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. 3

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel zorgt voor een uitbreiding van de bevoegdheid van het Nationaal Cyber Security Centrum (hierna: NCSC) om namens de Minister van Justitie en Veiligheid informatie te verstrekken aan of ten behoeve van aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen. Deze aanbieders worden in deze toelichting *andere aanbieders* genoemd. Het voorstel bevat daartoe wijzigingen van twee artikelen in de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni).

De eerste wijziging ziet op artikel 3 Wbni. In het eerste lid van dit artikel is de primaire taakuitoefening van het NCSC geregeld. Dit betreft het bijstaan van vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid (bijvoorbeeld ministeries) bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen. Ook ziet deze taakuitoefening op het informeren en adviseren van deze aanbieders over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. Vitale aanbieders zijn overheidsorganisaties en privaatrechtelijke rechtspersonen die diensten aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving (bijvoorbeeld drinkwaterbedrijven). Het NCSC verkrijgt bij het verrichten van analyses en technisch onderzoek ten behoeve van de primaire taakuitoefening dreigings- en incidentinformatie (inclusief persoonsgegevens) over netwerk- en informatiesystemen van *andere aanbieders*. Het tweede lid van dit artikel bepaalt dat het NCSC de taak heeft om, ter voorkoming van nadelige maatschappelijke gevolgen, die informatie over

kst-36084-3
ISSN 0921 - 7371
's-Gravenhage 2022

netwerk- en informatiesystemen van *andere aanbieders* aan een aantal hierin genoemde organisaties te verstrekken, zoals computercrisisteams. De voorgestelde wijziging van artikel 3, tweede lid, Wbni houdt in dat het NCSC in gevallen zoals omschreven in het voorgestelde artikel 3, tweede lid, onder e, deze informatie ook aan *andere aanbieders* zelf kan verstrekken. Van dergelijke gevallen is sprake indien een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening van de betrokken aanbieder en voor de verstrekking van gegevens een in artikel 3, eerste lid, a tot en met c, bedoelde organisatie ontbreekt.

De tweede wijziging ziet op artikel 20 Wbni. Het tweede lid van dit artikel regelt de bevoegdheid voor het NCSC om zonder instemming van de betrokken aanbieders, ter uitvoering van de in artikel 3 Wbni genoemde taken, vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder te verstrekken aan een aantal hierin genoemde organisaties. De voorgestelde wijziging van artikel 20, tweede lid, Wbni maakt het mogelijk dat het NCSC deze gegevens ook kan delen met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (hierna: OKTT's). Hierdoor kunnen aanbieders in de doelgroepen van deze OKTT's door tussenkomst van die OKTT's komen te beschikken over de voor hen relevante dreigings- en incidentinformatie.

2. Aanleiding voor het wetsvoorstel

Er is in toenemende mate sprake van (geslaagde) digitale aanvallen op *andere aanbieders*. Ook groeit de impact van die aanvallen door de toenemende mate van verwevenheid van de digitale wereld met de fysieke wereld. Een voorbeeld van een geslaagde digitale aanval is de besmetting van een in de Rotterdamse haven gevestigd containeroverslagbedrijf met Petya-*ransomware*, waardoor de dienstverlening van dit bedrijf in 2017 dagenlang stil kwam te liggen. Een recenter voorbeeld is de in de e-mailsoftware van Microsoft Exchange aanwezige kwetsbaarheid, die gebruikt is om gijzelsoftware te installeren bij een logistiek bedrijf voor voedselwaren in 2021. Deze aanval leidde ertoe dat de distributie van kaas aan diverse supermarkten circa een week stil kwam te liggen. In hetzelfde jaar is een ICT-leverancier van bijna honderd notarissen getroffen door een digitale aanval. Dit leidde er onder andere toe dat geen aktes gepasseerd konden worden. Als dreigings- of incidentinformatie over de netwerk- en informatiesystemen van deze *andere aanbieders* bij hen terecht was gekomen, dan hadden deze nadelige gevolgen mogelijk kunnen worden voorkomen of had de impact van deze aanvallen mogelijk kunnen worden beperkt.

De bovengenoemde voorbeelden illustreren dat het niet wenselijk is dat *andere aanbieders* verstoken blijven van informatie over dreigingen en incidenten met betrekking tot hun eigen netwerk- en informatiesystemen, indien het NCSC daar wel over beschikt. Zo heeft NCSC met regelmaat – vanuit analyses ten behoeve van de primaire taakuitoefening – de beschikking over informatie betreffende kwetsbare of getroffen netwerk- en informatiesystemen van *andere aanbieders*. Indien die informatie niet bij *andere aanbieders* bekend raakt, kan dit tot gevolg hebben dat één of meer van hun netwerk- en informatiesystemen kwetsbaar blijven. Hierdoor bestaat een vergroot risico op bijvoorbeeld het door derden succesvol installeren van gijzelsoftware *(ransomware)* waarmee bestanden worden versleuteld. Een ander risico is bijvoorbeeld het door derden binnendringen van de systemen om kennis te nemen van de daarin aanwezige gegevens of om deze te wijzigen. Dit kan leiden tot de uitval van de beschikbaarheid of het verlies van de integriteit van netwerk-

en informatiesystemen die aanbieders voor hun dienstverlening nodig hebben, met alle nadelige consequenties voor de continuïteit van hun dienstverlening van dien.

Met de wijzigingen in dit wetsvoorstel wordt het in ruimere zin mogelijk om *andere aanbieders* in het bezit te laten komen van informatie over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen. Zij kunnen deze informatie gebruiken voor het nemen van maatregelen om digitale incidenten te voorkomen of te verhelpen en daarmee de continuïteit van hun dienstverlening zo goed mogelijk te waarborgen. Daarmee kan bovendien mogelijk ook worden voorkomen dat vitale aanbieders of rijksoverheidsorganisaties nadelige effecten ondervinden van digitale dreigingen en incidenten bij die andere aanbieders wanneer die andere aanbieders hun ketenpartners zijn. Dit voorstel zorgt ervoor dat de digitale weerbaarheid van de Nederlandse samenleving verder wordt versterkt.[1]

3. Inhoud van het wetsvoorstel

Dit wetsvoorstel strekt tot de volgende aanpassingen van de Wbni:
a. het in bepaalde gevallen delen van dreigings- en incidentinformatie met aanbieders die geen vitale aanbieder of onderdeel van de rijksoverheid zijn (andere aanbieders);
b. het zonder instemming van aanbieders delen van vertrouwelijke herleidbare gegevens met betrekking tot die aanbieders aan OKTT's; en
c. de aanwijzing van OKTT's bij ministeriële regeling.

Paragraaf 3.1 gaat in op de onder a. omschreven aanpassing, paragraaf 3.2 gaat in op de onder b. en c. omschreven aanpassingen.

3.1 Delen van dreigings- en incidentinformatie met andere aanbieders

3.1.1 Probleembeschrijving

Op grond van artikel 3, eerste lid, Wbni is de primaire taak van het NCSC het verlenen van bijstand aan vitale aanbieders en aanbieders die onderdeel zijn van de rijksoverheid bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen, en het daartoe verrichten van analyses en technisch onderzoek. Het NCSC kan bij die analyses en dat technisch onderzoek ook dreigings- en incidentinformatie (waaronder persoonsgegevens) verkrijgen met betrekking tot netwerk- en informatiesystemen van *andere aanbieders*. Dit kan bijvoorbeeld een veiligheidsregio, politieke partij of beheerder van parkeervoorzieningen betreffen. Andere voorbeelden hiervan zijn een distributeur van voedselwaren, containeroverslagbedrijf en ICT-leverancier, zoals hierboven in de In- en aanleiding benoemd. In dit kader wordt doorgaans gesproken van «restdata» of «bijvangst».

Artikel 3, tweede lid, Wbni regelt dat het NCSC deze informatie, met inbegrip van persoonsgegevens, kan verstrekken aan verschillende zogeheten schakelorganisaties, in het bijzonder de organisaties genoemd in onderdelen a tot en met c. Hieronder vallen onder meer bij ministeriële regeling aangewezen computercrisisteams en OKTT's, die *andere aanbieders* als doelgroep hebben en hen over de voor hen relevante dreigingen of incidenten kunnen informeren en adviseren. Een voorbeeld

[1] In dit kader is de Tweede Kamer meerdere malen op het voornemen tot en voortgang van dit wetsvoorstel gewezen, zie o.a. *Kamerstukken II* 2020/21, 26 643, nrs. 738 en 767.

van een computercrisisteam is de stichting Z-CERT, het *computer emergency response team* voor aanbieders in de zorgsector. Een voorbeeld van een OKTT is Cyberweerbaarheidscentrum Brainport, waarover meer in paragraaf 3.2.1.

