en redundanties;
f. de voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

2. De procedures, voor het maken, terugzetten en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens, bedoeld in artikel 9, tweede lid, van het besluit, omvatten in ieder geval:
a. hersteltijden;
b. herstelpunten;
c. waarborging van volledigheid en nauwkeurigheid van back-ups, ook configuratiegegevens en gegevens die zijn opgeslagen in cloudcomputingdiensten worden meegenomen;
d. passende waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
e. de wijze van herstel van software en gegevens uit back-ups;
f. bewaartermijnen.

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

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

2. De processen en procedures inzake beveiligingspatchbeheer zorgen ervoor dat:
a. waar passend, beveiligingspatches afkomstig zijn van betrouwbare bronnen en op integriteit worden gecontroleerd;
b. waar passend, beveiligingspatches worden getest voordat zij in productiesystemen worden toegepast;
c. beveiligingspatches worden toegepast binnen een redelijke termijn nadat zij beschikbaar zijn, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen. De entiteiten legt de onderbouwing van een dergelijk besluit vast.

3. Ter uitvoering van artikel 21, derde lid, onderdeel e, van de wet:
a. implementeert de essentiële entiteit of belangrijke entiteit maatregelen om het gebruik van kwaadaardige en ongeoorloofde software te detecteren en te voorkomen;
b. voert de essentiële entiteit of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit en legt zij de resultaten van deze scans vast;
c. evalueert de essentiële entiteit of belangrijke entiteit haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft, voor zover artikel 17 van het 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 verholpen wordt en documenteert dit;
e. segmenteert de essentiële entiteit of belangrijke entiteit systemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het besluit bedoelde risicoanalyse.

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

Artikel 6. Beveiligingsaspecten ten aanzien van toegangsbeleid

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

Artikel 7. Nadere criteria significante incidenten

1. Een operationele verstoring is 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 is gedurende ten minste 24 uur geheel of gedeeltelijk onderbroken;
   b. ten minste 50% van de totale productie, verwerking of distributie van levensmiddelen is gedurende ten minste 12 uur onderbroken;
   c. de productie, verwerking of distributie van levensmiddelen is gedurende ten minste 6 uur geheel onderbroken.
2. In afwijking van het eerste lid is een geplande dienstonderbreking of een ander gevolg van onderhoudswerkzaamheden die door of namens een essentiële entiteit of een belangrijke entiteit worden uitgevoerd, geen ernstige operationele verstoringen.
3. Materiële of immateriële schade is 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 dit veroorzaken;
   b. het incident heeft aanzienlijke schade aan de gezondheid van een of meer natuurlijke personen veroorzaakt of kan veroorzaken;
   c. de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienst of levensmiddelen die de essentiële entiteit of de belangrijke entiteit verleent of 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 een essentiële entiteit of een belangrijke entiteit.

Artikel 8. 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 9. Inwerkingtreding

[PM: Deze regeling treedt in werking met ingang van [DATUM].]

Artikel 10. Citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging levensmiddelensector.

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

's-Gravenhage,

De Minister van Landbouw, Visserij, Voedselzekerheid en Natuur

Regeling van de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur, van [PM datum], nr. WJZ/[PM nummer], houdende nadere regels over cyberbeveiliging voor essentiële en belangrijke entiteiten in de levensmiddelensector (Regeling cyberbeveiliging levensmiddelensector)

(KetenID WGK 28488)

De Minister van Landbouw, Visserij, Voedselzekerheid en Natuur,

Gelet op de artikelen 20, 24, eerste lid, en 29 van het Cyberbeveiligingsbesluit;

Besluit:

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:
- *besluit:* Cyberbeveiligingsbesluit;
- *criteria:* de drempelwaarden die bepalen wanneer een incident significant is, binnen de parameters van artikel 25, tweede lid, van de wet;
-*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.

Artikel 2. Reikwijdte

Deze regeling is van toepassing op essentiële entiteiten en belangrijke entiteiten in de sector productie, verwerking en distributie van levensmiddelen, genoemd in bijlage 2 van de wet.

