Besluit van [datum], houdende regels ter uitvoering van de Cyberbeveiligingswet (Cyberbeveiligingsbesluit)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Justitie en Veiligheid van [datum], Directie Wetgeving en Juridische Zaken, nr. [nummer], gedaan in overeenstemming met Onze Ministers van PM;

Gelet op de artikelen 3, 16, eerste en zevende lid, 17, eerste lid, 21, vijfde lid, 24, zesde lid, 25, derde lid, 35, 44, eerste lid, onderdeel f, 51, tweede lid, onderdeel i, en 65, eerste lid, van de Cyberbeveiligingswet, de artikelen 14, vijfde lid, en 15, vierde lid, van de Wet weerbaarheid kritieke entiteiten, de artikelen 1:3a, vierde lid, 1:24, derde lid, en 1:25, derde lid, onderdeel b, van de Wet op het financieel toezicht, artikel 54a van de Drinkwaterwet en de artikelen 11a.1, tweede en vierde lid, en 11a.3, zesde lid, van de Telecommunicatiewet;

De Afdeling advisering van de Raad van State gehoord (advies van [datum], nr. [PM]);

Gezien het nader rapport van Onze Minister van Justitie en Veiligheid van [datum], Directie Wetgeving en Juridische Zaken, nr. [nummer], uitgebracht in overeenstemming met Onze Ministers van [PM];

Hebben goedgevonden en verstaan:

Hoofdstuk 1. Begripsbepaling

Artikel 1 (begripsbepaling)

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

Hoofdstuk 2. Aanwijzing CSIRT en coördinator bekendmaking kwetsbaarheden

Artikel 2 (aanwijzing CSIRT)

1. Onze Minister wordt voor essentiële entiteiten en belangrijke entiteiten aangewezen als het CSIRT, bedoeld in artikel 16, eerste lid, van de wet.

2. Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, kan in afwijking van het eerste lid voor essentiële entiteiten en belangrijke entiteiten uit specifieke sectoren en subsectoren, voor specifieke soorten entiteiten en voor specifieke entiteiten een ander dan Onze Minister worden aangewezen als het CSIRT, bedoeld in artikel 16, eerste lid, van de wet.

Artikel 3 (aanwijzing coördinator bekendmaking kwetsbaarheden)

Onze Minister is de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden, bedoeld in artikel 17 van de wet.

Hoofdstuk 3. Toepassingsbereik

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

Gelet op artikel 1 van de Uitvoeringsverordening (EU) 2024/2690 zijn de artikelen 6 tot en met 17 en 19 niet van toepassing op de volgende essentiële entiteiten en belangrijke entiteiten:
a. DNS-dienstverleners;
b. registers voor topleveldomeinnamen;
c. aanbieders van cloudcomputingdiensten;
d. aanbieders van datacentrumdiensten;
e. aanbieders van netwerken voor de levering van inhoud;
f. aanbieders van beheerde diensten;
g. aanbieders van beheerde beveiligingsdiensten;
h. aanbieders van onlinemarktplaatsen;
i. aanbieders van onlinezoekmachines;
j. aanbieders van platforms voor socialenetwerkdiensten; en
k. verleners van vertrouwensdiensten.

Hoofdstuk 4. Zorgplicht

Artikel 5 (uitvoering van artikel 21 van de wet)

Ter uitvoering van artikel 21 van de wet neemt de essentiële entiteit of belangrijke entiteit ten minste de maatregelen, bedoeld in de artikelen 6 tot en met 19.

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

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over de beveiliging van haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, de rollen, verantwoordelijkheden en bevoegdheden in relatie tot de beveiliging van haar netwerk- en informatiesystemen vast. De entiteit zorgt er zoveel mogelijk voor dat conflicterende rollen, verantwoordelijkheden en bevoegdheden gescheiden worden.

3. De essentiële entiteit of belangrijke entiteit verlangt van haar personeel en andere binnen de entiteit werkzame personen dat zij de beveiliging van haar netwerk- en informatiesystemen toepassen overeenkomstig het beleid, bedoeld in het eerste lid.

4. De essentiële entiteit of belangrijke entiteit hanteert een managementsystematiek voor de beveiliging van haar netwerk- en informatiesystemen om aantoonbaar te kunnen voldoen aan het bepaalde bij of krachtens artikel 21 van de wet.

