Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

36 084 Wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 16 februari 2022 en het nader rapport d.d. 20 april 2022, aangeboden aan de Koning door de Minister van Justitie en Veiligheid. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State van 16 februari 2022 en het nader rapport van 20 april 2022, aangeboden aan de Koning door de Minister van Justitie en Veiligheid. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Bij Kabinetsmissive van 28 januari 2022, no. 2022000202, heeft Uwe Majesteit, op voordracht van de Minister van Justitie en Veiligheid, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders, met memorie van toelichting.

Het Nationaal Cyber Security Centrum (NCSC) krijgt meer mogelijkheden om aanbieders te waarschuwen voor inbreuken op hun netwerk- en

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

kst-36084-4
ISSN 0921 - 7371
's-Gravenhage 2022

informatiesystemen, ook buiten sectoren die als vitaal zijn aangemerkt of tot de rijksoverheid behoren.

De Afdeling advisering van de Raad van State onderschrijft het belang van het voorstel, maar stelt vragen over de overlapping die kan ontstaan tussen de taken van het NCSC en het Digital Trust Center. Zij merkt daarnaast op dat onvoldoende wettelijk is gewaarborgd dat de organisaties die dreigingsinformatie van het NCSC doorgeven aan bepaalde sectoren («schakelorganisaties») voldoen aan eisen van beveiliging en privacy. De Afdeling adviseert met deze opmerkingen rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

1. Organisatie van de digitale veiligheid

Op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) heeft de Minister van Justitie en Veiligheid tot taak:
- *bijstand en advies te verlenen aan «vitale aanbieders» en andere aanbieders die deel uitmaken van de rijksoverheid. Vitale aanbieders bieden diensten aan die essentieel zijn voor de instandhouding van kritieke maatschappelijke of economische activiteiten, of waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving,[2]*
- *te reageren op incidenten die vrijwillig of verplicht worden gemeld, en*
- *informatie te verschaffen wanneer zich incidenten voordoen – of zich dreigen voor te doen – bij netwerk- en informatiesystemen van vitale sectoren en de rijksoverheid, maar ook bij die van andere aanbieders.[3]*

Deze taken worden, namens de Minister, uitgeoefend door het Nationaal Cyber Security Centrum (NCSC).

Sectoren zoals energie, drinkwater, internet en het betalingsverkeer zijn aangewezen als vitaal, omdat de uitval van deze voorzieningen maatschappelijk ontwrichtend kan werken.

Voor de uitvoering van zijn taak werkt het NCSC samen met twee soorten schakelorganisaties.

De eerste soort schakelorganisaties zijn organisaties die «Objectief Kenbaar Tot Taak» hebben om informatie ter voorkoming van digitale ontwrichting, onder meer verkregen via het NCSC, te delen met aangesloten organisaties (afgekort OKTT's). Voorbeelden hiervan zijn de Stichting Cyber Weerbaarheidscentrum Brainport, die bedrijven in de hightech industrie en haar toeleveranciers verbindt, en Cyberveilig Nederland met leden van de cybersecurity markt.

Het tweede type schakelorganisaties zijn Computercrisisteams («Computer Emergency Response Teams»). Zulke teams geven niet alleen informatie of advies, maar kunnen ook worden ingezet om de schade van een cyberprobleem te beperken en de dienstverlening zo snel mogelijk te herstellen. Voorbeelden hiervan zijn de Informatie Beveiligingsdienst waar gemeenten zich toe kunnen wenden en Z-CERT, dat zich richt op cybersecurity in de zorg.

---

[2] Artikel 5, tweede lid, van de NIB-richtlijn (richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194)); artikel 1 Wbni (definitie van «vitale aanbieder»).

[3] Artikel 3, 10 tot en met 16 en 20 van de Wet beveiliging netwerk- en informatiesystemen (Wbni).

In het voorstel krijgt het NCSC meer mogelijkheden om informatie over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen te verstrekken aan aanbieders die niet horen bij de vitale sectoren of de rijksoverheid. Dat kan gaan om bedrijven, maar bijvoorbeeld ook om onderwijsinstellingen. Het NCSC kan die informatie alleen verstrekken als de dreiging of het incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening. De verstrekking van informatie kan via een OKTT, of – als een schakelorganisatie ontbreekt – rechtstreeks aan de organisaties die mogelijk in gevaar zijn.[4]