Artikel 3. Beleid over beveiliging van netwerk- en informatiesystemen

Als onderdeel van haar managementsystematiek, bedoeld in artikel 6, vierde lid, van het besluit, en ter uitvoering van artikel 19, van het besluit, bepaalt de essentiële entiteit of de belangrijke entiteit:

g. welke maatregelen voor het beheer van cyberbeveiligingsrisico's moeten worden gemonitord en gemeten;
h. de methoden voor het monitoren, meten, analyseren en evalueren, al naargelang het geval, om te zorgen voor valide resultaten;
i. wanneer de monitoring en de meting moeten worden uitgevoerd;
j. wie verantwoordelijk is voor het monitoren en meten van de doeltreffendheid van de maatregelen voor het beheer van cyberbeveiligingsrisico's;
k. wanneer de resultaten van de monitoring en meting moeten worden geanalyseerd en geëvalueerd;
l. wie deze resultaten moet analyseren en evalueren.

Artikel 4. Bedrijfscontinuïteit

1. Het bedrijfscontinuïteitsplan, bedoeld in artikel 9, derde lid, van het besluit, houdt rekening met de uitgevoerde beoordeling en herbeoordeling van risico's, bedoeld in artikel 7 van het besluit, en omvat in ieder geval:

g. doel en reikwijdte;

h. taken en verantwoordelijkheden;
i. belangrijkste contacten en interne en externe communicatiekanalen;
j. voorwaarden voor activering en de-activering van het plan;
k. vereiste middelen, met inbegrip van back-ups en redundanties;
l. voorwaarden voor herstel en hervatting van activiteiten na afloop van tijdelijke maatregelen.

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

g. hersteltijden;
h. herstelpunten;
i. waarborging van volledigheid en nauwkeurigheid van back-ups, ook configuratiegegevens en gegevens die zijn opgeslagen in cloudcomputingdiensten worden meegenomen;
j. passende waarborgen voor integriteit, vertrouwelijkheid en beschikbaarheid van back-ups;
k. de wijze van herstel van software en gegevens uit back-ups;
l. bewaartermijnen.

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

1. De procedures, bedoeld in artikel 11, derde lid, van het besluit, hebben betrekking op ten minste de processen en procedures inzake:

c. beveiligingstesten;
d. beveiligingspatchbeheer.

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

d. waar passend, beveiligingspatches afkomstig zijn van betrouwbare bronnen en op integriteit worden gecontroleerd;
e. waar passend, beveiligingspatches worden getest voordat zij in productiesystemen worden toegepast;
f. beveiligingspatches worden toegepast binnen een redelijke termijn nadat zij beschikbaar zijn, tenzij de nadelen van de toepassing van de beveiligingspatches zwaarder wegen dan de voordelen. De entiteiten legt de onderbouwing van een dergelijk besluit vast.

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

f. implementeert de essentiële entiteit of belangrijke entiteit maatregelen om het gebruik van kwaadaardige en ongeoorloofde software te detecteren en te voorkomen;
g. voert de essentiële entiteit of belangrijke entiteit, waar passend, periodiek kwetsbaarheidsscans uit en legt zij de resultaten van deze scans vast;
h. evalueert de essentiële entiteit of belangrijke entiteit haar blootstelling aan relevante kwetsbaarheden en dreigingen waar ze kennis van heeft, voor zover artikel 17 van het besluit daar niet reeds toe verplicht;
i. 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;
j. segmenteert de essentiële entiteit of belangrijke entiteit systemen in netwerken of zones overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het besluit bedoelde risicoanalyse.

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

Artikel 6. Beveiligingsaspecten ten aanzien van toegangsbeleid

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

Artikel 7. Nadere criteria significante incidenten

1. Een operationele verstoring is 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 is gedurende ten minste 24 uur geheel of gedeeltelijk onderbroken;
   b. ten minste 50% van de totale productie, verwerking of distributie van levensmiddelen is gedurende ten minste 12 uur onderbroken;
   c. de productie, verwerking of distributie van levensmiddelen is gedurende ten minste 6 uur geheel onderbroken.
2. In afwijking van het eerste lid is een geplande dienstonderbreking of een ander gevolg van onderhoudswerkzaamheden die door of namens een essentiële entiteit of een belangrijke entiteit worden uitgevoerd, geen ernstige operationele verstoringen.
3. Materiële of immateriële schade is 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 dit veroorzaken;
   b. het incident heeft aanzienlijke schade aan de gezondheid van een of meer natuurlijke personen veroorzaakt of kan veroorzaken;
   c. de integriteit, de vertrouwelijkheid of de authenticiteit van gegevens die in verband met de dienst of levensmiddelen die de essentiële entiteit of de belangrijke entiteit verleent of produceert, verwerkt of distribueert, worden opgeslagen, verzonden of verwerkt, is aangetast; of
   d. er is sprake van een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van een essentiële entiteit of een belangrijke entiteit.