Artikel 7 (beleid over risicomanagement)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over risicomanagement voor de beveiliging van haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Het beleid, bedoeld in het eerste lid, omvat ten minste:
a. een risicomanagementmethodiek; en
b. criteria voor risicoacceptatie.

3. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast voor risicoanalyse, risicobeoordeling en risicobehandeling. De entiteit past deze processen en procedures aantoonbaar toe.

4. De essentiële entiteit of belangrijke entiteit maakt op basis van de uitgevoerde risicoanalyse een overzicht van de risico’s met betrekking tot de beveiliging van haar netwerk- en informatiesystemen.

5. De essentiële entiteit of belangrijke entiteit stelt op basis van het overzicht van de risico’s, bedoeld in het vierde lid, eisen met betrekking tot de beveiliging van haar netwerk- en informatiesystemen. Indien de risicoanalyse hiertoe aanleiding geeft, neemt de entiteit maatregelen om de beveiliging van haar netwerk- en informatiesystemen op structurele en aantoonbare wijze te borgen.

Artikel 8 (incidentenbehandeling)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over incidentenbehandeling. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, de rollen, verantwoordelijkheden en bevoegdheden vast voor:
a. het tijdig detecteren van incidenten;
b. het analyseren en beoordelen van incidenten;
c. het reageren op, beperken van de gevolgen van, wegnemen van de oorzaak van en herstellen van incidenten;
d. het documenteren van incidenten;
e. het rapporteren van incidenten; en
f. het leren van incidenten.

3. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast om relevante gebeurtenissen in haar netwerk- en informatiesystemen te monitoren teneinde incidenten te detecteren, analyseren en classificeren. De entiteit past deze processen en procedures aantoonbaar toe.

4. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast voor:
a. het tijdig detecteren van incidenten;
b. het analyseren en beoordelen van incidenten;
c. het reageren op, beperken van de gevolgen van, wegnemen van de oorzaak van en herstellen van incidenten;
d. het documenteren van incidenten;
e. het rapporteren van incidenten; en
f. het leren van incidenten.

5. De essentiële entiteit of belangrijke entiteit past de processen en procedures, bedoeld in het vierde lid, aantoonbaar toe.

6. De essentiële entiteit of belangrijke entiteit logt de voor de beveiliging van haar netwerk- en informatiesystemen relevante gebeurtenissen in haar netwerk- en informatiesystemen. De entiteit houdt gedurende een vooraf bepaalde periode deze logbestanden bij en beschermt deze tegen ongeautoriseerde wijzigingen.

Artikel 9 (bedrijfscontinuïteit en crisisbeheer)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld bedrijfscontinuïteitsbeleid met betrekking tot haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast voor het borgen van haar bedrijfscontinuïteit, waaronder in ieder geval processen en procedures voor het herstellen van haar netwerk- en informatiesystemen en voor het maken en periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens. De entiteit past deze processen en procedures aantoonbaar toe en test deze periodiek.

3. De essentiële entiteit of belangrijke entiteit heeft een vastgesteld bedrijfscontinuïteitsplan met betrekking tot haar netwerk- en informatiesystemen. De entiteit legt dat plan schriftelijk vast, past dat plan toe in geval van een incident die de bedrijfscontinuïteit in gevaar brengt, en test dit plan periodiek.

4. De essentiële entiteit of belangrijke entiteit heeft een herstelplan. De entiteit legt dat plan schriftelijk vast, past dat plan toe in geval van een incident en test dit plan periodiek.

5. De essentiële entiteit of belangrijke entiteit heeft een plan voor crisisbeheer, legt dit plan schriftelijk vast, past dat plan toe in geval van een crisis en test en beoefent dit plan periodiek. Het plan bevat ten minste:

a. de taken, verantwoordelijkheden en bevoegdheden ten tijde van crisis voor het personeel en andere binnen de entiteit werkzame personen;
b. een beschrijving van de communicatiemiddelen ten tijde van crisis; en
c. wanneer passend, een beschrijving van de beschikbare noodvoorzieningen, waaronder het gebruik van beveiligde noodcommunicatiesystemen ten tijde van crisis.

