

Vergaderjaar 2016–2017

**34 388**

**Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)**

**E**

**NADERE MEMORIE VAN ANTWOORD**

Ontvangen 6 juli 2017

In het nader voorlopig verslag inzake het bovenvermelde voorstel wordt de regering verzocht om de concepttekst van het Besluit meldplicht cybersecurity (Bmc) na de verwerking van de ontvangen reacties in de consultatiefase, toe te zenden aan de Eerste Kamer der Staten-Generaal. De gevraagde tekst treft u aan in de bijlage bij deze nadere memorie van antwoord.

De Staatssecretaris van Veiligheid en Justitie,  
K.H.D.M. Dijkhoff

**Bijlage bij nadere memorie van antwoord wetsvoorstel 34 388  
concept-Besluit meldplicht cybersecurity, versie 4 juli 2017 na  
consultatie**

**Besluit van (datum) tot aanwijzing van aanbieders, producten en  
diensten ten aanzien waarvan een plicht geldt om ernstige  
ICT-incidenten te melden (Besluit meldplicht cybersecurity)**

Op de voordracht van de Staatssecretaris van Veiligheid en Justitie van ..... (datum en nummer), gedaan in overeenstemming met Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Economische Zaken en met Onze Minister en de Staatssecretaris van Infrastructuur en Milieu;

Gelet op artikel 5 van de Wet gegevensverwerking en meldplicht cybersecurity;

De Afdeling advisering van de Raad van State gehoord (advies van ..... (datum en nummer));

Gezien het nader rapport van de Staatssecretaris van Veiligheid en Justitie van ..... (datum en nummer), uitgebracht in overeenstemming met Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Economische Zaken en met Onze Minister en de Staatssecretaris van Infrastructuur en Milieu;

Hebben goedgevonden en verstaan:

**Artikel 1**

De artikelen 6 tot en met 8 van de Wet gegevensverwerking en meldplicht cybersecurity zijn van toepassing op de volgende vitale aanbieders en producten en diensten:

Sector	Vitale aanbieder	Product of dienst
Drinkwater	Drinkwaterbedrijf als bedoeld in artikel 1, eerste lid, van de Drinkwaterwet	Het leveren van deugdelijk drinkwater door middel van een openbare drinkwatervoorziening
Energie	<ul style="list-style-type: none"><li>De netbeheerder van het landelijk hoogspanningsnet, aangewezen op grond van artikel 10, tweede lid, of 14 van de Elektriciteitswet 1998</li><li>De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998</li></ul>	Transmissie en distributie van elektriciteit
	<ul style="list-style-type: none"><li>De netbeheerder van het landelijk gastransportnet, aangewezen op grond van artikel 2, eerste lid, of artikel 5 van de Gaswet</li><li>De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of artikel 5 van de Gaswet</li></ul>	Transmissie en distributie van gas

Sector	Vitale aanbieder	Product of dienst
Nucleair	Houder van een vergunning als bedoeld in artikel 15, onderdeel b, van de Kernenergiewet	De bescherming van inrichtingen, waarin kernenergie kan worden vrijgemaakt, splijtstoffen kunnen worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen worden opgeslagen of inrichtingen, waarin kernenergie kon worden vrijgemaakt, splijtstoffen konden worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen werden opgeslagen
	Bedrijf vallend onder het Geheimhoudingsbesluit Kernenergiewet, Bedrijf vallend onder het Toepassingsbesluit 24 september 1971/nr.671/524	<ul style="list-style-type: none"> <li>De bescherming van inrichtingen, waarin kernenergie kan worden vrijgemaakt, splijtstoffen kunnen worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen worden opgeslagen of inrichtingen, waarin kernenergie kon worden vrijgemaakt, splijtstoffen konden worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen werden opgeslagen</li> <li>Het waarborgen van de beveiliging en geheimhouding van gegevens, welke noodzakelijk zijn voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges en het produceren van hulpmiddelen en materialen, welke zijn benodigd voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges</li> </ul>
Financieel	De bij besluit van De Nederlandse Bank N.V. aangewezen financiële instellingen	<p>Het afwikkelen van:</p> <ul style="list-style-type: none"> <li>toonbankbetalingsverkeer</li> <li>massaal giraal betalingsverkeer</li> <li>hoogwaardig betalingsverkeer</li> <li>effectenverkeer</li> </ul>
Elektronische communicatienetwerken en -diensten/ICT	Een aanbieder van een elektronisch communicatienetwerk of -dienst die een netwerk of infrastructuur beheert dat of die direct of indirect wordt gebruikt ten behoeve van het verlenen van een telefoon-, sms- of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers	Het verlenen van een telefoon-, sms- of internettoegangsdienst
	Een aanbieder van een internetknooppunt als bedoeld in artikel 4, onder 13, van Richtlijn (EU) 2016/1148 met een totale poortcapaciteit van minimaal 8 terabits per seconde	Het faciliteren van het internet- en dataverkeer
Mainport Rotterdam	De Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.	Het afwikkelen van scheepvaartverkeer
Mainport Schiphol	<ul style="list-style-type: none"> <li>Royal Schiphol Group N.V.</li> <li>Aircraft Fuel Supply B.V.</li> <li>Luchtverkeersleiding Nederland</li> <li>Koninklijke marechaussee</li> <li>elke luchtvaartmaatschappij met minimaal 25% van het totaal aantal vliegbewegingen op Schiphol in een kalenderjaar</li> </ul>	Een veilige en vlotte vlucht- en vliegtuigafhandeling
Keren en Beheren	Onze Minister van Infrastructuur en Milieu	De bij besluit van Onze Minister van Infrastructuur en Milieu aangewezen waterkeringen of onderdelen daarvan

