eLaw
Working Paper Series

No 2018/014 - ELAW– 24 April 2019

Een nieuw kader voor network en informatiebeveiliging: een cultuuromslag?

J.P. Kalis and G.P. van Duijvenvoorde

Universiteit Leiden
eLaw

Een nieuw kader voor netwerk- en informatiebeveiliging: een cultuuromslag?
J.P. Kalis LL.M. en prof. mr. G.P. van Duijvenvoorde[1]

Introductie

Veiligheid en beveiliging van netwerk- en informatiesystemen[2] zijn belangrijke speerpunten van de Europese Commissie bij het realiseren van een interne digitale markt. In 2016 is een richtlijn van kracht geworden waarin wordt beoogd een hoger niveau van beveiliging van netwerk- en informatiesystemen van vitale infrastructuur te bereiken (hierna NIB-richtlijn).[3] De NIB-richtlijn introduceert een *governance*-kader en een systeem waarin het uitwisselen van informatie tussen de betrokken instanties en het melden van incidenten centraal staat. Via zogenoemde *just culture* wordt gestreefd een beveiligingscultuur te bereiken waarin het leren van incidenten vooropstaat. De implementatie van de NIB-richtlijn in de Nederlandse wetgeving – uiterlijk op 10 mei 2018 – zal voor een breed palet aanbieders relevant zijn.[4] Deze implementatie zal plaatsvinden in de Cybersecuritywet (Csw), waartoe begin 2018 een voorstel bij de Tweede Kamer is ingediend.[5] Met de onlangs in werking getreden Wet gegevensverwerking en meldplicht cybersecurity[6] (Wgmc) zijn echter ook al voor de implementatie relevante stappen gezet. De Wgmc heeft namelijk al met de Csw vergelijkbare meldplichten van ICT-incidenten[7] geïntroduceerd en heeft krachtens een algemene maatregel van bestuur specifieke meldplichtige vitale aanbieders aangewezen. Het is de bedoeling dat deze regeling straks onderdeel wordt van de Csw. Om deze reden staan in deze bijdrage beide wetten centraal. Daarnaast zullen de belangrijkste aspecten van de NIB-richtlijn worden besproken en wordt ingegaan op de relatie met reeds bestaande meldplichten en de beveiligingsverplichtingen in de telecommunicatiesector.[8]

Achtergrond

Regulering van beveiliging van netwerk- en informatiesystemen in de EU is geen nieuw verschijnsel. Het Europese regelgevend kader voor de telecommunicatiesector bevat reeds sinds

---

[1] J.P. (Pieter) Kalis is werkzaam als promovendus Telecommunicatierecht bij het Centrum voor Recht en Digitale Technologie (eLaw) aan de Universiteit Leiden. Prof. mr. G.P. (Gera) van Duijvenvoorde is als bijzonder hoogleraar Telecommunicatierecht verbonden aan eLaw van de Universiteit Leiden. Zij werkt daarnaast als advocaat-in-dienstbetrekking bij KPN.
[2] Hiermee wordt voornamelijk bedoeld: computers en ICT-systemen en -netwerken.
[3] 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 (NIB-richtlijn), *PbEU* 2016, L 194/1.
[4] Art. 25 lid 1 NIB-richtlijn.
[5] Voorstel van wet, Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet), *Kamerstukken II* 2017/18, 34883, 2.
[6] Wet van 25 juli 2017, houdende 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), *Stb*. 2017, 316.
[7] Gedefinieerd als ‘een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen’.
[8] Aangezien elektronische communicatienetwerken ook worden geschaard onder netwerk- en informatiesystemen, volgens art. 4 lid 1 sub a NIB-richtlijn, worden de laatste ontwikkelingen in deze gebieden hier samen besproken.

2009 specifieke beveiligingseisen en meldplichten[9] voor ondernemingen die openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten aanbieden. In het kort gezegd zijn deze aanbieders verplicht om passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen, en de integriteit en continuïteit daarvan te waarborgen. Daarnaast moeten zij inbreuken op de veiligheid of elk verlies van integriteit van deze netwerken en diensten met een belangrijke *impact* melden aan de bevoegde instanties.[10] Deze beveiligingsverplichtingen hebben als voorbeeld gediend voor de met de NIB-richtlijn geïntroduceerde beveiligingseisen en meldplichten voor de ICT-infrastructuur van aanbieders van diensten die essentieel zijn voor de economie en maatschappij van de EU. Deze worden hieronder besproken.

Nu zijn de eerste initiatieven voor regulering van vitale infrastructuren al veel eerder genomen. Reeds in 2001 benadrukte de Europese Commissie de noodzaak van regelgeving op het gebied van beveiliging van ICT-systemen van vitale infrastructuur en verscheen het eerste voorstel voor een beleidsaanpak op dit punt.[11] Regulering van de veiligheid van vitale infrastructuur en telecommunicatie valt onder de internemarktregulering.[12] In 2013 werd een voorstel[13] gepubliceerd voor een NIB-richtlijn.[14] Deze publicatie werd tegelijkertijd gepubliceerd met de EU-cyberbeveiligingsstrategie[15] en maakt daarvan deel uit. Deze richtlijn en strategie zijn vervolgens een belangrijk onderdeel geworden van de beleidsstrategie van de EU. De Europese Commissie heeft in 2015 haar beleidsstrategie gepubliceerd voor het tot stand brengen van een interne digitale markt (Digital Single Market of DSM).[16] Het stimuleren van de ontwikkeling van digitale

[9] Zie Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronischecommunicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronischecommunicatienetwerken en -diensten, *PbEU* 2009, L 337/37. In verband met de bescherming van persoonsgegevens waren er in 2002 al beveiligingsverplichtingen neergelegd in Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie), *PbEU* 2002, L 201/37.

[10] Zie art. 13bis Richtlijn 2009/140/EG. Deze verplichtingen zijn in de Nederlandse Telecommunicatiewet (Tw) geïmplementeerd in de art. 11.3 en 11.3a Tw over de bescherming van persoonsgegevens en persoonlijke levenssfeer, en de art. 11a.1 en 11a.2 Tw over de beveiliging en het waarborgen van de continuïteit van netwerken en diensten.

[11] Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's, Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak COM(2001)298 definitief.

[12] Zie art. 114 Verdrag betreffende de werking van de Europese Unie (VWEU).

[13] Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM(2013)48 final.

[14] Voor een uitgebreide behandeling van het voorstel zie J. Toet en A.R. Lodder, 'Voorstel richtlijn netwerkveiligheid als onderdeel van EU cyber security-strategie: naar een open, veilig en betrouwbaar internet?', *NtEr* 2014/2-3, p. 89-97.

[15] Gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace, JOIN(2013)1 final.

[16] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Strategie voor een digitale eengemaakte markt

netwerken en diensten, en het vergroten van het vertrouwen en de veiligheid op dit gebied, staan voorop in deze strategie.[17] Het reguleren van beveiliging van netwerk- en informatiesystemen en gegevensbescherming (anders dan persoonsgegevens) is inmiddels een prominent onderdeel van de Digital Single Market strategie. Op 6 juli 2016 is de NIB-richtlijn aangenomen[18] en op 8 augustus 2016 is ze in werking getreden.[19]

De Richtlijn beveiliging van netwerk- en informatiesystemen (NIB-richtlijn)

De inhoud van de NIB-richtlijn zal in dit artikel op hoofdlijnen worden weergegeven.[20] De richtlijn heeft drie centrale doelstellingen. De eerste doelstelling is het voorzien in een *governance*-kader voor aanbieders van essentiële diensten en digitaledienstverleners (zie hieronder) waarin beveiligingseisen en meldplichten van ICT-inbreuken centraal staan. Hierbij moet iedere lidstaat een nationale beveiligingsstrategie[21] geïmplementeerd hebben, en ten minste één nationale bevoegde autoriteit[22] en ten minste één *computer security incident response team*[23] (CSIRT) aangewezen hebben voor de toepassing van de verplichtingen van de richtlijn. De tweede doelstelling is het bereiken van een tweede een hoger nationaal niveau van beveiliging van netwerk- en informatiesystemen in de lidstaten door middel van minimumharmonisatie.[24] Dit wil zeggen dat een aantal minimumeisen wordt gesteld die alle lidstaten moeten implementeren in hun nationale wetgeving. Uitdrukkelijk wordt toegestaan (en aangemoedigd) een hoger niveau van beveiliging na te streven dan voorgeschreven door de richtlijn, maar lidstaten mogen geen lager niveau hebben. Zo wordt de mogelijkheid opengehouden dat lidstaten ook andere organisaties onder de reikwijdte van de richtlijn brengen.[25] De derde doelstelling betreft de samenwerking: de richtlijn bevat veel bepalingen die gaan over de (Europese) samenwerking en communicatie op het gebied van netwerk- en informatiebeveiliging en het bevorderen van 'cultuur van risicobeheer'[26] tussen de verschillende instanties, onder andere door middel van het uitwisselen van informatie.[27]
Zo dient elke lidstaat een centraal contactpunt[28] te hebben die een samenwerkingsfunctie vervult met andere lidstaten, er is een samenwerkingsgroep[29] (hierna NIS-samenwerkingsgroep)[30]