Artikel 10 (beveiliging van de toeleveringsketen)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over de beveiliging van de toeleveringsketen. De entiteit bepaalt in dat beleid haar omgang met afhankelijkheden van de producten en diensten van haar leveranciers en dienstverleners die invloed kunnen hebben op de beveiliging van haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit toetst of haar rechtstreekse leveranciers en rechtstreekse dienstverleners, bedoeld in het eerste lid, voldoen aan de beveiligingseisen, bedoeld in artikel 7, vijfde lid. De entiteit controleert dit periodiek.

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

1. De essentiële entiteit of belangrijke entiteit heeft op basis van de beveiligingseisen, bedoeld in artikel 7, vijfde lid, vastgesteld beleid voor het mitigeren en beheersen van risico's die voortvloeien uit het verwerven van software, hardware of diensten die betrekking hebben op haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Indien van toepassing stelt de essentiële entiteit of belangrijke entiteit processen en procedures vast voor de veilige ontwikkeling van haar netwerk- en informatiesystemen. De entiteit past deze processen en procedures aantoonbaar toe. Deze processen en procedures hebben betrekking op alle ontwikkelingsfasen van de netwerk- en informatiesystemen van de entiteit.

3. De essentiële entiteit of belangrijke entiteit stelt processen en procedures vast voor het onderhoud en beheer van haar netwerk- en informatiesystemen. De entiteit past deze processen en procedures aantoonbaar toe. Deze processen en procedures hebben ten minste betrekking op het configuratiebeheer en het wijzigingsbeheer van de netwerk- en informatiesystemen van de entiteit.

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

1. De essentiële entiteit of belangrijke entiteit zorgt ervoor dat haar personeel en andere binnen de entiteit werkzame personen, voor zover relevant voor hun functie:
a. bewust zijn van de risico's met betrekking tot de netwerk- en informatiesystemen van de entiteit; en
b. praktijken op het gebied van cyberhygiëne toepassen.

2. De essentiële entiteit of belangrijke entiteit wijst het personeel en andere binnen de entiteit werkzame personen aan waarvan de rollen, verantwoordelijkheden en bevoegdheden vaardigheden en deskundigheid vereisen op het gebied van de beveiliging van netwerk- en informatiesystemen en zorgt ervoor dat zij regelmatig opleiding krijgen over de beveiliging van netwerk- en informatiesystemen.

Artikel 13 (beleid over het gebruik van cryptografie)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over het gebruik van cryptografie. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast over het gebruik van cryptografie. De entiteit past deze processen en procedures aantoonbaar toe.

3. In het beleid en de processen en procedures, bedoeld in het eerste en tweede lid, worden in ieder geval uitgewerkt:

a. in welke gevallen cryptografie ingezet wordt;
b. in voorkomende gevallen, welke typen encryptie worden gebruikt en de wijze waarop deze worden toegepast;
c. wie binnen de entiteit verantwoordelijk zijn voor de implementatie van cryptografie; en
d. wie binnen de entiteit verantwoordelijk zijn voor het sleutelbeheer.

Artikel 14 (beveiligingsaspecten ten aanzien van personeel)

1. De essentiële entiteit of belangrijke entiteit wijst het personeel en andere binnen de entiteit werkzame personen aan die worden belast met rollen, verantwoordelijkheden en bevoegdheden met betrekking tot de beveiliging van haar netwerk- en informatiesystemen.

2. De essentiële entiteit of belangrijke entiteit evalueert periodiek de aanwijzing, bedoeld in het eerste lid, en werkt deze aanwijzing indien nodig bij.

3. De essentiële entiteit of belangrijke entiteit stelt betrouwbaarheidseisen op waaraan haar personeel en andere binnen de entiteit werkzame personen moeten voldoen, voor zover deze passend en noodzakelijk zijn voor hun taakuitoefening met betrekking tot de beveiliging van de netwerk- en informatiesystemen van de entiteit.

Artikel 15 (beveiligingsaspecten ten aanzien van toegangsbeleid)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over de logische en fysieke toegang tot haar netwerk- en informatiesystemen. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Het beleid, bedoeld in het eerste lid, omvat in ieder geval het uitgeven, monitoren, gebruiken, wijzigen en intrekken van identiteiten en autorisaties, en het beheer van identiteiten en autorisaties.