## Artikel 2

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

## Artikel 3

Dit besluit wordt aangehaald als: Besluit meldplicht cybersecurity.

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

De Staatssecretaris van Veiligheid en Justitie,

## NOTA VAN TOELICHTING

### 1. Algemeen

Dit besluit, het Besluit meldplicht cybersecurity (Bmc) wijst de vitale aanbieders en producten en diensten aan ten aanzien waarvan de verplichting geldt – zoals opgenomen in artikel 6 van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) – om ernstige ICT-incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het Ministerie van Veiligheid en Justitie.

#### *Rijksbrede aanpak vitale infrastructuur*

Sommige processen zijn zo vitaal voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen tezamen vormen de Nederlandse vitale infrastructuur.<sup>1</sup> De impact van incidenten in de vitale infrastructuur, de snelheid van technologische ontwikkelingen, de verandering van (cyber)dreigingen en de toenemende onderlinge verwevenheid van vitale infrastructuur maken dat blijvende aandacht voor het verhogen en borgen van de weerbaarheid van de vitale infrastructuur noodzakelijk is.

De beoordeling of een proces vitaal is, wordt gemaakt wanneer maatschappelijke ontwikkelingen (bijvoorbeeld veranderende dreigingen of risico's en evaluaties van incidenten) daar aanleiding toe geven. Daarbij wordt onderscheid gemaakt tussen twee categorieën vitaal, A en B, waarbij uitval van A-vitale processen grotere potentiële gevolgen op de samenleving heeft dan uitval van B-vitale processen. Daarnaast moeten A-vitale processen voldoen aan het criterium van cascade/domino-effecten. Het onderscheid tussen A- en B-vitaal maakt het mogelijk om bij incidenten of bij de ontwikkeling van weerbaarheid verhogende capaciteiten onderling te prioriteren.

#### *Vitale aanbieders*

Binnen vitale processen zijn één of meerdere organisaties (overheidsorganisaties of privaatrechtelijke rechtspersonen) vitaal voor de continuïteit en weerbaarheid van het proces. Deze organisaties worden aangeduid als vitale aanbieders. Het vakdepartement is voor zijn eigen sectoren verantwoordelijk voor het identificeren van de vitale processen en de daarbij behorende vitale aanbieders. De NCTV heeft hierin een coördinerende rol.

### 2. Reikwijdte meldplicht

Gedurende de totstandkoming van de Wgmc is gesproken met relevante private en publieke organisaties uit diverse vitale sectoren, vertegenwoordigers van de betrokken vakdepartementen en het Ministerie van Veiligheid en Justitie. Daarbij is per sector geïnventariseerd welke vitale aanbieders en bijbehorende producten of diensten onder de meldplicht bij het NCSC kunnen komen te vallen. Voor deze eerste inventarisatie is aangesloten bij de selectie van vitale sectoren zoals beschreven in de brief aan de Tweede Kamer van 6 juli 2012,<sup>2</sup> te weten Energie, Drinkwater, Keren en Beheren, Telecom, de Mainports Rotterdam en Schiphol en Financiën, en is samengewerkt met de Commissie Vitale Infrastructuur. Digitale overheid en Nucleair zijn hier later aan toegevoegd.

<sup>1</sup> Zie Kamerstukken II 2014/15, 30 821, nr. 23 en Kamerstukken II 2015/16, 30 821, nr. 32.

<sup>2</sup> Kamerstukken II 2011/12, 26 643, nr. 247.

Hoewel de meldplicht alleen kan gelden voor vitale aanbieders, hoeft deze niet per se voor alle vitale aanbieders te gelden. Ook zijn niet alle producten of diensten die door een vitale aanbieder worden aangeboden onderdeel van een vitaal proces. Dit houdt in dat inbreuken op andere bedrijfsprocessen dan de vitale processen niet onder de meldplicht vallen. Om die reden zijn in dit besluit specifieke producten en diensten aangewezen waarvan de beschikbaarheid en betrouwbaarheid van essentieel belang zijn om maatschappelijke ontwrichting te voorkomen.

