WIJ WILLEM ALEXANDER,
BIJ DE GRATIE GODS,
KONING DER NEDERLANDEN,
PRINS VAN ORANJE-NASSAU,
ENZ. ENZ. ENZ.

Besluit van

tot wijziging van het Besluit beveiliging netwerk- en informatiesystemen (aanwijzing vitale aanbieders en nadere regels over beveiliging aanbieders van een essentiële dienst)

Op de voordracht van Onze Minister van Justitie en Veiligheid van 29 september 2020, directie Wetgeving en Juridische Zaken, nr. 3040835, gedaan in overeenstemming met Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Klimaat en Infrastructuur en Waterstaat;

Gelet op de artikelen 5, eerste lid, en 9 van de Wet beveiliging netwerk- en informatiesystemen;

De Afdeling advisering van de Raad van State gehoord (advies van … , nummer W…)

Gezien het nader rapport van Onze Minister van Justitie en Veiligheid van … ,
nr. …, directie Wetgeving en Juridische Zaknen, uitgebracht in overeenstemming met Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Klimaat en Infrastructuur en Waterstaat;

Hebben goedgevonden en verstaan:

Artikel I

Het Besluit beveiliging netwerk- en informatiesystemen wordt als volgt gewijzigd:

A

De tabel in artikel 2 wordt als volgt gewijzig

1. De tekst bij de sectoren **Energie: elektriciteit** en **Energie: gas** komt te luiden:

Energie: elektriciteit	De netbeheerder van het landelijk hoogspanningsnet, aangewezen op grond van artikel 10, tweede lid, of 14 van de Elektriciteitswet 1998	Transmissie en distributie van elektriciteit
	De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998	
	BritNed Development Ltd.	Transmissie van elektriciteit (landsgrensoverschrijdend)
	Een elektriciteitsbedrijf als bedoeld in Bijlage II van de NIB-richtlijn, dat één of meerdere productie-installaties als bedoeld in artikel 1, eerste lid, onder ah, van de Elektriciteitswet 1998, beheert met een cumulatief nominaal vermogen van ten minste 100 MegaWatt	Productie van elektriciteit
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen elektriciteitsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering of aankoop van elektriciteit
Energie: gas	De netbeheerder van het landelijk gastransportnet, aangewezen op grond van artikel 2, eerste lid, of 5 van de Gaswet	Transmissie en distributie van gas
	De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet	
	De Nederlandse Aardolie Maatschappij B.V.	Het opsporen en winnen van gas op basis van de concessie voor de aardgaswinning uit het Groningenveld op grond van het koninklijk besluit van 30 mei 1963, nr. 39 (Stcrt. 1963, 126) Het opslaan van gas op basis van de opslagvergunning 'Norg' van 31 maart 2003 (Stcrt. 2003, 68)
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen leveringsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering van gas
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen opslagsysteembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Opslag van gas
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen LNG-systeembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Het vloeibaar maken van aardgas of de invoer, de verlading en de hervergassing van LNG
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aardgasbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Productie of aankoop van aardgas, met inbegrip van LNG

	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van voorzieningen voor de raffinage en behandeling van aardgas, als bedoeld in Bijlage II van de NIB-richtlijn	Raffinage of behandeling van aardgas

2. In de sector **Energie: aardolie** wordt ingevoegd:

Energie: aardolie	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van oliepijpleidingen, als bedoeld in Bijlage II van de NIB-richtlijn	Beheer van oliepijpleidingen
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van voorzieningen voor de productie, opslag, transport, raffinage en behandeling van olie, bedoeld in Bijlage II van de NIB-richtlijn	Productie, opslag, transport, raffinage, of behandeling van olie

3. De tekst bij de sector **Digitale infrastructuur** komt te luiden:

Digitale infrastructuur	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van internetknooppunten, bedoeld in bijlage II van de NIB-richtlijn	Het faciliteren van het internet- en dataverkeer
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van registers voor topleveldomeinnamen, als bedoeld in bijlage II van de NIB-richtlijn	Het beheren en registreren van domeinnamen onder een topleveldomein
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van DNS-dienstverleners, als bedoeld in bijlage II van de NIB-richtlijn	Het verlenen van DNS-diensten

4. De tekst bij de sector **Vervoer** komt te luiden:

Vervoer: luchtvervoer	• Royal Schiphol Group N.V. • Luchtverkeersleiding Nederland • Maastricht Upper Area Control Centre (MUAC) • Aircraft Fuel Supply B.V. • Koninklijke marechaussee • elke luchtvaartmaatschappij met minimaal 25% van het totaal aantal vliegbewegingen op Schiphol in een kalenderjaar	Een veilige en vlotte vlucht- en vliegtuigafhandeling voor wat betreft de luchthaven Schiphol
Vervoer: spoorvervoer	De bij besluit van Onze Minister van Infrastructuur en Waterstaat aangewezen	Het beheer van de hoofdspoorweginfrastructuur, bedoeld in artikel 16 van de Spoorwegwet

	infrastructuurbeheerders, bedoeld in artikel 3 van richtlijn 2012/34/EU	
	De bij besluit van Onze Minister van Infrastructuur en Waterstaat aangewezen spoorwegondernemingen, bedoeld in artikel 3 van richtlijn 2012/34/EU	Het vervoer van personen of goederen over (hoofd)spoorweginfrastructuur
Vervoer: vervoer over water	De Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.	Het afwikkelen van scheepvaartverkeer
Vervoer: wegvervoer	De bij besluit van Onze Minister van Infrastructuur en Waterstaat aangewezen wegenautoriteiten, bedoeld in artikel 2 van verordening (EU) 2015/962	Het beheer van weginfrastructuur
	De bij besluit van Onze Minister van Infrastructuur en Waterstaat aangewezen exploitanten van intelligente vervoerssystemen, bedoeld in artikel 4 van richtlijn 2010/40/EU	Het exploiteren van een intelligent vervoerssysteem als bedoeld in artikel 4 van richtlijn 2010/40/EU

B

Onderaan de tabel in artikel 3 wordt toegevoegd:

Digitale overheid	De Kamer van Koophandel, bedoeld in artikel 2 van de Wet op de Kamer van Koophandel	Het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 2007
	Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties	• De centrale voorzieningen, bedoeld in artikel 1.9, derde lid, van de Wet basisregistratie personen • De voorziening voor uitgifte of activatie van elektronische authenticatiemiddelen en voor elektronische authenticatie die bereikbaar is via het webadres www.digid.nl
	De aanbieder van een digitale overheidsvoorziening als bedoeld in de derde kolom	Een digitale overheidsvoorziening, aangewezen bij besluit van Onze Minister die het aangaat

C

Na artikel 3 wordt een artikel ingevoegd, luidende:

Artikel 3a (beveiliging aanbieders van een essentiële dienst)
1. Ter uitvoering van de artikelen 7 en 8 van de wet neemt een aanbieder van een essentiële dienst ten minste de maatregelen, beschreven in de bijlage bij dit besluit.
2. Bij regeling van Onze Minister die het aangaat, na overleg met Onze Minister, kunnen nadere regels worden gesteld over de te nemen maatregelen.

D

In artikel 4 wordt na "De artikelen 7, 8, 9, 26 en 27 van de wet" ingevoegd ", artikel 3a van dit besluit en de bijlage bij dit besluit".

E

Aan het Besluit beveiliging netwerk- en informatiesystemen wordt de bijlage, opgenomen in de bijlage bij dit besluit, toegevoegd.

Artikel II

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

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,

Bijlage bij artikel I, onderdeel C, van het Besluit tot wijziging van het Besluit beveiliging netwerk- en informatiesystemen (aanwijzing vitale aanbieders en nadere regels over beveiliging aanbieders van een essentiële dienst)

Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen

BEVEILIGING AANBIEDERS VAN EEN ESSENTIELE DIENST

Ter uitvoering van de artikelen 7 en 8 van de wet neemt de aanbieder van een essentiële dienst (hierna: de aanbieder) ten minste de in deze bijlage beschreven maatregelen. De maatregelen worden door de aanbieder periodiek geëvalueerd en bijgesteld.

1. Risicogebaseerde aanpak

De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen. De aanbieder stelt een risicoanalyse op waarin hij de risico's met betrekking tot de beveiliging beschrijft en ingaat op de wijze waarop hij de risico's naar een passend niveau verkleint. Hij motiveert daarbij waarom dit niveau volgens hem proportioneel en aanvaardbaar is. In die motivering gaat hij in ieder geval in op de organisatiespecifieke en sectorspecifieke risico's, het maatschappelijke belang van zijn essentiële dienst en de stand van de techniek. Hij legt de resultaten van de risicoanalyse schriftelijk vast en verwerkt de resultaten in beveiligings- en beheersmaatregelen.

2. Organisatie van netwerk- en informatiebeveiligingsbeheer

De aanbieder heeft een informatiebeveiligingsbeleid en -strategie en past deze actief toe. Hij heeft de taken, bevoegdheden en verantwoordelijkheden voor de beveiliging en beheer van zijn netwerk- en informatiesystemen in de organisatie belegd.

3. Incidenten voorkomen

De aanbieder heeft een gelaagde beveiligingsstrategie die is gebaseerd op de risico's die volgen uit de risicoanalyse. *Defense in depth*, lifecycle-, asset-, patch-, identificatie- en toegangsmanagement vormen in ieder geval onderdeel van deze strategie. Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau. De aanbieder legt de bevindingen van zijn beoordeling schriftelijk vast.

4. Detectie en respons

De aanbieder heeft de beveiliging van zijn netwerk- en informatiesystemen zodanig ingericht dat hij daarmee incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zo veel mogelijk kan beperken. Hij monitort netwerk- en informatiesystemen structureel op kwetsbaarheden en mogelijke compromittatie en houdt hierbij rekening met de beschikbare dreigingsinformatie. Hij verzorgt het loggen van de handelingen op de netwerk- en informatiesystemen en bewaart deze gegevens lang genoeg om incidenten te kunnen analyseren. Hij hanteert procedures omtrent het optreden bij incidenten.

5. Gevolgen van incidenten beperken

De aanbieder stelt een bedrijfscontinuïteitsbeleid en crisismanagementbeleid op voor de netwerk- en informatiesystemen. Het crisismanagementbeleid bestaat in ieder geval uit een plan om de essentiële dienst zo spoedig mogelijk te herstellen na een incident. Het crisismanagementbeleid wordt daartoe periodiek in de praktijk beoefend.

NOTA VAN TOELICHTING

1. Algemeen

Deze eerste wijziging van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) strekt tot aanvulling van de aanwijzing van *aanbieders van een essentiële dienst* (AED's) als bedoeld in de zogenoemde NIB-richtlijn van de Europese Unie[1] en de Wet beveiliging netwerk- en informatiesystemen (Wbni) en van de aanwijzing van *andere vitale aanbieders* als bedoeld in artikel 5, eerste lid, onder b, Wbni.

Ook stelt dit besluit nadere regels over de maatregelen die AED's moeten nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen (artikel 7 Wbni) en om ernstige ICT-incidenten te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken (artikel 8 Wbni). Daartoe voegt dit besluit aan het Bbni een bijlage toe waarin de maatregelen zijn beschreven die een AED ten minste moet nemen.

De NIB-richtlijn is volledig geïmplementeerd in de Wbni en het Bbni zoals zij in werking zijn getreden op 9 november 2018 en 1 januari 2019. Dit wijzigingsbesluit geeft met de wijziging van artikel 2 Bbni uitvoering aan artikel 5, vijfde lid, NIB-richtlijn, dat de lidstaten opdraagt om de lijst van aangewezen AED's in voorkomend geval ("where appropriate") te actualiseren. Indirect strekt ook het nieuwe artikel 3a ter uitvoering van de NIB-richtlijn, namelijk als nadere invulling van de open normen over beveiliging in de artikelen 7 en 8 Wbni. De wijziging van artikel 3 Bbni (aanwijzing van *andere vitale aanbieders*) staat los van de NIB-richtlijn.