3. De essentiële entiteit of belangrijke entiteit controleert identiteiten, authenticatiemiddelen en autorisaties periodiek op de noodzakelijkheid, juistheid en actualiteit en voert indien nodig wijzigingen door in de identiteiten, authenticatiemiddelen en autorisaties.

Artikel 16 (beveiligingsaspecten ten aanzien van beheer van assets)

1. De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid voor het beheer van haar assets die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

2. Het beleid, bedoeld in het eerste lid, omvat in ieder geval:
a. een systeem om assets op verschillende niveaus te kunnen classificeren, indien van toepassing op basis van de eisen voor vertrouwelijkheid, integriteit en beschikbaarheid; en
b. regels voor het aanvaardbaar gebruik van haar assets.

3. De essentiële entiteit of belangrijke entiteit stelt in het kader van de toepassing van het beleid, bedoeld in het eerste lid, processen en procedures vast voor het beheer van haar assets. De entiteit past deze processen en procedures aantoonbaar toe.

4. De essentiële entiteit of belangrijke entiteit heeft een volledige en actuele inventaris van haar assets, en houdt deze bij.

Artikel 17 (attenderingen, adviezen en informatie)

Indien de essentiële entiteit of belangrijke entiteit door relevante partijen, waaronder CSIRT's, bevoegde autoriteiten, andere betrokken overheidsinstanties of rechtstreekse leveranciers of dienstverleners, gericht wordt geattendeerd op de voor de beveiliging van haar netwerk- en informatiesystemen relevante kwetsbaarheden of cyberdreigingen, of van die partijen gerichte beveiligingsadviezen of dreigingsinformatie ontvangt die relevant zijn voor de beveiliging van haar netwerk- en informatiesystemen, beoordeelt zij of op basis daarvan aanpassingen of aanvullingen nodig zijn van de maatregelen die nodig zijn ter uitvoering van artikel 21 van de wet. De entiteit legt de uitkomsten van die beoordeling schriftelijk vast.

Artikel 18 (weren producten en diensten van leveranciers)

1. Indien dat naar het oordeel van Onze Minister die het aangaat noodzakelijk is om risico's voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen, legt hij in overeenstemming met Onze Minister een essentiële entiteit of een belangrijke entiteit de verplichting op om in de daarbij aangewezen onderdelen van haar netwerk- en informatiesystemen uitsluitend gebruik te maken van producten of diensten van anderen dan de daarbij door Onze Minister die het aangaat genoemde partij die:
a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft om de beveiliging van de netwerk- en informatiesystemen van de essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij de essentiële entiteit of belangrijke entiteit te veroorzaken; of
b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld in onderdeel a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

2. Indien de verplichting, bedoeld in het eerste lid, betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen, stelt Onze Minister die het aangaat in het belang van de continuïteit van de dienstverlening een termijn vast voor het vervangen respectievelijk beëindigen van de betreffende producten en diensten.

3. Het eerste lid is niet van toepassing ten aanzien van essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn.

Artikel 19 (evaluatie)

De essentiële entiteit of belangrijke entiteit evalueert periodiek de doeltreffendheid van de maatregelen die zij heeft genomen op grond van artikel 21, eerste lid, van de wet en de effecten ervan in de praktijk, en legt het resultaat daarvan schriftelijk vast. De entiteit past naar aanleiding van de uitkomst van die evaluaties de maatregelen waar nodig aan.

Artikel 20 (nadere regels)

Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, kunnen nadere regels worden gesteld over de maatregelen, bedoeld in artikel 21, eerste lid, van de wet, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten.

Hoofdstuk 5. Training

Artikel 21 (doel van de training)

De training, bedoeld in artikel 24, vijfde lid, van de wet, stelt het lid van het bestuur van de essentiële entiteit of belangrijke entiteit in staat om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen. Ook stelt de training het lid van het bestuur van de entiteit in staat om risicobeheersmaatregelen op het gebied van cyberbeveiliging en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

Artikel 22 (eisen aan de training)

1. Ten behoeve van het verkrijgen van kennis en vaardigheden om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren als bedoeld in artikel 24, tweede lid, onderdeel a, van de wet en de gevolgen van deze risico's te kunnen beoordelen, bedoeld in artikel 24, tweede lid, onderdeel c, van de wet, behandelt de training, bedoeld in artikel 24, vijfde lid, van de wet, daartoe in ieder geval de volgende onderwerpen:
a. de soorten risico's voor netwerk- en informatiesystemen;
b. risicomanagementprocessen; en
c. risicobeoordelingsmethodiek.