Daarnaast zijn niet alle vitale processen afhankelijk van informatiesystemen. Daar de hulpverlening door het NCSC tot doel heeft om de informatiesystemen van Rijk en Vitaal te beschermen, is bij de voorbereiding van het Bmc samen met de vitale aanbieders en vakdepartementen onderzocht welke van hun producten of diensten afhankelijk zijn van informatiesystemen en hoe groot de sociaal-economische gevolgen zijn bij een aanzienlijke verstoring van de beschikbaarheid en betrouwbaarheid van dat product of die dienst. Deze gevolgen zijn gezien op duur van het incident en aantal gebruikers dat door het incident wordt geraakt. Voor een aantal sectoren zijn aanvullende sectorspecifieke criteria gezien, zoals het aantal tonnen vracht dat niet meer vanuit de Mainports Schiphol en Rotterdam kan worden geleverd of wordt verhinderd door de verstoring.

De resultaten van deze inventarisatie waren leidend voor de selectie van de meldplichtige vitale aanbieders en bijbehorende producten en diensten.

### **3. Regeldruk**

De door de Wgmc geïntroduceerde meldplicht zal leiden tot een bescheiden stijging van de regeldruk voor de in dit besluit aangewezen vitale aanbieders. Zoals hierboven reeds aangegeven is de intentie van de meldplicht dat slechts incidenten die (kunnen) leiden tot maatschappelijke ontwrichting, onder de meldplicht vallen. Dat is een hoge drempel, die per sector zal worden geconcretiseerd in richtsnoeren, zo veel mogelijk in de vorm van concrete drempelwaarden (nadere uitwerking van «in belangrijke mate» in artikel 6, eerste lid, Wgmc).<sup>3</sup> Naar verwachting vallen ongeveer 60 organisaties onder de meldplicht. De verwachting is dat in totaal slechts enkele incidenten per jaar onder de meldplicht zullen vallen. Ter indicatie van de kosten van een melding is in de memorie van toelichting bij de Wgmc gekeken naar de in 2010 geraamde administratieve lasten van de meldplicht van artikel 11a.2 Telecommunicatiewet, die is ingevoerd in 2012. De verwachte lasten per melding bedroegen toen 212,50 euro.

### **4. Financiële consequenties**

Het in ontvangst nemen van meldingen en de afhandeling van incidenten is reeds onderdeel van de werkzaamheden van het NCSC. Hoewel wellicht meer meldingen zullen binnenkomen dan tot nu toe, wordt niet verwacht dat dit een merkbare verandering in kosten met zich mee zal brengen.

### **5. Evaluatie**

Het Bmc zal periodiek worden geëvalueerd en waar nodig worden aangepast of aangevuld.

---

<sup>3</sup> Kamerstukken II 2015/16, 34 388, nr. 6, p. 8.

## 6. Consultatiereacties

Een eerdere versie van het BMC is opengesteld voor consultatie op [www.internetconsultatie.nl](http://www.internetconsultatie.nl)<sup>4</sup> en voor commentaar toegezonden aan belangenorganisaties en vitale aanbieders. Hieronder volgt een globale bespreking van de ontvangen reacties.

Een aantal organisaties vraagt waarom een bepaalde sector of organisatie niet is meegenomen in het BMC. Zo vindt Arthur's Legal de reikwijdte van de aangewezen elektronische communicatienetwerken of -diensten/ICT te beperkt en pleit het bedrijf ervoor om de algehele digitale infrastructuur onder de meldplicht te laten vallen. Ook pleit het bedrijf voor aanwijzing van aanbieders in de gezondheidszorg, aangezien zorginstellingen volledig afhankelijk zijn van digitale systemen, die in veel gevallen ook sterk verouderd zijn.

Wat betreft de digitale infrastructuur en de gezondheidszorg verwijs ik naar de toelichting bij de selectie van vitale aanbieders en bij de reikwijdte van de meldplicht in paragraaf 1 en 2. Niet elk proces wordt als vitaal aangemerkt, binnen een vitaal proces is niet elke aanbieder vitaal, en de meldplicht geldt niet per se voor elke vitale aanbieder. Wat de gezondheidszorg betreft is uit de in paragraaf 1 besproken vitaliteitsbeoordeling niet gebleken dat dit proces tot de vitale infrastructuur behoort. In dit verband is van belang dat de gevolgen van eventuele uitval of verstoring in systemen zijn op te vangen. Dit komt voornamelijk omdat de zorg in Nederland niet centraal georganiseerd is. Een incident zal zich doorgaans beperken tot één instelling. Er kan dan voor specifieke diensten en processen altijd teruggevallen worden op zorginstellingen in de omgeving of regio. Zelfs wanneer een incident meer dan één instelling treft, is zorg in de regio meestal nog voorhanden. Scenario's waarbij grote aantallen instellingen in een of meerdere regio's tegelijkertijd worden geraakt door een incident zijn zeer onwaarschijnlijk, mede gelet op het feit dat instellingen software zelfstandig inkopen, eigen afspraken maken en updates niet gelijktijdig verwerken.

Andere organisaties vragen waarom alternatieve diensten voor sms en telefonie, zoals een berichtendienst als WhatsApp en andere over-the-top-diensten (OTT-diensten), niet als vitaal zijn aangemerkt.