---

voor Europa, COM(2015)192 final. De grondslagen voor dit beleid vormen de art. 3, 26 jo. 114 VWEU.
[17] Strategie voor een digitale eengemaakte markt voor Europa, p. 4 en p. 13-14.
[18] NIB-richtlijn.
[19] Zie art. 26 NIB-richtlijn.
[20] Voor een uitgebreide behandeling van de NIB-richtlijn, zie J.P. Kalis, 'De Netwerk- en beveiligingsrichtlijn', *Computerrecht* 2017/48, afl. 2, p. 61-66.
[21] Art. 7 NIB-richtlijn.
[22] Art. 8 lid 1-2 en lid 5-7 NIB-richtlijn.
[23] Art. 9 NIB-richtlijn. CSIRT is een nieuwe term voor *Computer Emergency Response Teams* (CERTs), ofwel computercrisisteams.
[24] Art. 3 NIB-richtlijn.
[25] Mededeling van de Commissie aan het Europees Parlement en de Raad, De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, COM(2017)476 final, p. 5.
[26] Zie NIB-richtlijn overweging 5.
[27] Art. 1 NIB-richtlijn.
[28] Art. 8 lid 3-7 NIB-richtlijn.
[29] Art. 11 NIB-richtlijn.
[30] In recente mededelingen van de Commissie wordt gerefereerd aan de samenwerkingsgroep onder de naam 'NIS-samenwerkingsgroep', zie bijvoorbeeld Mededeling van de Commissie aan het

opgericht met als primaire taak de uitwisseling van informatie en het stimuleren van vertrouwen tussen de lidstaten, en er is een CSIRTs-netwerk[31] opgericht voor operationele samenwerking tussen de lidstaten.
De richtlijn verplicht de lidstaten zorg te dragen voor beveiligingseisen en meldplichten voor aanbieders van essentiële diensten[32] en digitaledienstverleners.[33] De essentiële diensten behoren tot zeven in de NIB-richtlijn gespecificeerde vitale sectoren van de economie, te weten de sectoren energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater, en digitale infrastructuur.[34] Opvallend is dat de telecommunicatiesector niet onder de richtlijn valt.[35] Lidstaten dienen te bepalen welke entiteiten onder de definitie van aanbieders van essentiële diensten moeten worden geschaard en als zodanig moeten worden aangewezen zodat ze onder de reikwijdte van de richtlijn vallen.[36] Er is evenwel geen aanwijzingssystematiek voor de digitaledienstverleners. Onder deze groep dienstverleners vallen de aanbieders van online marktplaatsen, online zoekmachines of *cloud computer*-diensten. Zij behoeven evenwel niet door de lidstaten te worden aangewezen: iedere onderneming die als digitaledienstverlener werkzaam is, valt automatisch onder het bereik van deze richtlijn. De NIB-richtlijn schrijft voor dat de lijst iedere twee jaar door de lidstaten geëvalueerd moet worden, en waar nodig moet worden geactualiseerd.[37]
De aanbieders van essentiële diensten en de digitaledienstverleners dienen alleen 'ernstige' ICT-incidenten te melden bij de bevoegde autoriteit of het CSIRT. De richtlijn biedt enkele algemene handvatten om te bepalen welke incidenten ernstig genoeg zijn om te moeten melden,[38] maar dit zal zowel op nationaal niveau (zie hieronder) als op Unieniveau[39] later nog gespecificeerd worden. Let wel dat het bij ICT-incidenten niet alleen gaat om moedwillige aanvallen. Uit de richtlijn valt op te maken dat ook incidenten ten gevolg van menselijke fouten of incidenten die de beschikbaarheid van gegevens of diensten in gevaar brengen, voor zover deze incidenten 'aanzienlijke gevolgen voor de continuïteit van de diensten' hebben, gemeld moeten worden.[40]
De meldplicht heeft als algemeen doel het voorkomen dan wel beheersen van beveiligingsincidenten. Hiertoe heeft de meldplicht de volgende specifieke functies. Ten eerste biedt een melding van een beveiligingsincident de bevoegde autoriteit of het CSIRT de

---

Europees Parlement, de Europese Raad en de Raad. Vierde voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie, COM(2017)41 final, p. 7.
[31] Art. 12 NIB-richtlijn.
[32] Art. 14 NIB-richtlijn en bijlage II.
[33] Art. 16 NIB-richtlijn en bijlage III.
[34] Zie NIB-richtlijn bijlage II.
[35] Zie art. 4 lid 1 sub a NIB-richtlijn. Hoewel een elektronisch communicatienetwerk onder de definitie valt van een netwerk- en informatiesysteem, valt de telecomsector buiten de reikwijdte van de richtlijn omdat de sector reeds eigen beveiligingseisen en meldplichten kent. De afbakening met de aanbieders van digitale infrastructuren verdient aandacht. Zo valt een internetknooppunt onder de sector van digitale infrastructuur terwijl het aanbieden van interconnectie van fysieke netwerken op basis van een interconnectie-overeenkomst als telecommunicatiedienst onderhevig is aan de regelgeving voor de sector elektronische communicatie. Zie Bijlage bij Mededeling van de Commissie aan het Europees Parlement en de Raad, De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, COM(2017)476 final ANNEX 1, p. 21-22.
[36] Art. 5 NIB-richtlijn en bijlage II.
[37] Zie art. 5 lid 5 NIB-richtlijn.
[38] Art. 14 lid 4 en art. 16 lid 4 NIB-richtlijn.
[39] Zie bijvoorbeeld art. 14 lid 7 NIB-richtlijn.
[40] Zie hierbij art. 4 lid 2 jo. art. 14 en 16 NIB-richtlijn. Zie eveneens Overweging 3.

mogelijkheid om snel te kunnen bepalen of er sprake is van grensoverschrijdende gevolgen, om zo de andere getroffen lidstaten in te kunnen lichten.[41] Een tweede doel is het centraal verzamelen van informatie over incidenten ten behoeve van de ontwikkeling van de capaciteiten en het kennisniveau van de lidstaten. Zo moet er ieder jaar door het centrale contactpunt een samenvatting naar de NIS-samenwerkingsgroep gestuurd worden over het aantal en de typen gemelde incidenten en de uitvoering na een incident van de door de NIB-richtlijn voorgeschreven handelingen.[42] Hierbij werkt de NIS-samenwerkingsgroep nauw samen met het Europees agentschap voor netwerk- en informatiebeveiliging (ENISA).[43] ENISA publiceert geregeld nuttige openbaar toegankelijke informatie over beveiligingsincidenten, beste praktijken en vele andere documenten die dieper op de materie ingaan.[44]
Meldingen moeten vertrouwelijk kunnen worden gedaan om eventuele bedrijfsgevoelige informatie te beschermen.[45] Ook biedt artikel 20 NIB-richtlijn de mogelijkheid vrijwillig melding te maken van inbreuken, ook voor entiteiten die niet onder de reikwijdte van de richtlijn vallen. Kleine en micro-ondernemingen zijn bijvoorbeeld uitgesloten van de reikwijdte van de richtlijn,[46] maar het is niet ondenkbaar dat kleinere bedrijven ook te maken kunnen krijgen met ernstige ICT-incidenten.
Bij een melding worden eventuele getroffen andere lidstaten geïnformeerd,[47] wordt wanneer mogelijk relevante follow-up informatie aan de meldende partij verstrekt,[48] en wordt zo nodig het publiek geïnformeerd.[49] Een melding is dus primair bedoeld om informatie te verschaffen en te delen. Mocht er vermoeden zijn van een misdrijf, dan zal er overleg en samenwerking plaatsvinden tussen de bevoegde nationale autoriteit en het centrale contactpunt en de relevante rechtshandhavingsinstanties.[50] De richtlijn voorziet verder niet in regelingen ter bestrijding van hackers of andere cybercrime.[51]
Een melding zal niet leiden tot *verhoogde* aansprakelijkheid van de meldende partij.[52] Hiermee lijkt te worden bedoeld dat de enkele handeling van de melding geen verhoging van de aansprakelijkheid tot gevolg heeft ten opzichte van hetgeen mogelijk al van toepassing is ten aanzien van, bijvoorbeeld, de schade.[53]
De NIB-richtlijn laat enkele specifieke implementatiekeuzes aan de lidstaten. Elke lidstaat moet één of meer nationale bevoegde autoriteiten aanwijzen. Men onderscheidt ruwweg twee soorten aanpak: de gedecentraliseerde en de gecentraliseerde aanpak.[54] De gedecentraliseerde aanpak wordt gekenmerkt door een sectorspecifieke aanpak, waarbij iedere sector een aparte eigen autoriteit