2. Consultatie

2.1 Adviescollege toetsing regeldruk

Bij brief van 12 februari 2020 is het Adviescollege toetsing regeldruk gevraagd het ontwerpbesluit te toetsen op regeldruk. Het college is positief over de onderbouwing van het nut en de noodzaak van deze wijziging van het Bbni en de regeldrukgevolgen. Het college ziet, binnen het licht van de gewenste beveiliging van essentiële diensten, geen minder belastende alternatieven. Over de werkbaarheid merkt het college het volgende op. De aangewezen AED's moeten voldoen aan de beveiligingseisen uit het Bbni. Deze eisen vloeien voort uit de wettelijke zorgplicht die een essentiële dienst heeft voor veilige netwerk- en informatiesystemen. De toelichting vermeldt dat is gekozen voor een invulling die de benodigde ruimte laat aan de AED en de toezichthouder om tot een voor de sector passende invulling te komen. Ook is er zo veel mogelijk ruimte om aan te sluiten bij bestaande en eventuele nieuwe normenkaders. De toelichting geeft tevens aan dat de regeldruk deels afhangt van de uitleg die de bevoegde autoriteit de komende jaren zal geven aan de concrete invulling van de beveiligingseisen. Het college geeft in overweging om de bevoegde autoriteiten te verzoeken om, in goed overleg met de sectoren, spoedig met een nadere invulling van de beveiligingseisen te komen, zodat de uitvoerders weten wat van hen concreet wordt verwacht.

Hierover merk ik op dat de AED's zelf primair verantwoordelijk zijn voor het binnen genoemde wettelijke kaders voldoen aan de zorgplicht door het treffen van concrete maatregelen. De AED's zullen daarover steeds in contact staan met de toezichthouder. Daar waar nodig wordt geacht, kan de minister die het aangaat besluiten om de zorgplicht voor een of meerdere sectoren in een ministeriële regeling nog verder in te vullen (zie artikel 3a, tweede lid).

2.2 Openbare consultatie

Op een eerdere versie van dit wijzigingsbesluit zijn reacties ingewonnen door middel van een openbare consultatie op www.internetconsultatie.nl. Elke reactie is openbaar. De reacties zijn afkomstig van Puur Water & Natuur (PWN), Centraal Orgaan Voorraadvorming Aardolieproducten,

[1] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).

Vereniging van waterbedrijven in Nederland (Vewin), Uniper, Nederlandse Spoorwegen, Stek advocaten, RWE, Energie Nederland, Netbeheer Nederland en twee particulieren.

Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA)

COVA geeft aan moeite te hebben met de reikwijdte van de Wbni en het Bbni naar AED's toe en met de volgorde waarin onderdelen van een vitale sector aangewezen worden. Volgens COVA moeten primair de reguliere bedrijven (zoals olieopslagbedrijven) in een vitale sector AED zijn of als AED worden aangewezen en secundair de crisisorganisatie (zoals COVA).

Gegeven de wettelijke taak van COVA en het belang van de stabiliteit van de olievoorziening van de Nederlandse samenleving is COVA aangewezen als AED. Het beheer door leveranciers en de fysieke opslaglocaties zijn daar onderdeel van. De AED is verantwoordelijk voor de levering van de essentiële dienst. Juist bij afhankelijkheid van het operationeel zijn van opslagfaciliteiten, is het leveranciersmanagement door de AED, als onderdeel van de Wbni zorgplicht, van groot belang. Na deze wijziging van het Bbni zal de minister van EZK, met daarbij ook specifieke aandacht voor dit punt van COVA, nagaan of er nog andere organisaties in de energiesector zijn die in aanmerking komen voor een aanwijzing als AED.

Vewin

Vewin heeft in de consultatie gereageerd op het concept van het wijzigingsbesluit namens de 10 drinkwaterbedrijven. Vewin geeft aan dat de drinkwatersector in 2018, ter invulling van de zorgplicht uit de Wbni, een risico-gebaseerd normenkader voor de beveiliging van de procesautomatisering heeft opgesteld (PA-beveiligingsnorm). De procesautomatisering wordt gebruikt voor de bediening, bewaking en aansturing van de gehele drinkwatervoorziening. Met dit normenkader, tezamen met het wettelijk verplichte leveringsplan waarin alle huidige en toekomstige gevaren en dreigingen worden geanalyseerd en voorzien van maatregelen, is de drinkwatersector van mening dat zij invulling kan geven aan de beheersdoelstellingen zoals opgenomen in het ontwerpbesluit tot wijziging van het Bbni.

Vewin benadrukt het belang dat vanuit het Rijk doelvoorschriften worden voorgeschreven. De invulling ervan in termen van concrete maatregelen is volgens Vewin primair een verantwoordelijkheid van de drinkwaterbedrijven zelf, onder meer afhankelijk van het eigen risicoprofiel en de type netwerk- en informatiesystemen.

In opdracht van IenW heeft TNO in 2019 een expertbeoordeling van de PA-beveiligingsnorm voor drinkwater verricht. De conclusie van TNO is dat de norm een stevige basis heeft, externe audits mogelijk maakt en aanzienlijke inspanningen vergt om eraan te voldoen. IenW beraadt zich - naar aanleiding van de adviezen van de ILT en het ATR - erop om ingevolge het voorgestelde artikel 3a, tweede lid, nadere regels in een ministeriele regeling voor de sectoren drinkwater, luchtvaart en maritiem op te nemen. In deze ministeriele regeling kan eventueel worden verwezen naar niet-publiekrechtelijke sectorspecifieke normen, zoals de PA-beveiligingsnorm voor drinkwater. Sectorspecifieke normen vormen geen algemeen verbindend voorschrift, maar zijn facultatieve (niet dwingende) richtinggevende uitvoeringsnormen.

Uniper

Uniper wijst er, kort samengevat, op dat de voorgestelde formulering voor de aanwijzing van elektriciteitsproducenten in strijd is met de NIB-richtlijn, omdat volgens die richtlijn enkel elektriciteitsleveranciers en niet elektriciteitsproducenten als AED aangewezen kunnen worden. Door in de toelichting te stellen dat het gaat om producenten die tevens aan het elektriciteitsnet leveren, worden de rollen van 'producent' en 'leverancier' vereenzelvigd. Hiermee wordt volgens Uniper miskend dat dit binnen Nederlandse en Europese wetgeving twee apart gereguleerde rollen zijn.

Ik ben het met Uniper eens dat, door de combinatie van verschillende definities, met de voorgestelde formulering onduidelijkheid kan bestaan of de aanwijzing in lijn is met artikel 4 en 5, eerste lid, en bijlage II van de NIB-richtlijn. Om onduidelijkheid hierover weg te nemen heb ik de tabel in artikel I, onderdeel A, aangepast, zodat de formulering van de aanwijzing duidelijker aansluit op de formulering van bovenbedoelde beschrijving in de NIB-richtlijn. De materiële

reikwijdte van de aanwijzing blijft verder gelijk. Ook heb ik de artikelsgewijze toelichting bij artikel I, onderdeel A, subonderdelen 1 tot en met 3 aangepast om dit punt te verhelderen.

Uniper geeft verder aan dat het wijzigingsvoorstel tal van open normen ("aanvaardbaar", "proportioneel", "relevant", "adequaat", "passend" etc.) bevat die onduidelijk laten welke maatregelen precies verwacht worden van de AED's. De onzekerheid hierover, in combinatie met de boetes op het overtreden van open normen, leidt tot extra regeldruk (bovenop de mogelijk reeds aanzienlijke kosten) daar partijen druk ervaren om 'het zekere voor het onzekere te nemen'.

In verband met deze reactie heb ik de bijlage bij artikel I, onderdeel C, aangepast door de normstelling te concretiseren. Ook heb ik de bijbehorende artikelsgewijze toelichting aangepast. Naar mijn mening zijn de in de bijlage opgenomen maatregelen daarmee voldoende concreet geworden.

Nederlandse Spoorwegen

NS onderschrijft de voorgenomen wijziging die het mogelijk maakt dat ProRail als beheerder van de hoofdspoorweginfrastructuur en spoorwegondernemingen zoals NS, door de minister van IenW aangewezen zullen gaan worden als AED.

NS geeft aan dat de tekst bij de sector vervoer in de tabel in artikel 2 van het Bbni wordt gewijzigd. In de meest rechtse kolom worden de activiteiten van spoorwegondernemingen omschreven als *Het vervoer van personen of goederen*. De NS stelt voor om deze formulering nader te preciseren naar *Het vervoer van personen of goederen over hoofdspoorweginfrastructuur als bedoeld in artikel 1 Spoorwegwet*, zodat naar haar mening duidelijk wordt dat het om spoorvervoer gaat over het door ProRail beheerde landelijke netwerk en niet om bijvoorbeeld tram- of metrovervoer. Ook stelt de NS voor om in de toelichting op te nemen dat deze omschrijving ziet op het primaire spoorvervoerproces over de hoofdspoorweginfrastructuur en niet op aanpalende activiteiten, zoals ticketverkoop en het verstrekken van reizigersinformatie.

Naar aanleiding van deze reactie heb ik de desbetreffende tekst aangepast naar: "Het vervoer van personen en goederen over (hoofd)spoorweginfrastructuur". De verwijzing naar de Spoorwegwet acht ik niet nodig, omdat het onderscheid met tram en metro reeds wordt gemaakt met het begrip "spoorweg". Het voorstel van de NS over de uitbreiding van de toelichting neem ik niet over. IT-gerelateerde activiteiten die noodzakelijk zijn voor het functioneren van het vervoer van personen of het spoor, zoals ticketverkoop en het verstrekken van reizigersinformatie, zijn namelijk wel degelijk onderdeel van de te borgen cybersecurity van het spoor.

De NS wijst er op dat de nota van toelichting niet ingaat op de regeldruk voor de instanties vermeld onder artikel I, onderdeel A, onder 4. De NS stelt voor om in de toelichting ook in te gaan op de operationele, financiële en juridische gevolgen indien de minister van IenW gebruik zal maken van de hierin opgenomen bevoegdheid om AED's aan te wijzen binnen de deelsectoren spoor- en wegvervoer.

Omdat de reikwijdte van een dergelijke aanwijzing van AED's nog niet is bepaald, is het nog niet mogelijk om in te gaan op de operationele, financiële en juridische gevolgen van een eventuele aanwijzing. Dit wordt pas vastgelegd middels een ministerieel besluit van de minister van IenW. Bij de voorbereiding hiervan zal NS, als concessiehouder voor het hoofdrailnet, nadrukkelijk betrokken worden.

Stek advocaten

Volgens Stek advocaten is de aanwijzing van "elektriciteitsproducenten" als AED te rechtsonzeker. Kort samengevat meent Stek advocaten dat door het hanteren van brede definities en begrippen er discussie kan ontstaan over de vraag of een bedrijf elektriciteitsproducent is in de zin van het Bbni. Stek advocaten pleit voor een verduidelijking in de toelichting en wijst op het alternatief om de specifieke elektriciteitsproducenten in het Bbni aan te wijzen.

Allereerst merk ik op dat de inhoud van deze wijziging van het Bbni in de voorbereidingsfase in meerdere sessies met onder meer de aan te wijzen elektriciteitsproducenten is besproken. In deze voorbereidingsfase is de optie om hen individueel aan te wijzen overwogen, maar hier is niet voor gekozen. De afgelopen jaren zijn diverse transacties geweest waarbij grootschalige productie-

installaties van eigenaar gewisseld zijn. De verwachting is dat dit ook in de toekomst zal blijven gebeuren. Tevens zijn nieuwe 'kleinschalige' productie-installaties in opkomst (zonneparken, windparken), die ertoe kunnen leiden dat nieuwe partijen boven de gestelde drempel uit komen.