OTT-diensten worden via het open internet aangeboden en het aanbod en dus ook de alternatieven voor internetgebruikers zijn groot. Om deze reden zijn deze diensten bij de in paragraaf 1 bedoelde vitaliteitsbeoordeling dan ook niet als vitaal aangemerkt. De sms-dienst daarentegen is wel als vitaal aangemerkt, omdat deze functionaliteit een onlosmakelijk onderdeel vormt van de mobiele telefoniedienst en omdat deze dienst gebruikt wordt bij authenticatie- en verificatiediensten. Uitval of verstoring van de sms-dienst kan miljoenen gebruikers treffen met mogelijk zeer grote gevolgen.

In een reactie wordt opgemerkt dat de regionale gasnetbeheerders ontbreken in de tabel. Naar aanleiding van deze reactie zijn deze netbeheerders aan de tabel toegevoegd.

KPN merkt in haar reactie op dat ook leveranciers van hard- en software essentieel zijn voor het – weliswaar op indirecte wijze – leveren van telefoon-, sms- en internetdiensten aan eindgebruikers en dus ook onder de meldplicht zouden moeten vallen. Ten aanzien hiervan wijs ik erop dat bij de in paragraaf 1 besproken vitaliteitsbeoordeling niet is gebleken dat

<sup>4</sup> [www.internetconsultatie.nl/besluitmeldplichtcyber](http://www.internetconsultatie.nl/besluitmeldplichtcyber).

genoemde leveranciers diensten aanbieden die als vitaal dienen te worden aangemerkt. Daarom zijn bij de in paragraaf 2 besproken inventarisatie van vitale aanbieders, producten en diensten die onder de meldplicht moeten vallen, niet de afzonderlijke netwerkcomponenten betrokken, zoals hardware, software en alle overige apparatuur en faciliteiten die in of ten behoeve van elektronische communicatienetwerken en -diensten worden gebruikt.

Over de internetknooppunten merkt een organisatie op dat knooppunten niet de daadwerkelijke afhandeling van verkeer op zich nemen, maar deze enkel faciliteren. Ten aanzien hiervan wijs ik erop dat het voor de meldplicht van belang is dat dataverkeer fysiek via de infrastructuur van het knooppunt wordt geleid; als het knooppunt uitval of verstoring ondervindt, dan kan dat negatieve gevolgen hebben voor de dataverkeersstroom over dat knooppunt.

Enkele organisaties merken op dat er naast de 25% van het dataverkeer dat de in dit besluit genoemde knooppunten mogelijk voor hun rekening nemen een substantieel hoog percentage van 75% overblijft. Gevraagd wordt waarom aanbieders die bilateraal verkeer uitwisselen of transitverkeer faciliteren – en dus niet via een internetknooppunt – niet vitaal zijn. Ten aanzien hiervan wijs ik erop dat uit de in paragraaf 1 besproken vitaliteitsbeoordeling niet gebleken is dat er in deze overige categorieën daadwerkelijk aanbieders zijn met een dusdanig groot dataverkeersvolume en fysieke concentratie als die van internetknooppunten, dat uitval een maatschappelijk ontwrichtende werking kan hebben.

Een organisatie vraagt waarom niet gekeken is naar de daadwerkelijke verkeersstatistieken in plaats van de maximale poortcapaciteit van knooppunten. Ten aanzien hiervan merk ik op dat de reden hiervoor is dat verkeersstatistieken een grillig verloop kennen en variëren in tijd. De maximale poortcapaciteit geeft een meer stabiele indicatie; deze is gedimensioneerd voor het opvangen van piekcapaciteit en op die manier gecorreleerd aan de daadwerkelijke verkeersstromen.

KPN wijst op de belangrijke functie die vertrouwensdiensten vervullen en vraagt waarom deze niet zijn opgenomen in de tabel. Ten aanzien hiervan wijs ik erop dat de eIDAS-verordening<sup>5</sup> reeds voorziet in een plicht voor vertrouwensdiensten om incidenten te melden aan (onder meer) het nationale orgaan voor informatieveiligheid. In Nederland is dit krachtens de vanwege deze verordening tot stand gebrachte uitvoeringswetgeving de Minister van Veiligheid en Justitie (en in de praktijk het NCSC).

Daarnaast bepleit KPN een gelijk speelveld voor Nederlandse vertrouwensdiensten ten opzichte van buitenlandse concurrenten. Ten aanzien hiervan wijs ik erop dat, omdat voor alle Europese aanbieders van vertrouwensdienstverleners dezelfde regels gelden, er sprake is van een gelijk speelveld en borging van de veiligheid in de lidstaten van de Europese Unie.

In reactie op een opmerking van Nederland ICT kan ik bevestigen dat de meldplichtige aanbieders na inwerkingtreding van de wet expliciet over hun meldplicht worden geïnformeerd.

Naar aanleiding van allerlei specifieke vragen en opmerkingen zijn de in het besluit vermelde tabel en de nota van toelichting op diverse plaatsen gecorrigeerd en aangevuld.