De Afdeling begrijpt de wens om te regelen dat het NCSC deze aanbieders kan benaderen wanneer het over informatie beschikt die aanzienlijke gevolgen kan hebben voor hun dienstverlening. Naast de grote schade voor de getroffen aanbieder is immers het onderscheid tussen vitale en niet vitale sectoren relatief. Ook wanneer aanbieders in niet-vitale sectoren worden gehackt, kan dat leiden tot maatschappelijke ontwrichting.[5] Zo werden vorig jaar bijna honderd notarissen getroffen door een digitale aanval. Ook aanbieders in de voedselvoorziening en de gezondheidszorg, die niet het etiket «vitaal» hebben, zijn van groot belang voor het functioneren van de samenleving.[6] Daarnaast kunnen kwaadwillenden proberen binnen te dringen bij vitale aanbieders door eerst binnen te dringen bij (niet-vitale) leveranciers van zulke aanbieders («cascade-effecten»).[7]

2. Afbakening van taken

De Afdeling heeft vragen over de verhouding tussen de taakstelling van het NCSC en het Digital Trust Center (DTC) dat onder verantwoordelijkheid van de Minister van Economische Zaken en Klimaat is opgericht. Het DTC ondersteunt en informeert ondernemers die niet tot de vitale aanbieders behoren om digitaal weerbaar te zijn en hun digitale veiligheid op orde te brengen.

Het wetsvoorstel voorziet erin dat het NCSC zich meer dan tot nu toe zal gaan bezighouden met het informeren van niet-vitale aanbieders over specifieke kwetsbaarheden, waaronder aanbieders waar ook het DTC contacten mee onderhoudt.

De informatie van het NCSC kan via een OKTT worden doorgegeven of direct wanneer een schakelorganisatie ontbreekt. Het DTC heeft in september 2021 van het NCSC de OKTT-status gekregen, waardoor deze kan fungeren als schakelorganisatie voor de informatie van het NCSC. In de consultatie is naar voren gekomen dat er een overlapping kan ontstaan met het DTC, zodat het voor bedrijven onduidelijk kan worden bij welk loket zij moeten zijn en met wie zij in tijden van crisis in verbinding kunnen staan. Juist tijdens een crisis mag daarover geen enkele twijfel bestaan. Bovendien is het van belang om dubbel werk bij NCSC en DTC tegen te gaan.

---

[4] Wijziging van de artikel 3 en 20 Wbni in artikel I, onderdelen A en B.

[5] Zie bijvoorbeeld de consultatiereacties op het voorstel van VNO-NCW en MKB-Nederland en van de Stichting Digitale Infrastructuur Nederland, https://www.internetconsultatie.nl/wijzigingwbni/reacties.

[6] De Afdeling advisering heeft hier aandacht voor gevraagd in haar advies van 25 november 2020, W16.20.0357, Staatscourant 2021, nr. 16521. Uit het nader rapport blijkt dat het aanwijzen van processen in de zorg als vitale processen in onderzoek is. Vitale aanbieders zijn aangewezen in de artikelen 2 en 3 van het Besluit beveiliging netwerk- en informatiesystemen. De daarbij gehanteerde criteria zijn te vinden in Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).

[7] Wetenschappelijke Raad voor het Regeringsbeleid, Voorbereiden op digitale ontwrichting, Den Haag 2019, p. 86.

De vraag naar de taakafbakening raakt ook een wetsvoorstel dat in voorbereiding is op het Ministerie van Economische Zaken en Klimaat en dat beoogt om het DTC te belasten met een eigen wettelijke taak om bedrijven te informeren over concrete bedreigingen en specifieke kwetsbaarheden waar het nu vooral algemene informatie over dreigingen verspreidt.[8] Bij het uitoefenen van deze nieuwe taak lijkt nauwe samenwerking met het NCSC in de rede te liggen.

De Afdeling adviseert in de toelichting in te gaan op de taakafbakening tussen het NCSC en het DTC, en op verwachte toekomstige ontwikkelingen,[9] en daarbij ook nader in te gaan op de rol en relevantie van het onderscheid tussen vitale en niet-vitale aanbieders daarin. Zo nodig dient het wetsvoorstel te worden aangepast.