Individuele elektriciteitsproducenten die aan de criteria voldoen moeten ook bij 'afwijkende' (juridische) constructies qua samenwerking, zeggenschap en eigendom aangesproken kunnen worden op hun zorg- en meldplicht. Door de aanwijzing verder te specificeren ontstaat het risico dat partijen hun zorg- en meldplicht kunnen ontwijken, wat op gespannen voet staat met het principe van een level-playing-field in de markt.

Ik ben het met Stek advocaten eens dat de toelichting tot onduidelijkheid kan leiden over de kwalificatie van een bedrijf als elektriciteitsproducent in de zin van het Bbni. Om deze onduidelijkheid weg te nemen heb ik de toelichting aangepast.

Daarnaast meent Stek advocaten dat het gebrek aan concrete maatregelen c.q. voorschriften in de bijlage bij het nieuwe artikel 3a van het Bbni zich slecht verdraagt met de toezichts- en handhavingsinstrumenten (en de toepassing daarvan) uit de Wbni. Volgens Stek advocaten staat deze systematiek op gespannen voet met het rechtszekerheidsbeginsel en het legaliteitsbeginsel. Stek advocaten stelt daarom voor om – in het kader van de rechtszekerheid en legaliteit – gebruik te maken van de in het voorgestelde artikel 3a, tweede lid, van het Bbni opgenomen mogelijkheid om bij ministeriële regeling nadere sectorspecifieke maatregelen voor te schrijven.

In verband met deze reactie heb ik de bijlage bij artikel I, onderdeel C, aangepast door de normstelling te concretiseren. Ook heb ik de bijbehorende artikelsgewijze toelichting aangepast. Naar mijn mening zijn de in de bijlage opgenomen maatregelen na de aanpassingen voldoende concreet geworden.

Over de mogelijkheid om bij ministeriële regeling sectorspecifieke maatregelen voor te schrijven merk ik het volgende op. De afweging of een ministeriële regeling onder artikel 3a Bbni noodzakelijk is, is onder meer afhankelijk van het risicoprofiel van de beveiliging van netwerk- en informatiesystemen, het type en niveau van regulering, de behoefte aan rechtszekerheid, geanticipeerd nalevingsgedrag en beoordeling van de handhaafbaarheid, uitvoerbaarheid en fraudebestendigheid. Voor elke sector zal daarom een aparte afweging gemaakt worden.

Energie-Nederland

Volgens Energie-Nederland is de gekozen drempel van 100 MW een pragmatische keuze die resulteert in een zoveel mogelijk gelijk speelveld voor producenten.

Regeldrukkosten

Energie Nederland merkt op dat ten aanzien van de regeldrukkosten zowel de gehanteerde tijdsbesteding als het tarief te laag zijn ingeschat. De eenmalige en structurele kosten komen niet overeen met de inschatting van de regeldruk van de individuele producenten. Volgens Energie Nederland zijn de kosten ook sterk afhankelijk van de interpretatie van de maatregelen, die tal van open normen bevatten. Energie-Nederland stelt voor om bij de implementatie evaluatiemomenten op te nemen, met name om potentieel onredelijke eisen en ruimte voor compensatie te identificeren.

De kosten voor de meldplicht zijn mede ingeschat op basis van de gevoerde gesprekken met elektriciteitsproducenten en het aantal meldingen door netbeheerders in het afgelopen jaar. Tot nu toe is het aantal meldingen van netbeheerders in de elektriciteitssector beperkt geweest. Ik acht de inschatting van de regeldrukkosten van de meldplicht op basis van deze informatie realistisch.

De regeldrukkosten die samenhangen met de zorgplicht (beveiligingseisen) zijn omvangrijker. Ten aanzien van het tarief is, in lijn met het 'Handboek Meting Regeldrukkosten' (2018), gebruik gemaakt van het standaard uurtarief voor een 'hoogopgeleide expert', wat bij de introductie van de Wbni al verhoogd is naar € 60,-. Uit additionele informatie die Energie Nederland heeft aangeleverd blijkt dat, zeker bij de inzet van externe experts, eerder gedacht moet worden aan een uurtarief van € 100,- tot € 150,-. Hierop is paragraaf 3a, onderdeel B, aangepast.

Voor wat betreft de eenmalige en structurele kosten (tijdsbesteding) van de zorgplicht is gesproken met vrijwel alle individuele elektriciteitsproducenten die onder de aanwijzing zullen vallen. Deze

gesprekken tonen aan dat grote verschillen bestaan tussen de verschillende elektriciteitsproducenten. De gepresenteerde monetaire waarde betreft de cumulatie van al deze individuele inschattingen en geeft dus in beginsel een robuuste schatting.

Verduidelijking meldplicht en op te volgen acties

Energie-Nederland vindt dat er duidelijkheid moet komen over wanneer producenten een melding moeten maken van een ICT-incident en welke acties na de melding verwacht kunnen worden op aanwijzing van de toezichthouder.

De meldplicht voor AED's bij het NCSC en de toezichthouder geldt voor incidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening. Voor inbreuken met potentieel aanzienlijke gevolgen geldt de meldplicht bij het NCSC. Organisaties die onder de Wbni als AED zijn aangewezen hebben deze plicht. Het vakdepartement stelt, met inachtneming van de onderscheidenlijke wettelijke taken, in overeenstemming met de NCTV een indicatieve drempelwaarde voor de meldplicht vast na overleg met de AED en toezichthouder. Deze drempelwaarde is de richtlijn voor wanneer er gemeld moet worden. De minister van EZK zal hierover in individuele brieven aan elektriciteitsproducenten over de aanwijzing als AED verduidelijken wanneer gemeld dient te worden.

Internationale afstemming

Energie Nederland wijst erop dat veel elektriciteitsproducenten onderdeel zijn van internationaal opererende bedrijven en dat de elektriciteitsmarkt een grensoverschrijdend karakter heeft. Energie Nederland onderstreept dat in de implementatiefase hier aandacht voor moet zijn, met name ten aanzien van de invulling van het toezicht, de praktische invulling bij (grensoverschrijdende) dreigingen en het delen van informatie hierover buiten Nederland.

Hierover merk ik op dat de lidstaten op Europees niveau samenwerken in de NIS Cooperation Group. Hierin worden zaken besproken rondom de implementatie van wetgeving, partijen die aangewezen worden en hoe toezicht wordt gehouden. De toezichthouder zal bij het toezicht aandacht besteden aan het feit dat een aantal producenten in meerdere Europese landen onder toezicht staan.

Maatschappelijk belang

Energie Nederland geeft aan dat producenten bij de invulling van de Wbni ook rekening moeten houden met het maatschappelijk belang. Volgens Energie Nederland is de vraag of energieproducenten de afweging kunnen maken gelet op hun commerciële rol. In vergelijking met netbeheerders is de rol van de producent in relatie tot de maatschappelijke weerbaarheid een andere. Uitval van een enkele centrale resulteert niet in maatschappelijke ontwrichting, aldus Energie Nederland.

In reactie hierop merk ik op dat elektriciteitsproducenten in gezamenlijkheid een onmisbare rol spelen in de borging van elektriciteitsvoorziening van Nederland. De gelijktijdige uitval van meerdere productie-installaties kan leiden tot maatschappelijke ontwrichting. Hierbij speelt tevens mee dat in het geval van een grote calamiteit de balanshandhaving van het elektriciteitsnet ook afhankelijk is van soortgelijke productie-installaties. Zeker bij cybersecurity bestaat het risico dat een kwetsbaarheid meerdere productie-installaties tegelijk treft en daarmee ook een deel van de 'oplossing' wegvalt. Als een substantieel aandeel aan elektriciteitsproductie dan uitvalt, kan dit ertoe leiden dat de balans op het elektriciteitsnet niet meer gewaarborgd kan worden. Elektriciteitsproducenten hebben dus een rol in het voorkomen en/of beperken van maatschappelijke ontwrichting. Om deze reden dienen producenten het maatschappelijk belang mee te wegen in hun risicoanalyses. Bij deze analyses kunnen zij rekening houden met reeds bestaande beschermings- en beveiligingsmaatregelen in het systeem die een uitval van een productie-installatie kunnen opvangen. Dit laat onverlet dat zij ook oog dienen te hebben voor de afhankelijkheid van de verschillende netbeheerders in de energieketen, juist van de productie-installaties die zowel een probleem als de oplossing voor de balanshandhaving kunnen zijn. Dit is ter verduidelijking nog aan de toelichting op deze wijziging van het Bbni toegevoegd.

RWE

Volgens RWE zullen de regeldrukkosten van de Wbni erg hoog zijn en moet een compensatieregeling worden opgezet. Ook geeft RWE aan dat de kosten/regeldruk in belangrijke mate afhankelijk zijn van de uitleg van het besluit en de daarin gebruikte begrippen, die vrijwel zonder uitzondering bestaan uit open normen. RWE geeft verder aan moeite te hebben met het gebruik van open normen, waarvan de uitleg in grote mate afhankelijk is van de toezichthouder. Zij benoemt aan de hand van een voorbeeld dat de toezichthouder de meldplicht oprekt en daarmee buiten de reikwijdte van de Wbni en NIB-richtlijn acteert. Volgens RWE leidt dit tot meer rechtsonzekerheid, verplichtingen en kosten aan de zijde van de energieproducenten.

In verband met deze reactie van RWE over open normen heb ik de bijlage bij artikel I, onderdeel C, aangepast door de normstelling te concretiseren. Ook heb ik de bijbehorende artikelsgewijze toelichting aangepast. Naar mijn mening zijn de in de bijlage opgenomen maatregelen daarmee voldoende concreet geworden.

Elektriciteitsproducenten zijn in staat om de regeldrukkosten te dragen zonder dat dit nadelig hoeft te zijn voor hun individuele concurrentiepositie. Ik ben niet voornemens om deze kosten te compenseren. Met de gekozen drempel van 100 MW is geborgd dat gelijkwaardige partijen met dezelfde verplichte beveiligingsmaatregelen te maken hebben en dat op deze wijze het level playing field in stand blijft. Verder hebben individuele bedrijven ook een belang bij een niveau van cybersecurity dat goed op orde is. Gegeven de risico's en dreigingen die er zijn, zoals onder andere ook verwoord in het Cybersecuritybeeld Nederland (CSBN 2019), zijn stevige maatregelen met het oog op het verhogen van de digitale weerbaarheid gerechtvaardigd.

Netbeheer Nederland

De vereniging Netbeheer Nederland heeft in de consultatie gereageerd namens alle energienetbeheerders in Nederland.

Rolverdeling

Netbeheer Nederland wijst op de *checks and balances*, met de ministeries van JenV en EZK als wetgever, het Agentschap Telecom als toezichthouder, het NCSC als kennisinstituut en CERT en organisaties (waaronder netbeheerders) als uitvoerende organisaties. Volgens Netbeheer Nederland zijn deze *checks and balances* thans goed. Netbeheer Nederland geeft aan dat het NCSC volgens het Bbni toezichthoudende taken krijgt en vraagt zich af of dit verstandig is vanuit het oogpunt van *checks and balances*.