Artikel 8. 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 9. Inwerkingtreding

[PM: Deze regeling treedt in werking met ingang van [DATUM].]

Artikel 10. Citeertitel

Deze regeling wordt aangehaald als: Regeling cyberbeveiliging levensmiddelensector.

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

's-Gravenhage,

De Minister van Landbouw, Visserij, Voedselzekerheid en Natuur

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 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 ministeriële 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

Deze ministeriële regeling bevat nadere regels inzake de meldplicht van significante incidenten als bedoeld in artikel 25, tweede lid, van de Cyberbeveiligingswet, en betreft de implementatie van artikel 23, derde lid, de richtlijn (EU) 2022/2555 over cyberbeveiliging (NIS 2-richtlijn).
Tevens bevat deze regeling nadere regels inzake de zorgplicht als bedoeld in artikel 20 van het Cyberbeveiligingsbesluit (hierna ook: Cbb) De nadere invulling van de zorgplicht uit de Cbw en Cbb concretiseert belangrijke onderdelen voor de beveiliging van netwerk- en informatiesystemen en versterkt daarmee de digitale weerbaarheid van entiteiten.
Daarnaast worden in deze regeling andere autoriteiten aangewezen waarmee samenwerking en informatie-uitwisseling gewenst is, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cbw.
De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

3. Inhoud regeling

3.1 Nadere regels zorgplicht

In deze regeling worden voor de in artikel 2 genoemde sectoren nadere regels gesteld ten aanzien van de zorgplicht uit de Cbw en het Cbb. Het doel van deze nadere invulling is om de algemene normen uit de wet en het besluit verder te concretiseren op onderdelen die van groot belang zijn voor de beveiliging van netwerk- en informatiesystemen. Dit biedt duidelijkheid aan essentiële en belangrijke entiteiten en zorgt voor een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen. Bij het opstellen van deze nadere regels is getracht aan te sluiten bij de systematiek uit de wet, het Cbb en Uitvoeringsverordening (EU) 2024/2690. Daarmee zou de regeling goed toepasbaar moeten zijn voor entiteiten die tevens binnen het bereik van de uitvoeringsverordening vallen op basis van artikel 4, Cbb.

3.2 Nadere criteria meldplicht

---

[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).

Meldplicht
De nadere criteria meldplicht in deze regeling beogen duidelijkheid te verschaffen over wanneer de essentiële entiteit of de belangrijke entiteit een melding dient te maken van een significant incident. Deze nadere regels zijn van toepassing op de essentiële en belangrijke entiteiten binnen de sector productie, verwerking en distributie van levensmiddelen waarvoor de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur beleidsverantwoordelijkheid voor is.
De meldplicht heeft betrekking op incidenten die als significant worden beschouwd. Een 'incident' is gedefinieerd in artikel 1 van de Cbw als: "*een gebeurtenis die de beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit van netwerk- en informatiesystemen of diensten die worden aangeboden, in gevaar brengt*." Een incident wordt volgens de Cbw, artikel 25, tweede lid, gekenmerkt als 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 andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Fasen en wijze van melding
Een essentiële of belangrijke entiteit meldt een significant incident bij het aangewezen sectorale Computer Security Incident Response Team (CSIRT) en bij de aangewezen toezichthoudende instantie. Hiervoor is één centraal meldloket ingericht onder regie van de Minister van Justitie en Veiligheid. Op basis van artikel 26, eerste lid, van de Cbw doet de entiteit "onverwijld een vroegtijdige waarschuwing, of indien dat niet mogelijk is, binnen 24 uur nadat zij kennis heeft gekregen van het significante incident." Artikel 27, eerste lid, van de Cbw bepaalt voorts dat de entiteit onverwijld of, indien dit niet mogelijk is, binnen 72 uur nadat zij kennis heeft gekregen van het significante incident, daarvan een melding doet bij het CSIRT en de bevoegde autoriteit. De termijnen gaan lopen vanaf het moment waarop de entiteit kennisneemt van een incident waarvan op dat moment redelijkerwijs mag worden aangenomen dat het significant is. Daarbij ligt de nadruk op het tijdig onderzoeken van het incident om vast te stellen of het voldoet aan de parameters van artikel 25, tweede lid, van de Cbw. Deze parameters zien op ernstige operationele verstoring of financiële verliezen voor de betrokken entiteit, of op aanzienlijke materiële of immateriële schade voor andere entiteiten. De regels omtrent de verdere procedures voor het melden van incidenten, zoals het tijdstip van melding en de te verstrekken informatie, zijn in de artikelen 26 tot en met 29 van de Cbw en worden in deze regeling niet nader opgenomen.