In de praktijk is echter gebleken dat niet altijd een schakelorganisatie in de zin van artikel 3, tweede lid, onderdelen a tot en met c, aanwezig is voor *andere aanbieders*. In die gevallen is het niet mogelijk om die *andere aanbieders* in het bezit te laten komen van voor hen relevante dreigings- of incidentinformatie, terwijl het NCSC daar wel over beschikt. Dit heeft als nadelig maatschappelijk gevolg dat de beschikbaarheid of betrouwbaarheid van hun netwerk- en informatiesystemen en daarmee de continuïteit van de dienstverlening van die *andere aanbieders* in gevaar komt.

Een recent voorbeeld hiervan zijn de organisaties die onderdeel uitmaken van de vaccinatieketen voor de bestrijding van COVID-19, bijvoorbeeld omdat zij een rol vervullen binnen de logistieke keten of de (gekoelde) opslag van vaccins. Aan deze organisaties konden de hiervoor bedoelde gegevens niet worden verstrekt door het NCSC. Dat betekende in de praktijk dat zij niet op de hoogte waren van voor hen relevante dreigingen of incidenten en zij in verband daarmee geen maatregelen konden nemen om incidenten te voorkomen of te verhelpen. Hierdoor was het mogelijk dat risico's voor de dienstverlening van deze aanbieders (zoals sabotage of uitval van de logistieke processen in de vaccinatieketen) in stand bleven en de omstandigheden waaronder de opslag plaats diende te vinden of de planning van de leveringen daardoor mogelijk niet langer zouden kunnen worden geborgd.

3.1.2 Probleemaanpak

In verband met het hiervoor beschreven probleem wordt voorgesteld om artikel 3, tweede lid, Wbni aan te vullen, zodat het NCSC ook tot taak heeft om in bepaalde gevallen de voor aanbieders die geen vitale aanbieder zijn en evenmin onderdeel zijn van de rijksoverheid, relevante dreigings- en incidentinformatie aan hen zelf te verstrekken. Met deze voorgestelde wijziging kunnen zij vaker dan thans mogelijk informatie van het NCSC ontvangen over voor hen relevante digitale dreigingen en incidenten. Het is immers niet wenselijk dat zij, vanwege de omstandigheid dat zij (nog) niet in de doelgroep vallen van bijvoorbeeld een OKTT, verstoken blijven van informatie over dreigingen en incidenten met (mogelijke) aanzienlijke gevolgen voor hun dienstverlening, terwijl het NCSC daar wel over beschikt. De continuïteit van hun dienstverlening kan hierdoor in gevaar komen, met alle mogelijke nadelige maatschappelijke gevolgen van dien. Door in bepaalde gevallen zo nodig belangrijke dreigings- en incidentinformatie aan andere aanbieders te kunnen verstrekken, worden zij in de gelegenheid gesteld maatregelen te treffen om incidenten te voorkomen of de gevolgen daarvan te beperken.

Om de bovengenoemde verstrekking van dreigings- en incidentinformatie door het NSCS aan *andere aanbieders* in bepaalde gevallen mogelijk te maken is deze wijziging van artikel 3, tweede lid, Wbni noodzakelijk. De reden hiervoor is dat het voor *andere aanbieders* van groot belang is dat ook persoonsgegevens deel uitmaken van dreigings- en incidentinformatie én dat voor de verstrekking van die persoonsgegevens een specifieke taak in de wet moet zijn opgenomen. Zonder persoonsgegevens als IP-adressen, domeinnamen en e-mailadressen van gebruikers van kwetsbare systemen of aanvallers, is de verstrekking van dreigings- en incidentinformatie voor aanbieders niet zinvol. Zij kunnen dan namelijk niet bepalen welke van hun netwerk- en informatiesystemen kwetsbaar of

al getroffen zijn en welke maatregelen genomen zouden moeten worden om dreigingen weg te nemen of incidenten te verhelpen. Met de wijziging van artikel 3, tweede lid, Wbni wordt, in combinatie met artikel 17, eerste lid, Wbni, een krachtens de Algemene verordening gegevensbescherming (hierna: AVG) vereiste grondslag voor rechtmatige verwerking voor deze verstrekkingen gecreëerd.

De voorgestelde bevoegdheid tot het verstrekken van restdata is beperkt tot gevallen, zoals omschreven in het voorgestelde artikel 3, tweede lid, onder e. Dit houdt in dat restdata door het NCSC aan *andere aanbieders* kan worden verstrekt, indien er:

1) sprake is van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.
   Die aanzienlijke gevolgen voor de continuïteit van de dienstverlening komen dan voort uit het uitvallen van de beschikbaarheid of het verlies van integriteit van de netwerk- en informatiesystemen die voor de dienstverlening van de betrokken aanbieder worden gebruikt. Het NCSC zal per geval hieraan toetsen, mede met het oog op de voor verstrekking van persoonsgegevens vereiste noodzakelijkheidstoets uit de AVG.
2) geen schakelorganisatie in de zin van artikel 3, tweede lid, onderdelen a tot en met c, is die de aanbieder van die informatie kan voorzien. Het aan de hand van artikel 3, tweede lid, Wbni ingerichte stelsel van informatie-uitwisseling is zo ingericht dat het verstrekken van bijvangst ten behoeve van *andere aanbieders* telkens plaatsvindt door tussenkomst van een in dat lid bedoelde schakelorganisatie, indien een schakelorganisatie aanwezig is. De schakelorganisaties zoals genoemd in de onderdelen a tot en met c hebben nadrukkelijk tot taak om aanbieders in hun achterban over hen aangaande digitale dreigingen en incidenten te informeren en mogelijk ook te adviseren. Zij zijn het meest bekend met de in hun achterban aanwezige netwerk- en informatiesystemen, bijbehorende belangen en risico's en informatiebehoeften. Op deze wijze kan informatie via deze schakelorganisaties zo efficiënt en accuraat mogelijk aan belanghebbende *andere aanbieders* worden doorverstrekt.

Deze twee vereisten zijn cumulatief. Dit betekent dat alleen in de situaties waarin een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening van de andere aanbieder én voor de verstrekking van gegevens een schakelorganisatie in de zin van artikel 3, tweede lid, onderdelen a tot en met c, ontbreekt, kan worden overgegaan tot het delen van de restinformatie.

De bevoegdheid tot het verstrekken van restdata met *andere aanbieders* wordt tot enkele deze gevallen beperkt omdat:

– de primaire taken en dus ook de focus van de dienstverlening van het NCSC gericht zijn op het verlenen van bijstand aan vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid, om zo de meest ernstige maatschappelijke ontwrichting te voorkomen of te beperken;
– in het verlengde hiervan ervoor is gekozen om verstrekking van voor *andere aanbieders* relevante restdata door het NCSC krachtens artikel 3, tweede lid, Wbni door tussenkomst van schakelorganisaties te laten plaatsvinden;
– mede hierom een landelijk dekkend stelsel van schakelorganisaties c.q. cybersecurity samenwerkingsverbanden (LDS) in opbouw is;
– het door het NCSC vaker dan in incidentele gevallen informeren van *andere aanbieders* de taakuitoefening van andere partijen in het LDS kan doorkruisen; en

– een verdergaande informatietaak ten behoeve van *andere aanbieders* voor het NCSC een onevenredige extra belasting van de capaciteit oplevert, waarbij de primaire taakuitoefening in het gedrang kan komen.

3.2 Delen van vertrouwelijke herleidbare gegevens over aanbieders met OKTT's

3.2.1 Probleembeschrijving

Op grond van artikel 20, tweede lid, Wbni kan het NCSC, ter uitvoering van de in artikel 3 Wbni genoemde taken, zonder instemming van aanbieders, vertrouwelijke gegevens die herleid kunnen worden tot deze aanbieders (zoals namen van aanbieders) verstrekken aan een beperkte kring van organisaties. Deze beperkte kring van organisaties bestaat uit *computer security incident response teams* als bedoeld in artikel 9 van de NIB-richtlijn[2] (hierna: CSIRTs), de inlichtingen- en veiligheidsdiensten, en bij ministeriële regeling aangewezen computercrisisteams. OKTT's behoren thans niet tot de kring van organisaties die zijn opgesomd in artikel 20, tweede lid, Wbni. Hierdoor kan verstrekking van de vorengenoemde gegevens thans dus niet aan OKTT's plaatsvinden.

In de praktijk is echter gebleken dat OKTT's in belangrijke mate een vergelijkbare rol als computercrisisteams hebben. OKTT's fungeren ook als een schakelorganisatie voor een achterban van aanbieders die (grotendeels) geen vitale aanbieder zijn en ook geen deel uitmaken van de rijksoverheid, en kunnen deze rol slechts beperkt uitvoeren indien zij niet ook over de vorengenoemde vertrouwelijke herleidbare gegevens beschikken. Voorbeeld van een dergelijke OKTT is Cyberweerbaarheidscentrum Brainport, een stichting die is opgericht ten behoeve van ondernemingen die deel uitmaken van de Nederlandse kennisintensieve industrie, geïnitieerd door grote bedrijven in de Eindhovense hightech regio. Een grote hoeveelheid organisaties is geen vitale aanbieder of aanbieder die onderdeel is van de rijksoverheid en is ook niet aangesloten bij een bij ministeriële regeling aangewezen computercrisisteam, en is daarmee afhankelijk van OKTT's voor hun informatie over kwetsbare of getroffen systemen. Zonder die informatie weten zij niet dat ze kwetsbaar zijn en kunnen zij hier geen maatregelen tegen treffen.