Het NCSC en het DTC hebben beide duidelijk onderscheidenlijke primaire doelgroepen van organisaties waaraan informatie en advies over concrete dreigingen en incidenten wordt verstrekt. Het NCSC heeft krachtens de Wbni als primaire taak het informeren en het adviseren van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid over digitale dreigingen en incidenten. Naast het informeren en het adviseren verleent het NCSC de aanbieders in zijn doelgroep ook overige bijstand bij het treffen van maatregelen om incidenten te voorkomen en te verhelpen. Overige bijstand kan bijvoorbeeld inhouden dat aan de aanbieder uit de doelgroep ter plekke ondersteuning wordt geboden bij het duiden van het probleem en de maatregelen om dat probleem aan te pakken. Het DTC richt zich bij het informeren en het adviseren over digitale dreigingen en incidenten op de doelgroep van het niet-vitale bedrijfsleven. In tegenstelling tot het NCSC verleent het DTC bij incidenten geen overige bijstand aan de aanbieders in zijn doelgroep. Uitzondering op deze afbakening van doelgroepen zijn digitaledienstverleners. Zij zijn geen vitale aanbieder, maar vallen ook niet in de doelgroep van het DTC. Zij vallen namelijk op grond van de Wbni onder het *computer security incident response team* (CSIRT) voor digitale diensten, dat hen bijstaat bij het treffen van maatregelen om de continuïteit van de dienst te waarborgen of te herstellen.[10] Door deze afbakening van doelgroepen en taken kan er geen verwarring ontstaan over van welke overheidsinstantie een aanbieder op bijstand kan rekenen bij digitale dreigingen en incidenten.

Met de door de Minister van EZK voorgestelde Wet bevordering digitale weerbaarheid bedrijven, waarin de hiervoor bedoelde taak van het DTC regeling vindt, wordt de afbakening tussen de primaire doelgroepen van het NCSC en het DTC verder verduidelijkt. Op eventuele aanpassingen van nationale wetgeving ten gevolge van de herziening van de NIB-richtlijn kunnen dit wetsvoorstel en het voorstel van de Minister van EZK niet vooruitlopen, omdat over deze richtlijn nog wordt onderhandeld door de lidstaten.

Voor vitale aanbieders geldt dus al dat wettelijk is voorzien in bijstand van overheidswege bij digitale dreigingen en incidenten. De reden voor dit onderscheid met andere aanbieders is met name gelegen in het grotere maatschappelijke belang dat wordt toegekend aan vitale processen en

---

[8] Voorstel van wet bevordering digitale weerbaarheid bedrijven. Dat voorstel is van 28 juni tot en met 23 augustus in internetconsultatie geweest (https://www.internetconsultatie.nl/wbdwb), tegelijk met het aanhangige voorstel, maar is nog niet bij de Afdeling advisering aanhangig gemaakt. Er is al voorzien in samenloopbepalingen tussen de twee voorstellen (in het aanhangige voorstel: artikel II).

[9] Zoals het voorstel voor een nieuwe richtlijn betreffende een hoog gezamenlijk niveau van cyberbeveiliging (COM(2020) 823), waarin de NIB-richtlijn wordt ingetrokken, en het voorstel voor een nieuwe richtlijn over de veerkracht van «kritieke entiteiten» (COM(2020) 829).

[10] Zie artikel 4, vierde lid, van de Wbni.

binnen die processen aan vitale aanbieders. De uitval of verstoring van een vitaal proces leidt immers tot ernstige maatschappelijke ontwrichting en vitale aanbieders zijn belangrijk voor de continuïteit van een vitaal proces.

De doelgroep van het NCSC betreft, zoals hiervoor ook is aangegeven, vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid. Het NCSC kan bij zijn primaire taakuitoefening dreigings- en incidentinformatie verkrijgen die relevant is voor aanbieders die buiten de doelgroep vallen. Het NCSC heeft dan de taak om die informatie, voor zover die informatie relevant is voor die andere aanbieders, te verstrekken aan krachtens de Wbni (bijvoorbeeld als OKTT) aangewezen schakelorganisaties van die andere aanbieders. Het DTC is inmiddels krachtens artikel 3, tweede lid, van de Wbni als OKTT aangewezen en kan zodoende voor de doelgroep relevante dreigings- en incidentinformatie ontvangen. Voor aanbieders die niet onder de doelgroep van het NCSC, het CSIRT voor digitale diensten of het DTC vallen en evenmin onder de doelgroep van een andere krachtens artikel 3, tweede lid, van de Wbni aangewezen schakelorganisatie vallen, wordt in dit wetsvoorstel voorgesteld om informatieverstrekking vanuit het NCSC in bepaalde gevallen mogelijk te maken, namelijk indien een incident aanzienlijke gevolgen heeft of kan hebben voor de dienstverlening van die aanbieder. Hierbij valt te denken aan politieke partijen, provincies, veiligheidsregio's en semi-publieke organisaties.

Juist omdat het DTC inmiddels als OKTT is aangewezen, zal de voorgestelde wijziging van artikel 3, tweede lid, van de Wbni ertoe leiden dat het NCSC krachtens dat artikellid niet ook aan individuele aanbieders in de doelgroep van het DTC informatie kan verstrekken. Een dergelijke verstrekking is immers alleen mogelijk als een andere aanbieder niet tot de achterban van een schakelorganisatie behoort. Ook om die reden zal er geen sprake zijn van overlap in informatievoorziening ten behoeve van het bedrijfsleven vanuit de overheid.

