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 … , Directie Wetgeving en Juridische Zaken, nr. …, 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. …, 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 gewijzigd:

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 producent als bedoeld in artikel 1, eerste lid, van de Elektriciteitswet 1998 die een of meerdere productie-installaties als bedoeld in dat lid beheert met een cumulatief nominaal vermogen van ten minste 100 MegaWatt	Productie 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)

2. 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 infrastructuurbeheerders, bedoeld in artikel 3 van richtlijn 2012/34/EU	Het beheer van de hoofdspoorweginfrastructuur, bedoeld in artikel 16 van de Spoorwegwet
	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
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”.

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 hebben betrekking op de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de netwerk- en informatiesystemen die een essentiële dienst ondersteunen. De maatregelen zijn aantoonbaar, worden periodiek, maar in elk geval als zich relevante veranderingen voordoen, geëvalueerd en waar nodig bijgesteld. In de maatregelen wordt doorlopend rekening gehouden met actuele ontwikkelingen. Netwerk- en informatiebeveiliging maakt integraal deel uit van netwerk- en informatiesystemen gedurende de gehele levenscyclus.

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 met inachtneming van de relevante normen en ontwikkelingen. In de analyse beschrijft hij de risico's en de wijze waarop hij de risico's tot een aanvaardbaar niveau verkleint. Hij motiveert waarom dit niveau proportioneel en aanvaardbaar is. Hierbij houdt hij niet alleen rekening met de organisatie-specifieke en sectorspecifieke risico's, maar ook met het maatschappelijke belang van zijn essentiële dienst en met de stand van de techniek. Hij zorgt ervoor dat de resultaten van de risicoanalyse inzichtelijk en toetsbaar zijn en hij verwerkt de resultaten in risicogerichte beveiligings- en beheersmaatregelen.

2. Organisatie van netwerk- en informatiebeveiligingsbeheer

De aanbieder zorgt voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van een informatiebeveiligingsbeleid op basis van de relevante normen en de stand der techniek. Hij heeft een informatiebeveiligingsstrategie die in lijn is met zijn strategische doelen en met het maatschappelijke belang van zijn essentiële dienst. Hij heeft de taken, bevoegdheden en verantwoordelijkheden voor de beveiliging en beheer van zijn netwerk- en informatiesystemen duidelijk in de organisatie belegd.

3. Incidenten voorkomen

De aanbieder draagt zorg voor een gelaagde beveiligingsstrategie gericht op het adequaat beheersen van risico's voor de netwerk- en informatiesystemen die de essentiële dienst ondersteunen. Onderdeel van deze beveiligingstrategie vormt onder andere het toepassen van *defense in depth* en passend lifecycle-, asset- en patchmanagement. Deze en andere maatregelen, zoals identificatie- en toegangsmanagement, zijn op risicoanalyses gebaseerd. De aanbieder is daardoor in staat om tijdig en adequaat om te gaan met geïdentificeerde kwetsbaarheden en dreigingen. Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op voor hem relevante beveiligingsadviezen en dreigingsinformatie beoordeelt hij of gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's tot een aanvaardbaar niveau te reduceren.

4. Detectie en respons

De aanbieder neemt passende maatregelen om incidenten te kunnen detecteren, analyseren en vastleggen en om hun gevolgen zo veel mogelijk te beperken. Hij monitort structureel relevante netwerk- en informatiesystemen, legt relevante handelingen op die systemen onweerlegbaar vast en bewaart die gegevens lang genoeg om incidenten te kunnen analyseren. Hij houdt hierbij

rekening met door de overheid beschikbaar gestelde relevante dreigingsinformatie. Hij hanteert procedures om op consistente en doeltreffende wijze op te treden bij incidenten.

5. Gevolgen van incidenten beperken

De aanbieder zorgt voor het opstellen van een bedrijfscontinuïteitsbeleid en een crisismanagementbeleid voor de netwerk- en informatiesystemen. Onderdeel van zijn crisismanagementbeleid is ten minste een plan dat hem in staat stelt 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. Consultatiereacties

PM

3. Regeldruk

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

3a. Nieuwe AED's en nieuwe andere vitale aanbieders

Artikel I, onderdeel A, onder 1,[2] 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 beveiligingseisen 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

[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).
[2] Onderdeel 2 wijst zelf nog geen nieuwe AED's aan, maar geeft alleen een bevoegdheid aan de Minister van Infrastructuur en Waterstaat om bij besluit AED's aan te wijzen binnen de deelsectoren spoorvervoer en wegvervoer.

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.[3] 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

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 energieproducenten 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 energieproducenten, 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. De monetaire waarde hiervan is circa € 7,9 miljoen voor de eerste twee jaar (€ 4,0 miljoen per jaar). Daarnaast verwachten

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

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 circa € 1,9 miljoen per jaar. Daarnaast resulteren de gedane investeringen in IT enOT 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.

3b. 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.

3c. 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 en gas en spoor- en wegvervoer)

Onderdeel 1 (elektriciteit en gas)

Dit onderdeel voegt enkele AED's toe aan de tabel in artikel 2 Bbni en breidt de bestaande aanwijzing van de Nederlandse Aardoliemaatschappij B.V. uit met de ondergrondse gasopslag in Norg. Deze toevoegingen betreffen de sector energie en dan specifiek de subsectoren elektriciteit en gas. De aanwijzingen van de 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.