Ook is gebleken dat door het huidige artikel 20, tweede lid, Wbni de met artikel 3, tweede lid, Wbni juist beoogde verstrekking van ook persoonsgegevens (bijvoorbeeld getroffen IP-adressen en e-mailadressen) aan OKTT's ten behoeve van het informeren van organisaties in hun doelgroep vaak onbedoeld niet mogelijk is. OKTT's kunnen namelijk (net als de in artikel 20, tweede lid, Wbni wel opgenomen computercrisisteams) persoonsgegevens vaak tot specifieke aanbieders herleiden. Die (persoons)gegevens zijn daardoor ook gegevens als bedoeld in artikel 20, tweede lid, Wbni, maar kunnen door de afwezigheid van OKTT's in diezelfde bepaling niet met OKTT's gedeeld worden door het NCSC. Het gevolg hiervan is dat aanbieders in de doelgroepen van de OKTT's verstoken blijven van de voor hen relevante dreigings- en incidentinformatie. Hierdoor komen zij in onvoldoende mate in de gelegenheid om naar aanleiding van die informatie maatregelen te nemen om incidenten te voorkomen of te verhelpen, met alle nadelige maatschappelijke gevolgen van dien.

---

[2] 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).

Zoals hiervoor is vermeld kan bij de voor *andere aanbieders* relevante informatie bijvoorbeeld gedacht worden informatie over *ransomware*-besmettingen. Ook kan worden gedacht aan bij het NCSC beschikbare informatie over kwetsbaarheden in systemen.[3]

3.2.2 Probleemaanpak

In verband met het hiervoor omschreven probleem, dat in de afgelopen periode ook aandacht heeft gekregen in de media[4] en politiek[5], wordt voorgesteld om in artikel 20, tweede lid, Wbni OKTT's toe te voegen aan de opsomming van organisaties waaraan vertrouwelijke herleidbare gegevens met betrekking tot aanbieders kunnen worden verstrekt. Hiermee worden OKTT's in staat gesteld om, op basis van de van het NCSC ontvangen informatie, aanbieders in hun doelgroepen te informeren over voor hen relevante dreigingen en incidenten. Deze aanbieders kunnen op hun beurt dan maatregelen treffen die nodig zijn om dreigingen of incidenten te voorkomen of de gevolgen ervan te beperken.

Met bovenbedoelde wijziging blijft de kring van organisaties waaraan de in artikel 20, tweede lid, Wbni bedoelde informatie kan worden verstrekt beperkt. Ook wordt nog steeds recht gedaan aan de redenen die ten grondslag liggen aan het in artikel 20 Wbni strikt regelen van de voorwaarden waaronder vertrouwelijke gegevens met betrekking tot aanbieders aan derden kunnen worden verstrekt. Voor deze strikte regeling in artikel 20 Wbni is blijkens de wetsgeschiedenis aanleiding gezien om de vertrouwelijkheid van deze voor het NCSC beschikbaar gekomen gegevens zo veel mogelijk te waarborgen. De redenen daarvoor zijn gelegen in het zoveel mogelijk voorkomen van schade bij aanbieders, zoals reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor aanvallen, en in het door het NCSC voor hulpverlening kunnen gebruiken van deze gegevens zonder daarbij gehinderd te worden door mogelijk vroegtijdig openbaar worden daarvan. Met name als het gaat om niet verplicht te melden gegevens bestaat anders ook het risico dat aanbieders terughoudend worden met het delen van informatie en het NCSC daardoor serieus benadeeld wordt in de uitoefening van zijn taken.

Aanwijzing OKTT's bij ministeriële regeling

Organisaties worden thans als OKTT aangewezen door middel van een daartoe strekkende ministeriële aanwijzing. Aanwijzing van organisaties als computercrisisteams, bedoeld in de artikelen 3, tweede lid, en 20, tweede lid, Wbni, geschiedt daarentegen door middel van een ministeriële regeling. De aanwijzing van OKTT's vindt thans dus in juridische zin op een andere wijze plaats dan de aanwijzing van computercrisisteams. Voor dat verschil bestaat inmiddels echter om verschillende redenen geen aanleiding. Zo hebben OKTT's een in belangrijke mate vergelijkbare rol als computercrisisteams waar het gaat om informatiedeling met hun achterban. Bovendien zijn de eisen en voorwaarden die gesteld worden aan de aanwijzing van een organisatie als OKTT of als computercrisisteam

---

[3] *Kamerstukken II* 2019/20, 26 643, nr. 666.

[4] Zie onder meer de berichtgeving hierover in het Financieele Dagblad van 28 september 2021 («Bedrijfsleven start eigen alarmsysteem tegen hackers: «overheid te traag») en in de Volkskrant van 29 september 2021 («Informatie over op handen zijnde hacks wordt grotendeels weggegooid»).

[5] Zie de vragen van de leden Amhaouch en Palland (beiden CDA) aan de Minister van Justitie en Veiligheid (ingezonden 6 oktober 2021). Het belang van het breder delen van informatie over dreigingen en incidenten wordt wederom aangekaart in het recentelijk verschenen rapport van de Onderzoeksraad voor Veiligheid (OVV) «Kwetsbaar door software – Lessen naar aanleiding van de beveiligingslekken door software van Citrix» van 16 december 2021 jl.

al vrijwel gelijk aan elkaar. Voordat een organisatie bij ministeriële regeling wordt aangewezen als computercrisisteam, bedoeld in de artikelen 3, tweede lid, en 20, tweede lid, Wbni, vindt thans een grondige beoordeling plaats om te bepalen of verstrekking door het NCSC van de in die artikelen bedoelde informatie aan die organisatie verantwoord en gerechtvaardigd is. Vóór de aanwijzing van een organisatie als OKTT op grond van artikel 3, tweede lid, van de Wbni vindt ook al nagenoeg dezelfde grondige beoordeling plaats. 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.

Gelet op de hiervoor genoemde gelijkenissen bevat dit wetsvoorstel daarom ook een wijziging van de artikelen 3 en 20 Wbni die ertoe strekt om de aanwijzing van organisaties als OKTT ook in juridische zin op dezelfde manier te laten plaatsvinden als de aanwijzing van organisaties als computercrisisteam. Concreet houdt dit in dat de aanwijzing van een organisatie als OKTT voortaan, net als de aanwijzing van een computercrisisteam, bij ministeriële regeling geschiedt. In de praktijk leidt genoemde wijziging niet tot veranderingen voor OKTT's, anders dan de (juridische) wijze waarop zij worden aangewezen.

4. Verhouding NCSC – Digital Trust Center

Het NCSC en het Digital Trust Center (hierna: het DTC), onderdeel van het Ministerie van Economische Zaken en Klimaat (hierna: EZK), hebben 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 conti-

nuïteit van de dienst te waarborgen of te herstellen.[6] 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.

De Minister van EZK heeft inmiddels een voorstel voor de Wet bevordering digitale weerbaarheid bedrijven in procedure gebracht, waarin de hiervoor bedoelde taak van het DTC regeling vind. Hiermee wordt de afbakening tussen de primaire doelgroepen van het NCSC en het DTC verder verduidelijkt.

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 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.

Het NCSC kan, zoals onder meer in hoofdstuk 1 is toegelicht, bij zijn primaire taakuitoefening dreigings- en incidentinformatie verkrijgen die relevant is voor aanbieders die buiten zijn doelgroep (vitale aanbieders en rijksoverheidsorganisaties) vallen. Het NCSC heeft dan de taak om die informatie 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, zoals toegelicht in paragraaf 3.1.2, 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.

5. Verhouding tot hoger recht

5.1 Inleidende opmerkingen

Vooropgesteld wordt dat de voorgestelde wijzigingen van artikel 3 en 20 Wbni geen verandering betreffen in de aard van de gegevens die worden verwerkt door het NCSC, maar een beperkte uitbreiding van de kring van partijen aan wie dergelijke gegevens kunnen worden verstrekt. Hetgeen in paragraaf 9 van de memorie van toelichting bij de Wbni is uiteengezet over de grondrechtelijke aspecten (artikel 10 Grondwet, artikel 8 EVRM en

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

artikel 17 IVBPR) van de verwerking van (persoons)gegevens door het NCSC blijft dan ook van toepassing. Hiervoor wordt dan ook verwezen naar die memorie van toelichting. In deze paragraaf wordt volstaan met een aanvulling daarop die specifiek ziet op het door de voorgestelde wijzigingen voortaan in ruimere zin verstrekken van persoonsgegevens, als onderdeel van dreigings- en incidentinformatie, aan of ten behoeve van aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid.