Hierover merk ik op dat deze wijziging er niet toe strekt voor het NCSC toezichthoudende taken in het leven te roepen. Ook krachtens de huidige wetgeving (Wbni, Bbni) heeft het NCSC ten aanzien van vitale aanbieders niet al dergelijke taken. In deze wetgeving is ook nadrukkelijk onderscheid gemaakt tussen de verschillende rollen en taken van het NCSC en de toezichthouders. De minister van Justitie en Veiligheid (in de praktijk het NCSC) is krachtens artikel 3 van de Wbni belast met het verlenen van bijstand aan vitale aanbieders (waaronder ook de AED's) en rijksoverheidsorganisaties (informeren, adviseren over dreigingen, etc.). Daarnaast is het NCSC ook het centrale contactpunt als bedoeld in de NIB-richtlijn. Met het toezicht op en handhaving van deze wetgeving zijn daarentegen de betrokken vakministers (en DNB) belast; zie artikel 4 van de Wbni.

Network Code for Cybersecurity

Netbeheer Nederland wijst er op dat op Europees niveau een Network Code for Cybersecurity in ontwikkeling is. Als de beveiligingseisen in de Netwerkcode ten minste gelijkwaardig zijn aan die van NIB-richtlijn, dan verzoekt Netbeheer Nederland om de netbeheerders uit te sluiten van de eisen in de NIB-richtlijn.

Het is momenteel te vroeg om te oordelen of de implementatie van een dergelijke Netwerkcode ertoe kan leiden dat netbeheerders worden uitgezonderd van de beveiligingseisen in de NIB-richtlijn. Dit is namelijk afhankelijk van de inhoud van de Netwerkcode. Op het moment dat de inhoud van de Netwerkcode vaststaat, zal ik samen met het vakdepartement beoordelen of de daarin opgenomen beveiligingseisen ten minste gelijkwaardig zijn aan die krachtens de Wbni, en of het gelet daarop aangewezen is om bepalingen uit de Wbni en het Bbni buiten toepassing te verklaren.

Overig

Een particulier geeft aan dat strengere beveiligingseisen voor netwerk- en informatiesystemen ook moeten gelden voor de overheid, semioverheid en bedrijven waarmee de overheid samenwerkt. Tevens moeten onderwijsinstellingen op een hoger veiligheidsniveau worden gebracht. Ook zouden er regels moeten komen voor medewerkers van instanties in het kader van cybersecurity. Deze regels moeten streng zijn, evenals het toezicht daarop. Verder moet de overheid vriendelijke hackers in dienst nemen, zodat veiligheidslekken kunnen worden blootgelegd.

Het uitgangspunt is dat alle bedrijven, overheden en organisaties in Nederland hun verantwoordelijkheid op het gebied van cybersecurity moeten nemen. Bepaalde processen en diensten daarbinnen zijn echter dusdanig vitaal voor de Nederlandse samenleving dat uitval of verstoring tot maatschappelijke ontwrichting kan leiden en daarmee een bedreiging vormt voor de nationale veiligheid, dat ze aangewezen zijn als vitale infrastructuur. Voor vitale aanbieders gelden daarom onder meer op grond van de Wbni wettelijke verplichtingen teneinde de continuïteit van hun dienstverlening zo veel mogelijk te waarborgen. In de kabinetsreactie op het WRR-rapport "Voorbereiden op digitale ontwrichting" van 20 maart 2020 is overigens aangegeven dat een wetswijzigingstraject wordt voorbereid, dat tot doel heeft om alle in de Wbni geldende verplichtingen (zorgplicht, etc.) en het toezicht op de naleving daarvan, die nu nog alleen voor AED's gelden, ook voor alle andere vitale aanbieders van toepassing te laten zijn. Voor de rijksoverheid heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een belangrijke rol als stelselverantwoordelijke voor rijksoverheids-ICT en namens hem de CIO-Rijk. Voor organisaties binnen de rijksoverheid geldt: het eigen huis moet op orde zijn. Ook voor medeoverheden, waaronder gemeenten, veiligheidsregio's, waterschappen en provincies worden nadere afspraken over de kaders voor cybersecurity gemaakt.

3. Uitvoerbaarheid en handhaafbaarheid

3.1 Agentschap Telecom (AT)

Het concept-besluit is ook voor een uitvoerings- en handhavingstoets[2] voorgelegd aan Agentschap Telecom (AT). AT acht het concept-besluit voor haar uitvoerbaar en handhaafbaar. Zij meldt dat het aansluit bij zowel de gangbare normen op het gebied van informatiebeveiliging en continuïteit als bij de toezichtpraktijk van AT, zijnde systeemtoezicht op basis van open normen. Daarnaast biedt het concept-besluit haar als toezichthouder de ruimte om aan de voorkant proactief en preventief te interveniëren.

AT vraagt zich af waarom in de toelichting niet is gemotiveerd waarom de nadere invulling van de zorgplicht alleen ziet op AED's en niet op digitaledienstverleners. De artikelen 7 en 8 van de Wbni, waar de uitwerking van de wettelijke zorgplicht in de bijlage bij het Bbni betrekking op heeft, zien immers zowel op AED's als op digitaledienstverleners.

Het klopt dat deze artikelen in de Wbni ook zien op de digitaledienstverleners. Echter, de zorgplicht voor digitale dienstverleners is nader geregeld in een Uitvoeringsverordening[3] op Europees niveau.

AT merkt op dat met betrekking tot de aanwijzing van BritNed Development Ltd. een concrete rechtspersoon (ltd.) wordt aangewezen, terwijl dat bij andere onderdelen in de tabel niet het geval is. De betreffende rechtspersoon kan echter haar naam wijzigen of haar activiteiten verplaatsen naar een andere rechtspersoon binnen het concern. Dan wordt deze aanwijzing als essentiële dienst zinledig. AT beveelt aan om ook bij de aanwijzing van BritNed Development Ltd. te kiezen voor een ruimere omschrijving.

Bij de aanwijzing van BritNed is overwogen om de rechtspersoon in algemene termen te omschrijven, in plaats van bij naam te noemen. Om volgende redenen is gekozen om BritNed bij naam te noemen. Ten eerste is er geen drempel zoals bij elektriciteitsproducenten, waardoor geen risico bestaat dat BritNed na aanwijzing als AED door wijzigingen in capaciteit niet meer onder de verplichtingen krachtens de Wbni zou hoeven te vallen. Ten tweede worden interconnectoren op grond van de Elektriciteitswet 1998 voor tien jaar aangewezen (artikel 10a). Ze zijn verplicht om

[2] Brief van Agentschap Telecom van 16 maart 2020 (kenmerk AT-EZK/7959143).

[3] Uitvoeringsverordening (EU) 2018/151 van de Commissie van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148.

gewijzigde omstandigheden te melden (artikel 10, zevende lid), waardoor ze niet van naam, eigendom of vorm kunnen veranderen zonder dit van te voren te melden. Na het melden van een dergelijke wijziging, of wanneer BritNed niet opnieuw wordt aangewezen, is er voldoende tijd om het besluit aan te passen. Daarnaast wordt opgemerkt dat BritNed niet de enige rechtspersoon is die bij naam wordt aangewezen, zie bijvoorbeeld ook Royal Schiphol Group N.V., Aircraft Fuel Supply B.V., Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.

AT merkt naar aanleiding van de passage "*De maatregelen zijn daarom zo veel mogelijk abstract beschreven in de vorm van beheersdoelstellingen."* in de inleiding van de toelichting op de bijlage bij artikel 3a, eerste lid, Bbni het volgende op. De wet (artikel 9 Wbni) biedt alleen een grondslag om nadere regels te stellen over *maatregelen* en niet over *doelstellingen.* De doelstellingen staan immers al in de wet. AT stelt voor om *in de vorm van beheersdoelstellingen* te schrappen. Ik heb de bijlage naar aanleiding van de consultatie gewijzigd en deze passage in de toelichting op de bijlage is als gevolg daarvan komen te vervallen.

3.2 Inspectie voor Leefomgeving en Transport (ILT)

Het wijzigingsvoorstel voor de Bbni is voor een handhaafbaarheids-, uitvoerbaarheids- en fraudebestendigheidstoets (HUF-toets) voorgelegd aan de ILT. De ILT concludeert dat de voorgestelde wijzigingen voor de Bbni op termijn onder voorwaarden handhaafbaar zijn.[4] Daar het normenkader voor de zorgplicht (de voorgestelde wijziging van het Bbni, een ministeriele regeling krachtens het Bbni met nadere regels en andere sectorale wetgeving) nog niet formeel zijn vastgesteld is de regelgeving volgens de ILT nog niet handhaafbaar. Ten behoeve van de handhaafbaarheid moet er een eenduidige koppeling worden gelegd tussen een AED en de sectorspecifieke regelgeving. De ILT is van mening dat een eenduidige verwijzing, per AED, noodzakelijk is om het normenkader te completeren.

De ILT geeft aan voor het toezicht en handhaving op de Wbni meer richting nodig te hebben over wanneer door AED's aan de wettelijke eisen voor de zorgplicht wordt voldaan. De conclusie dat de handhaafbaarheid pas kan worden beoordeeld, als de complete set van nieuwe regelgeving voortvloeiend uit de Wbni beschikbaar is wordt door IenW onderschreven. Ook het ATR geeft ten aanzien van het wijzigingsvoorstel voor de Bbni in overweging om de bevoegde autoriteiten te verzoeken om, in goed overleg met de sectoren, spoedig met een nadere invulling van de beveiligingseisen te komen, zodat de uitvoerders weten wat van hen concreet wordt verwacht.

De voorgestelde bepalingen in het gewijzigde Bbni zijn sectoroverstijgend, maar geven ruimte om op grond van artikel 3a, tweede lid, in een ministeriele regeling nadere regels te stellen ten aanzien van de zorgplicht. Deze nadere regels kunnen sectoroverstijgend, sectoraal of zelfs bedrijfsspecifiek zijn, afhankelijk van de kenmerken en specifieke risico's die voor de AED's gelden. Om te bepalen of een ministeriele regeling voor de AED's van IenW noodzakelijk is een inhoudelijke gap-analyse uitgevoerd. De conclusie uit deze analyse is dat de open normering in de Wbni en Bbni als sectoroverstijgend kader een goede basis biedt, maar dat het voor het IenW-domein zinvol is om nadere regels over de zorgplicht in een ministeriele regeling op te nemen.

Gezien het risicoprofiel van de beveiliging van netwerk- en informatiesystemen en het type en niveau type van regulering bij de sectoren, alsmede de behoefte aan rechtszekerheid, het geanticipeerde nalevingsgedrag en de uitkomsten van de HUF-toets beraadt de Minister van IenW zich erop om het advies voor een ministeriele regeling over te nemen. Ook ten aanzien van het advies om in deze ministeriele regeling te verwijzen naar door de sector zelf gehanteerde sectorale uitvoeringsnormen - die in het kader van zelfregulering tot stand zijn gebracht – wordt in beginsel positief gedacht. Uitgangspunt daarbij is dat een eventuele opname of verwijzing naar niet-publiekrechtelijke uitvoeringsnormen voor AED's in de ministeriele regeling niet-dwingend is en het de AED vrij staat om in plaats daarvan een ander normenkader te kiezen dat het beste aansluit bij de bedrijfsspecifieke risico's en het risicoacceptatieniveau en evenzeer past binnen de wettelijke kaders. Bovendien moeten deze facultatieve uitvoeringsnormen van dien aard zijn dat met naleving hiervan ten minste wordt voldaan aan het basisbeschermingsniveau, zoals voorgeschreven in het bij en krachtens de Wbni bepaalde, alsook actueel en openbaar zijn. In de ministeriele regeling zal worden bepaald of en in hoeverre een AED, door het naleven van de bepalingen in de Wbni, het Bbni en de ministeriele regeling, alsook de uitvoeringsnormen waarnaar in de ministeriele regeling

[4] Brief van de ILT op 31 maart 2020 (kenmerk ILT-2020/16828)

wordt verwezen aan de wettelijke beveiligingseisen wordt geacht te voldoen of dat het vermoeden ontstaat dat daaraan is voldaan.