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.

Bij de aanwijzing van de elektriciteitsproducenten in artikel 2 is een drietal keuzes gemaakt. Leidend hierbij is de keuze voor brede definities en begrippen om zo de grote feitelijke verschillen tussen de verschillende producenten te ondervangen. Deze verschillen bestaan bijvoorbeeld ten aanzien van de rechtsvorm, de grootte, bestaande samenwerkingsafspraken, en het eigendom en beheer van de productie-installaties. Ten eerste is aangesloten bij de definities van producent en productie-installatie zoals deze zijn vastgelegd in de Elektriciteitswet 1998 (artikel 1, eerste lid, onderdelen g en ah), namelijk de organisatorische eenheid die zich bezighoudt met het opwekken van elektriciteit. Deze definities zijn ruim geformuleerd en overstijgen daarmee de verschillende (juridische) vormen waarin rechtspersonen zich kunnen organiseren en samenwerken, en de feitelijke productiesituatie van een individuele producent. Dit voorkomt dat energieproducenten 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. In lijn met artikel 5, tweede lid, Wbni en bijlage II van de NIB-richtlijn gaat het hier om producenten die tevens leveren aan het elektriciteitsnet. Producenten die geen elektriciteit leveren via het net en dus enkel voor eigen gebruik elektriciteit opwekken, vallen hierbuiten. Ten tweede is aangesloten op het begrip beheer, wat ten aanzien van producenten en productie-installaties reeds een grondslag kent in artikel 86f, eerste lid, van de Elektriciteitswet 1998. Dit beheer zal vaak gebaseerd zijn op een eigendoms- of gebruiksrecht van een productie-installatie, maar ook andere type rechten of overeenkomsten kunnen hier aan ten grondslag liggen. Tot slot is gekozen voor 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 15 producenten onder het bereik van de Wbni te vallen, met een gezamenlijk opgesteld vermogen van circa 20 GW.

Er is om drie redenen gekozen voor het criterium van 100 MW aan 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 Groningerveld. 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 Groningerveld uitvoert, verruimt dit wijzigingsbesluit het toepassingsbereik van de Wbni op dit onderdeel van de productieketen.

Onderdeel 2 (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.[4] Op grond daarvan heeft de Minister van Infrastructuur en Waterstaat beide deelsectoren geclassificeerd als vitaal, categorie B.[5] De volgende stap is om op basis van een dreigings- en risicoanalyse vitale aanbieders (AED's) te identificeren binnen de in de tabel genoemde categorieën (spoorinfrastructuurbeheerders, spoorwegondernemingen, wegenautoriteiten en exploitanten van intelligente vervoerssystemen). De AED's worden krachtens het Bbni 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.[6] 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.[7] 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.

[4] Zie Stb. 2018, 388, p. 8 (transponeringstabel).
[5] Zie voor deze aanduiding Kamerstukken II 2014/15, 30821, nr. 23, p. 4.
[6] Zie de omschrijving in de brief van 11 december 2017, Kamerstukken II 2017/18, 29517, nr. 136, p. 3.
[7] Zie vorige noot.

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) 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 tijdelijk vitaal zijn of 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 niet-limitatieve opsomming van een systeem waaruit de beveiliging van netwerk- en informatiesystemen bestaat. De concrete maatregelen die AED's nemen, moeten passen binnen de in de bijlage voorgeschreven maatregelen, welke primair als doel hebben om de digitale weerbaarheid te verhogen. 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.[8] 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, of in beleidsregels van de bevoegde autoriteit, beide na overleg met de Minister van Justitie en Veiligheid. In die regeling of beleidsregels kan desgewenst ook worden verwezen naar door de sector zelf gehanteerde sectorale uitvoeringsnormen.

Voor de bijlage bij het Bbni zijn 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 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)

1. 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 daarom zo veel mogelijk abstract beschreven in de vorm van beheersdoelstellingen. 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

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

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. Voorbeelden van beveiligings- en beheersmaatregelen om incidenten te voorkomen zijn patchmanagement, alsmede identificatie en toegangsmanagement.
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 als redelijkerwijs 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.

2. 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.

Met *proportioneel* wordt in de bijlage bedoeld dat maatregelen in redelijke verhouding dienen te 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.

3. 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.

4. Toepassing van open normen

Waar gebruik gemaakt wordt van open normen zoals *proportioneel* of *relevant* is het in eerste instantie aan de AED om op basis van relevante normen te bepalen hoe de organisatie deze normen uitlegt. Het is vervolgens de verantwoordelijkheid van de AED om op de risicoanalyse gebaseerde passende en proportionele maatregelen te nemen die het risico tot een acceptabel niveau terugbrengen. Uiteindelijk is het aan de toezichthouder om vast te stellen of de AED aan de zorgplicht voldoet. De toezichthouder kijkt daarbij onder andere naar het maatschappelijk belang van de essentiële dienst, de relevante normen die op de AED van toepassing zijn, en de stand der techniek.

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.

5. 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,