5.2 EVRM

De verwerking van persoonsgegevens door het NCSC is een inmenging door het openbaar gezag in het in artikel 8, eerste lid, EVRM, geformuleerde recht op respect voor de persoonlijke levenssfeer. Dat geldt dus ook voor de verstrekking van persoonsgegevens op grond van artikel 3, tweede lid, Wbni al dan niet in samenhang met artikel 20, tweede lid, aan *andere aanbieders* of hun OKTT's. Het tweede lid van artikel 8 EVRM staat inmenging in dit recht alleen toe voor zover zij bij wet is voorzien, een geoorloofd, expliciet genoemd doel dient en noodzakelijk is in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit.

Voor het in bepaalde gevallen aan *andere aanbieders* verstrekken van persoonsgegevens op grond van het voorgestelde artikel 3, tweede lid, onder e, geldt dat met de toevoeging van dit nieuwe onderdeel aan artikel 3, tweede lid, in samenhang met artikel 17, eerste lid, Wbni, een specifieke wettelijke grondslag wordt gecreëerd en deze verwerking hiermee bij wet voorzienbaar wordt. Diezelfde wettelijke grondslag geldt, in combinatie met artikel 20, tweede lid, voor de nieuw voorgestelde mogelijkheid van verstrekking aan OKTT's van persoonsgegevens die tevens vertrouwelijke tot aanbieders herleidbare gegevens zijn.

De verstrekking van «restdata», met inbegrip van persoonsgegevens, aan *andere aanbieders* of hun OKTT's heeft tot doel om nadelige maatschappelijke gevolgen te voorkomen. Door *andere aanbieders*, al dan niet door tussenkomst van een OKTT, in het bezit te laten komen van voor hen relevante dreigings- en incidentinformatie worden ook deze partijen in staat gesteld om maatregelen te nemen om digitale incidenten te voorkomen of te verhelpen.

Wat betreft het uit het noodzaakcriterium voortvloeiende vereiste van een dringende maatschappelijke behoefte wordt gewezen op het volgende. Door de grote afhankelijkheid van de samenleving van elektronische informatiesystemen, die bovendien onderling verweven zijn, bestaat er een dringende maatschappelijke behoefte aan het door het NCSC verwerken van persoonsgegevens. Hieronder valt ook het al dan niet door tussenkomst van schakelorganisaties verstrekken van dergelijke gegevens aan aanbieders die geen vitale aanbieder zijn en ook geen deel uitmaken van de rijksoverheid, ofwel *andere aanbieders*. De verstrekking van persoonsgegevens (IP-adressen, e-mailadressen en domeinnamen) aan *andere aanbieders*, al dan niet door tussenkomst van hun OKTT's zorgt ervoor dat zij worden geïnformeerd over digitale dreigingen en incidenten betreffende hun systemen, zodat zij maatregelen kunnen nemen om de gevolgen hiervan te mitigeren.

Ten aanzien van de proportionaliteit wordt het volgende opgemerkt. De voorgestelde nieuwe taak om persoonsgegevens aan *andere aanbieders* te verstrekken is gelet op de aard ervan, het doel en de overige

waarborgen waarmee deze verwerking is omkleed, geen forse inmenging in het recht op respect voor iemands privéleven. Datzelfde geldt voor de voorgestelde verstrekking van persoonsgegevens die tevens vertrouwelijke tot aanbieders herleidbare gegevens zijn, aan OKTT's van genoemde *andere aanbieders*. Daarbij geldt, in het geval van verstrekking aan *andere aanbieders* zelf, dat verstrekking ook enkel plaatsvindt in bepaalde gevallen, namelijk indien er geen schakelorganisatie in de zin van artikel 3, onderdelen a tot en met c voorhanden is die de aanbieder van die informatie kan voorzien en er sprake is van (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van die aanbieder. Verstrekking geschiedt alleen voor zover dat noodzakelijk is voor het uitvoeren van de in artikel 3, tweede lid, Wbni genoemde taak. Verwerking van persoonsgegevens vindt plaats met inachtneming van de AVG.

Ten aanzien van de subsidiariteit wordt erop gewezen dat de persoonsgegevens die het NCSC aan de in artikel 3, tweede lid, Wbni bedoelde partijen verstrekt telkens deel uitmaken van informatie die is verkregen bij het verrichten van analyses in het kader van de in artikel 3, eerste lid, Wbni bedoelde taakuitoefening. Voor de in het tweede lid bedoelde partijen geldt dat zij door het NCSC niet op een andere wijze kunnen worden voorzien van voldoende informatie om op basis daarvan maatregelen te nemen om incidenten te voorkomen of de gevolgen daarvan te beperken. Ook het anonimiseren of pseudonimiseren van dreigings- en incidentinformatie maakt het voor het NCSC niet mogelijk om deze partijen in het bezit te laten komen van informatie die hen in staat stelt genoemde maatregelen te nemen.

Geconcludeerd wordt dat ook de nieuwe voorgestelde verstrekkingen van persoonsgegevens door het NCSC een gerechtvaardigde beperking zijn van de persoonlijke levenssfeer.

6. Gevolgen voor burgers en bedrijven

De in paragraaf 3.1 bedoelde aanbieders en de in paragraaf 3.2 bedoelde OKTT's en aanbieders binnen hun doelgroepen kunnen als gevolg van deze wetswijziging (extra) dreigings- en incidentinformatie verkrijgen. Zij kunnen zelf bepalen hoe zij omgaan met deze informatie en aanbieders kunnen zelf bepalen of zij naar aanleiding van de informatie die zij ontvangen, maatregelen treffen om incidenten te voorkomen of de gevolgen ervan te beperken. Dit voorstel leidt niet tot verplichtingen voor deze partijen. Van toezicht en handhaving is ook geen sprake. Het wetsvoorstel kent dus geen regeldruk(kosten), administratieve lasten en nalevingskosten voor burgers en bedrijven.

7. Uitvoering

Dit voorstel brengt in de uitvoering gevolgen met zich mee voor het NCSC. De voorgestelde wijzigingen zorgen ervoor dat aan OKTT's in ruimere zin dan tot nu toe het geval is gegevens kunnen worden verstrekt, en dat voortaan in bepaalde gevallen, zoals omschreven in het voorgestelde artikel 3, tweede lid, onder e, aan *andere aanbieders* informatie over digitale dreigingen en incidenten kan worden verstrekt.

Voor deze verstrekkingen zijn al de nodige processen ingericht voor de uitvoering als het gaat om verstrekking van gegevens aan OKTT's. Voor het in bepaalde gevallen verstrekken van restdata aan andere aanbieders zal het per geval verschillen op welke wijze de data verstrekt kunnen worden, maar ook hiervoor zijn er al methoden voorhanden bij het NCSC ter uitvoering daarvan. De verwachting is derhalve dat ten aanzien van beide wijzigingen bepaalde werkprocessen aangepast moeten worden,

maar dat de impact daarvan minimaal is. De technische aanpassing van ICT-systemen is hiervoor niet noodzakelijk. Door het in meer gevallen dan momenteel mogelijk verstrekken van bij het NCSC beschikbare dreigings- en incidentinformatie komt de in artikel 3, eerste lid, Wbni bedoelde primaire taakuitoefening van het NCSC niet in het geding. Van belang is in dat verband dat die bredere verstrekking steeds informatie betreft die wordt verkregen bij het verrichten van analyses in het kader van die primaire taakuitoefening.

8. Toezicht en handhaving

Dit voorstel leidt niet tot verplichtingen voor de aanbieders en OKTT's als bedoeld in paragraaf 3.1 en 3.2. Van toezicht op en handhaving van de naleving van verplichtingen is dan ook geen sprake.

9. Financiële gevolgen

De voorgestelde wijzigingen hebben geen financiële gevolgen voor de OKTT's, die als gevolg van de wijziging van artikel 20, tweede lid, Wbni vertrouwelijke herleidbare gegevens over aanbieders van het NCSC verstrekt kunnen krijgen. Evenmin zijn er financiële gevolgen voor de aanbieders in de doelgroepen van die OKTT's waarop deze gegevens betrekking hebben. Het is aan deze partijen zelf om te bepalen hoe zij omgaan met de ontvangen dreigings- en incidentinformatie.
Ook voor de aanbieders, die als gevolg van de wijziging van artikel 3, tweede lid, Wbni in bepaalde gevallen restdata kunnen verkrijgen van het NCSC, zijn er geen financiële gevolgen. Voor hen geldt eveneens de eigen afweging of en welke maatregelen zij zullen treffen naar aanleiding van de ontvangen informatie.