<sup>5</sup> Verordening (EU) Nr. 910/2014 van het Europees parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257).

## **Artikelsgewijze toelichting**

### **Artikel 1 (tabel)**

#### **Drinkwater**

##### *Aangewezen vitale aanbieders*

In Nederland zijn er momenteel tien drinkwaterbedrijven zoals bedoeld in artikel 1, eerste lid, Drinkwaterwet.

De eigenaren van een collectieve watervoorziening en een collectief leidingnet in de zin van artikel 1, eerste lid, Drinkwaterwet vallen niet onder de meldplicht, onder meer omdat het functioneren daarvan niet afhankelijk is van ICT. Daarnaast zijn collectieve watervoorzieningen en collectieve leidingnetten van beperkte schaal in vergelijking tot openbare drinkwatervoorzieningen en distributienetten, waardoor de effecten van een verstoring relatief klein zullen zijn. Drinkwaterbedrijven kunnen afnemers van collectieve watervoorzieningen «nooddiensten» leveren, waarmee de gevolgen van een verstoring beperkt blijven.

##### *Aangewezen producten en diensten*

Net als met het begrip «drinkwaterbedrijf» wordt met de begrippen «drinkwater» en «openbare drinkwatervoorziening» gedoeld op de betekenis die artikel 1 Drinkwaterwet daaraan geeft.

De dienst waarvoor de meldplicht geldt, is het leveren van deugdelijk drinkwater door middel van een openbare drinkwatervoorziening. Die omschrijving ziet zowel op de leveringszekerheid als op de kwaliteit van drinkwater. De omschrijving is ontleend aan de definitie van «verstoring» in artikel 1 van de Drinkwaterwet: «uitval of aantasting van watervoorzieningswerken, waardoor de continuïteit van de levering van deugdelijk drinkwater wordt verbroken of in gevaar komt».

#### **Energie**

Bij de transmissie en distributie van elektriciteit en gas zijn verschillende partijen betrokken, waaronder producenten, programmaverantwoordelijken, leveranciers, meetbedrijven en netbeheerders. Niet alle partijen die betrokken zijn bij het proces van energielevering dienen onder de meldplicht te vallen. Bepaalde partijen zijn verantwoordelijk voor specifieke processtappen, waarvan redelijkerwijs kan worden aangenomen dat deze niet kritiek zijn voor een betrouwbare levering van de kerndienst. Deze partijen zijn dan ook niet vitaal en vallen daarmee niet onder de reikwijdte van de Wgmc. Dit komt onder meer doordat voor landelijke en regionale netbeheerders geldt dat eerder sprake zal zijn van een «single point of failure». Daarnaast bestaat er een grotere mate van afhankelijkheid tussen de verschillende partijen dan bijvoorbeeld bij partijen die verantwoordelijk zijn voor de productie van elektriciteit. Uitval van dienstverlening bij deze netbeheerders zou eerder kunnen leiden tot ernstige maatschappelijke gevolgen, en wordt om die reden als vitaal gezien. Daarnaast heeft de beheerder van het landelijk gastransportnet een «peakshaver». Deze bestaat uit grote gasopslagtanks die worden ingezet op het moment dat de levering van gas in gevaar dreigt te komen als gevolg van extra vraag bij extreem lage temperaturen. In de winter van 2009–2010 is de peakshaver voor het eerst in lange tijd weer ingezet. Vanwege het single-point-of-failure-karakter van deze peakshaver wordt deze als vitaal gezien.



## **Financiën**

### *Aangewezen vitale aanbieders*

Op grond van het Bmc wijst De Nederlandsche Bank (DNB) de financiële instellingen aan die onder de meldplicht vallen. Hierbij gaat het niet slechts om financiële instellingen als bedoeld in artikel 1:1 van de Wet op het financieel toezicht, maar om een ruimer begrip, namelijk zoals dat in het dagelijks spraakgebruik wordt gehanteerd. Als zodanig zullen worden aangewezen de instellingen die deel uitmaken van de zogeheten financiële kerninfrastructuur (FKI). Dat zijn de instellingen die verantwoordelijk zijn voor de belangrijkste transactiestromen en betaal- en effectenafwikkelingsystemen in Nederland. Dit zijn zowel marktinfrastructuren als deelnemers aan deze infrastructuren. DNB bepaalt jaarlijks op grond van kwantitatieve criteria welke instellingen deel uitmaken van de FKI. Die criteria zijn voor zowel het Retail- (toonbank- en massaal giraal betalingsverkeer) als Wholesale- (hoogwaardig) betalingsverkeer en effectenverkeer op hoofdlijnen gebaseerd op de regel dat de instellingen toegevoegd worden aan de FKI als zij deel uitmaken van de lijst van instellingen die in afnemende omvang van aandeel, cumulatief 80% verwerken van het totale transactievolume of de totale transactiewaarde. Deze regel geldt voor de clearinginstellingen, settlementinstellingen en deelnemers afzonderlijk.