[41] Art. 14 lid 3 en art. 16 lid 3 NIB-richtlijn.
[42] Art. 10 lid 3 NIB-richtlijn.
[43] Zie bijvoorbeeld art. 11 lid 2 en lid 3 sub c NIB-richtlijn.
[44] Zie <www.enisa.europa.eu/publications>.
[45] Art. 1 lid 5, art. 14 lid 5 en art. 16 lid 6 NIB-richtlijn.
[46] Zie art. 16 lid 11 NIB-richtlijn, ook voor de definitie van zulke ondernemingen.
[47] Art. 14 lid 5 en art. 16 lid 6 NIB-richtlijn.
[48] Art. 14 lid 5 NIB-richtlijn.
[49] Art. 14 lid 6 en art. 16 lid 7 NIB-richtlijn.
[50] Art. 8 lid 6 NIB-richtlijn.
[51] Zie hiervoor bijvoorbeeld Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, *PbEU* 2013, L 218/8.
[52] Art. 14 lid 3 en art. 16 lid 3 NIB-richtlijn,
[53] Zie de paragraaf over de Wgmc hieronder voor meer detail.
[54] Mededeling van de Commissie aan het Europees Parlement en de Raad, De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, COM(2017)476 final, en de Bijlage bij deze Mededeling, COM(2017)final ANNEX 1, p. 11e.v.

heeft. De Commissie waarschuwt bij deze aanpak dat samenwerking tussen de verschillende sectoren van belang is om de onderlinge verschillen niet te groot te laten worden. Een gecentraliseerde aanpak kent één enkele autoriteit voor alle sectoren, en de implementatie vindt plaats door middel van een enkel stuk wetgeving. Verder stelt de NIB-richtlijn dat de *Computer Security Incident Response Teams* (CSIRT's) binnen een bevoegde autoriteit mogen worden opgezet (art. 9 lid 1 NIB-richtlijn). Lidstaten mogen ten slotte beslissen dat CSIRT's geen meldingen van incidenten mogen ontvangen (art. 10 lid 2 NIB-richtlijn).

Implementatie van de NIB-richtlijn in Nederland

De NIB-richtlijn moet door de lidstaten vóór 10 mei 2018 in de nationale wetgeving zijn geïmplementeerd. De implementatie van de NIB-richtlijn in de Nederlandse wet zal geschieden door middel van de Csw. Vooruitlopend op de implementatie van de NIB-richtlijn is gefaseerd de Wgmc in werking getreden.[55] De Wgmc is strikt genomen geen directe implementatie van de NIB-richtlijn, maar bevat onderdelen die in de Csw zullen opgaan. Daarom is de Wgmc ook relevant om in het kader van de implementatie van de NIB-richtlijn te bespreken. Op basis van de Wgmc kunnen vitale aanbieders worden aangewezen.[56] Deze aanwijzing heeft plaatsgevonden in het Besluit meldplicht cybersecurity[57] (hierna: het Besluit). Het is de bedoeling dat de Wgmc weer wordt ingetrokken als de Csw van kracht wordt. De Wgmc geeft een invulling van de meldplichten van vitale aanbieders. Dit onderdeel zal op termijn geheel en ongewijzigd worden geïntegreerd in de Csw en worden ingetrokken. De Csw zal zodoende, onder meer, de beveiligingsverplichtingen en meldplichten bevatten voor vitale aanbieders uit de Wgmc.
Hieronder zullen de Wgmc, het Besluit, de Csw en de nieuwe telecomregulering worden besproken in het licht van en in relatie tot de NIB-richtlijn. Het voornaamste doel hiervan is om met dit overzicht inzicht te geven in welke meldplichten er gelden voor welke aanbieders.
Hierbij moet voor de duidelijkheid worden vermeld dat de NIB-richtlijn specifieke categorieën van 'aanbieders van essentiële diensten' gebruikt, en de Wgmc de term 'vitale aanbieders' hanteert. De Csw bevat bepalingen voor beide. Deze termen lijken op elkaar maar zijn, zoals hieronder ook nader zal worden toegelicht, niet gelijk of inwisselbaar. Het is dus, zoals ook uit onderstaand overzicht zal blijken, van belang om in de implementatiewet per regeling goed in ogenschouw te nemen wie als welk type aanbieder precies is aangewezen en moet voldoen aan welke bepalingen.

De Wgmc

Gefaseerde inwerkingtreding

De Wgmc is in twee delen in werking getreden, deels op 1 oktober 2017[58] en in z'n geheel op 1 januari 2018.[59] Het deel dat op 1 oktober 2017 in werking is getreden geeft een wettelijke grondslag

[55] Zie volgende paragraaf.
[56] Een vitale aanbieder is een 'aanbieder van een product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving', zie art. 1 Wgmc. Welke aanbieders dat in de praktijk zijn, moet worden bepaald door deze aan te wijzen.
[57] Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-inbreuken te melden (Besluit meldplicht cybersecurity), *Stb.* 2017, 476.
[58] *Stb*. 2017, 347. De nota van toelichting stelt dat een wet dient in te gaan op 1 januari of 1 juli. Het deel van de Wgmc dat op 1 oktober in werking treedt, bevat geen tot derden gerichte verplichtingen, en men vond een uitzondering op zijn plaats om haast te maken met duidelijkheid verschaffen over de taken en bevoegdheden van het NCSC.
[59] *Stb*. 2017, 477.

aan de taken en bevoegdheden van het Nationaal Cyber Security Centrum (NCSC). Dit deel (namelijk de art. 1 t/m 4 en 9 t/m 11) is eerder in werking getreden om snel duidelijkheid te scheppen over de taken en bevoegdheden van het NCSC. Het tweede deel (de art. 5 tot en met 8), dat op 1 januari 2018 in werking is getreden, bevat de meldplicht van aangewezen vitale aanbieders. Deze artikelen hebben een meldplicht van inbreuken op de veiligheid of een verlies van integriteit van hun ICT-systemen geïntroduceerd. De aangewezen vitale aanbieders dienen ernstige ICT-incidenten te melden bij het NCSC. Welk soort inbreuken ernstig genoeg is om onder de meldplicht te vallen, zal op een later tijdstip nader worden bepaald, aldus de memorie van toelichting van de Wgmc.[60]

Taken van het NCSC

De Wgmc voorziet allereerst in een wettelijke grondslag voor de taken van het NCSC. De voornaamste taken van het NCSC zijn het bijstaan, informeren en adviseren van vitale aanbieders en aanbieders die onderdeel zijn van de rijksoverheid omtrent beveiligingsmaatregelen, dreigingen en incidenten. Daarnaast doet het NCSC onderzoek en verstrekt het relevante informatie aan de bevolking, computercrisisteams, en aan internetproviders.[61] Ook bevat de Wgmc een kader voor de gegevensverwerking. Als uitgangspunt voor de verwerking van persoonsgegevens door het NCSC geldt dat alleen die gegevens worden verwerkt die nodig zijn voor het uitvoeren van die taken. De Wgmc voorziet ook in een grondslag voor de verwerking van andere gegevens, zoals over *malware* of kwetsbaarheden. Ook voorziet de Wgmc in een grondslag voor het opvragen van noodzakelijke gegevens.[62] De minister Justitie en Veiligheid is verantwoordelijk voor deze verwerking.[63]

Meldplicht

Daarnaast introduceert de Wgmc een meldplicht van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna: ICT-inbreuken). Overigens stamt het Nederlandse initiatief voor een meldplicht voor ICT-inbreuken reeds van voor het voorstel voor de NIB-richtlijn uit 2013 en de Wgmc. Een dergelijke meldplicht werd al aangekondigd in een brief aan de Tweede Kamer uit 2012,[64] voor 'organisaties betrokken bij voor de samenleving vitale informatiesystemen',[65] naar aanleiding van de ICT-inbreuk bij Diginotar van 2011. De meldplicht in de Wgmc geldt in beginsel alleen voor bij het Besluit aangewezen (categorieën van) vitale aanbieders en voor aanbieders die onderdeel zijn van de rijksoverheid. Er is geen regeling voor vrijwillige melding door partijen die buiten de reikwijdte van de Wgmc vallen.[66] De melding moet worden gedaan aan de staatssecretaris van Justitie en Veiligheid en wordt behandeld door het NCSC. In de uitvoering van de taken van het NCSC, dus ook in de behandeling van ontvangen meldingen van ICT-inbreuken, moet de vertrouwelijkheid van de gegevens met betrekking tot de aanbieder gewaarborgd worden.[67]

---

[60] *Kamerstukken II* 2015/16, 34388, 3, p. 17.
[61] Zie art. 2 Wgmc.
[62] Zie art. 9 Wgmc.
[63] Zie art. 2 Wgmc.
[64] *Kamerstukken II* 2012/13, 26643, 247.
[65] *Kamerstukken II* 2012/13, 26643, 247, p. 2. Deze komen in de kern overeen met de in het Besluit aangewezen vitale sectoren, zie hieronder.
[66] Partijen die binnen de reikwijdte vallen, mogen incidenten die strikt genomen niet onder de meldplicht vallen wel vrijwillig melden, zie Mvt Wgmc, p. 3.
[67] Art. 9 Wgmc. Dit teneinde onder meer schade aan de reputatie of de concurrentiepositie van de getroffen organisatie zo veel mogelijk te voorkomen, zie MvT Wgmc, p. 6 en 9-10.