De voorgestelde wijzigingen hebben wel financiële gevolgen voor het NCSC en daarmee voor het Ministerie van Justitie en Veiligheid. Omdat dit wetsvoorstel echter een beperkte uitbreiding van de taken van het NCSC inhoudt, zijn de financiële gevolgen van dit voorstel gering. Geschat wordt dat voor de uitvoering van de voorgenomen wijziging van de Wbni tot maximaal 11.000 euro per jaar aan extra financiële middelen nodig zijn. Deze kunnen binnen de bestaande begroting van het Ministerie van Justitie en Veiligheid worden opgevangen.

10. Advies en consultatie[7]

10.1 Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (hierna: AP) heeft eind oktober 2021 advies uitgebracht over het wetsvoorstel.

De AP wijst er ten eerste op dat het NCSC de taak krijgt om «andere aanbieders» te informeren over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen en dat dit onder andere IP-adressen betreft van waaruit digitale aanvallen afkomstig zijn. Volgens de AP kunnen zulke aanvallen strafbaar zijn op grond van artikel 138ab, 139d of 350a van het Wetboek van Strafrecht. De AP merkt op dat deze IP-adressen daarom mogelijk kwalificeren als persoonsgegevens betreffende strafbare feiten in de zin van artikel 10 AVG. De AP adviseert daarom in de memorie van toelichting aan te geven of de hierboven bedoelde IP-adressen moeten worden beschouwd als persoonsgegevens betreffende strafbare feiten in de zin van artikel 10 AVG, en zo ja, welke

[7] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

consequenties de toepasselijkheid van artikel 10 AVG heeft voor de verwerking van deze IP-adressen in het kader van dit wetsvoorstel.

Uit jurisprudentie van de Hoge Raad[8] volgt dat voor de vraag of persoonsgegevens strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG betreffen, van belang is of sprake is van zodanige concrete feiten en omstandigheden dat zij een als een als strafbaar feit te kwalificeren bewezenverklaring – in de zin van artikel 350 Wetboek van Strafvordering – kunnen dragen. Hieruit volgt de maatstaf of vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan. Daarnaast speelt attributie – de mate waarin een strafbaar feit daadwerkelijk aan een persoon kan worden toegerekend – een rol in de vraag of een persoonsgegeven kan worden gekwalificeerd als strafrechtelijk persoonsgegeven.

Verstrekking van dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, door het NCSC aan of ten behoeve van *andere aanbieders* heeft tot doel om hen in de gelegenheid te brengen om maatregelen te nemen om digitale incidenten te voorkomen of te verhelpen en daarmee de digitale weerbaarheid van die aanbieders te vergroten, en bijvoorbeeld niet tot doel om handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. Ten aanzien van de enkele verwerking van IP-adressen met het oog op vorengenoemd doel geldt dat niet kan worden afgeleid dat sprake is van een gedraging die een zwaardere verdenking dan een redelijk vermoeden van schuld oplevert. Om te constateren dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld zullen naast IP-adressen namelijk meer concrete feiten en omstandigheden nodig zijn. Bovendien zullen de te verwerken IP-adressen alleen in combinatie met andere tot een persoon herleidbare gegevens kunnen leiden tot attributie. Aan de bovengenoemde twee criteria (vaststellen dat sprake is van zodanige concrete feiten en omstandigheden dat zij op zich zelf genomen als een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren én aan een persoon kunnen toerekenen van een strafbaar feit) wordt aldus niet voldaan. De IP-adressen dienen in dit verband derhalve niet als strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG te worden beschouwd.

De AP adviseert ten tweede de verstrekking aan «andere aanbieders» beter af te bakenen. Daarbij merkt de AP op dat het begrip «andere aanbieders» een zeer ruim bereik heeft en de voorwaarden waaronder mag worden verstrekt (geen schakelorganisatie die de aanbieder van die informatie kan voorzien én informatie over een dreiging of incident met aanzienlijke gevolgen voor de continuïteit van de dienstverlening) niet strikt zijn geformuleerd. Volgens de AP is daarnaast sprake van overlap met de door de Minister van EZK voorgestelde Wet bevordering digitale weerbaarheid bedrijven en adviseert de AP gelet daarop te overwegen bedrijven uit te zonderen van het begrip «andere aanbieders».[9]

Inzake het voorgestelde artikel 3, tweede lid, onder e, Wbni is, zoals uiteengezet in de memorie van toelichting (paragraaf 3.1.2), ervoor gekozen om de daarin geregelde bevoegdheid tot verstrekking van

---

[8] Zie het arrest van de Hoge Raad van 29 mei 2009, ECLI:NL:HR:2009:BH4720.

[9] De voorgestelde Wet bevordering digitale weerbaarheid bedrijven regelt de taken en bevoegdheden van de Minister van EZK op het gebied van de verbetering van de digitale weerbaarheid van niet-vitale bedrijven in Nederland, waaronder het (in de praktijk door het Digital Trust Center van het ministerie) informeren en adviseren van die bedrijven over digitale dreigingen en incidenten.

dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, te beperken tot gevallen waarin:
– een aanbieder niet een vitale aanbieder of organisatie die deel uitmaakt van de rijksoverheid is;
– die aanbieder geen schakelorganisatie in de zin van artikel 3, tweede lid, onderdelen a tot en met c, heeft door tussenkomst waarvan informatie zou kunnen worden verstrekt, en;
– informatie een dreiging of incident betreft met (potentiële) aanzienlijke gevolgen voor diens netwerk- en informatiesystemen.

Hiermee wordt de reikwijdte van deze bevoegdheid voldoende concreet omschreven. Er is geen aanleiding voor een nadere afbakening van de groep aanbieders waaraan verstrekking mogelijk wordt met de voorgestelde bepaling. Met de voorgestelde bepaling wordt ook ruimte gelaten voor het aan aanbieders verstrekken van belangrijke dreigings- en incidentinformatie, en het daardoor voorkomen van nadelige maatschappelijke gevolgen, indien in een concrete situatie voor die aanbieder op dat moment nog geen of niet meer een schakelorganisaties als bedoeld in artikel 3, tweede lid, onderdelen a tot en met c, Wbni is. In dit licht bezien is het dan ook niet aangewezen om bepaalde categorieën andere aanbieders, waaronder niet-vitale bedrijven waarvoor het DTC (mede als gevolg van de voorgestelde Wet bevordering digitale weerbaarheid bedrijven schakelorganisatie) zal zijn, specifiek uit te zonderen van toepasselijkheid van het voorgestelde artikel 3, tweede lid, onder e. In plaats daarvan wordt in algemene zin bepaald dat bij aanwezigheid van een schakelorganisatie in bovenbedoelde zin verstrekking niet aan andere aanbieders zelf kan geschieden. Daarnaast merk ik nog op dat het criterium «aanzienlijke gevolgen voor de dienstverlening» ook wordt gehanteerd in onder meer artikel 16 Wbni en aldus geen ongebruikelijk criterium is om de reikwijdte van een wettelijke taak of bevoegdheid (mede) af te bakenen.

De AP adviseert ten derde aan te geven welke grondslag van toepassing is op de verwerking door publieke «andere aanbieders».

Zoals hierboven reeds benadrukt, heeft de voorgestelde wijziging van artikel 3 Wbni tot doel om voor het NCSC de krachtens de AVG vereiste wettelijke grondslag voor verstrekking van dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, aan andere aanbieders te creëren. Dit wetsvoorstel regelt niet de grondslag voor verwerking van die gegevens na ontvangst daarvan door die andere aanbieders. Voor zowel publieke organisaties als private organisaties, die op grond van het voorgestelde artikel 3, tweede lid, onder e, Wbni informatie van het NCSC zullen kunnen verkrijgen, geldt dat zij zelf verantwoordelijk zijn voor het bepalen van de grondslag op basis waarvan zij die informatie verder verwerken.

Tot slot wijst de AP op een opmerking in de toelichting die ten onrechte de indruk wekt dat het gebruik van VPN-software als zodanig leidt tot kwetsbaarheden in systemen. De AP merkt op dat kwetsbaarheden in iedere soort software kunnen voorkomen en dus niet specifiek zijn voor VPN-software. Naar aanleiding hiervan is de toelichting (paragraaf 3.2.1) aangepast.

10.2 Cyber Security Raad

De Cyber Security Raad (hierna: CSR) spreekt zijn steun uit voor de in dit wetsvoorstel geregelde uitbreiding van de bevoegdheid van het NCSC om namens de Minister van Justitie en Veiligheid dreigings- en incidentinformatie te verstrekken, en is van mening dat zowel dit wetsvoorstel als het wetsvoorstel over de Wet bevordering digitale weerbaarheid bedrijven

van de Staatssecretaris van Economische Zaken en Klimaat een grote en belangrijke stap vormt in het verwezenlijken van het LDS om meer dreigingsinformatie die bij de overheid aanwezig is te delen met alle bedrijven en organisaties in Nederland. In zijn reactie op de voorgestelde wijziging van de Wbni adviseert de CSR om de drempel in het voorgestelde artikel 3, tweede lid, onder e, Wbni niet hoger te maken dan noodzakelijk, opdat niet-vitale organisaties erop kunnen rekenen dat het NCSC hen waarschuwt in geval er een risico op substantiële schade is (in welke vorm dan ook).