Totstandkoming nadere criteria
In artikel 24, eerste lid, van het Cbb is bepaald dat de Minister die het aangaat, 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 het opstellen van de nadere criteria van de meldplicht is er contact geweest met diverse, stakeholder uit de levensmiddelensector en de Nederlandse Voedsel- en Warenautoriteit als toezichthoudende instantie. Deze afstemming had als doel de regels goed te laten aansluiten op de praktijk en bestaande kaders, om de uitvoerbaarheid en handhaafbaarheid te borgen en onnodige regeldruk te beperken.
Uitgangspunt bij het uitwerken van de nadere criteria van de meldplicht was het waarborgen van de continuïteit van de levering van essentiële diensten en de leveringszekerheid van levensmiddelen. Voor de nadere uitwerken van de ernst van de operationele verstoring is gekeken naar de gevolgen van een operationele verstoring van de eigen essentiële dienst van de betrokken essentiële entiteit en belangrijke entiteit en niet aan de hand van de gevolgen voor derden.
Bij het uitwerken van de nadere criteria voor het bepalen van materiële en

immateriële schade is rekening gehouden met de aard van de risico's die zich kunnen voordoen binnen de sectoren waarop de wet van toepassing is, en met de doelstelling van de wet. De in deze regeling opgenomen drempelwaarden bieden objectieve aanknopingspunten voor de beoordeling of sprake is van aanzienlijke materiële of immateriële schade.

3.3 Aanwijzing autoriteiten

Voor een aantal wetten geldt dat zij nauwe raakvlakken hebben met de Cbw. Het is daarom gewenst dat de bevoegde autoriteiten, CSIRT's en het centrale contactpunt onder de Cbw (hierna: Cbw-instanties) voor de doeltreffende en doelmatige uitvoering van hun taken samenwerken en informatie uitwisselen met de autoriteiten die toezicht houden op de naleving van deze andere wetgeving, als bedoeld in artikel 51, tweede lid, onderdeel i, van de Cbw.
Het betreft hierbij de samenwerking met de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur uit hoofde van de Wet dieren en de samenwerking met de Minister van Volksgezondheid, Welzijn en Sport voor de taken uit hoofde van de Warenwet. De Nederlandse Voedsel- en Warenautoriteit houdt namens beide ministers toezicht op de naleving van de Wet dieren en de Warenwet. Het betreft hierbij voor een deel ook toezicht op entiteiten die ook onder de reikwijdte van de Cbw vallen. Het is daarom gewenst dat de samenwerking een grondslag krijgt.

4. Notificatie

[PM]

5. Regeldruk

Deze regeling veroorzaakt geen nieuwe regeldruk ten opzichte van de Cbw en het Cbb. De regeldruk voor essentiële entiteiten en belangrijke entiteiten is verantwoord in de bijbehorende toelichtingen van het wetsvoorstel en het besluit.

6. Uitvoering

[PM]

7. Advies en consultatie

7.1 Internetconsultatie

PM

7.2 Advies Adviescollege Toetsing Regeldruk

PM

8. Evaluatie

Deze regeling wordt periodiek geëvalueerd en waar nodig aangepast, zo volgt uit artikel 24, tweede lid, van het Cbb. Op grond van die bepaling evalueert de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur ten minste elke vier jaar de doeltreffendheid van de nadere regels over de meldplicht en de effecten daarvan in de praktijk, en past deze zo nodig aan.