ICT-inbreuken kunnen allerlei oorzaken hebben, en die oorzaken veranderen en evolueren ook in hoog tempo. Het delen van tijdige en accurate informatie over ICT-inbreuken is daarom van groot belang voor alle vitale aanbieders. De meldplicht heeft hierbij een dubbel doel. Enerzijds kan een meldplicht duidelijkheid verschaffen over de gevolgen en de potentiële maatschappelijke ontwrichting van een ICT-inbreuk. Anderzijds kan het NCSC naar aanleiding van een inbreuk hulp verschaffen en adviseren, informeren en waarschuwen, en anticiperen op bredere effecten van een inbreuk. Deze taken van het NCSC in geval van een ICT-inbreuk zijn beschreven in artikel 2 Wgmc. De meldplicht is primair gericht op hulp, en op het faciliteren van het NCSC in zijn taak als een informatieknooppunt voor alle betrokken partijen, zowel nationaal als internationaal, aldus de memorie van toelichting van de Wgmc[68] (zie ook art. 2 Wgmc). Onder de Csw krijgt de meldplicht een bredere functie, namelijk tevens het door de centrale contactpunten delen van informatie met de NIS-samenwerkingsgroep over gemelde incidenten (zie de paragraaf over de Csw hieronder) teneinde beste praktijken te delen en het kennisniveau te verhogen, en daarmee bij te dragen tot een hoger algemeen niveau van beveiliging in de Unie.
In het kader van het bewerkstelligen van een dergelijk hoog niveau van beveiliging haalt de wetgever het principe van '*just culture*' (oftewel 'cultuur van billijkheid') uit de luchtvaartsector aan.[69] Dit principe houdt in dat fouten die betrekking hebben op de veiligheid van het vliegverkeer (gemaakt door bijvoorbeeld piloten) gemeld kunnen worden zonder dat de melder gestraft wordt voor zijn of haar fouten (binnen redelijke grenzen).[70] De vergelijking gaat enigszins mank. ICT-inbreuken zijn immers niet per se het gevolg van een fout van de melder. Ook stelt de Wgmc[71] nergens dat een melding van een ICT-inbreuk een vermindering van aansprakelijkheid inhoudt. De Wgmc vermeldt niets over de relatie tussen meldplicht en aansprakelijkheid.[72] In vergelijking met de NIB-richtlijn[73] is dit opvallend,[74] gezien de bepaling in de richtlijn die stelt dat een melding niet zal leiden tot verhoogde aansprakelijkheid van de meldende partij. Een vergelijkbare situatie kan men vinden in de gezondheidszorg. Volgens de Gedragscode openheid medische incidenten (GOMA) staat de melding van een fout door de zorgaanbieder aan de patiënt niet gelijk aan civielrechtelijke aansprakelijkheid.[75] Zo ook bij melding van een ICT-inbreuk. Niettemin brengen de beveiligingseisen in de richtlijn een zorgplicht met zich mee en zou bij een ICT-inbreuk sprake kunnen zijn van schending van die zorgplicht. In later onderzoek kan alsnog vast komen te staan dat er sprake is van aansprakelijkheid, maar de melding op zich is dus geen schuldbekentenis. Toch spreekt de memorie van toelichting, met *just culture* als leidraad, de hoop uit dat de meldplicht kan

[68] Zie MvT Wgmc, p. 2.
[69] Verordening (EU) nr. 376/2014 van het Europees Parlement en de Raad van 3 april 2014 inzake het melden, onderzoeken en opvolgen van voorvallen in de burgerluchtvaart en tot wijziging van Verordening (EU) nr. 996/2010 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2003/42/EG van het Europees Parlement en de Raad en de Verordeningen (EG) nr. 1321/2007 en (EG) nr. 1330/2007 van de Commissie, *PbEU* 2014, L 122/18.
[70] Verordening (EU) nr. 376/2014; de definitie wordt gegeven in art. 2 lid 12: '"cultuur van billijkheid": een cultuur waarbij eerstelijnspersoneel of andere personen niet worden gestraft voor hun acties, nalatigheden of beslissingen die in overeenstemming zijn met hun ervaring en opleiding, maar waarbij grove nalatigheid, opzettelijke overtredingen en destructieve handelingen niet worden getolereerd'.
[71] Evenals de Csw, zie hieronder.
[72] Zie MvT Wgmc, p. 2.
[73] De Wgmc is strikt genomen niet gebaseerd op de NIB-richtlijn, maar het vergelijken met de Wgmc is in verband met de implementatie in de Csw toch interessant.
[74] De Csw bevat ook geen bepalingen over aansprakelijkheid in dit kader, zie hieronder.
[75] Zie Gedragscode Openheid medische incidenten; betere afwikkeling Medische Aansprakelijkheid (GOMA), p. 14. Te vinden op <https://deletselschaderaad.nl/downloads/GOMA1.pdf>, laatst bezocht 16 april 2018.

bijdragen tot een cultuur van gezamenlijk bijdragen aan veiligheid, waarin samenwerking[76] centraal staat.
De memorie van toelichting verduidelijkt wat moet worden verstaan onder 'te melden ICT-inbreuken'. In de NIB-richtlijn worden andere criteria gehanteerd dan in de Wgmc. In de richtlijn wordt de ondergrens om te melden vooral gerelateerd aan de gevolgen van een incident. De wet doet dat in principe ook maar gaat daarnaast ook in op de aard van incidenten. De uitleg die gehanteerd wordt, is dat enkel 'een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit' van een ICT-systeem geldt als te melden inbreuk. Daarnaast gaat het om inbreuken 'die een serieuze bedreiging voor de Nederlandse samenleving inhouden'. Dit brengt met zich mee dat incidenten naar aanleiding van zogeheten *distributed denial-of-service* (DDoS)[77] aanvallen, of 'een interne fout van een medewerker' niet als te melden ICT-inbreuk gelden tenzij er door die fout een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van het betreffende ICT-systeem mogelijk werd. De ondergrens voor het moeten melden wordt gesteld bij inbreuken waarbij ten eerste de 'beschikbaarheid of betrouwbaarheid' van het product of de dienst 'in belangrijke mate' kan worden of wordt onderbroken, en welke ten tweede zou kunnen leiden tot 'maatschappelijke ontwrichting'. De memorie van toelichting legt uit dat DDoS-aanvallen een 'eenvoudig karakter' hebben en slechts een 'tijdelijke beperking van de bereikbaarheid' zullen veroorzaken, en dat daardoor niet gesproken kan worden van een onderbreking in belangrijke mate en maatschappelijke ontwrichting. De meldplicht ziet enkel op ICT-inbreuken in vitale processen.[78] ICT-inbreuken in niet-vitale processen van de bedrijfsvoering van vitale aanbieders vallen niet onder de meldplicht, net zo min als andere inbreuken dan in ICT-systemen. Een voorbeeld is de ICT van de winkels op Schiphol (dat dus geen vitaal proces ondersteunt), in vergelijk met bijvoorbeeld de ICT die gebruikt wordt voor passagiersafhandeling (dat wel tot de vitale processen behoort[79]).
De vertrouwelijkheid ten opzichte van derden van de aan het NCSC gemelde, of anderszins verkregen, gegevens over incidenten en kwetsbaarheden van ICT-systemen is van groot belang.[80] Dit is noodzakelijk om te voorkomen dat het NCSC in zijn taken wordt gehinderd door het mogelijk vroegtijdige openbaar worden van de gegevens, bijvoorbeeld bij het verlenen van hulp bij incidenten. Men kan zich voorstellen dat een grote ICT-inbreuk bij een bank[81] de nodige paniek kan veroorzaken bij het publiek. Een run op de bank kan de ICT-infrastructuur nog verder belasten, wat het oplossen van het probleem kan bemoeilijken. Het kan raadzaam zijn eerst hulp te verlenen alvorens men naar buiten treedt met het nieuws van een inbreuk. Ook dienen hiermee de belangen van betrokken aanbieders beschermd te worden.[82] Er dient voorkomen te worden dat deze aanbieders door het niet waarborgen van de vertrouwelijkheid schade lijden, zoals reputatieschade, benadeling van de concurrentiepositie en een toegenomen kwetsbaarheid voor aanvallen.[83] Onvoldoende waarborgen zouden kunnen leiden tot een terughoudendheid bij het melden van incidenten door aanbieders in vitale sectoren. Het NCSC heeft geen toezichts- of handhavingsbevoegdheden en is voor informatie voor een belangrijk deel afhankelijk van dergelijke

[76] Met name publiek-private samenwerking, zie MvT Wgmc, p. 2.
[77] Een DDoS-aanval is een manier om een website of computersysteem tijdelijk onbereikbaar te maken door het te overspoelen met informatie afkomstig van een netwerk van computers.
[78] Dit zijn alle processen die noodzakelijk voor het verlenen van de vitale dienst.
[79] Zie bijvoorbeeld de 'Herijkte lijst vitale infrastructuur', *Kamerstukken II* 2014/15, 30821, 23, p. 5.
[80] Met name opdat dat men niet terughoudend wordt bij het melden van incidenten. Zie MvT Wgmc, p. 9.
[81] Voor zover het een kredietinstelling betreft die valt onder de reikwijdte van de NIB-richtlijn, zie Annex II van de richtlijn.
[82] Zie MvT Wgmc, p. 9.
[83] Zie MvT Wgmc, p. 12.