Bij het vaststellen van de criteria in het voorgestelde artikel 3, tweede lid, onder e, Wbni is, zoals uiteengezet in deze memorie van toelichting (paragraaf 3.1.2), met name ook belang gehecht aan het uitgangspunt van informatieverstrekking ten behoeve van *andere aanbieders* door tussenkomst van schakelorganisaties en tegelijk rekening gehouden met de mogelijkheid dat niet voor elke *andere aanbieder* een schakelorganisatie kan worden aangewezen en informatieverstrekking vanuit het NCSC in die gevallen ook nodig kan zijn vanwege (mogelijke) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder. De inschatting of sprake is of kan zijn van aanzienlijke gevolgen voor de continuïteit van de dienstverlening van die aanbieder zal per geval gemaakt moeten worden. Daarbij is met name relevant of de dreiging of het incident waarop data van het NCSC betrekking hebben zodanige gevolgen heeft of kan hebben voor de continuïteit van dienstverlening van de aanbieder dat hierdoor nadelige maatschappelijke gevolgen (kunnen) optreden. In gevallen waarin van dergelijke gevolgen geen sprake zal (kunnen) zijn is overheidsinspanning in relatie tot een digitale dreiging of digitaal incident minder aangewezen.

Met de in artikel 3, eerste lid, onder e, gekozen formulering wordt ook aangesloten bij het criterium dat in artikel 16 Wbni al is opgenomen voor het al dan niet verlenen van bijstand vanuit het NCSC in geval van vrijwillige meldingen van andere aanbieders. Het NCSC zal de inschatting of al dan niet sprake is van bovenbedoelde aanzienlijke gevolgen telkens voldoende kunnen maken op basis van de alsdan beschikbare informatie over de aard en ernst van de specifieke dreiging en de functie van de bij die dreiging in het geding zijnde netwerk- en informatiesystemen. Ook de inschalingsmatrix voor kwetsbaarheden die het NCSC nu al gebruikt, en waaruit een inschatting volgt van de kans op en de schade door misbruik van een kwetsbaarheid, kan daarbij behulpzaam zijn.

Een «risico op substantiële schade» is breder dan het thans voorgestelde criterium en kan bijvoorbeeld financiële schade betreffen zonder dat er sprake is van belemmering van de continuïteit van de dienstverlening. Die inschatting zal veel moeilijker zijn uit te voeren dan de beoordeling of er aanzienlijke gevolgen voor de dienstverlening zijn, mede omdat het voor het NCSC in de praktijk telkens uitermate lastig of zelfs onmogelijk zal zijn om in te kunnen schatten welke andere concrete schade een andere aanbieder zal (kunnen) hebben in verband met een dreiging of incident. Hantering van het door de CSR voorgestelde andere criterium zou dan ook een onevenredige belasting van het NCSC in de taakuitoefening opleveren. Naar mijn oordeel werpt het nu opgenomen criterium daarom geen te hoge drempel op voor situaties waarin het aangewezen is om het NCSC, ter voorkoming van nadelige maatschappelijke gevolgen, informatie aan andere aanbieders zelf te kunnen laten verstrekken.

Verder geeft de CSR aan te hechten aan snelle aanwijzing van het Digital Trust Center (hierna: DTC) van het Ministerie van EZK als OKTT, verdere stimulering van de uitrol van het LDS, het verschaffen van helderheid richting bedrijven en maatschappelijke organisaties over wat zij van

partijen in het LDS kunnen verwachten, het onderzoeken van de mogelijkheid van één overheidsloket van waaruit informatie over cybersecurity wordt verstrekt en het in afwachting van de inwerkingtreding van het onderhavige wetsvoorstel nu al dienovereenkomstig delen van dreigings- en incidentinformatie met OKTT's. Hoewel deze adviezen kwesties betreffen die niet zozeer de inhoud van dit wetsvoorstel betreffen, kan daarover nog wel het volgende worden opgemerkt.

Binnen de rijksoverheid hebben het NCSC en DTC, zoals in hoofdstuk 4 al toegelicht, duidelijk onderscheidenlijke primaire doelgroepen van organisaties waaraan informatie en advies over concrete dreigingen en incidenten wordt verstrekt, namelijk vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid respectievelijk niet-vitale bedrijven. Inmiddels is het DTC krachtens de Wbni ook als OKTT aangewezen en is het NCSC gelet daarop bevoegd om het DTC op grond van artikel 3, tweede lid, Wbni relevante informatie over dreigingen en incidenten te verstrekken, zodat het DTC mede op basis daarvan bedrijven in hun doelgroep van informatie en advies kunnen voorzien. Duidelijkheid over de onderscheidenlijke primaire doelgroepen volgt voor het NCSC reeds uit de Wbni en wordt vanwege de voorgestelde Wet bevordering digitale weerbaarheid bedrijven van de Minister van EZK ook in relatie tot het DTC vergroot. Door de voortgaande ontwikkeling van het LDS zal er tevens voor steeds meer aanbieders een eigen schakelorganisatie gaan bestaan, met kennis van onder meer de voor die sector of regio in gebruik zijnde netwerk- en informatiesystemen en ontwikkelingen, die ook krachtens artikel 3, tweede lid, Wbni als bijvoorbeeld OKTT kunnen worden aangewezen.

10.3 OKTT's

FERM juicht de wijziging toe die ziet op het delen van vertrouwelijke herleidbare gegevens over aanbieders met OKTT's. Voor wat betreft de wijziging die ziet op het in bepaalde gevallen delen van dreigings- en incidentinformatie met *andere aanbieders*, ziet FERM bezwaren in het niet transparant zijn van de «bijzonderheid» van de gevallen. Een suggestie van FERM is om voor het delen van restinformatie de OKTT's en het (ook als OKTT aan te wijzen) DTC te gebruiken. **Cyberweerbaarheidscentrum Brainport (CWB)** geeft aan dat ongeveer de helft van haar leden heeft gereageerd op hun uitvraag om een reactie op het voorstel en dat de reacties positief waren: de leden zijn blij dat zij meer dreigings- en incidentinformatie gaan ontvangen. Ze hebben er begrip voor dat er ook vertrouwelijke tot hun bedrijven herleidbare gegevens met CWB zullen worden gedeeld. Het is belangrijk dat deze gegevens veilig opgeslagen, verwerkt en gedeeld worden en niet elders terechtkomen. **Cyberveilig Nederland (CvNL)** is verheugd over het voorstel, maar vraagt om aandacht voor een aantal zaken. Zo pleit CvNL voor het in verband met de hoge urgentie van digitale dreigingen vooruitlopend op de inwerkingtreding van het wetsvoorstel al delen van informatie, is het volgens CvNL van belang dat OKTT's niet als filter gaan werken voor de van het NCSC afkomstige informatie, zijn twee loketten (NCSC en DTC) met dreigingsinformatie voor het Nederlandse bedrijfsleven vanuit de overheid suboptimaal, levert het hanteren van de term «bijzondere gevallen» een belemmering op, is onduidelijk hoe erop wordt toegezien dat tot personen herleidbare informatie op de juiste wijze behandeld wordt, en is de stelling dat «de kring van organisaties waaraan de in artikel 20, tweede lid, Wbni bedoelde informatie kan worden verstrekt, niet te groot [wordt]» voorbarig, nu nog niet bekend is hoeveel OKTT's er zullen komen. **Connect2Trust** staat ten principale positief tegenover het voorstel, maar waarschuwt voor overlap door de toename van schakelorganisaties die als OKTT of computercrisisteam worden aangewezen. Connect2Trust

adviseert daarom om de criteria voor aanwijzingen als OKTT uit te breiden ter voorkoming van het door organisaties dubbel ontvangen van dreigings- en incidentinformatie, de inrichting van een clearinghouse voor het LDS vanuit publiek-private samenwerking, en in de Wbni op basis van heldere en juridisch publiek getoetste criteria aan te geven wanneer dreigings- en incidentinformatie wel of geen persoonsgegeven betreft. **Abuse Information Exchange (AbuseIX)**[10] juicht de voorgestelde wijziging toe, gelet op het belang van de verhoging van de digitale weerbaarheid van organisaties die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, en dringt aan op duidelijkheid met betrekking tot de selectie van potentiële OKTT's, het proces voorafgaand aan de aanwijzing als OKTT middels ministeriële regeling en de vraag hoe een reeds aangewezen OKTT de aanwijzing ongedaan zou kunnen maken.