Voor de volledigheid, om verder zorg te dragen voor een correcte operationele samenwerking werken het NCSC en DTC aan samenwerkingsafspraken.

Naar aanleiding van dit advies van de Afdeling is in de memorie van toelichting na paragraaf 3.3.2 een nieuw hoofdstuk (hoofdstuk 4) ingevoegd, dat ingaat op de verhouding van het NCSC tot het DTC, en zijn de daarna volgende hoofdstukken en paragrafen vernummerd.

3. Regulering van en toezicht op schakelorganisaties

In het stelsel van de Wbni spelen schakelorganisaties een belangrijke rol. Zij ontvangen dreigingsinformatie en hebben de taak[11] die door te geven aan de aanbieders die bij hen zijn aangesloten. Het kan daarbij gaan om vertrouwelijke gegevens die herleid kunnen worden tot een specifieke organisatie, indien nodig zonder toestemming van die organisatie.[12] Als die gegevens terechtkomen in de handen van kwaadwillenden, kunnen ze die gebruiken om binnen te dringen in kwetsbare informatiesystemen.

[11] Artikel 3, tweede lid, onderdeel a; voorgesteld artikel 20, tweede lid, onderdeel d, Wbni.
[12] Artikelen 3, tweede lid, en 20, tweede lid, Wbni.

OKTT's kunnen daarnaast informatie doorgeven aan het publiek. In de wet zoals die nu luidt kan het alleen gaan om algemene informatie, maar in het voorstel kunnen zij ook vertrouwelijke gegevens die herleid kunnen worden tot een specifieke organisatie aan het publiek doorgeven.[13]

De overheid is verantwoordelijk voor de bescherming van die gegevens. Daarom is het van belang dat de schakelorganisaties voldoen aan beveiligingseisen en privacynormen.[14]

Wanneer de Minister organisaties aanwijst als schakelorganisatie, toetst hij of die organisaties daaraan voldoen; bij OKTT's doet hij dat met behulp van een beleidsregel, de Handreiking OKTT. Vanzelfsprekend moeten de OKTT's daarnaast ook voldoen aan de verplichtingen van de Algemene verordening gegevensbescherming. Die verplichtingen gelden echter voor alle soorten en vormen van gegevensverwerking die zich waar dan ook voordoen en vormen alleen de grootste gemene deler. OKTT's hoeven niet te voldoen aan de veel concretere en specifiekere eisen die bij en krachtens hoofdstuk 4 van de Wbni gelden voor aanbieders van essentiële diensten en digitaledienstverleners. Daardoor vallen zij ook niet onder het stelsel van toezicht en handhaving van hoofdstuk 6 van de Wbni.

De Afdeling merkt op dat hiermee onvoldoende wettelijk is gewaarborgd dat schakelorganisaties het vereiste niveau van beveiliging en privacybescherming hebben op het moment dat zij worden aangewezen, en dat zij aan dat niveau blijven voldoen.

De Afdeling adviseert hierop in de toelichting in te gaan en het voorstel aan te vullen.

Voordat een schakelorganisatie krachtens artikel 3, tweede lid, van de Wbni als OKTT wordt aangewezen wordt thans al een grondige beoordeling verricht. Met deze beoordeling wordt bepaald of de verstrekking door het NCSC van de in dat artikel bedoelde informatie aan die schakelorganisatie verantwoord en gerechtvaardigd is. In het kader daarvan wordt onder meer, op basis van de uitkomsten van een navraag hiernaar bij de betrokken schakelorganisatie, getoetst of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen met betrekking tot de netwerk- en informatiesystemen heeft genomen en hierdoor geacht kan worden de van het NCSC ontvangen informatie zorgvuldig te verwerken en de vertrouwelijkheid van deze informatie voldoende te waarborgen. Ook wordt, op basis van diezelfde navraag, beoordeeld of de betrokken schakelorganisatie afdoende maatregelen heeft genomen om persoonsgegevens rechtmatig te verwerken. Tevens wordt beoordeeld of de organisatie een voldoende afgebakende doelgroep heeft van aanbieders die (in hoofdzaak) niet vitaal zijn en geen deel uitmaken van de rijksoverheid. Verder wordt beoordeeld of de van het NCSC te ontvangen informatie niet voor andere doeleinden wordt gebruikt dan het informeren en adviseren van aanbieders in hun doelgroep. Deze beoordeling zal na de inwerkingtreding van de in dit wetsvoorstel voorgestelde wijzigingen uiteraard ook blijven plaatsvinden bij de aanwijzing van een schakelorganisatie als OKTT, waarbij het bepaalde in artikel 20, tweede lid, van de Wbni nauwkeurig in het oog zal worden gehouden.