meldingen. Er wordt dan ook, ondanks dat melden verplicht is, naar een balans gezocht in het belang van communicatie en uitwisseling aan de ene kant en vertrouwelijkheid aan de andere kant. Voorkomen dient te worden dat bedrijven niet toch eieren voor hun geld kiezen bij een ICT-inbreuk, en die verborgen proberen te houden.[84]

Relatie met meldplichten in andere sectoren

De memorie van toelichting benadrukt dat, hoewel verscheidene sectoren zoals de sector van banken en financiële instellingen[85] of de luchtvaartsector en natuurlijk de telecommunicatiesector, reeds meldplichten aan de desbetreffende sectorale toezichthouders kennen, deze meldplichten niet in de plaats mag komen van de meldplicht neergelegd in de Wgmc.[86] Het argument is dat sectorale meldplichten vaak enkel tot doel hebben de toezichthouder in staat te stellen de naleving van de wettelijke zorgplichten te toetsen.[87] Toch moet gewaakt worden dat de regeldruk niet te groot wordt (wat de memorie van toelichting ook specifiek beaamt[88]). Opvallend is dat de memorie van toelichting aandacht besteedt aan 'cascade-effecten' tussen sectoren. Dit zijn domino-effecten waarbij incidenten in één sector voor problemen in andere sectoren zorgen.[89] De aandacht voor mogelijke cascade-effecten in de Csw is een waardevolle toevoeging op de eisen neergelegd in de NIB-richtlijn.[90] De onderlinge afhankelijkheid van verscheidene sectoren wordt in de NIB-richtlijn onvoldoende belicht als risicofactor waar rekening mee gehouden moet worden. Hoewel sommige verbanden voor de hand liggen, zou het toch raadzaam zijn de meest essentiële interdependenties tussen sectoren in kaart te brengen en daarop bepaalde meldingskanalen in te richten.

Relatie met meldplichten voor andere incidenten

De meldplicht in de Wgmc moet niet worden verward met de meldplicht datalekken.[91] Deze meldplicht, die geldt vanaf 1 januari 2016, ziet op inbreuken op beveiliging van persoonsgegevens, en dergelijke meldingen moeten worden gedaan aan de Autoriteit persoonsgegevens (AP). Mochten er bij te melden ICT-inbreuken ook persoonsgegevens in het geding zijn, dan moet zowel bij het NCSC als bij het AP melding worden gedaan.

Het Besluit meldplicht cybersecurity

[84] De Wgmc bevat geen bepalingen omtrent sancties, maar onder de Csw kan een bestuurlijke boete worden opgelegd.
[85] Zo kent de Nederlandse financiële sector sectorale toezichthouders zoals de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB).
[86] Zie MvT Wgmc, p. 4.
[87] De MvT noemt de telecomsector als voorbeeld. Toch moet gezegd worden dat de meldplichten neergelegd in art. 13bis van Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronischecommunicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronischecommunicatienetwerken en -diensten, *PbEU* 2009, L 337/37, breder zijn dan alleen voor dat doel. Dit blijkt bijvoorbeeld uit de rol van ENISA in de meldplicht, zie ook Overweging 44.
[88] MvT Wgmc, p. 17-18.
[89] Een bekend voorbeeld is een grote uitval in de energiesector, die vervolgens leidt tot storingen in bijv. transport, de gezondheidszorg, telecommunicatie, enz.
[90] Zie art. 6 lid 1 sub b NIB-richtlijn en MvT, p. 7.
[91] Art. 34a Wet bescherming persoonsgegevens.

Een voorbeeld van een ICT-inbreuk die onder de meldplicht van het Besluit meldplicht cybersecurity zou kunnen vallen is de ransomware-aanval van 27 juni 2017. Containerterminals van APM (dochteronderneming van Maersk), waarvan twee in Rotterdam, konden niet functioneren omdat de ICT-infrastructuur van Maersk onklaar gemaakt was door de ransomware.[92] Het opstarten van de terminals heeft enkele dagen geduurd. Deels bleek gebrekkige beveiliging het probleem.[93] Ook een ICT-systeemfout van de grootte zoals die van British Airways op 27 mei 2017[94] zou op Schiphol waarschijnlijk al snel gelden als een onder de Wgmc te melden ICT-inbreuk.
Het Besluit wijst acht soorten vitale aanbieders (en hun producten en diensten) aan die aan de meldplichten van de Wgmc moeten voldoen.[95] Dit zijn aanbieders in de categorieën Drinkwater,[96] Energie,[97] Nucleair,[98] Financieel,[99] Elektronische communicatienetwerken en -diensten/ICT,[100] Mainport Rotterdam,[101] Mainport Schiphol,[102] en Keren en beheren.[103] De verwachting is dat ongeveer 60 organisaties onder de meldplicht vallen, volgens de nota van toelichting bij het Besluit.

---

[92] <www.trouw.nl/home/grootschalige-aanval-met-ransomware-treft-nu-ook-nederland~af37e686/>.
[93] <www.volkskrant.nl/economie/rotterdamse-containerbedrijf-voor-cyberaanval-meermaals-gewaarschuwd-voor-gebrekkige-ict-beveiliging~a4505228>.
[94] <www.ft.com/content/de12aa5a-42cf-11e7-ab92-4c27fbc26eed>.
[95] De lijst van vitale aanbieders is gebaseerd op de 'Herijkte lijst vitale infrastructuur' uit mei 2015, zie *Kamerstukken II* 2014/15, 30821, 23, p. 5. De huidige lijst van vitale aanbieders in het Besluit telt minder vitale sectoren dan deze lijst vitale infrastructuur uit 2015. Zo zijn de sectoren Chemie, Openbare orde en veiligheid, en Openbaar bestuur niet in de huidige lijst opgenomen. De reden hiervoor wordt niet gegeven.
[96] De tien betreffende bedrijven in dit geval zijn Brabant Water, Dunea, Evides, Oasen, PWN Waterleidingbedrijf Noord-Holland, Vitens, Waterbedrijf Groningen, Waterleidingmaatschappij Drenthe en Waternet.
[97] De Netbeheerder voor het landelijk hoogspanningsnet is Tennet, de Netbeheerder van het landelijk gastransportnet is Gasunie Transport Services. De regionale netbeheerders van elektriciteit en gas zijn Coteq Netbeheer, Enduris, Enexis, Liander, RENDO Netbeheer, Stedin en Westland Infra. Tot slot behoort tot deze sector De Nederlandse Aardolie Maatschappij B.V. (NAM).
[98] Tot de sector Nucleair behoren COVRA, ECN (Hoge Flux Reactor Petten), EPZ (Kerncentrale Borssele), NRG, Reactor Instituut Delft, en URENCO.
[99] DNB wijst jaarlijks de instellingen aan die deel uitmaken van de zogeheten Financiële kerninfrastructuur (FKI). Deze zijn meldplichtig.
[100] Meldplichtige aanbieders van elektronische communicatienetwerken en -diensten zijn volgens de nota van toelichting bij het Besluit in ieder geval KPN, Tele2, T-Mobile en Vodafone. De meldplicht geldt ten behoeve van het verlenen van een telefoon-, sms-, of internettoegangsdienst. Voor wat betreft ICT zijn aanbieders van internetknooppunten meldplichtig zolang zij minimaal 8 terabits per seconde (tb/s) poortcapaciteit hebben. Dit lijkt een vergissing. Amsterdam Internet Exchange (AMS-IX) behoort tot de grootste internet exchanges ter wereld met een piekcapaciteit van 5 tb/s. De grootste aanbieders in Nederland zijn volgens de nota van toelichting AMS-IX en NL-ix (zie *Kamerstukken I* 2016/17, 34888, E, p. 12 en 13.
[101] In principe is alleen de Divisie Havenmeester meldplichtig. Deze maakt zelf afspraken met andere entiteiten binnen Mainport Rotterdam aangaande ICT-inbreuken.
[102] Volgens de nota van toelichting bij het Besluit vallen onder de meldplicht de Luchtverkeersleiding Nederland (LVNL), de Royal Schiphol Group N.V., Aircraft Fuel Supply B.V., de Koninklijke Marechaussee en de luchtvaartmaatschappijen die minimaal 25 procent van het totaal aantal vliegbewegingen op Schiphol voor hun rekening nemen.