Met betrekking tot het advies een regeling te maken die – vooruitlopend op de vaststelling van de EASA-rules – voor de Nederlandse luchtvaartsector, en in het bijzonder de KMar en AFS, de voorgestelde EASA-rules als vrijwillige sectorspecifieke norm vaststelt merk ik het volgende op. De voorwaarden zoals gesteld in de concept EASA rule, die nadere voorwaarden stelt aan de zorgplicht van luchtvaartorganisaties, zullen naar verwachting als richtlijn voor de AED's - waaronder de KMar en AFS - worden opgenomen in de ministeriele regeling. Dit betekent dat hiermee, in afwachting van de inwerkingtreding van de EASA rule, alvast de koppeling wordt gelegd met het normenkader welke ook van toepassing is op KMar en AFS. Hiermee wordt ook invulling gegeven voor de luchtvaart AED's aan de cybersecurityverplichtingen die voortvloeien uit de ICAO security regelgeving (Annex 17) die reeds van toepassing is.

4. Regeldruk

De door dit besluit veroorzaakte regeldruk bestaat uit een verantwoorde stijging van de administratieve lasten en inhoudelijke nalevingskosten.

4a. Nieuwe AED's en nieuwe andere vitale aanbieders

Artikel I, onderdeel A, onder 1,[5] wijst enkele nieuwe AED's aan, waardoor voor hen de Wbni en het Bbni gaan gelden. Het gaat met name om de verplichting om ernstige ICT-incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het Ministerie van Justitie en Veiligheid, en bij de sectorale toezichthouder (de bevoegde autoriteit, aangewezen in artikel 4, eerste lid, Wbni), zie artikel 10, eerste, tweede en derde lid, Wbni, en om de beveiligingsverplichtingen van de artikelen 7 en 8 Wbni, zoals nader uitgewerkt in de bijlage bij het nieuwe artikel 3a Bbni.

A. Meldplicht

Voor het verrichten van een melding zal het veelal gaan om handelingen als het verzamelen van informatie, het schriftelijk en eventueel telefonisch doen van een melding en het eventueel verstrekken van nadere informatie aan het NCSC of de bevoegde autoriteit. De tijd die het organisaties zal kosten om een melding en vervolghandelingen te doen onder de meldplicht zal verschillen per incident en zal onder andere afhankelijk zijn van de ernst en complexiteit van het incident. De meldplicht geldt alleen voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door de AED verleende dienst. Daarom wordt uitgegaan van grootschalige en complexe incidenten en zullen de melding en extra vervolghandelingen naar schatting gemiddeld 300 minuten per incident kosten. Hierbij wordt aangesloten bij de inschatting van 260 minuten, zoals die is vermeld in de memorie van toelichting bij de Wbni.[6] Onder de Wbni kunnen ook vervolghandelingen voor een organisatie ontstaan als gevolg van vragen of optreden van de bevoegde autoriteit naar aanleiding van de melding. Hoewel veelal vergelijkbare informatie wordt opgevraagd door het NCSC en de bevoegde autoriteit, zullen mogelijk extra handelingen verricht dienen te worden op verzoek van de bevoegde autoriteit. Hiervoor is een opslag van 15% gerekend, zodat de vereiste tijd uitkomt op 300 minuten per melding. Als uurtarief wordt € 60 gehanteerd, een gangbaar tarief voor hoogopgeleide kenniswerkers. Gezien de ervaringen met meldingen op grond van de Wbni in 2019 zal een AED waarschijnlijk niet meer dan 2 keer per jaar melden. In dat geval bedragen zijn kosten (300 minuten x 2 meldingen per jaar x € 60 =) € 3600 per jaar.

B. Beveiligingseisen

[5] Onderdelen 2, 3 en 4 wijzen geen nieuwe AED's aan, maar geven een bevoegdheid aan de Minister van Infrastructuur en Waterstaat en de Minister van Economische Zaken en Klimaat om bij besluit AED's aan te wijzen binnen de in de tabel genoemde deelsectoren.

[6] Kamerstukken II 2017/18, 34883, nr. 3, p. 31.

AED's moeten passende technische en organisatorische maatregelen treffen ter beveiliging van hun netwerk- en informatiesystemen. Die zorgplicht is nader uitgewerkt in de bijlage die dit wijzigingsbesluit toevoegt aan het Bbni.

Ook zonder wetgeving hebben AED's al de nodige beveiligingsmaatregelen getroffen, zijnde een combinatie van organisatorische en technische maatregelen. Voor de continuïteit van hun eigen bedrijfsvoering is het immers cruciaal dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging. Zonder maatregelen is men zeer kwetsbaar voor tal van dreigingen, zoals cybercrime, stroomstoringen en menselijke fouten. Daarbij zouden AED's een reëel risico kunnen lopen waarbij een correcte levering van hun eigen diensten in gevaar komt, zoals de levering van gas en het vervoeren van personen en goederen door de lucht of over water.

AED's hebben dus al de nodige investeringen gedaan ter beveiliging van hun ICT-systemen om zodoende incidenten en – als gevolg daarvan – mogelijk grote schadeposten zo veel mogelijk te voorkomen.

Voor de sector energie is met de nieuwe AED's gesproken over hun huidige niveau van beveiligingsmaatregelen ('business as usual') en tot welke additionele kosten de Wbni en het Bbni leiden. Voor deze groep van elektriciteitsproducenten is van belang dat er grote onderlinge variëteit bestaat, met name qua bedrijfsvoering, schaalgrootte, ouderdom van de productie-installaties, complexiteit van ICT-infrastructuur en mate waarin men internationaal opereert. Zo geldt voor enkele van deze nieuwe AED's dat de productie van elektriciteit slechts een nevenactiviteit is en dat hun primaire productieproces een geheel andere focus heeft (bijvoorbeeld chemie en raffinage). De gevoerde gesprekken laten zien dat enkele van deze nieuwe AED's verwachten dat hun beveiligingsmaatregelen nu reeds of nagenoeg op het niveau van de Wbni en het Bbni zijn en dat de additionele kosten beperkt zullen zijn. Voor andere producenten geldt echter dat hun aanwijzing als AED de belangrijkste reden is om extra beveiligingsmaatregelen te treffen. Voor sommige partijen geldt hierbij dat er op het niveau van de Europese holding is besloten aan welke beveiligingseisen alle landenorganisaties dienen te voldoen, bijvoorbeeld door de implementatie van een bepaalde cybersecuritystandaard. Ook zijn er enkele nieuwe AED's die vrij jonge productie-installaties beheren, waarbij in het ontwerp al rekening is gehouden met de beveiliging van netwerk- en informatiesystemen. Bovenstaande leidt tot een heterogeen beeld van regeldrukkosten binnen de groep van elektriciteitsproducenten, waarbij onderscheid gemaakt kan worden naar eenmalige (tijdelijke) kosten en structurele kosten:

- **Eenmalige (of tijdelijke) kosten** – Voor de producenten betreft dit primair de additionele kosten die zij maken om te voldoen aan de beveiligingseisen van de Wbni en het Bbni. Hierbij gaat het voor de producenten vooral om de inzet van extra capaciteit en expertise ten behoeve van de implementatie en/of certificering. Voor alle producenten samen gaat het naar schatting om circa 35 fte (fulltime-equivalenten) extra in de eerste twee jaar. Dit betreft zowel interne als externe capaciteit. Uitgaande van een standaard uurtarief van € 60 is de monetaire waarde hiervan circa € 7,9 miljoen voor de eerste twee jaar (€ 4,0 miljoen per jaar). Op basis van de inschatting van de sector is een gemiddeld uurtarief van € 100 tot € 150 realistischer. Uitgaande van een uurtarief van € 120, verdubbelt de monetaire waarde naar € 15,8 miljoen voor de eerste twee jaar (€ 7,9 miljoen per jaar). Daarnaast verwachten producenten dat er in de eerste twee jaar ook circa € 4,5 miljoen (€ 2,3 miljoen per jaar) aan eenmalige investeringen gedaan moeten worden in informatietechnologie (IT) en operationele technologie (OT).
- **Structurele kosten** – Na deze eerste periode zullen de regeldrukkosten dalen. Naar schatting van de producenten is er structureel voor hen samen circa 16 fte noodzakelijk om blijvend te voldoen aan de beveiligingseisen van de Wbni en het Bbni. De monetaire waarde hiervan is, bij een standaard tarief van € 60, circa € 1,9 miljoen per jaar. Uitgaande van tarief van € 120, komt de monetaire waarde uit op circa € 3,7 miljoen per jaar. Daarnaast resulteren de gedane investeringen in IT en OT structureel ook in extra onderhouds- en vervangingskosten. Geschat wordt dat dit circa € 0,4 miljoen per jaar bedraagt.

De verschillende producenten wijzen erop dat de regeldruk deels afhangt van de uitleg die de bevoegde autoriteit de komende jaren zal geven aan de beveiligingseisen van de Wbni en het Bbni.

C. Eenmalige kennisnamekosten en toezichtlasten

AED's zullen eenmalig tijd besteden aan het verdiepen in en kennisnemen van de Wbni. Organisaties zullen hier naar schatting 16 uur (2 werkdagen) voor nodig hebben. Uitgaande van een uurtarief van € 60 komt dit uit op € 960 eenmalige kennisnamekosten per organisatie.

Ook het te woord staan van de bevoegde autoriteit in haar rol als toezichthouder veroorzaakt administratieve lasten voor AED's. Ook deze werkzaamheden kosten een AED naar schatting 16 uur dus € 960, maar dan per jaar.

4b. Gevolgen voor de regeldruk van de bijlage bij artikel 3a Bbni voor bestaande AED's

De bijlage bij artikel 3a Bbni bevat een nadere uitwerking van de zorgplicht van de artikelen 7 en 8 Wbni. Die zorgplicht gold al voor de al eerder aangewezen AED's. De bijlage geeft invulling aan bestaande wetgeving, waarmee AED's meer rechtszekerheid wordt geboden. De nalevingskosten van de nadere invulling van de zorgplicht zijn naar verwachting relatief beperkt aangezien dit in belangrijke mate aansluit bij de beveiligingseisen die reeds in de verschillende sectoren worden toegepast.

Omdat deze zorgplicht van toepassing is op verschillende organisaties in diverse sectoren die elk een eigen risicoprofiel en volwassenheidsniveau van netwerk- en informatiesystemen en daarbij passende veiligheidscultuur, normen en regulering kennen, zal er tussen sectoren en individuele organisaties variatie zitten in de te verwachten nalevingskosten. Naar verwachting zullen diverse organisaties aanvullende investeringen moeten doen om aan de gestelde eisen te voldoen. Hierbij gaat het zowel om eenmalige investeringen (bijvoorbeeld voor de tijdelijke inzet van extra experts) als structurele investeringen (in capaciteit en de netwerk en informatiesystemen). De hoogte hiervan varieert echter op organisatieniveau aangezien deze zeer afhankelijk is van de reeds gedane investeringen.