### *Aangewezen producten en diensten*

Met betrekking tot de diensten gelden de volgende overwegingen: Voor het bepalen van de diensten, waarvoor de meldplicht komt te gelden, is zo veel mogelijk aangesloten bij reeds uitgevoerde analyses naar de bescherming van de vitale processen in Nederland. Op basis hiervan is besloten vier hoofdcategorieën van diensten te onderscheiden: 1) toonbankbetalingsverkeer, 2) massaal giraal betalingsverkeer, 3) hoogwaardig betalingsverkeer, en 4) effectenverkeer.

Onder het toonbankbetalingsverkeer (contant en elektronisch) vallen chartale betalingen (betalingen met bankbiljetten en munten), elektronische betalingen met de pinpas (debitcard) en creditcardbetalingen. Hieronder valt ook het opnemen van contant geld (bijv. bij geldautomaten of balies). Webwinkels kunnen gezien worden als «virtuele toonbankinstellingen». Betalingen in webwinkels vinden met name plaats via internetbankieren met behulp van iDEAL of via creditcard.

Tot het massale girale betalingsverkeer («betalen op afstand») dat door de financiële sector wordt afgewikkeld, behoren crediteurenbetalingen (overschrijvingen via internetbankieren, acceptgiro's), incasserende instrumenten (incasso's) en periodieke betalingen (bijv. salarissen, uitkeringen en pensioenen). Ook het toonbankbetalingsverkeer (via betaalautomaten) en de geldopnamen bij geldautomaten en aan de balie worden in de systemen voor massaal giraal betalingsverkeer verwerkt.

Het hoogwaardig betalingsverkeer tussen banken betreft het betalingsverkeer tussen banken en andere kapitaal- en geldmarktbetalingen (waaronder treasury verkeer van grote bedrijven). Voorts valt hieronder de afwikkeling van valutatransacties.

Onder het effectenverkeer valt de gereguleerde handel, de vereffening (clearing) en de afwikkeling (settlement) van effecten- en derivatentransacties. Hieronder vallen zowel de handel door particulieren als door partijen binnen het wholesale segment.

Betalings- en effectenverkeer binnen de verschillende categorieën zijn afhankelijk van elkaar. De toonbankbetalingen via betaalautomaten, geldopnamen bij geldautomaten en geldopnamen aan de balie worden in de systemen voor massaal giraal betalingsverkeer verwerkt. Daarnaast zal langdurige uitval van hoogwaardig betalingsverkeer nadelige gevolgen kunnen hebben voor massaal giraal betalingsverkeer en/of toonbankbetalingsverkeer.

### **Mainport Rotterdam**

#### *Aangewezen vitale aanbieder*

De Divisie Havenmeester, onderdeel van het Havenbedrijf Rotterdam, neemt een centrale functie in binnen Mainport Rotterdam. Het Havenbedrijf Rotterdam zorgt voor de ontwikkeling, aanleg, beheer en exploitatie van het Rotterdamse havengebied. De Divisie Havenmeester is vanuit haar publieke taak verantwoordelijk voor een veilige, vlotte, duurzame en beveiligde afwikkeling van het scheepvaartverkeer in de Rotterdamse haven en het aanloopgebied voor de kust en heeft een eigenstandige verantwoordingsplicht naar de gemeente Rotterdam en het Rijk. Vanuit deze verantwoordelijkheid werkt de havenmeester samen met verschillende andere partijen.

Er zijn diverse partijen die de havenmeester (als de eindaanbieder) ondersteunen in de uitvoering van zijn processen, zoals Rijkswaterstaat, Portbase en verschillende IT-dienstenleveranciers. Deze partijen zijn niet als meldplichtig aangewezen omdat zij geen dienst of product aanbieden aan een eindgebruiker, maar aan de havenmeester.

Indien door de eindaanbieder wordt ingeschat dat een ICT-inbreuk bij dergelijke dienstverleners kan leiden tot een voor hem meldplichtig incident, dient hij de nodige afspraken met dergelijke dienstverleners te maken (bijvoorbeeld met betrekking tot het melden van ICT-inbreuken).

#### *Aangewezen producten en diensten*

De toegankelijkheid van een haven staat of valt bij een vlot en veilig scheepvaartverkeer en een adequate afhandeling van lading. Binnen de Mainport Rotterdam werkt een groot aantal dienstverleners samen om deze mainportfunctie waar te kunnen maken. Hierbij valt te denken aan de havenmeester, loodsen, sleepdiensten, roeiers, douane, terminals, inspectiediensten et cetera. Bij de afwikkeling van het scheepvaartverkeer speelt de havenmeester een centrale rol in het samenbrengen van de dienstverleners en het verschaffen van de voor deze dienstverleners essentiële informatie. Deze spilfunctie is onmisbaar voor het operationeel houden van alle activiteiten die de Mainport Rotterdam tot mainport maakt.