2. Ten behoeve van het verkrijgen van kennis en vaardigheden om risicobeheersmaatregelen op het gebied van cyberbeveiliging als bedoeld in artikel 24, tweede lid, onderdeel b, van de wet en

de gevolgen van risicobeheersmaatregelen te kunnen beoordelen, bedoeld in artikel 24, tweede lid, onderdeel c, van de wet, behandelt de training, bedoeld in artikel 24, vijfde lid, van de wet, in ieder geval de onderwerpen, genoemd in artikel 21, derde lid, onderdelen a tot en met j, van de wet.

Artikel 23 (eisen aan het certificaat)

1. Het certificaat van de training, bedoeld in artikel 24, vijfde lid, van de wet, bevat in ieder geval:
a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit;
b. de datum of data waarop de training is gevolgd;
c. de behandelde onderwerpen in de training; en
d. de naam van de aanbieder van de training.

2. Het certificaat van de training, bedoeld in artikel 24, vijfde lid, van de wet, is opgesteld in de Nederlandse taal of de Engelse taal.

Hoofdstuk 6. Meldingen van significante incidenten, incidenten, bijna-incidenten, significante cyberdreigingen, cyberdreigingen en kwetsbaarheden

Artikel 24 (significante incidenten)

1. Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, worden de criteria vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, van de wet, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en soorten entiteiten.

2. Onze Minister die het aangaat evalueert ten minste elke vier jaar de doeltreffendheid van de criteria, bedoeld in het eerste lid, en de effecten daarvan in de praktijk. Indien nodig past hij de criteria, na overleg met Onze Minister, aan.

3. Het eerste lid is niet van toepassing ten aanzien van de entiteiten waarvoor in uitvoeringshandelingen op grond van artikel 23, elfde lid, van de NIS2-richtlijn nader is gespecificeerd in welke gevallen een incident bij die entiteiten als significant wordt beschouwd.

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

De vroegtijdige waarschuwing, bedoeld in artikel 26, eerste lid, van de wet, omvat naast de gegevens, genoemd in artikel 26, tweede lid, van de wet, tevens de volgende gegevens:
a. het vermoedelijke tijdstip van de aanvang van het significante incident;
b. zo mogelijk, een beschrijving van de aard en op dat moment merkbare gevolgen van het incident;
c. zo mogelijk, een prognose van de hersteltijd; en
d. zo mogelijk, de door de essentiële entiteit of belangrijke entiteit voorgenomen of genomen maatregelen om de gevolgen van het significante incident te beperken of herhaling hiervan te voorkomen.

Artikel 26 (wijze waarop een melding geschiedt)

De melding, bedoeld in artikel 25, eerste lid, van de wet, wordt gedaan bij een hiervoor door Onze Minister ingericht meldpunt.

Artikel 27 (nadere regels over meldingen)

Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, kunnen regels worden gesteld ter uitwerking van de artikelen 26 tot en met 30, 33 en 34 van de wet.

Hoofdstuk 7. Informatieverstrekking ten behoeve van nationaal register

Artikel 28 (informatieverstrekking ten behoeve van nationaal register)

1. Naast de informatie, genoemd in artikel 44, eerste lid, onderdelen a tot en met e, van de wet, verstrekt een essentiële entiteit, belangrijke entiteit en entiteit die domeinnaamregistratiediensten

verleent tevens aan Onze Minister de volgende informatie ten behoeve van de registratie in het nationaal register, bedoeld in artikel 43 van de wet:
a. de vermelding of zij de registratie doet als essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent; en
b. het nummer, bedoeld in artikel 9, onderdeel a, van de Handelsregisterwet 2007 of, indien zij niet in het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 2007, is ingeschreven, een daarmee vergelijkbaar registratienummer van het land waarin zij is gevestigd.

2. In afwijking van het eerste lid, onderdeel b, verstrekt een overheidsinstantie, indien zij geregistreerd staat in het Register van Overheidsorganisaties, de identificatiecode waarmee zij geregistreerd staat in het Register van Overheidsorganisaties.