Bijzondere gevallen

Enkele reacties van bovenbedoelde OKTT's gaan in op de term «bijzondere gevallen» in de memorie van toelichting in relatie tot de voorgestelde wijziging van artikel 3, tweede lid, Wbni. Ook in verschillende internetconsultatiereacties is de opmerking gemaakt dat «bijzondere gevallen» een onvoldoende objectief en onvoldoende duidelijk criterium betreft. Ook wordt in deze reacties gesteld dat het LDS op zeer korte termijn sluitend zal zijn en de mogelijkheid van verstrekking in deze «bijzondere gevallen» daardoor overbodig zal zijn.

Naar aanleiding van deze ontvangen reacties heb ik vastgesteld dat de term «bijzondere gevallen» verwarring heeft doen ontstaan over de voorwaarden waaronder verstrekking van restdata aan *andere aanbieders* mogelijk is. Over die voorwaarden is de tekst van het voorgestelde artikel 3, tweede lid, onder e, Wbni, waarnaar met de term «bijzondere gevallen» steeds bedoeld is te verwijzen, naar mijn oordeel echter voldoende duidelijk. Krachtens dat artikelonderdeel gelden er twee cumulatieve criteria waaraan het NCSC per verstrekking zal moeten toetsen alvorens tot verstrekking van restdata te kunnen overgaan, namelijk dat:

1. er geen hierin genoemde schakelorganisatie is, die de aanbieder van die informatie kan voorzien, en
2. er sprake is van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.

Om de verwarring hierover weg te nemen zijn in de memorie van toelichting de verwijzingen naar «in bijzondere gevallen» aangepast, zodat duidelijk wordt dat het telkens gaat om de gevallen, zoals omschreven in het voorgestelde artikel 3, tweede lid, onder e, Wbni. De Minister van Justitie en Veiligheid (in de praktijk: het NCSC) beoordeelt per geval of wordt voldaan aan de in dat artikel genoemde vereisten.

Voor de in het voorgestelde artikel 3, tweede lid, onder e, Wbni bedoelde bevoegdheid tot verstrekking van restdata aan *andere aanbieders* bestaat ook in relatie tot de aanwezigheid van schakelorganisaties die deel uitmaken van het LDS reden, zolang niet voor alle *andere aanbieders* een dergelijke schakelorganisatie krachtens de Wbni bijvoorbeeld als OKTT is aangewezen en informatie over dreigingen en incidenten met (mogelijke) aanzienlijke gevolgen voor hun dienstverlening niet door tussenkomst van een schakelorganisatie kan plaatsvinden.

[10] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer

Rol van OKTT's

In reactie op de opmerkingen over het voortaan verstrekken van de in het voorgestelde artikel 20, tweede lid, bedoelde gegevens aan OKTT's merk ik het volgende op. Enige vorm van filtering en daardoor mogelijk enige vertraging in informatieverstrekking ten behoeve van *andere aanbieders* in verband met de tussenkomst van OKTT's zal in de praktijk niet volledig te voorkomen zijn. Die filtering is in veel gevallen juist ook nodig om ervoor te zorgen dat de aanbieders in de doelgroepen van de OKTT's slechts de voor hen relevante informatie doorverstrekt krijgen, op basis van een beoordeling door de OKTT voor welke aanbieders binnen de doelgroep de van het NCSC ontvangen informatie relevant is. Een OKTT is vaak een samenwerkingsverband van belanghebbende organisaties, die de netwerk- en informatiesystemen van de onderliggende organisaties en hun informatiebehoefte het beste kent en dus ook het beste kan inschatten of en welke vorm van informatiefiltering of ander maatwerk in informatievoorziening ten behoeve van organisaties in hun doelgroep nodig is.

Zoals in paragraaf 3.2.2 geschetst, vindt – alvorens een organisatie wordt aangewezen als OKTT – een beoordeling plaats of verstrekking van gegevens over dreigingen of incidenten aan die organisatie verantwoord en gerechtvaardigd is, waaronder een toets of de organisatie gegevens, waaronder persoonsgegevens en bedrijfsvertrouwelijke informatie, op een zorgvuldige, veilige en rechtmatige wijze verwerkt. Er vindt geen toezicht plaats vanuit het NCSC op de schakelorganisaties die krachtens de Wbni als OKTT zijn aangewezen. Wel is het zo dat in geval van de aanwijzing als OKTT, de schakelorganisatie een verklaring ondertekent 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. Hiermee wordt, 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.

De kring van organisaties waaraan de in artikel 20, tweede lid, Wbni bedoelde informatie krachtens dat lid kan worden verstrekt omvat momenteel de CSIRT's, andere computercrisisteams en Nederlandse inlichtingen- en veiligheidsdiensten. Dit voorstel regelt dat OKTT's aan deze kring worden toegevoegd. Met deze toevoeging blijft de kring naar mijn oordeel beperkt tot enkele categorieën organisaties die maatregelen kunnen bevorderen ter voorkoming of beperking van nadelige maatschappelijke gevolgen. Het huidige aantal OKTT's is overigens bekend en zal,

door de voorgestelde wijziging om OKTT's voortaan bij ministeriële regeling aan te wijzen, inzichtelijk worden en blijven voor eenieder.

Meerdere malen dezelfde dreigingsinformatie

In enkele reacties wordt de zorg geuit dat aanbieders bij een incident door verschillende overheidsinstanties worden geïnformeerd en dat het voor aanbieders mogelijk onvoldoende duidelijk is waar zij terecht kunnen. Hiervoor verwijs ik naar bovenstaande reactie op het advies van de CSR. In reactie op de opmerkingen over mogelijke overlap in doelgroepen van schakelorganisaties, merk ik op dat overlap niet volledig kan worden voorkomen. Het is primair van belang dat andere aanbieders van voor hen relevante informatie worden voorzien en, gelet daarop, daarom minder bezwaarlijk dat een aanbieder door tussenkomst van diens schakelorganisatie(s) mogelijk dubbel informatie over concrete dreigingen en incidenten ontvangt dan dat die informatie in het geheel niet voor die aanbieder beschikbaar komt. Aanvullende criteria stellen in het kader van het krachtens de Wbni aanwijzen van OKTT's of computercrisisteams om die overlap tegen te gaan, is onwenselijk, omdat dit tot gevolg kan hebben dat een keuze moet worden gemaakt tussen mogelijk als zodanig aan te wijzen schakelorganisaties met overlap in doelgroepen. Dit zou kunnen leiden tot een subjectievere toets dan de huidige. Derhalve bestaat geen reden om aanvullende criteria te gaan hanteren ter voorkoming van mogelijke overlap.

Dreigings- of incidentinformatie en persoonsgegevens

Uit de AVG – niet de Wbni – volgt welke gegevens kwalificeren als persoonsgegevens. Het gaat dan om gegevens die tot personen herleidbaar zijn. Hieronder vallen bijvoorbeeld e-mailadressen, domeinnamen en IP-adressen. Omdat dreigings- en incidentinformatie in de praktijk e-mailadressen, domeinnamen of IP-adressen kan bevatten, is het noodzakelijk om, voor de gevallen waarin die als persoonsgegevens moeten worden beschouwd, een grondslag voor rechtmatige verwerking daarvan te creëren.

10.4 Adviescollege toetsing regeldruk

Het Adviescollege toetsing regeldruk (ATR) heeft het dossier niet geselecteerd voor een formeel advies, omdat het naar verwachting geen (omvangrijke) gevolgen voor de regeldruk heeft.

10.5 Internetconsultatie

Een concept van het wetsvoorstel en de toelichting daarop zijn van 28 juni 2021 tot en met 23 augustus 2021 opengesteld voor consultatie via www.internetconsultatie.nl. Verschillende reacties vanuit die consultatie hierop geven blijk van steun voor de wijzigingen in het wetsvoorstel. De opmerkingen in deze reacties komen deels overeen met opmerkingen in de adviezen van de CSR en de OKTT's. Voor een bespreking daarvan verwijs ik naar de hierboven weergegeven reacties daarop.

Naar aanleiding van de reacties vanuit de internetconsultatie is de tekst van het wetsvoorstel op een enkel punt gewijzigd. Hieronder wordt op deze wijziging ingegaan en wordt daarnaast ingegaan op een aantal punten die eveneens uit de internetconsultatie naar voren zijn gekomen.