### **Mainport Schiphol**

#### *Aangewezen vitale aanbieders*

De vlucht- en vliegafhandeling is primair een taak van de Luchtverkeersleiding Nederland (LVNL). LVNL is voor civiele luchtverkeersaangelegenheden de schakel tussen de overheid en alle overige partijen die bij luchtverkeersleiding betrokken zijn.

Het faciliteren en regisseren van passagiersafhandeling met bagageafhandeling en vrachtafhandeling is primair een taak van de Royal Schiphol Group N.V. Zij is een internationale luchthavenonderneming met als

belangrijkste activiteit de exploitatie van de luchthaven Schiphol. Ze stelt faciliteiten en noodzakelijke nutsvoorzieningen ter beschikking aan o.a. afhandelaren en luchtvaartmaatschappijen. De passagiersafhandeling met bagageafhandeling en vrachtafhandeling worden door haar ook getypeerd als kritische processen binnen de eigen activiteiten. Het crisismanagement vormt een belangrijk proces binnen het proces passagiersafhandeling met bagageafhandeling.

Vanwege hun grote belang voor een veilige en vlotte vlucht- en vliegtuigafhandeling worden ook Aircraft Fuel Supply B.V., de Koninklijke Marechaussee en de luchtvaartmaatschappijen onder de meldplicht gebracht, waarbij de aanwijzing van luchtvaartmaatschappijen beperkt is tot de bedrijven die minimaal 25% van het totaal aantal vliegbewegingen op Schiphol voor hun rekening nemen. Uitval of verstoring van de dienstverlening van kleinere luchtvaartmaatschappijen zal niet leiden tot maatschappelijke ontwrichting.

#### *Aangewezen producten en diensten*

De aangewezen dienst «een veilige en vlotte vlucht- en vliegtuigafhandeling» is de kerndienst van Mainport Schiphol aan zijn klanten. De dienst omvat het laten landen en stijgen van vliegtuigen op en van Schiphol, dat betrekking heeft op de luchtzijde van Mainport Schiphol waar vliegtuigen landen, taxiën, parkeren en opstijgen, het laten doorstromen van passagiers op Schiphol, dat betrekking heeft op het aankomen, inchecken, grenscontrole, veiligheidscontrole, boarden en goederencontrole in het passagiersverkeer, en het afhandelen van bagage van passagiers op Schiphol, dat betrekking heeft op het afgeven en claimen van bagage door passagiers, het screenen, laden, transporteren en uitladen van bagage door verschillende partijen op Schiphol, en het controleren van bagage door de douane.

### **Nucleair**

#### *Aangewezen vitale aanbieders*

In Nederland is een aantal bedrijven actief in de nucleaire sector die ieder hun eigen karakterisering hebben. Voor de definitie van aanbieders in de sector Nucleair wordt aangesloten bij artikel 15, onder b, van de Kernenergiewet (KEW) alsmede het Geheimhoudingsbesluit Kernenergiewet.

In artikel 15, onder b, KEW is bepaald dat nucleaire installaties voor hun activiteiten een vergunning nodig hebben. Nucleaire installaties zijn volgens de KEW inrichtingen «waarin kernenergie kan worden vrijgemaakt, splijtstoffen kunnen worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen worden opgeslagen». In het Geheimhoudingsbesluit Kernenergiewet is vastgelegd dat, als gegevens zijn verkregen onder een verplichting tot geheimhouding, of door de in het besluit genoemde Ministers zijn aangewezen, diegene die deze informatie heeft, maatregelen moet nemen om de geheimhouding daarvan te verzekeren. De houders van een KEW-vergunning vallen automatisch onder het Geheimhoudingsbesluit. Dat besluit verdient desondanks aparte vermelding in de Bmc-tabel aangezien ook andere bedrijven onder het Geheimhoudingsbesluit vallen.

#### *Aangewezen producten en diensten*

De vitaliteitsbeoordeling van de nucleaire sector wordt in sterke mate beïnvloed door het non-proliferatie-aspect gepaard gaande met (internationaal) politieke gevoeligheid, alsmede de potentiële financiële en sociaal-maatschappelijke gevolgen van een incident. Gezien de potentiële

gevolgen en het unieke karakter van de sector zijn alle nucleaire objecten vallend onder de KEW dan wel het Geheimhoudingsbesluit Kernenergie wet als A-vitaal aangemerkt.

De vitale producten en diensten zijn gericht op de bescherming en beveiliging van inrichtingen als bedoeld in de KEW waarin kernenergie kan worden vrijgemaakt, splijtstoffen kunnen worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen worden opgeslagen of inrichtingen, waarin kernenergie kon worden vrijgemaakt, splijtstoffen konden worden vervaardigd, bewerkt of verwerkt, dan wel splijtstoffen werden opgeslagen. Daarnaast worden bedrijven aangemerkt als vitale aanbieders als deze bedrijven de beschikking hebben over gegevens die noodzakelijk zijn voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges en het produceren van hulpmiddelen en materialen die nodig zijn voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges. Deze gegevens dienen op grond van het Geheimhoudingsbesluit Kernenergie wet uit overwegingen van non-proliferatie geheim te worden gehouden.