9. Inwerkingtreding

PM

II. Artikelsgewijs

Artikel 3 - Beleid over beveiliging van netwerk- en informatiesystemen

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

Artikel 4 - Bedrijfscontinuïteit

Dit artikel 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 essentiële entiteit en de belangrijke entiteit dienen 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. Zo worden de duur en gevolgen van dergelijke incidenten beperkt. Bij het opstellen daarvan moet de entiteit 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 elementen 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 bedrijfsvoeringcontext 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 of 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 of belangrijke entiteit ervoor dat er voldoende middelen beschikbaar zijn om de primaire processen doorgang te laten vinden. Bij redundantie worden systemen, veelal kritieke systemen, dubbel uitgevoerd om hiermee de beschikbaarheid te verhogen en hierdoor wordt het netwerk kwetsbaar.

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 van artikel 9, tweede lid, omschrijven welke aspecten in de back-upplannen terug dienen te komen. Het bepalen van hersteltijden, in het Engels bekend als *recovery time objective (RTO),* heeft betrekking op de tijdsspannen waarbinnen back-ups teruggeplaatst moeten kunnen worden. Herstelpunten, in het Engels bekend als *recovery point objective (RPO),* heeft betrekking op de frequentie van de back-ups. Het voorschrift dat back-ups volledig zijn, ziet erop dat alle gegevens die nodig zijn voor het herstellen van de betreffende netwerk- en informatiesystemen zijn opgenomen, waaronder maar ook 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 back-ups nauwkeurig te zijn. Dit houdt in dat de gemaakte back-ups een juiste en consistente weergave vormen van de gebruikte software en gegevens, zodat deze bij herstel zonder afwijkingen kunnen worden teruggezet en opnieuw inzetbaar zijn.
Voorts moeten de beschikbaarheid en integriteit van back-ups zijn gewaarborgd, zodat deze in geval van een incident daadwerkelijk kunnen worden gebruikt. In het bijzonder is het van belang om waarborgen te treffen tegen incidenten waardoor back-ups, al dan niet als gevolg van kwaadwillende handelingen, zoals ransomware-aanvallen, onbruikbaar kunnen worden. Tevens moet de vertrouwelijkheid van back-ups zijn gewaarborgd, om ongeautoriseerde toegang tot de daarin opgenomen gegevens te voorkomen.
De risicobeoordelingen op grond van artikel 7 van het Cyberbeveiligingsbesluit zijn derhalve zowel relevant voor het bepalen van welke software en 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 essentiële en belangrijke entiteit tijdig wordt geïnformeerd over tekortkomingen. Het back-upplan 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 essentiële entiteit of belangrijke 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. Anderzijds biedt het testen meer zekerheid dat er geen technische belemmeringen zijn om de back-ups daadwerkelijk terug te zetten.

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

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

Tweede lid
Om potentiële risico's voor de beveiliging van netwerk- en informatiesystemen weg te nemen dienen essentiële en belangrijke entiteiten processen en procedures in te richten voor het toepassen van beveiligingspatches. Beveiligingspatchbeheer is van belang om bekende kwetsbaarheden in software en systemen tijdig te verhelpen en misbruik daarvan te voorkomen. Op grond van het tweede lid, onderdeel a, geldt dat waar passend gecontroleerd moet worden of beveiligingspatches afkomstig zijn van betrouwbare bronnen en of de integriteit van deze patches gewaarborgd is. Het vereiste geldt waar passend, omdat bij patches zoals reguliere systeemupdates van besturingssystemen doorgaans geen afzonderlijke controle door de essentiële en belangrijke entiteit op herkomst en integriteit nodig is vanwege reeds ingebouwde technische controles. Op grond van onderdeel b geldt dat beveiligingspatches, waar passend, getest moeten worden voordat zij in de productieomgeving worden toegepast. De noodzaak van een dergelijke test is afhankelijk van de risico's die het installeren van de patch met zich meebrengt. Voornoemde stappen dragen ertoe bij dat de toepassing van patches geen nieuwe kwetsbaarheden of verstoringen veroorzaakt. Vervolgens bepaalt onderdeel c dat beveiligingspatches binnen een redelijke termijn nadat zij beschikbaar zijn moeten worden toegepast, tenzij de nadelen van de toepassing van de 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 om te toetsen is of dit een terechte keuze was. Het is aan de entiteit om te bepalen hoe dit wordt gedocumenteerd.