Met de implementatie van de NIB-richtlijn in de Csw moeten zowel de *vitale aanbieders* als de *aanbieders van essentiële diensten* per koninklijk besluit worden aangewezen.[104] Het is daarom te verwachten dat wanneer de aanbieders van essentiële diensten zullen worden aangewezen (uiterlijk op 9 november 2018, zie art. 5 lid 1 NIB-richtlijn), de vitale aanbieders tegelijkertijd opnieuw zullen worden aangewezen. De lijst vitale aanbieders kan daarbij hetzelfde blijven, maar ook anders zijn dan de huidige. Enkele opmerkingen over de huidige lijst volgen hieronder.
De meest opvallende afwezige sector in het Besluit is de sector Gezondheidszorg. De nota van toelichting bij het Besluit stelt dat de zorgsector niet als vitale aanbieder gezien dient te worden omdat de sector niet centraal georganiseerd is. Er valt het een en ander af te dingen op deze redenering. Een voorbeeld is de WannaCry malware[105] van 2017, die een groot aantal ziekenhuizen in het Verenigd Koninkrijk zo goed als stil heeft gelegd, waardoor van een zekere maatschappelijke ontwrichting sprake was.[106] Onder de Csw zal de sector Gezondheidszorg wel als aanbieder van essentiële dienst worden aangewezen omdat de richtlijn dat duidelijk voorschrijft. Daarnaast kan het Nederlandse stelsel van meldplichten aangepast en aangevuld worden. Daarbij is het instrument van het koninklijk besluit voor de lijst met name geschikt omdat een KB makkelijker gewijzigd kan worden dan een wet.
In het Besluit zijn aanbieders van elektronische communicatienetwerken en -diensten[107] als vitale aanbieder opgenomen. Deze sector wordt door de NIB-richtlijn uitgesloten van de aanbieders van essentiële diensten.[108] Voor de categorie van aanbieders uit de elektronischecommunicatiesector geldt dat zogenoemde over-the-top aanbieders, zoals WhatsApp, in principe niet onder de meldplicht uit het Besluit vallen.[109] De reden hiervoor is dat zij niet als vitaal worden aangemerkt. De sms-dienst wordt daarentegen 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.[110]

De Cybersecuritywet

De implementatie van de NIB-richtlijn zal plaatsvinden krachtens de Csw. De Raad van State heeft op 4 januari 2018 over het wetsvoorstel voor de Csw advies uitgebracht,[111] en op 15 februari 2018

---

[103] De nota van toelichting bij het Besluit stelt dat de meldplichtige vitale waterkeringen bij besluit van de minister van Infrastructuur en Waterstaat worden aangewezen. Dit zijn enkel objecten die digitaal worden aangestuurd.
[104] *Kamerstukken II* 2017/18, 34883, 7, p. 1.
[105] WannaCry is een virus dat een computersysteem ontoegankelijk kan maken, in beginsel voor bepaalde tijd, waarbij losgeld geëist wordt om de gegevens weer toegankelijk te maken. Wordt niet betaald, dan blijven de gegevens voor altijd ontoegankelijk.
[106] Het zorgstelsel in het VK is onder de National Health Service (NHS) centraler geregeld dan in Nederland, maar de redenen van de grote gevolgen van de ICT-inbreuk lagen vooral bij het gebruik van verouderde systemen. Dit probleem bestaat ook in Nederland.
[107] Zolang zij een netwerk of infrastructuur beheren dat of die direct wordt gebruikt ten behoeve van het verlenen van een telefoon-, sms- of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers. Let wel dat men in het Besluit niet spreekt van ‘openbare’ elektronische communicatienetwerken en -diensten, hoewel dat in de praktijk naar verwachting geen verschil zal opleveren.
[108] Zie de paragraaf over de Csw voor meer toelichting.
[109] In het vernieuwde kader voor de telecommunicatiesector zal dit wel het geval zijn, zie hieronder.
[110] Zie NvT Besluit, p. 6.
[111] *Kamerstukken II* 2017/18, 34883, 4. Het advies bevat enkele kleine wijzigingen, en deze zijn voor het overgrote deel overgenomen.

is het wetsvoorstel naar de Tweede Kamer gegaan.[112] Hoewel de tekst nog niet definitief is, volgen hieronder enkele observaties.
Er zijn enkele verschillen tussen de Csw en de NIB-richtlijn in het kader van keuzevrijheid gegeven door de richtlijn in de implementatie alsmede de minimumharmonisatie. Zoals gezegd, de NIB-richtlijn hanteert de term 'aanbieders van essentiële diensten' voor de aanbieders van kritieke infrastructuur die onder de reikwijdte van de richtlijn vallen. De Wgmc is van toepassing op 'vitale aanbieders'. De Csw lijkt er vooralsnog van uit te gaan dat aanbieders van essentiële diensten een subcategorie zijn van de vitale aanbieders, en bevat bepalingen voor beide categorieën aanbieders. Vitale aanbieders die niet onder de NIB-richtlijn vallen, hoeven niet te voldoen aan de beveiligingseisen uit de NIB-richtlijn en vallen evenmin onder het daaraan gerelateerde toezicht.[113] Zij dienen wel te voldoen aan de meldplicht in de Csw. De aanbieders van essentiële diensten moeten voldoen aan alle verplichtingen.[114] De Csw heeft zich weliswaar strikt genomen gehouden aan de bepaling uit de NIB-richtlijn die stelt dat aanbieders van openbare elektronische communicatienetwerken en -diensten en verleners van vertrouwensdiensten[115] zijn uitgesloten van de reikwijdte van de richtlijn (art. 1 lid 3 NIB-richtlijn), maar de Csw laat wel uitdrukkelijk de ruimte open om deze bij koninklijk besluit aan te wijzen als vitale aanbieders.[116] Nu het Besluit de aanbieders van openbare elektronische communicatienetwerken en -diensten als vitale aanbieder heeft aangewezen, zal dat onder de Csw naar alle waarschijnlijkheid zo blijven.
De reden voor uitsluiting van de telecomsector is dat er al een regeling is. Deze regeling is echter – zoals in de inleiding is aangegeven – beperkter in omvang. Bij de herziening van de regelgeving zal aansluiting worden gezocht bij de NIB-richtlijn (zie hieronder).
Dit betekent in de praktijk dat aanbieders van openbare elektronische communicatienetwerken en -diensten niet zouden hoeven te voldoen aan de beveiligingsplichten van de Csw (de beveiligingsplichten van de Tw gelden onverkort), maar wel aan de meldingsplichten van de Csw. Dit zou er ook toe kunnen leiden dat in Nederland voor deze aanbieders in specifieke gevallen een plicht bestaat om te melden aan drie instanties, namelijk aan het Agentschap Telecom,[117] de Autoriteit Persoonsgegevens [118] en het NCSC.[119]
In het Besluit bij de Wgmc staan daarnaast de sectoren Nucleair en 'Keren en Beheren' (de waterschappen) als vitale aanbieders aangemerkt. Deze sectoren worden niet benoemd in de richtlijn. Aanbieders van deze sectoren zullen dus vooralsnog[120] wel aan de meldingsplichten van de Wgmc (en later van de Csw), maar niet aan de beveiligingseisen van de Csw moeten voldoen. Artikel 5 Csw stelt dat zowel de aanbieders van essentiële diensten als de vitale aanbieders bij

[112] *Kamerstukken II* 2017/18, 34883, 1.
[113] Neergelegd in art. 14 lid 1 en 2 en art. 15 NIB-richtlijn.
[114] *Kamerstukken II* 2017/18, 34883, 3, p. 4-5 (MvT).
[115] Voor de vertrouwensdiensten zijn er specifieke meldingsplichten bij inbreuken op de veiligheid of het verlies van integriteit, zie Besluit vertrouwensdiensten, *Stb*. 2017, 75 en meer specifiek over de relatie met de NIB-richtlijn, *Kamerstukken II* 2015/16, 344413, 3, p. 16.
[116] *Kamerstukken II* 2017/18, 34883, 3, p. 33 (MvT). En art. 5 lid 1 sub b laat de ruimte deze aanbieders wel als vitale aanbieders aan te wijzen.
[117] Meldingen van een inbreuk die invloed heeft op de continuïteit van het netwerk moeten worden gedaan bij het Agentschap Telecom.
[118] Meldingen van een inbreuk op de bescherming van persoonsgegevens moet worden gedaan bij de Autoriteit Persoonsgegevens.
[119] Meldingen van ICT-inbreuken moeten worden gedaan aan het NCSC.
[120] Het is denkbaar dat meer sectoren dan de zeven genoemd in de NIB-richtlijn worden aangewezen als aanbieders van essentiële diensten; de richtlijn verbiedt dit niet.