### **Elektronische communicatienetwerken of -diensten/ICT**

#### *Het verlenen van een telefoon-, sms- of internettoegangsdienst*

Voor elektronische communicatienetwerken of -diensten zijn aanbieders van elektronische communicatienetwerken of -diensten aangewezen die een netwerk of infrastructuur beheren dat of die direct of indirect wordt gebruikt ten behoeve van het verlenen van een telefoon-, sms- of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers.

Ten eerste gaat het om aanbieders die zelf rechtstreeks diensten leveren aan de eindgebruiker. Zo zijn er momenteel met betrekking tot mobiele communicatie vier landelijk dekkende mobiele netwerken (Vodafone, Tele2, KPN, T-Mobile) die zelf mobiele telefoniediensten aan eindgebruikers aanbieden; zij leveren direct aan eindgebruikers. Omdat bovendien meer dan 1 miljoen eindgebruikers thans van hun telefoon-diensten gebruik maken, behoren zij tot de meldplichtige vitale aanbieders.

Ten tweede gaat het om aanbieders van netwerken en diensten die niet zelf een telefoondienst, sms-dienst of internettoegangsdienst rechtstreeks aanbieden aan eindgebruikers, maar zij kunnen essentieel zijn in de keten van het verlenen van telefoon-, sms- en internetdiensten aan eindgebruikers. Dat is bijvoorbeeld het geval als een aanbieder een netwerk aanbiedt aan een derde partij die het netwerk vervolgens gebruikt om zelf de bedoelde diensten aan te bieden. Hierdoor kan een partij (mede) door zijn activiteiten op de wholesalemarkt onder de reikwijdte van de meldplicht vallen.

Zoals hiervoor aangegeven is er pas sprake van een meldplichtige vitale aanbieder in geval van directe en indirecte dienstverlening aan meer dan 1 miljoen eindgebruikers. Hiervoor is gekozen omdat het bij 1 miljoen eindgebruikers of meer ondoenlijk is om binnen een redelijke termijn (enkele dagen) een alternatief voor die eindgebruikers te vinden.

#### *Het faciliteren van het internet- en dataverkeer*

Voor het goed functioneren van de integrale Nederlandse digitale dienstverlening, waaronder internet, telefonie, sms en datadiensten is het faciliteren van het internet- en dataverkeer dat daarvoor nodig is

essentieel. Dit gebeurt op verschillende manieren. Het grootste deel van het internet- en dataverkeer vindt plaats via bilaterale uitwisseling tussen aanbieders van netwerken onderling, ook wel peer-to-peer-verkeer genoemd.

Tot mogelijk 25% van het totale Nederlandse dataverkeer wordt afgehandeld door zogenoemde internetknooppunten. Een internetknooppunt is een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel het faciliteren van het internetverkeer. Op dit moment nemen twee knooppunten, namelijk AMS-IX en NL-ix, samen het overgrote deel van die facilitering door internetknooppunten voor hun rekening. Uitgedrukt in poortcapaciteit (de som van de capaciteit van de koppelingen naar de infrastructuur) is dit meer dan 90%. Uitval van een van deze twee grote internetknooppunten kan ontwrichtende gevolgen hebben; het wegvallen van zo'n grote capaciteit zal niet direct opgevangen kunnen worden door de restcapaciteit bij andere knooppunten en netwerkaanbieders. In de tabel komt dit tot uitdrukking door de grens te leggen bij een minimale poortcapaciteit van 8 terabit per seconde (tbp/s), wat nu overeenkomt met circa 25% van de totale minimale poortcapaciteit van alle internetknooppunten tezamen. Aanbieders die 8 tbp/s of meer poortcapaciteit ter beschikking stellen, zijn dus meldplichtige vitale aanbieders.

### **Keren en Beheren**

De onder de meldplicht vallende vitale waterkeringen worden krachtens het Bmc aangewezen bij besluit van de Minister van Infrastructuur en Milieu. Als zodanig zullen slechts digitaal aangestuurde objecten worden aangewezen (waterkeringen of onderdelen daarvan).

### **Digitale Overheid**

Blijkens de in paragraaf 1 besproken vitaliteitsbeoordeling zijn de processen van de beschikbaarheid en uitwisseling van betrouwbare basisinformatie, en beschikbaarheid van datasystemen waarvan het functioneren van meerdere overheidsorganisaties afhankelijk is, aangemerkt als onderdeel van de vitale infrastructuur. Momenteel wordt door het Nationaal Beraad Digitale Overheid een beoordeling uitgevoerd welke specifieke aanbieders van tot die processen behorende producten en diensten als vitale aanbieder dienen te worden aangemerkt en met het oog daarop in de tabel in dit besluit moeten worden opgenomen. Op basis van de uitkomst hiervan zal dit besluit daartoe bij de eerstvolgende gelegenheid worden aangevuld.

De Staatssecretaris van Veiligheid en Justitie,