Het bovenstaande is ter toetsing voorgelegd aan de reeds aangewezen AED's binnen de sectoren energie en digitale infrastructuur. De resultaten zijn hierna kort samengevat:

- **Regeldruk als gevolg van de Wbni** – De meeste AED's geven aan dat als gevolg van de inwerkingtreding van de Wbni er vooral extra kosten zijn ontstaan rondom de beveiligingseisen. De AED's hebben in de afgelopen periode extra (interne en externe) capaciteit moeten inzetten om te gaan voldoen aan de beveiligingsmaatregelen die de wet stelde. In totaal gaat het om circa 9 fte voor de eerste twee jaar, wat een monetaire waarde vertegenwoordigt van circa € 2,0 miljoen (€ 1,0 miljoen per jaar). De verwachting is dat, mede als gevolg van de aankomende uitbreiding van de digitalisering bij enkele netbeheerders, deze kosten structureel uitkomen op circa 11 fte per jaar. Dit vertegenwoordigt een monetaire waarde van circa € 1,2 miljoen per jaar. Hierbij geldt overigens dat voor sommige AED's de additionele kosten als gevolg van de Wbni zeer beperkt waren, met name omdat men voordien al een hoog beveiligingsniveau hanteerde. Voor deze AED's zijn de (beperkte) regeldrukkosten vooral gerelateerd aan het beter inzichtelijk maken van de reeds bestaande praktijk.
- **Regeldruk als gevolg van de bijlage bij artikel 3a Bbni** – De meeste AED's geven aan dat de extra regeldruk als gevolg van de bijlage bij artikel 3a Bbni relatief beperkt zal zijn, ervan uitgaande dat de bijlage dusdanig kunnen worden geïnterpreteerd dat deze goed aansluiten op de maatregelen die zij de afgelopen periode al hebben genomen om te voldoen aan de Wbni.

4c. Burgers en overige organisaties

Dit besluit veroorzaakt geen regeldruk voor burgers en evenmin voor andere organisaties dan bedoeld in de artikelen 2 en 3 Bbni.

Artikelsgewijze toelichting

Artikel I, onderdeel A (wijziging artikel 2: aanwijzing van AED's in de sectoren elektriciteit, gas, olie, digitale infrastructuur en spoor- en wegvervoer)

Onderdelen 1 tot en met 3

Deze onderdelen voegen ten eerste enkele AED's in de deelsector elektriciteit toe aan de tabel in artikel 2 Bbni en breiden de bestaande aanwijzing van de Nederlandse Aardoliemaatschappij B.V. uit met de ondergrondse gasopslag in Norg. De aanwijzingen van deze nieuwe AED's in deze sectoren, die zijn besproken met de betrokken marktpartijen, beogen met name om de risico's van de onderlinge afhankelijkheid in de keten te verkleinen. Daarnaast regelen deze onderdelen de bevoegdheid van de minister van EZK om, mede in aanvulling op de aanwijzing van AED's in de energiesector, bij besluit bepaalde aanbieders in de sectoren energie en digitale infrastructuur als bedoeld in bijlage II van de NIB-richtlijn als AED aan te wijzen.

Elektriciteit

De netbeheerder van het landelijke hoogspanningsnet en de regionale netbeheerders waren al aangewezen als aanbieders van een essentiële dienst (AED). Dit wijzigingsbesluit wijst als zodanig ook de beheerder van een (grensoverschrijdende) interconnector aan, en een deel van de elektriciteitsproducenten die actief zijn op de Nederlandse markt.

Het Nederlandse elektriciteitsnet is door middel van zogeheten interconnectoren verbonden met het elektriciteitsnet van buurlanden zoals Duitsland, België en het Verenigd Koninkrijk. Deze interconnectoren dragen bij aan de leveringszekerheid en stabiliteit van het Nederlandse net (en het Europese net als geheel), daar dit de mogelijkheid biedt om reservecapaciteit te delen en onregelmatigheden in de energiebalans op te vangen. Alle Nederlandse interconnectoren maken integraal deel uit van het landelijk hoogspanningsnet (van TenneT), behalve de interconnector tussen Nederland en het Verenigd Koninkrijk met een capaciteit van 1 Gigawatt. De beheerder hiervan is BritNed Development Limited, een *joint venture* tussen de netbeheerders van het landelijk hoogspanningsnet in het Verenigd Koninkrijk (National Grid) en Nederland (TenneT). De aanwijzing van BritNed Development Limited als AED zorgt ervoor dat alle Nederlandse interconnectoren voor elektriciteit onder het bereik van de Wbni vallen. Dat vergroot de digitale weerbaarheid en beperkt de maatschappelijke gevolgen van cyberincidenten bij een dergelijke vitale aanbieder.

De reeds als AED aangewezen netbeheerder van het landelijke hoogspanningsnet en de regionale netbeheerders hebben op grond van de Elektriciteitswet 1998, naast diverse andere taken, de taak om de energiebalans van het gehele systeem te bewaken (of te herstellen) en daarmee de betrouwbaarheid van de netten en van het transport van elektriciteit over de netten te waarborgen. De goede uitvoering van de taken door de netbeheerders hangt nauw samen met de primaire productie van de elektriciteit en de voorzieningen die producenten bieden in geval van (dreigende) verstoringen van de energiebalans. Vanwege de onderlinge afhankelijkheid in het borgen van de energiebalans en algehele betrouwbaarheid van het energiesysteem wordt middels dit wijzigingsbesluit een deel van de producenten die actief zijn op de Nederlandse markt onder het bereik van de Wbni gebracht. Het is hierbij belangrijk op te merken dat het, juist vanwege de onderlinge ketenafhankelijkheid, voor de producenten gaat om een gedeelde verantwoordelijkheid. In de uitvoering van hun zorgplicht kunnen de producenten rekening houden met de systeemmaatregelen die de netbeheerder van het landelijke hoogspanningsnet en de regionale netbeheerders nemen om de energiebalans van het gehele systeem te bewaken. Hier zal, ook in overleg met deze netbeheerders, een goede balans in moeten worden gevonden. Een inbreuk op de beveiliging van de netwerk- en informatiesystemen van een individuele energiecentrale zal door de huidige systeemmaatregelen opgevangen kunnen worden. Bij een inbreuk die meerdere energiecentrales raakt, die mogelijk ook onderdeel uit maken van de voorzieningen om de energiebalans te herstellen, voldoen deze systeemmaatregelen niet meer en ontstaan er nadelige maatschappelijke gevolgen.

Bij de aanwijzing van de elektriciteitsproducenten in artikel 2 is allereerst aangesloten bij de afbakening die de NIB-richtlijn in bijlage II geeft, namelijk dat het moet gaan om (i) een 'elektriciteitsbedrijf' zoals gedefinieerd in artikel 2, punt 35, van Richtlijn 2009/72/EG van het Europees Parlement en de Raad, dat (ii) tevens de functie verricht van 'levering' zoals gedefinieerd in artikel 2, punt 19, van die richtlijn. De definitie van 'elektriciteitsbedrijf' is echter breed en omvat niet enkel de functie van productie, maar ook van transmissie, distributie, levering en aankoop van elektriciteit. De toevoeging in de NIB-richtlijn dat tevens de functie van levering verricht moet worden, creëert nadere afbakening. Conform de richtlijn betekent dit namelijk dat er sprake moet zijn van de (weder)verkoop van elektriciteit aan afnemers, wat zowel grootafnemers ('wederverkopers') of eindafnemers kunnen zijn. Dit betekent dat een producent die enkel voor eigen gebruik elektriciteit opwekt, niet onder de definitie valt daar hij deze elektriciteit niet levert.

Om te komen tot de juiste afbakening van de als AED aan te wijzen producenten zijn twee nadere keuzes gemaakt. Ten eerste stelt de aanwijzing dat het moet gaan om een elektriciteitsbedrijf dat het beheer voert over één of meerdere productie-installaties, zoals gedefinieerd in de Elektriciteitswet. Hierbij is aangesloten op het begrip beheer, wat ten aanzien van productie-installaties reeds een grondslag kent in artikel 86f, eerste lid, van de Elektriciteitswet 1998. De keuze voor dit open begrip is bewust gemaakt omdat uit de praktijk blijkt dat producenten zichzelf op veel verschillende manieren georganiseerd hebben, zowel qua eigendoms- en bedrijfsstructuren als qua feitelijke organisatie van bedrijfsprocessen. Met het begrip beheer is bedoeld om de juridische en feitelijke verschillen tussen de verschillende producenten te ondervangen en de entiteit aan te wijzen die het eigenlijke beheer voert en daarmee ook in staat is om de productie-installaties tegen inbreuken van buitenaf te beschermen. Dit voorkomt dat elektriciteitsproducenten zich eventueel kunnen beroepen op feitelijke omstandigheden of juridische organisatievormen en zich daarmee aan hun zorg- en meldplicht op grond van de Wbni kunnen onttrekken. Dit borgt ook het gelijke speelveld tussen de onderling concurrerende producenten. Dit beheer zal in de praktijk vaak gekoppeld zijn aan een eigendoms- of gebruiksrecht van een productie-installatie, maar ook andere type rechten of overeenkomsten kunnen hier aan ten grondslag liggen. De gekozen rechtsvorm, gelaagde eigendomsconstructies en samenwerkingsafspraken zijn daarbij wel relevant, maar mogen niet verhinderen dat niet voldaan wordt aan de zorg- en meldplicht. Dit betekent in de praktijk dat nagegaan moet worden welke partij het eigenlijke beheer voert en daarmee in staat is om de noodzakelijke maatregelen te nemen om de productie-installaties tegen inbreuken van buitenaf te beschermen. In veel gevallen zal het eigenlijke beheer door de rechtspersoon gevoerd worden die ook eigenaar is en daarmee besluit over exploitatie en investeringen. Echter, een rechtspersoon die geen eigenaar is en enkel het dagelijkse werk en onderhoud aan een productie-installatie uitvoert, maar geen verder geen zeggenschap of beslissingsbevoegdheid heeft over de exploitatie en investeringen, zal waarschijnlijk niet het eigenlijke beheer voeren.

Een tweede keuze betreft het opnemen van een criterium voor de schaal van de activiteiten van de producenten, namelijk het beheren van een nominaal vermogen van ten minste 100 MegaWatt (MW). Door deze beperking wijst het Bbni de grootste producenten aan die actief zijn op de Nederlandse markt. Volgens cijfers van het Centraal Bureau voor de Statistiek was het opgestelde (elektrische) vermogen eind 2017 ruim 34 GigaWatt (GW), waarvan circa 60% werd afgedekt door 43 centrale installaties ('energiecentrales'). De overige 40% aan opgesteld vermogen betreft meer dan 6.000 decentrale installaties, met name warmtekrachtkoppelinginstallaties (WKK's). Met deze wijziging van het Bbni komen circa 16 producenten onder het bereik van de Wbni te vallen, met een gezamenlijk opgesteld vermogen van circa 21 GW.

Er is om drie redenen gekozen voor het criterium van 100 MW aan cumulatief opgesteld vermogen. Ten eerste houdt de huidige wet- en regelgeving in de eisen aan het netontwerp van de hoogspanningsnetten rekening met grootschalige storingen van 100 MW of meer. Netbeheerders melden grootschalige storingen aan de Autoriteit Consument en Markt en (in specifieke gevallen) ook Agentschap Telecom. Deze melding hangt samen met de taken en verplichtingen voor netbeheerders op grond van de Elektriciteitswet 1998. In onderliggende regelgeving, zoals de Netcode Elektriciteit, en daaruit voorvloeiende plannen en afspraken is in meer detail bepaald hoe moet worden omgegaan met onderbrekingen in het transport van elektriciteit. Omdat storingen

van een dergelijke omvang ook gerelateerd kunnen zijn aan een inbreuk op de beveiliging van de netwerk- en informatiesystemen van een enkele producent met een opgesteld vermogen van 100 MW of meer, wordt hierop in het Bbni aangesloten. Ten tweede wordt aangesloten bij Europese normen die gelden voor de publicatie van gegevens over de elektriciteitsmarkten van de lidstaten. Verordening (EU) 543/2013 van de Europese Commissie (artikelen 14-16) bepaalt onder meer dat productie-eenheden met een geïnstalleerde capaciteit van 100 MW of meer zich kenbaar maken aan de beheerder van het hoogspanningsnet (TenneT) en informatie verstrekken ten behoeve van de publieke bekendmaking van de beschikbaarheid en onbeschikbaarheid van opwekkings- en productie-eenheden. Dit betekent dat de producenten die onder het bereik van de Wbni vallen ook duidelijk identificeerbaar zijn. Ten derde leidt het criterium van 100 MW aan opgesteld vermogen ertoe dat ook grootschalige decentrale opwekking binnen het bereik van de Wbni komt.