algemene maatregel van bestuur of bij besluit van een bij die maatregel genoemd bestuursorgaan worden aangewezen.[121]
De Nederlandse situatie zal nog een belangrijk verschil vertonen met de NIB-richtlijn in de identificatie van de vitale aanbieders, namelijk dat binnen het huidige beleid twee categorieën vitale aanbieders worden onderscheiden, te weten categorie A en B.[122] Categorie A bevat de aanbieders waarbij incidenten grotere potentiële gevolgen voor de maatschappij hebben dan bij aanbieders behorende tot categorie B. Categorie A bevat daarnaast het criterium van cascade-effect. Dat wil zeggen dat incidenten bij vitale aanbieders van de A-categorie ten minste twee andere sectoren zullen doen uitvallen. Deze manier van rekening houden met een dergelijk 'domino-effect' is geen specifiek onderdeel van de NIB-richtlijn.
Al met al zijn de genoemde verschillen deels te verklaren uit de bijzondere voorgeschiedenis van de voorloper van de Wgmc en zijn ze geheel in lijn met de beoogde minimumharmonisatie van de NIB, en daarom toe te juichen.
Naast de meldplichten voor vitale aanbieders en aanbieders van essentiële diensten bevat de Csw ook beveiligingseisen en meldplichten voor digitaledienstverleners.
Zoals gezegd krijgt de NIS-samenwerkingsgroep elk jaar een verslag van de centrale contactpunten van de lidstaten over de ontvangen incidentmeldingen.[123] Onder de Wgmc had de meldplicht voornamelijk als functie om het NCSC te ondersteunen in zijn taken. In de Csw dient de meldplicht ook om informatie te delen om het kennisniveau te verhogen voor de lidstaten.
De NIB-richtlijn laat enkele specifieke implementatiekeuzes aan de lidstaten ten aanzien van de aanwijzing van nationale autoriteiten, welke de Csw als volgt invult. De wetgever heeft ervoor gekozen om meerdere autoriteiten aan te wijzen, verdeeld per sector (art. 4 lid 1 Csw) in plaats van een enkele autoriteit voor alle sectoren. De Csw laat de taken van de CSIRT en de bevoegde autoriteit gescheiden (art. 2 sub b en art. 4 lid 1-2 Csw).[124] De Csw bepaalt voorts dat meldingen van incidenten ook moeten worden gedaan bij het betreffende CSIRT (art. 10-13 Csw).
Bij de implementatie van de NIB-richtlijn kan overigens worden voortgebouwd op reeds bestaande elementen en instituties. Zo zijn er reeds CSIRT's voor enkele van de genoemde sectoren, zoals de financiële sector en de telecommunicatiesector.[125] Daarnaast heeft Nederland sinds 2011 een nationale cybersecuritystrategie, waarvan in 2013 de tweede versie is gepubliceerd.[126]
Het waarborgen van de vertrouwelijkheid is, net als in de Wgmc, van groot belang.[127] De bepaling rond het verstrekken van vertrouwelijke gegevens (art. 1 lid 5 NIB-richtlijn) is in drie artikelen, te weten de artikelen 20 tot en met 22 in de Csw, uitgewerkt. De reden hiervoor is dat de verplichting apart wordt uitgewerkt voor de minister (art. 20), voor de CSIRT's (art. 21) en voor de bevoegde autoriteit (art. 22). Artikel 20 bevat een bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens die afwijkt van de Wob.
Ook biedt artikel 16 Csw de mogelijkheid vrijwillig melding te maken van inbreuken, ook voor entiteiten die (vooralsnog) niet onder de reikwijdte van de richtlijn vallen.

De telecommunicatiesector

[121] Conform art. 5 lid 2 Csw jo. art. 5 lid 7 sub b NIB-richtlijn moet de lijst van aangewezen aanbieders van essentiële diensten ook iedere twee jaar aan de Commissie verstrekt worden.
[122] *Kamerstukken II* 2014/15, 30821, 23, p. 3-4.
[123] Dit is niet direct in de Csw geïmplementeerd, want betreft feitelijk handelen, zie Mvt Csw, p. 30.
[124] Het CSIRT voor essentiële diensten is echter ook het centrale contactpunt (art. 2 sub a en b Csw). Het CSIRT voor digitale diensten wordt nader bij koninklijk besluit aangewezen, zie art. 4 lid 2 sub b Csw en *Kamerstukken II* 2017/18, 34883, 7, p. 1.
[125] Zie <www.cert.nl/>.
[126] Zie <www.ncsc.nl/organisatie/nationale+cybersecurity+strategie>.
[127] <www.ncsc.nl/organisatie/nationale+cybersecurity+strategie>, p. 6 en p. 45-51.

Zoals besproken zijn de aanbieders van elektronische communicatienetwerken en -diensten uitgesloten van de reikwijdte van de NIB-richtlijn omdat er al een sectorspecifieke regeling is opgenomen in de Kaderrichtlijn. In artikel 13bis van de Kaderrichtlijn wordt bepaald dat ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden, passende technische en organisatorische maatregelen nemen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen. Er worden met name maatregelen genomen om de impact van veiligheidsincidenten op gebruikers en onderling verbonden netwerken zo laag mogelijk te houden. Voor de aanbieders van openbare elektronische communicatienetwerken geldt dat daarnaast moet worden gezorgd voor de integriteit van hun netwerken zodat de continuïteit van de diensten kan worden gewaarborgd. Elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact had op de exploitatie van netwerken of diensten moet worden gemeld bij de bevoegde nationale regelgevende instantie. De nationale regelgevende instantie brengt ook ENISA en (betrokken) regelgevende instanties van andere lidstaten op de hoogte. Naast artikel 13bis Kaderrichtlijn regelt artikel 13ter Kaderrichtlijn de bevoegdheden van de nationale regelgevende instanties. De bepalingen 13bis en 13ter zijn geïmplementeerd in hoofdstuk 11a Tw met, onder andere, een meldplicht bij het Agentschap Telecom.
Het is de verwachting dat eind 2018 een geheel nieuw Europees telecommunicatiekader zal worden aangenomen. De herziening van dit regelgevend kader voor de elektronische communicatiesector heeft tot doel de vier richtlijnen uit het bestaande telecompakket en de BEREC-verordening te vernieuwen en de richtlijnen te verenigen in een enkele richtlijn met de titel 'Europees wetboek voor elektronische communicatie' (European Electronic Communications Code of EECC).[128] In het concept voor deze Elektronische Communicatie Code wordt het belang van het nemen van adequate maatregelen op het gebied van veiligheid benadrukt en wordt invulling gegeven aan een meldplicht. Daarbij wordt ook ingegaan op de relatie tot de NIB-richtlijn.
Het voorstel is om het huidige artikel 13bis van de Kaderrichtlijn, waarin de beveiligingseisen en meldplichten voor aanbieders van openbare elektronische communicatienetwerken en -diensten vervat zijn, te vervangen door artikel 40 EECC. De voornaamste veranderingen zijn de volgende. In artikel 13bis lid 3 wordt gesteld dat de aanbieders inbreuken met een 'belangrijke impact' moeten melden zonder uitleg van wat de term inhoudt. In het nieuwe artikel 40 lid 3 worden nadere criteria gegeven voor wat deze term betekent. Deze wijzigingen zijn overigens geheel in lijn met artikel 16 lid 4 NIB-richtlijn. Verder wordt gesteld dat de Algemene verordening gegevensbescherming onverminderd geldt (art. 40 lid 4) en dat de Europese Commissie gedelegeerde handelingen mag vaststellen om de verplichtingen in het artikel te specificeren. Lidstaten kunnen de assistentie van de CSIRT's inroepen (nieuw art. 41 lid 4), en er wordt tevens een rol weggelegd voor de nationale autoriteiten in de zin van de NIB-richtlijn. Al met al zullen deze aanpassingen de beveiligingseisen en meldplichten in lijn brengen met de NIB-richtlijn.
Daarnaast wordt de reikwijdte van de EECC uitgebreid, zodat er nu ook nummeronafhankelijke diensten (zoals WhatsApp en Skype) onder vallen, evenals Internet of Things (IoT) en machine-to-machine (M2M) communicatie. In de concepttekst van de ECC worden deze diensten ook onder de beveiligingsverplichtingen gebracht, waar dat nu nog niet het geval is.
De eerste trialoog over de ECC vond plaats op 25 oktober 2017.[129] Het is de bedoeling dat er in de zomer van 2018 overeenstemming over de definitieve tekst van de ECC zal worden bereikt zodat

[128] Zie G.P. van Duijvenvoorde, 'Naar een Europees wetboek voor elektronische communicatie', *NtEr* 2016/9, p. 319-332.
[129] Zie voor een gecombineerde tekst van de Raad en van het Europees Parlement, Interinstitutional File: 2016/0288 (COD) van 9 november 2017, te raadplegen via <http://data.consilium.europa.eu/doc/document/ST-14186-2017-INIT/en/pdf> (geraadpleegd op 8 maart 2018).

een nieuwe richtlijn eind 2018 in werking kan treden (met een implementatietermijn van twee jaar). Er zal vanaf dat moment ook voor de telecommunicatiesector meer aansluiting zijn bij de bepalingen van de NIB-richtlijn.