---

[13] Artikel 3, tweede lid, onderdeel a; voorgesteld artikel 20, tweede lid, onderdeel d, Wbni. Deze taak wordt impliciet toegekend, namelijk door een definitiebepaling.

[14] In het navolgende beperkt de Afdeling zich tot de schakelorganisaties, genoemd in artikel 20, tweede lid, Wbni (zoals gewijzigd in het voorstel) die vertrouwelijke en herleidbare informatie kunnen ontvangen. In dat artikel worden ook de inlichtingen- en veiligheidsdiensten genoemd, maar die zijn geen schakelorganisatie en hebben een heel eigen wettelijk regime. Daarom blijven die buiten beschouwing.

In geval van de aanwijzing als OKTT ondertekent de schakelorganisatie een verklaring waarin is opgenomen dat aan het NCSC melding wordt gemaakt van onder meer belangrijke wijzigingen van de getroffen (technische en organisatorische) beveiligingsmaatregelen of van de doelgroep en de taken die ten behoeve van die doelgroep worden verricht. Indien er op basis van een dergelijke melding óf blijkens anderszins door het ministerie ontvangen informatie aanwijzingen zijn voor bijvoorbeeld een onvoldoende vertrouwelijke omgang door een schakelorganisatie met gegevens, dan kan het NCSC het delen van informatie met die organisatie opschorten. Ook kan de aanwijzing als OKTT worden ingetrokken als uit verdere navraag blijkt dat niet meer aan de toetsingscriteria wordt voldaan.

Voor schakelorganisaties geldt voorts uiteraard, als het gaat om de verwerking van persoonsgegevens na de ontvangst daarvan van het NCSC, dat zij dienen te voldoen aan de daaraan gestelde eisen op grond van de Algemene verordening gegevensbescherming en dat op de naleving daarvan toezicht wordt gehouden door de Autoriteit persoonsgegevens.

Naar mijn oordeel wordt hiermee, ook met inachtneming van de onderscheidenlijke verantwoordelijkheden van de verstrekker van en de ontvanger van informatie, in voldoende mate gewaarborgd dat de verstrekking door het NCSC van de in de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni bedoelde informatie alleen geschiedt aan schakelorganisaties die onder meer adequate maatregelen hebben getroffen voor een vertrouwelijke omgang met die informatie. Voor het daarnaast ten aanzien van genoemde schakelorganisaties in wetgeving stellen van beveiligingsverplichtingen, zoals die krachtens hoofdstuk 4 van de Wbni, zie ik geen aanleiding. Die verplichtingen betreffen de implementatie van de Europese NIB-richtlijn en hebben dientengevolge alleen betrekking op bij algemene maatregel van bestuur aangewezen aanbieders van essentiële diensten, oftewel vitale aanbieders die hun diensten verlenen binnen in die richtlijn limitatief opgesomde sectoren. Er is geen reden gezien om deze verplichtingen ook van toepassing te verklaren op andere aanbieders of hun schakelorganisaties. De continuïteit van hun dienstverlening wordt niet in dezelfde mate van belang geacht voor de Nederlandse samenleving en de aantasting van bijvoorbeeld de beschikbaarheid van die dienstverlening wordt in mindere mate geacht maatschappelijk ontwrichtend te zijn.

Naar aanleiding van dit advies van de Afdeling zijn de paragrafen 3.2.2 en 10.3 (voorheen paragraaf 9.3) van de memorie van toelichting aangevuld.

4. De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

Naar aanleiding van het redactioneel advies van de Afdeling zijn artikel I, onderdeel B en artikel II, onder a, onderdeel B aangepast.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

De vicepresident van de Raad van State,
Th.C de Graaf

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no. W16.22.0008/II

– In artikel I, onderdeel A, onder 1, en onderdeel B, de toevoeging niet invoegen na «informeren», maar na «organisaties». Datzelfde geldt voor artikel II.
– In artikel I, onderdeel A, onder 2, «vitale aanbieders of andere aanbieders die onderdeel zijn» wijzigen in: een vitale aanbieder of een andere aanbieder die onderdeel is. Datzelfde geldt voor artikel II.
– In artikel I, onderdeel B, het nieuw in te voegen onderdeel invoegen als onderdeel a (in dezelfde volgorde als in artikel 3, tweede lid).