Derde lid
Onderdeel a
Ter bescherming van diens netwerk- en informatiesystemen dienen essentiële entiteiten en belangrijke entiteiten op grond van dit onderdeel maatregelen te nemen tegen kwaadaardige en ongeoorloofde software. Typische oplossingen voor netwerkbeveiliging omvatten het gebruik van firewalls en *intrusion prevention systems* om de interne netwerken van de relevante entiteiten te beschermen, alsmede het gebruik van antivirussoftware om potentiële kwaadaardige software op te kunnen sporen.

Onderdeel b
Op grond van dit onderdeel voeren essentiële en belangrijke entiteiten, waar passend, periodiek kwetsbaarheidsscans uit en leggen zij de resultaten daarvan vast. Het is aan de entiteit om te bepalen hoe dit wordt gedocumenteerd. 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. Door de resultaten te documenteren, kan worden vastgesteld welke maatregelen nodig zijn en kan tevens worden geborgd dat opvolging plaatsvindt.

Onderdeel c
Op grond dit onderdeel evalueren essentiële en belangrijke entiteiten hun blootstelling aan relevante kwetsbaarheden en dreigingen waar zij kennis van hebben. Door deze evaluatie structureel uit te voeren, ontstaat een actueel beeld van het risicolandschap en kan tijdig worden bepaald welke aanvullende maatregelen nodig zijn om de weerbaarheid te vergroten.

Onderdeel d
Op grond dit onderdeel nemen essentiële entiteiten en belangrijke entiteiten maatregelen om kwetsbaarheden te adresseren. Indien een kwetsbaarheid niet of op een later moment verholpen wordt dient de essentiële entiteit en belangrijke entiteit dit te motiveren en te documenteren. Het is aan de entiteit om te bepalen hoe dit wordt gedocumenteerd. Evenals bij het niet toepassen van een beveiligingspatch wordt voor de toezichtspraktijk dan duidelijk waarom er wordt afgeweken en kan de toezichthouder oordelen of deze beslissing terecht is genomen.

Onderdeel e
Essentiële entiteiten en belangrijke entiteiten dienen ook te waarborgen dat bij incidenten met betrekking tot de beveiliging van een netwerk- en informatiesysteem de gevolgen voor andere netwerk- en informatiesystemen worden beperkt. Op grond van dit onderdeel dienen essentiële entiteiten en belangrijke entiteiten hun netwerken te segmenteren overeenkomstig de resultaten van de in artikel 7, vijfde lid, van het Cyberbeveiligingsbesluit bedoelde risicobeoordeling. Hierbij kunnen entiteiten zelf in acht nemen op welke wijze ze de netwerksegmentatie toepassen. Daarbij wordt rekening gehouden 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 waar mogelijk van elkaar te scheiden
Het is daarnaast best practice om toegang tot een netwerk of zone te verlenen op basis van een beoordeling van de beveiligingsvoorschriften, om systemen die van cruciaal belang zijn voor de werking van de entiteit of voor de veiligheid in beveiligde zones te houden, en om een gedemilitariseerde zone in communicatiekanalen uit te rollen om te waarborgen dat communicatie die afkomstig is van of bestemd is voor haar netwerken beveiligd is.
Andere goede praktijken zijn het specifieke netwerk voor het beheer van netwerk- en informatiesystemen te scheiden van het operationele netwerk van de entiteit, de kanalen voor netwerkbeheer te scheiden van ander netwerkverkeer, en de productiesystemen voor de diensten van de entiteit te scheiden van de systemen die worden gebruikt voor de ontwikkeling en tests, met inbegrip van back-ups.