3. In aanvulling op de informatie, genoemd in het eerste lid, en indien van toepassing, de informatie, genoemd in het tweede lid, verstrekt een essentiële entiteit of belangrijke entiteit tevens aan Onze Minister de volgende informatie ten behoeve van de registratie in het nationaal register, bedoeld in artikel 43 van de wet:
a. indien van toepassing, de soort entiteit, bedoeld in bijlage 1 of 2 van de wet, waartoe zij behoort; en
b. haar domeinnamen.

Hoofdstuk 8. Aanwijzing autoriteiten

Artikel 29 (aanwijzing autoriteiten)

Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, kunnen de autoriteiten, bedoeld in artikel 51, tweede lid, onderdeel i, van de wet, worden aangewezen.

Hoofdstuk 9. Persoonsgegevens

Artikel 30 (bewaring van persoonsgegevens)

1. De persoonsgegevens, niet zijnde de persoonsgegevens, bedoeld in artikel 64, tweede lid, van de wet, die door het centrale contactpunt, het CSIRT en Onze Minister bij of krachtens de wet worden verwerkt, worden niet langer bewaard dan noodzakelijk is ter uitvoering van hun taken op grond van de wet, doch uiterlijk binnen 60 maanden na de eerste verwerking verwijderd.

2. In afwijking van het eerste lid worden de persoonsgegevens die zijn opgenomen in het nationale register, bedoeld in artikel 43 van de wet, niet langer bewaard dan noodzakelijk is ter uitvoering van de taken van Onze Minister op grond van artikel 43 van de wet, doch uiterlijk binnen 60 maanden na de laatste bevestiging van de juistheid van de betreffende persoonsgegevens verwijderd.

3. De persoonsgegevens, niet zijnde de persoonsgegevens, bedoeld in artikel 64, eerste lid, van de wet, die door de bevoegde autoriteit bij of krachtens de wet worden verwerkt, worden niet langer bewaard dan noodzakelijk is ter uitvoering van haar taken op grond van de wet, doch uiterlijk binnen 120 maanden na de eerste verwerking verwijderd.

Hoofdstuk 10. Slotbepalingen

Artikel 31 (wijziging Besluit EU-verordeningen Wft)

In bijlage 35 van het Besluit EU-verordeningen Wft wordt een onderdeel toegevoegd, luidende:

5. Lidstaatoptie artikel 19, eerste lid, zesde paragraaf, en tweede lid, derde paragraaf (meldplicht ICT-incidenten)
Banken, handelsplatformen, centrale effectenbewaarinstellingen en centrale tegenpartijen doen de melding, bedoeld in artikel 19, eerste lid, eerste paragraaf, van de verordening, en de vrijwillige melding, bedoeld in artikel 19, tweede lid, eerste paragraaf, van de verordening, tevens bij het bij of krachtens artikel 16, eerste lid, van de Cyberbeveiligingswet aangewezen CSIRT voor de sectoren bankwezen en infrastructuur voor de financiële markt.

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

Het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten wordt als volgt gewijzigd:

A

Artikel 1 komt te luiden:

Artikel 1

In dit besluit en de daarop berustende bepalingen wordt onder wet verstaan: Telecommunicatiewet.

B

Artikel 2 komt te luiden:

Artikel 2

Bij ministeriële regeling kunnen regels worden gesteld omtrent de maatregelen, bedoeld in artikel 11a.1, eerste en derde lid, van de wet.

C

De artikelen 2a tot en met 5 vervallen.

D

Artikel 5b wordt als volgt gewijzigd:
a. in het eerste lid, onderdeel a wordt "de artikelen 11a.1, eerste lid, en 11a.3, eerste lid, van de wet" vervangen door "artikel 11a.3, eerste lid, van de wet";
b. in het eerste lid onderdeel b wordt "de artikelen 11a.1, eerste lid, en artikel 11a.3, eerste lid, van de wet," vervangen door "artikel 11a.3, eerste lid, van de wet,";
c. in het tweede lid wordt "in de artikelen 2a en 5a, tweede lid" vervangen door "in artikel 5a, tweede lid".

E

Paragraaf 3 vervalt.

F

Onder vernummering van de artikelen 10 en 11 tot de artikelen 7 en 8 wordt in hoofdstuk 4 een artikel ingevoegd luidende:

Artikel 6

Dit besluit berust op artikel 11a.3, zesde lid, van de Telecommunicatiewet.