Gas

De Nederlandse Aardoliemaatschappij B.V. (NAM) was al aangewezen als AED, maar alleen voor het opsporen en winnen van gas uit het Groningenveld. In de bedrijfsvoering van de NAM fungeert de ondergrondse gasopslag Norg als een belangrijke buffer voor fluctuaties in de vraag naar gas gedurende het jaar en het op peil houden van de voorzieningszekerheid. Gezien het belang van de opslag Norg voor de essentiële dienst die de NAM vanuit het Groningenveld uitvoert, verruimt dit wijzigingsbesluit het toepassingsbereik van de Wbni op dit onderdeel van de productieketen.

Aanwijzingsbevoegdheid sectoren energie- en digitale infrastructuur

Vanwege de energietransitie vinden in de energiesector momenteel in een kort tijdsbestek grote veranderingen plaats. Hierbij spelen gedigitaliseerde oplossingen een steeds grotere rol, wat betekent dat de cybersecurityrisico's in de energiesector toenemen. Verder groeit het gebruik van de digitale infrastructuur, waarbij de afhankelijkheid van gebruikers (waaronder andere essentiële diensten) toeneemt. Naar verwachting zullen in de toekomst ook andere partijen in de sectoren energie en digitale infrastructuur als AED moeten worden aangewezen. Om de cybersecurity in het licht van deze snelle ontwikkelingen te waarborgen, wordt in deze wijziging van het Bbni bewerkstelligd dat de minister van Economische Zaken en Klimaat de bevoegdheid krijgt om bij besluit AED's aan te wijzen in de sectoren energie en digitale infrastructuur. Deze aanwijzingsbevoegdheid is meer passend in het kader van de snelle ontwikkelingen, omdat een aanwijzing van AED's door middel van een wijziging van het Bbni minder passend is bij de behoefte van een (snellere) aanwijzing.

Alvorens partijen middels besluit als AED worden aangewezen, zal de minister van EZK de partijen de mogelijkheid bieden om middels een openbare consultatie te reageren op het voornemen van de minister. Gezien de coördinerende verantwoordelijkheid voor cybersecurity van de minister van JenV en de voor deze minister in de Wbni opgenomen wettelijke taken, zal de minister van EZK de minister van JenV telkens vroegtijdig betrekken bij het aanwijzingsproces.

De aanwijzingsbevoegdheid in de sector energie komt in aanvulling op deze aanwijzing in het Bbni, de bevoegdheid in de sector digitale infrastructuur komt in de plaats van de aanwijzing in het Bbni. De thans krachtens het Bbni aangewezen AED's in de sector digitale infrastructuur zullen in elk geval deel uitmaken van de voorgenomen aanwijzing bij ministerieel besluit van EZK na inwerkingtreding van dit besluit.

Onderdeel 4 (spoor- en wegvervoer)

Zoals aangekondigd in de nota van toelichting bij het Bbni is voor de deelsectoren spoorvervoer en vervoer over de weg een nieuwe vitaliteitsbeoordeling uitgevoerd aan de hand van een actueel cyberscenario.[7] Op grond daarvan heeft de Minister van Infrastructuur en Waterstaat de processen vervoer van personen en goederen over (hoofd)spoorweginfrastructuur en vervoer over het (hoofd)wegennet beide geclassificeerd als vitaal, categorie B.[8] De volgende stap is om op basis van een dreigings- en risicoanalyse binnen deze vitale processen vitale aanbieders te identificeren

[7] Zie Stb. 2018, 388, p. 8 (transponeringstabel).

[8] Zie voor deze aanduiding Kamerstukken II 2014/15, 30821, nr. 23, p. 4.

behorende tot de in de tabel genoemde categorieën (spoorweginfrastructuurbeheerders, spoorwegondernemingen, wegenautoriteiten en exploitanten van intelligente vervoerssystemen). Deze vitale aanbieders zullen dan als AED krachtens het Bbni worden aangewezen bij besluit van de Minister van Infrastructuur en Waterstaat.

De tabel bevat alleen voor spoor- en wegvervoer inhoudelijke wijzigingen. Bij de deelsectoren luchtvervoer en vervoer over water is alleen de eerste kolom gewijzigd, waarin bijlage II van de NIB-richtlijn is gevolgd voor de aanduiding van sector en deelsector. Verder is ook voor de volgorde van de deelsectoren binnen de sector vervoer de volgorde in die bijlage aangehouden.

Artikel I, onderdeel B (wijziging artikel 3: aanwijzing van andere vitale aanbieders)

De digitale overheid is het stelsel van digitale overheidsvoorzieningen, bestaande uit digitale processen en diensten waaronder de tien basisregistraties, die de digitale publieke dienstverlening mogelijk maken en onderdeel zijn van de digitale gegevensverwerking tussen overheidsorganisaties en tussen overheidsorganisaties en burgers. Bepaalde processen van deze digitale infrastructuur zijn zó belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen maken deel uit van de Nederlandse vitale infrastructuur.[9] De minister die eerstverantwoordelijk is voor een digitale voorziening beoordeelt of de voorziening moet worden beschouwd als een "andere dienst" (dan een essentiële dienst als bedoeld in artikel 2 Bbni) "waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving" (zie de definitie van *vitale aanbieder* in artikel 1, laatste streepje, Wbni). Als dat zo is, dan kunnen die voorziening en degene die haar aanbiedt, desgewenst worden toegevoegd aan de tabel van artikel 3. De aanbieder van de voorziening wordt daarmee een *andere vitale aanbieder* als bedoeld in artikel 5, eerste lid, onder b, Wbni. Dat betekent concreet dat de aanbieder ernstige ICT-incidenten moet melden bij het NCSC (zie artikel 10, eerste lid, Wbni).

Handelsregister
Het Handelsregister, dat beheerd wordt door de Kamer van Koophandel, voldoet aan de definitie van een vitale digitale voorziening zoals opgenomen in de brief van de Minister van Justitie en Veiligheid van 11 december 2017.[10] Het Handelsregister is een basisregister van ondernemingen en rechtspersonen en vervult meerdere belangrijke functies voor ondernemend Nederland en de Nederlandse samenleving. De belangrijkste is de rechtszekerheidsfunctie: dat gegevens over rechtspersonen en ondernemingen die deelnemen aan het economisch verkeer door eenieder kunnen worden ingezien en geverifieerd. Ook dient het basisregister als de bron van informatie voor overheidsdienstverlening aan bedrijven en ondernemers, bijvoorbeeld door gemeenten en de Belastingdienst. Ook dragen de gegevens uit het Handelsregister bij aan het toezicht op rechtspersonen en aan de rechtshandhaving door de overheid. De uitval of compromittering van het Handelsregister zal naar verwachting leiden tot een verstoring van het economische verkeer en onderliggende activiteiten van banken, notarissen en verzekeraars. Om deze reden is ervoor gekozen om de Kamer van Koophandel in het Bbni aan te wijzen als "andere vitale aanbieder" van de dienst Handelsregister.

Basisregistratie personen
Verder voegt artikel I, onderdeel B, toe aan de tabel van artikel 3 Bbni de centrale voorzieningen, bedoeld in artikel 1.9, derde lid, van de Wet basisregistratie personen (Wet BRP). De basisregistratie personen (BRP) bevat persoonsgegevens over de ingezetenen van Nederland en bestaat uit gemeentelijke en centrale voorzieningen. De onderhavige aanwijzing betreft het deel van de BRP waarvoor de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verantwoordelijk is en dat wordt beheerd door de Rijksdienst voor Identiteitsgegevens: de centrale voorzieningen die het stelsel van berichtuitwisseling en verstrekking van gegevens faciliteren ten behoeve van de bijhouding (door gemeenten) en de raadpleging (door geautoriseerde organisaties)

[9] Zie de omschrijving in de brief van 11 december 2017, Kamerstukken II 2017/18, 29517, nr. 136, p. 3.
[10] Zie vorige noot.

van de basisregistratie. De BRP heeft tot doel overheidsorganen te voorzien van authentieke gegevens die nodig zijn voor de vervulling van hun taak alsmede derden te voorzien van authentieke gegevens, ingeval zij beschikken over een zogeheten autorisatiebesluit op basis van de Wet BRP. De persoonsgegevens in de BRP hebben een rechtszekerheidsfunctie: de gebruiker mag erop vertrouwen dat deze gegevens kloppen. Uitval of compromittering van de centrale voorziening BRP leidt tot verstoring van de effectieve en doelmatige taakuitoefening en dienstverlening van de (semi-)overheid.

DigID
Ook voegt artikel I, onderdeel B, toe aan de tabel van artikel 3 Bbni de voorziening voor uitgifte en activatie van elektronische authenticatiemiddelen en voor elektronische authenticatie, kortweg aangeduid met DigiD. Het betreft het van rijkswege uitgegeven middel dat persoonsidentificatiegegevens, zoals het burgerservicenummer, bevat en dat gebruikt wordt voor de authenticatie van een natuurlijke persoon die toegang wenst tot elektronische dienstverlening in het publieke domein. De voorziening wordt beheerd door de dienst Logius en is essentieel voor het veilig en betrouwbaar kunnen inloggen bij (semi-)overheden, zoals gemeenten, de Belastingdienst, het UWV en de SVB. Uitval of compromittering leidt tot onderbreking van de beschikbaarheid van belangrijke overheidsdiensten, hetgeen maatschappelijk zeer onwenselijk is.

Overig
Als in de toekomst blijkt dat er nog andere digitale overheidsvoorzieningen zijn waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving, dan kunnen zij uiteraard bij een volgende wijziging van het Bbni worden toegevoegd aan de tabel van artikel 3. Ook kan de eerstverantwoordelijke minister de voorziening bij besluit aanwijzen krachtens het Bbni. De voorziening kan bijvoorbeeld zodanig onverwijld als vitaal moeten worden aangemerkt, dat aanpassing van het Bbni niet kan worden afgewacht. Ook kan het nodig zijn om vanuit informatiebeveiligingsoptiek en het voorkomen van kwetsbaarheid (verscherpte aandacht van kwaadwillenden), specifieke (onderdelen van) overheidsinfrastructuur, systemen en processen niet algemeen te openbaren.

Artikel I, onderdeel C (nieuw artikel 3a: nadere regels over beveiliging AED's)

Het eerste lid schrijft voor dat de AED bij het implementeren van de zorgplicht uit de artikelen 7 en 8 Wbni in ieder geval de in de bijlage beschreven maatregelen neemt. De bijlage biedt een gemeenschappelijk kader voor aangewezen AED's om nadere invulling te geven aan de zorgplicht. Dit gemeenschappelijk basisniveau van digitale en fysieke maatregelen bestaat uit een opsomming van de maatregelen die AED's ter beveiliging van hun netwerk- en informatiesystemen in elk geval moeten nemen. De bewijslast of aan de zorgplicht wordt voldaan is in eerste instantie aan de AED (d.m.v. audits etc.). Het is uiteindelijk aan de toezichthouder om hierover een oordeel te vormen. Doordat de bijlage onderliggende uniforme gemeenschappelijke maatregelen voorschrijft, wordt sectoroverstijgende afstemming voor categorieën van AED's en samenwerking tussen toezichthouders vereenvoudigd. Dit draagt bij aan effectief toezicht.