Vierde lid
Op grond van het vierde lid dienen essentiële en belangrijke entiteiten, waar passend, hun systemen en netwerken te segmenteren van de systemen en netwerken van derden. Bij netwerksegmentatie gaat het om het onderverdelen van een fysiek netwerk in verschillende logische onderdelen die van elkaar afgeschermd kunnen worden. Op elk netwerksegment kunnen verschillende beveiligingsmaatregelen worden toegepast. Zo krijgt een kwaadwillende die in een bepaald netwerksegment is gekomen, niet automatisch ook toegang tot andere delen van het netwerk. Deze verplichting beoogt te voorkomen dat de beveiliging van de eigen netwerk- en informatiesystemen wordt ondermijnd door kwetsbaarheden of incidenten bij externe partijen waarmee wordt samengewerkt, zoals leveranciers, onderhoudspartners of dienstverleners. Door een duidelijke scheiding aan te brengen tussen interne en externe netwerken kan worden beperkt dat een beveiligingsincident bij een derde partij zich verspreidt naar de systemen van de entiteit zelf. De mate waarin segmentatie noodzakelijk is, hangt af van de aard van de samenwerking en de gevoeligheid van de uitgewisselde gegevens. In de praktijk kan dit bijvoorbeeld worden vormgegeven door het toepassen van strikte toegangscontroles, het gebruik van beveiligde

communicatiekanalen en het beperken van directe netwerkverbindingen met derden tot het strikt noodzakelijke.

Artikel 6 - Beveiligingsaspecten ten aanzien van toegangsbeleid
Essentiële entiteiten en belangrijke entiteiten dienen vastgesteld beleid te hebben voor het gebruik van bevoorrechte accounts en systeembeheeraccounts voor de logische en fysieke toegang tot netwerk- en informatiesystemen. Met bevoorrechte accounts wordt bedoeld dat gebruikers over extra rechten beschikken die nodig zijn om kritieke functies uit te voeren, zoals systeembeheer, installatie, configuratie of onderhoud. Het beleid legt vast hoe deze accounts worden toegewezen, gebruikt en beheerd, en wordt schriftelijk vastgelegd zodat de toepassing aantoonbaar is.
Het tweede lid geeft nadere invulling aan het beleid voor bevoorrechte accounts en systeembeheeraccounts door te specificeren welke maatregelen en procedures moeten worden toegepast. Het beleid moet ervoor zorgen dat sterke identificatie- en authenticatieprocedures, zoals multifactorauthenticatie, worden toegepast en dat authorisatie zorgvuldig wordt geregeld. Zo wordt de dreiging van phishing en andere misbruik van dergelijke accounts zoveel mogelijk tegengegaan. Daarnaast schrijft het lid voor dat specifieke accounts uitsluitend worden gebruikt voor systeembeheer en dat de voorrechten van deze accounts zoveel mogelijk worden geïndividualiseerd en beperkt tot het strikt noodzakelijke. Dit draagt bij aan een duidelijke scheiding van functies. Ook voorkomt het dat accounts voor meerdere doeleinden worden gebruikt en dat acties niet herleidbaar zijn tot specifieke personen. Daardoor wordt het risico op fouten of misbruik verminderd. Tevens is vastgelegd dat systeembeheeraccounts alleen verbinding maken met de systemen waarvoor zij zijn bedoeld, zodat activiteiten traceerbaar en controleerbaar blijven en de veiligheid van de netwerk- en informatiesystemen gewaarborgd is.

Artikel 7 Nadere criteria significante incidenten
Dit artikel bevat nadere criteria om te bepalen wanneer sprake is van een significant incident. De criteria gelden voor alle entiteiten waarop deze regeling van toepassing is. 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 essentieel 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 hun toezichthouder, de NVWA, en bij hun CSIRT, het NCSC.
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 geen 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 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
Onderhoudswerkzaamheden die leiden tot beperkte beschikbaarheid of niet-beschikbaarheid van diensten worden niet als significante incidenten beschouwd, voor zover deze plaatsvinden in het kader van een geplande onderhoudsactiviteit en de gevolgen daarvan voorzien waren. Evenmin worden geplande onderbrekingen van de dienstverlening, zoals onderbrekingen of niet-beschikbaarheid op basis van een vooraf bepaalde contractuele overeenkomst, als significant 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, de vertrouwelijkheid of de 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 kwaadwillenden

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 voorraadbeheersystemen, 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 word de authenticiteit meegenomen in dit meldcriterium, omdat dit een belangrijk aspect is om vertrouwelijkheid en integriteit te waarborgen.
De meldplicht is echter 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. Er is tevens sprake van een significant incident als er een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen heeft plaatsgevonden. Dit is uitgewerkt onderdeel d. 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.

De Minister van Landbouw, Visserij, Voedselzekerheid en Natuur.