Enkele slotopmerkingen en conclusies

Met de Wgmc en het Besluit, en in de nabije toekomst via de Csw en de ECC, wordt een stelsel van meldplichten in het leven geroepen (dan wel versterkt) om daarmee de beveiligingscapaciteiten en het kennisniveau van de lidstaten, het algemene beveiligingsniveau, en de transparantie op het gebied van informatie- en netwerkbeveiliging te vergroten.
De Nederlandse wetgever geeft met de Csw de noodzakelijke implementatie van de NIB-richtlijn. Met de Csw wordt niet alleen voldaan aan de eisen van de richtlijn, maar het niveau ligt zelfs wat hoger door de regelingen voor vitale aanbieders uit de Wgmc. Dit illustreert treffend de minimumharmonisatie van de richtlijn. Dit betekent echter wel dat aanbieders zullen moeten nagaan onder welke meldplichten zij vallen en hun organisatie daarop zullen moeten inrichten.
Bovenstaand overzicht laat zien dat de verschillende typen wetgeving elkaar deels overlappen, deels aansluiten en er ook nog lacunes zijn.
Overlap ontstaat omdat de meldplichten van de Wgmc en later de Csw naast de huidige meldplicht datalekken bestaan. Met de invoering van de AVG zal de meldplicht voor lekken van persoonsgegevens ook een nieuwe grondslag krijgen.[130] Er zullen ongetwijfeld overlaps bestaan in de beveiligingseisen en meldplichten van de AVG en de Csw. Vanwege de verschillende grondslag (bescherming van persoonsgegevens en bescherming van vitale infrastructuur) is dit niet eenvoudig te voorkomen. Het hoeft ook niet nadelig te zijn, aangezien voor de verschillende inbreuken verschillende expertise nodig is.
Daarnaast geldt dat, bijvoorbeeld, de aanbieder van elektronische communicatiediensten bij het lekken van persoonsgegevens ook moet voldoen aan de meldplichten neergelegd in de sectorspecifieke wetgeving in artikel 11.3a Tw. Dit zou er ook toe kunnen leiden dat in Nederland voor deze aanbieders in specifieke gevallen een plicht bestaat om te melden aan drie instanties, namelijk aan het AT,[131] de AP[132] en het NCSC.[133] Het is echter wel zo dat de Csw niet belet deze meldplicht op den duur te vereenvoudigen, door bijvoorbeeld een enkele instantie aan te wijzen voor het melden van ICT-inbreuken en inbreuken in de continuïteit.
De telecommunicatiesector zou ook een voorbeeld kunnen zijn van het aansluiten van regels. Zo ligt de uitsluiting van de telecomsector voor meldingen ook wel voor de hand. De sector heeft al veel langer eigen beveiligingseisen en meldplichten die in grote lijnen overeenkomen met die in de NIB-richtlijn. Echter, zoals gezegd, het kader van de meldingen in de huidige telecomregulering verschilt van dat van de NIB en Csw. De nieuwe ECC tracht de telecomregulering meer in lijn te brengen met de NIB. Deze aansluiting valt toe te juichen. Een ander voorbeeld is hierboven al aangestipt en betreft het verschil tussen enerzijds interconnectie van netwerken van netwerkaanbieders door een internetknooppunt, dat daarbij onder de NIB-richtlijn valt, en anderzijds een interconnectie-overeenkomst tussen netwerkaanbieders, die daarbij onder de

[130] De AVG stelt bijvoorbeeld strengere eisen aan de interne registratie van datalekken. Deze registratie moet alle datalekken bevatten, niet alleen de lekken die gemeld moeten worden, zie art. 33 lid 5 AVG. Voor een uitgebreide bespreking van de beveiligingseisen en meldplichten onder de AVG, zie bijv. M. Jansen, 'AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren', *Computerrecht* 2017/152, afl. 4, p. 208-216.
[131] Meldingen van een inbreuk die invloed heeft op de continuïteit van het netwerk moeten worden gedaan bij het Agentschap Telecom.
[132] Meldingen van een inbreuk op de bescherming van persoonsgegevens moeten worden gedaan bij de Autoriteit Persoonsgegevens.
[133] Meldingen van ICT-inbreuken moeten worden gedaan aan het NCSC.

regulering van elektronische communicatie valt. Deze regels sluiten nauw aan, maar hierdoor kan onduidelijkheid bestaan in de afbakening tussen internetknooppunten en netwerkaanbieders. De eerste categorie zal aan alle verplichtingen van de Csw moeten voldoen, de laatste alleen aan de meldplicht.
Daarnaast sluit (vanwege de verschillende voorgeschiedenis) de Wgmc niet geheel aan bij de NIB-richtlijn, zoals is besproken, maar dat wordt door de wetgever in de Csw in principe op een consistente wijze gedaan, bijvoorbeeld (en met name) door het onderscheid tussen vitale aanbieders en aanbieders van essentiële diensten in stand te houden.
Toch zijn hierbij nog enkele voorbeelden van lacunes te noemen. De uitsluiting van DDoS-aanvallen en fouten van medewerkers als te melden ICT-inbreuken kan problematisch zijn omdat deze aanvallen grote gevolgen kunnen hebben. Het is bekend dat zowel interne fouten van medewerkers alsook DDoS-aanvallen dermate gevolgrijk kunnen zijn dat ze kunnen leiden tot maatschappelijke ontwrichting.[134] In beide gevallen verdient het aanbeveling om bij de implementatie van de richtlijn in de Csw[135] de *aard* van een aanval of inbreuk[136] minder een criterium van invloed te laten zijn, en de nadruk te leggen op de *gevolgen* van de ICT-inbreuk.
De Wgmc noch de Csw geeft een specifieke invulling van eventuele aansprakelijkheid als gevolg van meldingen. Het is aan te bevelen om dit in de Csw wel expliciet te maken, aangezien de gevolgen voor wat betreft eventuele aansprakelijkheid een grote drempel zouden kunnen zijn om ICT-inbreuken te melden. Uit angst voor represailles zullen naar verwachting veel organisaties het zekere voor het onzekere nemen, en dat is precies wat de richtlijn probeert te vermijden. Daarentegen is het principe van ‘just culture’ mogelijk misleidend. De NIB-richtlijn refereert nergens aan dit principe, en de EU-regelgeving voor de telecomsector ook niet. Het is dan ook niet de bedoeling dat aansprakelijkheid voor eventuele fouten wordt weggenomen wanneer deze gemeld worden, alleen dat de aansprakelijkheid door het doen van de melding niet toeneemt. Het principe van ‘just culture’ in de luchtvaartsector moet gezien worden binnen een groter kader van een ‘veiligheidscultuur’[137] (‘safety culture’ in de Engelse versie). In het kader van doelstellingen van de NIB-richtlijn en de Csw – het gezamenlijk bijdragen aan security – zou hier wellicht beter gesproken kunnen worden van het bevorderen van een ‘beveiligingscultuur’ of ‘security culture’.
De omzettingsdatum van de NIB-richtlijn van 10 mei 2018 is niet gehaald. In de behandeling van het wetsvoorstel voor de Csw in de Tweede Kamer zijn hierover zorgen geuit,[138] en op het moment van schrijven is die vertraging beaamd. De verwachting is nu dat de Csw in twee delen in werking zal treden. Het eerste deel kan, wanneer het parlement de Csw voor het zomerreces aanvaardt, deze zomer in werking treden voor het centrale contactpunt, voor digitaledienstverleners en voor de vrijwillige melding van incidenten (art. 16 Csw). Het tweede deel (te weten de rest van de Csw) kan op 9 november 2018 in werking treden, wanneer de essentiële dienstverleners en de vitale aanbieders moeten worden aangewezen.[139]

---

[134] In het geval van DDoS-aanvallen is dat in de consultatieronden ook betoogd door Bits of Freedom, zie MvT Wgmc, p. 12.
[135] Uit de NIB-richtlijn valt op te maken dat ook incidenten ten gevolge van menselijke fouten of incidenten die de beschikbaarheid van gegevens of diensten in gevaar brengen, voor zover deze incidenten ‘aanzienlijke gevolgen voor de continuïteit van de diensten’ hebben, gemeld moeten worden. Zie hierbij art. 4 lid 2 jo. art. 14 en 16 NIB-richtlijn. Zie eveneens Overweging 3.
[136] De MvT spreekt zichzelf bijvoorbeeld tegen door de ‘eenvoudige’ aard van een DDoS-aanval als criterium te gebruiken, zie MvT Wgmc, p. 3, terwijl het karakter van een dergelijke aanval geregeld niet slechts eenvoudig is.
[137] Verordening (EU) nr. 376/2014, Overweging 36.
[138] *Kamerstukken II* 2017/18, 34883, 5, p. 2.
[139] *Kamerstukken II* 2017/18, 34883, 7, p. 2.

Te late implementatie kan ertoe leiden dat de Europese Commissie een procedure start bij het Europese Hof van Justitie,[140] maar verdere consequenties voor het te laat implementeren voor de praktijk zullen waarschijnlijk beperkt zijn. Hoewel de Wgmc beperkter is in doel en reikwijdte dan de Csw, is de Wgmc wel van kracht tot het moment van inwerkingtreding van de Csw.[141] Bovendien moeten de aanbieders van essentiële diensten onder de Csw zoals gezegd pas in november 2018 worden aangewezen. Toch zal late implementatie van de richtlijn ervoor zorgen dat de Nederlandse invulling van de verplichtingen van netwerk- en informatiebeveiliging, en daarmee de harmonisatie op Unieniveau, langer op zich zal laten wachten dan nodig of gewenst is.
De Csw beoogt een integrale aanpak voor de vitale infrastructuren te bereiken. De definitieve invulling van deze regeling zal in de komende periode moeten plaatsvinden. Daarna zal ook in de praktijk moeten worden ervaren of de Csw – maar ook de andere meldplichten – een substantiële bijdrage zullen leveren aan het tot stand komen van een daadwerkelijke omslag in de beveiligingscultuur.

[140] Op basis van art. 258 VWEU.
[141] *Kamerstukken II* 2017/18, 34883, 7, p. 2.