G

In artikel 8 (nieuw) wordt "Besluit beveiliging en continuïteit openbare elektronische communicatienetwerken en -diensten" vervangen door "Besluit beveiliging openbare elektronische communicatienetwerken en- diensten en antenne-opstelpunten".

Artikel 33 (wijziging Besluit veiligheid en integriteit telecommunicatie)

In het Besluit veiligheid en integriteit telecommunicatie wordt na artikel 2 een artikel ingevoegd, luidende:

Artikel 2a

Dit besluit berust op artikel 11a.1, tweede lid, van de Telecommunicatiewet.

Artikel 34 (wijziging Drinkwaterbesluit)

Het Drinkwaterbesluit wordt als volgt gewijzigd:

A

Artikel 15 wordt als volgt gewijzigd:

1. Het opschrift komt te luiden:

Artikel 15. Toezicht door de eigenaar en risicobeoordeling en risicobeheer van het watervoorzieningssysteem

2. Het eerste lid wordt als volgt gewijzigd:
a. in onderdeel a wordt "verstoringen en andere risico's" vervangen door "het risico op verstoringen en overige risico's met betrekking tot het watervoorzieningssysteem";
b. in onderdeel b wordt "Legionella:" vervangen door "het risico op Legionella:".

B

In het opschrift van artikel 46a wordt na "Risicobeoordeling" ingevoegd: "en risicobeheer".

C

Artikel 47 wordt als volgt gewijzigd:

1. Aan het slot van het opschrift wordt toegevoegd "en -beheer".

2. Het eerste lid komt te luiden:

1. Een verstorings-risicoanalyse omvat het inventariseren en analyseren van de voor het leveringsgebied van een drinkwaterbedrijf bestaande en te verwachten dreigingen voor de openbare drinkwatervoorziening. Van de verstorings-risicoanalyse maken in elk geval deel uit:
a. de risicobeoordeling, bedoeld in artikel 14 van de Wet weerbaarheid kritieke entiteiten;
b. de benadering die alle gevaren omvat, bedoeld in artikel 21, derde lid, van de Cyberbeveiligingswet;
c. nationale dreigingen en scenario's als bedoeld in het tweede lid.
De verstorings-risicoanalyse wordt met het oog op goedkeuring van het leveringsplan, bedoeld in artikel 37, derde lid, van de wet, voorafgaand aan de indiening van het leveringsplan aan de inspecteur ter beoordeling voorgelegd.

3. In het vijfde lid vervalt de zinsnede "overeenkomstig de vereisten, opgenomen in bijlage B, onderdeel 3, behorende bij dit besluit,".

4. Er worden twee nieuwe leden toegevoegd, luidende:

6. In de verstoringsparagraaf worden in elk geval opgenomen:
a. de maatregelen, bedoeld in artikel 15 van de Wet weerbaarheid kritieke entiteiten;
b. de maatregelen, bedoeld in artikel 21 van de Cyberbeveiligingswet;
c. maatregelen in verband met de dreigingen en scenario's, bedoeld in het tweede lid.

7. De vereisten, opgenomen in bijlage B, onderdeel 3, behorende bij dit besluit, zijn van toepassing op de verstoringsparagraaf.

D

Na artikel 47 wordt een artikel ingevoegd, luidende:

Artikel 47a. Geïntegreerde aanpak risicoanalyse en risicobeheer

Met het oog op een doelmatige uitvoering kunnen:

a. de risicobeoordeling van het watervoorzieningssysteem, bedoeld in artikel 46a, en de verstoringsrisicoanalyse, bedoeld in artikel 47, geïntegreerd worden voorbereid en uitgevoerd;
b. de paragraaf risicobeheer watervoorzieningssysteem, bedoeld in artikel 46a, en de verstoringsparagraaf, bedoeld in artikel 47, geïntegreerd worden voorbereid en opgenomen in het leveringsplan, bedoeld in artikel 53, en geïntegreerd worden uitgevoerd.

Artikel 35 (intrekking Besluit beveiliging netwerk- en informatiesystemen)

Het Besluit beveiliging netwerk- en informatiesystemen wordt ingetrokken.

Artikel 36 (inwerkingtreding)

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 37 (citeertitel)

Dit besluit wordt aangehaald als: Cyberbeveiligingsbesluit.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Minister van Justitie en Veiligheid,