De in de bijlage beschreven maatregelen maken continue en adaptieve risicobeheersing mogelijk, alsook het systeemtoezicht daarop. Dat past in het 'Programma Adaptieve weerbaarheid' dat ik heb aangekondigd in mijn brief van 12 juni 2019.[11] Passende maatregelen zijn soms sectorspecifiek, soms sectoroverstijgend; daarom moeten de in de bijlage beschreven maatregelen als een dynamisch instrument worden gezien en worden ingezet aan de hand van sector- en bedrijfsspecifieke risico's.

Waar gewenst kunnen de in de bijlage beschreven maatregelen verder worden uitgewerkt bij regeling van de sectoraal verantwoordelijke bewindspersoon op grond van artikel 3a, tweede lid, Bbni, na overleg met de Minister van Justitie en Veiligheid. In die regeling kan desgewenst ook worden verwezen naar door de sector zelf gehanteerde sectorale uitvoeringsnormen.

[11] Kamerstukken II 2018/19, 26643, nr. 614, p. 3.

Voor de bijlage bij het Bbni is een aantal (inter)nationale documenten als uitgangspunt of inspiratie gebruikt:
- de door het Europees Agentschap voor netwerk- en informatiebeveiliging de (ENISA) gebruikte indeling voor beheersdomeinen,
- de indeling van de guidance vanuit het Verenigd Koninkrijk, ISO 27001/2 en het US National Institute of Standards and Technology (NIST) Cybersecurity framework,
- de Nederlandse uitvoeringsverordening voor DSP's,
- sectorspecifieke normen en standaarden, zoals het PA-normenkader voor de drinkwatersector.

Artikel I, onderdeel D (wijziging artikel 4 naar aanleiding van nieuw artikel 3a en de bijlage)

Artikel 4 Bbni regelt dat de beveiligingseisen van de Wbni niet gelden voor de als AED krachtens artikel 2 Bbni aangewezen kredietinstellingen, centrale tegenpartijen en exploitanten van handelsplatformen. Het nieuwe artikel 3a Bbni en de bijlage bij dat artikel zijn gebaseerd op de bevoegdheid van artikel 9 Wbni om nadere regels te stellen over de door AED's te nemen beveiligingsmaatregelen. Voor alle duidelijkheid regelt artikel I, onderdeel D, dat ook artikel 3a Bbni en de bijlage bij dat artikel niet van toepassing zijn op de in artikel 4 bedoelde AED's.

Voor de luchtvaart is overigens Europese regelgeving in ontwikkeling in de vorm van een verordening van het European Union Aviation Safety Agency (EASA). Die conceptverordening (zoals opgenomen in de Notice of Proposed Amendment 2019-07) stelt regels over de maatregelen die luchtvaartbedrijven moeten nemen om zich te beschermen tegen informatiebeveiligingsrisico's. De verordening treedt naar verwachting in werking in het tweede kwartaal van 2021. Als de beveiligingseisen van de verordening ten minste gelijkwaardig zijn aan die van de NIB-richtlijn, zullen de betrokken luchtvaart-AED's bij een volgende wijziging van het Bbni worden toegevoegd aan artikel 4 Bbni, zodat voor hen de beveiligingseisen van de Wbni niet langer gelden.

Artikel I, onderdeel E (toevoegen van de bijlage aan het Bbni)

In de ter internetconsultatie voorgelegde versie van dit wijzigingsbesluit ontbreekt per abuis het onderdeel waarin de bijlage wordt toegevoegd aan het Bbni. De toevoeging van onderdeel E aan artikel I herstelt deze omissie.

Artikel II (inwerkingtreding)

Zekerheidshalve is de mogelijkheid opgenomen om het tijdstip van inwerkingtreding van deze Bbni-wijziging voor de verschillende artikelen of onderdelen daarvan verschillend vast te stellen.

Bijlage bij artikel 3a, eerste lid, Bbni (beveiliging AED's)

Inleiding

De term maatregelen is overgenomen uit de NIB-richtlijn en de artikelen 7 en 8 Wbni. De term omvat ook beleidsmaatregelen en procedures. De zorgplicht is van toepassing op architectuur, governance, veiligheidscultuur en processen gericht op de netwerk- en informatiesystemen van de aanbieder. De maatregelen zijn niet limitatief van aard en passen binnen bestaande internationale normenkaders, waardoor deze voor veel organisaties herkenbaar zijn. Het uitgangspunt vormt de eigen verantwoordelijkheid van de AED ten aanzien van de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de netwerk- en informatiesystemen die noodzakelijk zijn voor het in stand houden van de essentiële dienst.

Omdat deze zorgplicht van toepassing is op diverse sectoren met elk een eigen risicoprofiel van de beveiliging van netwerk- en informatiesystemen en daarbij passende veiligheidscultuur, normen en regulering, is gekozen voor een invulling die de benodigde ruimte laat aan de AED en de toezichthouder om tot een voor de sector passende invulling te komen, en die zo veel mogelijk ruimte laat om aan te sluiten bij bestaande en eventuele nieuwe normenkaders. Het ingevoegde

artikel 3a, tweede lid, biedt de mogelijkheid om desgewenst bij ministeriële regeling nadere sectorspecifieke maatregelen voor te schrijven.

De Wbni is van toepassing op netwerk- en informatiesystemen die noodzakelijk zijn voor het correct functioneren van de essentiële dienst. Het is primair de verantwoordelijkheid van de AED om deze systemen in kaart te brengen en een risicoanalyse uit te voeren.

Daarbij moet worden opgemerkt dat de Wbni en de bijlage uitgaan van de definities van *incident*, *beveiliging van netwerk- en informatiesystemen* en *risico* in de NIB-richtlijn. De risicoanalyse dient daarom rekening te houden met elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijk of daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen. Ook ligt het in de rede om het begrip *acties* in de definitie van *beveiliging van netwerk- en informatiesystemen* uit te leggen als 'elke omstandigheid of gebeurtenis'. Met *beveiliging* wordt gedoeld op beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid.

De onderdelen 1, 2 en 3 van de bijlage beschrijven voorzorgsmaatregelen.
De onderdelen 4 en 5 hebben betrekking op detectie, respons en herstel van en na incidenten. Het doel is onder meer om de aanbieder in staat te stellen de essentiële dienst zo snel mogelijk te herstellen. Het doel van de Wbni is hierbij het zo veel mogelijk beperken van de schade voor de maatschappij en het voorkomen van maatschappelijke ontwrichting.

Risicoanalyse

Onder risicoanalyse wordt verstaan het gestructureerd en gewogen gebruik van beschikbare kennis om te bepalen wat de kans is dat scenario's zich kunnen voordoen en hoe groot de gevolgen daarvan kunnen zijn, en het doen van voorstellen hoe het geïdentificeerde risico door middel van proportionele maatregelen terug te brengen naar een acceptabel niveau. Daarbij kunnen risico's tegen elkaar afgewogen worden. Zo kan verdere digitalisering van een essentiële dienst klassieke risico's doen afnemen ten koste van nieuwe risico's. Uiteindelijk telt voor de zorgplicht het totale beeld.

De maatregelen moeten in redelijke verhouding staan met het beoogde doel en de stand van de techniek. De AED maakt daarin een afweging of kosten en eventuele nadelen van te nemen maatregelen opwegen tegen de verwachte verhoging van de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de netwerk- en informatiesystemen. Daarbij kan de AED diverse belangen en risico's voor zijn essentiële dienst afwegen, daarmee rekening houdend met de aard en positie van de essentiële dienst binnen de keten.

De AED dient in de risicoanalyse waar relevant rekening te houden met eventuele externe afhankelijkheden van netwerk- en informatiesystemen die betrokken worden van of beheerd worden door externe partijen en toeleveranciers die de essentiële dienst ondersteunen en daarbij af te wegen welke risico's acceptabel zijn.

Toepasselijke normenkaders

De AED baseert zich bij de risicoanalyse en daaropvolgende maatregelen op de voor de AED relevante internationale, nationale, sectorspecifieke of bedrijfseigen normen. Denk daarbij aan internationale normenkaders als ISO, IEC of NIST of nationale normen als NEN. De bijlage stelt niet één norm of één specifieke versie daarvan verplicht, daar veel sectoren al bepaalde normen gebruiken. Het staat de AED daarmee vrij om het normenkader te kiezen dat het beste aansluit bij de sectorspecifieke risico's en het risicoacceptatieniveau, behoudens eventuele beperking van die vrijheid in een ministeriële regeling op grond van het ingevoegde artikel 3a, tweede lid, Bbni.

Verantwoordelijkheid AED

Het is de verantwoordelijkheid van de AED om op de risicoanalyse gebaseerde maatregelen te nemen die risico's met betrekking tot de beveiliging naar een passend niveau terugbrengen. Uiteindelijk is het aan de toezichthouder om vast te stellen of de AED aan de zorgplicht voldoet.

Om ruimte te laten aan de eigen verantwoordelijkheid van de AED en gegeven de verschillende snelheden waarmee ontwikkelingen in de verschillende sectoren zich voordoen, de mate waarin sprake is van legacy-infrastructuren en de verschillende investeringstermijnen die daarbij passen tussen essentiële diensten is er bewust geen invulling gegeven aan het begrip *periodiek*. De vraag welke maatregelen nodig zijn, is nadrukkelijk geen statisch gegeven. Wanneer het belang van de essentiële dienst voor de maatschappij verandert, nieuwe risico's ontstaan, relevante normen zich ontwikkelen of de stand der techniek evolueert, dient de AED zijn risicoanalyse en bijbehorende maatregelen te actualiseren. Dat geldt ook als zich andere relevante ontwikkelingen voordoen. Zo kan de dreiging op een essentiële dienst in de tijd fluctueren, kan nieuwe informatie over een dreiging beschikbaar worden of kan de AED een zwaarwegend advies van overheidszijde ontvangen. Ook kan de afhankelijkheid van netwerk- en informatiesystemen veranderen. Te denken valt aan de implementatie van een nieuwe architectuur of aan de keuze voor een nieuwe toeleverancier, het wegvallen van een analoog alternatief of de verdere digitalisering van een systeem dat kritisch is voor de essentiële dienst.

Van de AED wordt verlangd dat hij zich bewust is van de stand der techniek en passende en proportionele maatregelen neemt om deze te volgen. Met de stand der techniek wordt gedoeld op technologische ontwikkelingen en nieuwe inzichten die voortkomen uit kennisopbouw in de voor de AED relevante vakgebieden in binnen- en buitenland. Dit houdt geen verplichting in om nieuwe technologische ontwikkelingen of inzichten direct te implementeren, maar slechts wanneer dit passend en proportioneel is.

Tot slot

Het uiteindelijke doel van de Wbni en de bijlage is het verhogen van de weerbaarheid en het beperken van de gevolgen van cyberincidenten. Daartoe is het van belang dat de AED zich bewust is van het maatschappelijk belang van de essentiële dienst. Geëist wordt niet dat de AED volledig zicht heeft op de gevolgen van verstoringen van de dienst voor afnemers. Wel wordt verlangd dat de maatregelen van de AED om de beschikbaarheid van de essentiële dienst te verhogen, in verhouding staan tot de schade voor de maatschappij die een incident tot gevolg kan hebben. Hiervoor kan, voor zover dit gezien de aard van de essentiële dienst en de positie van de AED binnen de keten mogelijk is, een inschatting gemaakt worden op basis van ervaringen en kennis uit eerdere incidenten en analyse van ontwikkelingen in de sector.

De Minister van Justitie en Veiligheid,