Aanwezigheid van schakelorganisatie

In een reactie is aangegeven dat de in het voorgestelde artikel 3, tweede lid, onder e, Wbni gestelde voorwaarde «voor verstrekking van gegevens een onder a tot en met d bedoelde organisatie ontbreekt» ertoe kan leiden dat de verstrekking te sterk beperkt wordt, omdat de aanbieders van internettoegangs- en internetcommunicatiediensten (internetserviceproviders) tot genoemde organisaties behoren (onderdeel d) en bijna elke aanbieder in Nederland dienstverlening van een internetserviceprovider geniet. In reactie hierop is geconcludeerd dat de aanvankelijk voorgestelde bepaling inderdaad te restrictief is geformuleerd. Van belang in dit verband is dat internetserviceproviders, anders dan computercrisisteams en OKTT's, niet nadrukkelijk tot taak hebben om andere aanbieders te voorzien van voor hen specifiek relevante dreigings- en incidentinformatie. Zij vervullen niet een rol die vergelijkbaar is met de andere in het tweede lid genoemde (schakel)organisaties. Hierdoor bestaat het onwenselijke risico dat dreigings- en incidentinformatie, in gevallen waarin een andere aanbieder niet ook een schakelorganisatie als bedoeld in de onderdelen a tot en met c kent maar wel een internetserviceprovider heeft niet voor die aanbieder beschikbaar komt. Daarom is in het wetsvoorstel artikel 3, tweede lid, onderdeel e, Wbni in die zin gewijzigd, dat verstrekking van informatie aan andere aanbieders, indien de informatie een dreiging of incident betreft die aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening, kan plaatsvinden bij afwezigheid van een (schakel)organisatie, genoemd in onderdeel a tot en met c. De memorie van toelichting is op enkele plekken in gelijke zin aangepast.

Taken en bevoegdheden NCSC

Een consultatiereactie spreekt over verregaande bevoegdheden die het wetsvoorstel aan het NCSC geeft om op netwerken van private organisaties (pogen) in te breken om te kunnen bepalen of deze beveiligingslekken hebben en de organisatie daarvan in kennis te stellen. Volgens deze reactie is het niet de taak van de overheid om private bedrijven op gaten in hun systemen te wijzen, maar om deze organisaties op hun verantwoordelijkheden te wijzen en om beveiligingseisen te stellen, controles uit te voeren en sancties op te leggen wanneer er toch een inbraak ontstaat. Deze reactie bevat de vraag wat er gebeurt als een organisatie gehackt wordt, terwijl het NCSC geen dreigingen heeft geconstateerd.

Uit de huidige tekst van de Wbni noch de in dit wetsvoorstel vervatte wijziging van die wet volgt de taak of bevoegdheid van het NCSC om zonder voorafgaande toestemming van de betrokken organisaties zich toegang te verschaffen tot de netwerk- en informatiesystemen van die organisaties. Wel bevat de Wbni thans al voor het NCSC de taak om vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid, op basis van informatie die langs andere weg is verkregen (open bronnen, meldingen van aanbieders, informatie van CSIRTs van andere landen, etc.) en geanalyseerd, te informeren en adviseren over voor die aanbieders relevante dreigingen en incidenten. Voor zover bij die analyses in het kader van de primaire taakuitoefening informatie beschikbaar komt die relevant is voor andere aanbieders, kan verstrekking daarvan geschieden aan schakelorganisaties die krachtens de Wbni bijvoorbeeld als OKTT zijn aangewezen. Het onderhavige voorstel regelt dat die restdata voortaan ook in bepaalde gevallen met *andere aanbieders* én in ruimere zin met OKTT's kan worden gedeeld. Het is vervolgens aan *andere aanbieders* zelf om te bepalen of zij naar aanleiding van de ontvangen informatie maatregelen nemen met betrekking tot de beveiliging van hun netwerk-

en informatiesystemen. Voor alle aanbieders – of het nu gaat om vitale aanbieders, aanbieders die deel uitmaken van de rijksoverheid of *andere aanbieders* – blijft gelden dat het primair de eigen verantwoordelijkheid van de aanbieder zelf is om passende maatregelen te nemen om uitval of verstoring van zijn dienstverlening te voorkomen of te beperken. Het NCSC houdt hier geen toezicht op.

Delen van vertrouwelijke, herleidbare gegevens

In enkele reacties wordt ervoor gepleit om vertrouwelijke tot aanbieders herleidbare gegevens niet aan OKTT's te verstrekken zonder instemming van de betrokken aanbieders. Ook wordt gevraagd om verduidelijking van de zinsnede «zonder instemming van de betrokken aanbieders». In reactie hierop merk ik op dat het delen van vertrouwelijke tot aanbieders herleidbare gegevens met instemming van de betrokken aanbieder reeds mogelijk is. Artikel 20, tweede lid, Wbni regelt in aanvulling daarop de bevoegdheid om ook in gevallen waarin die instemming ontbreekt dergelijke informatie in het kader van de taakuitoefening van het NCSC in beperkte kring te delen. In het geval van als OKTT aangewezen schakelorganisaties wordt, net als nu al voor aangewezen computercrisisteams, reden gezien om die tot die kring te laten behoren, teneinde die OKTT's in staat te stellen andere aanbieders binnen hun doelgroep op basis van de van het NCSC ontvangen (rest)data gericht te kunnen informeren en adviseren over voor die aanbieders relevante digitale dreigingen en incidenten. Om voor deze andere aanbieders zo snel als mogelijk die voor hen zo belangrijke informatie beschikbaar te laten zijn, en daardoor niet onnodig nadelige maatschappelijke gevolgen te laten bestaan, is het van belang dat er geen vertraging ontstaat vanwege het eerst bij elke voorgenomen verstrekking van alle betrokken aanbieders instemming moeten verkrijgen.

Ook wordt gevraagd op welke wijze de vertaalslag plaatsvindt naar niet herleidbare informatie voordat deze door een OKTT wordt doorverstrekt aan tot de doelgroep van die OKTT behorende organisaties. Deze vertaalslag is niet noodzakelijk. De desbetreffende OKTT informeert, na beoordeling voor welke aanbieders de van het NCSC ontvangen informatie relevant is, de organisaties in de doelgroep waarvoor blijkens die beoordeling van dergelijke relevantie is gebleken, over de dreiging of het incident dat hun netwerk- en informatiesystemen aangaat. Daarmee is de door de OKTT door te verstrekken informatie vanzelfsprekend ook dan nog herleidbaar naar de organisatie waarmee de informatie gedeeld wordt. Zoals hierboven reeds toegelicht is het voor een OKTT nodig om ook tot aanbieders herleidbare informatie van het NCSC te kunnen ontvangen om organisaties in hun doelgroep over voor hen relevante dreigingen incidenten te kunnen informeren.

Herziening NIB-richtlijn

In enkele reacties is gewezen op de aanstaande herziening van de NIB-richtlijn[11]. Daarbij wordt aangegeven dat in de Nederlandse wetgeving hierop kan worden voorgesorteerd door enkele benodigde wijzigingen als gevolg van die herziening alvast mee te nemen in het onderhavige wetsvoorstel tot wijziging van de Wbni. Over het voorstel tot herziening van de NIB-richtlijn worden momenteel echter in Europees verband nog onderhandelingen gevoerd. Het is daardoor nog onduidelijk wat de richtlijn tot herziening van de NIB-richtlijn zal gaan inhouden en

[11] 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).

welke gelet daarop benodigde aanpassingen van nationale wetgeving daaruit zullen volgen. Ik zie dan ook geen reden om hierop vooruitlopend in dit wetsvoorstel aanvullende wijzigingen van de Wbni op te nemen.

ARTIKELSGEWIJZE TOELICHTING

Artikel I, onderdeel A

Artikel 3 Wbni bevat een opsomming van de taken die het NCSC namens de Minister van Justitie en Veiligheid uitvoert en in het kader waarvan onder meer persoonsgegevens worden verwerkt. Ook omschrijft dit artikel in de aanhef van het eerste en tweede lid de doeleinden van die taken.

Artikel I, onderdeel A, eerste subonderdeel, strekt tot de wijziging van artikel 3, tweede lid, onderdeel a, Wbni. Met deze wijziging wordt geregeld dat OKTT's worden aangewezen bij ministeriële regeling. Voor een nadere toelichting hierop wordt verwezen naar paragraaf 3.2.2.

Artikel I, onderdeel A, tweede subonderdeel, strekt tot de toevoeging van een onderdeel aan artikel 3, tweede lid, Wbni. Met deze toevoeging wordt geregeld dat de Minister van Justitie en Veiligheid, ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland, ook tot taak heeft om in bepaalde gevallen aan aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, de in dit voorstel bedoelde informatie te verstrekken. Het ingevoegde onderdeel e bepaalt dat van dergelijke gevallen sprake is als de dreiging of het incident waarop de informatie betrekking heeft aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening van de aanbieder én er geen schakelorganisatie in de zin van artikel 3, tweede lid, onderdelen a tot en met c, Wbni, is die de aanbieder van die informatie kan voorzien. Voor een nadere toelichting hierop wordt verwezen naar paragraaf 3.1.2.

Artikel I, onderdeel B

Artikel 20 Wbni bevat regels over de voorwaarden waaronder vertrouwelijke gegevens met betrekking tot aanbieders, waarover het NCSC beschikt, door het NCSC namens de Minister van Justitie en Veiligheid verstrekt kunnen worden aan derden. Voor een nadere toelichting op deze regeling wordt verwezen naar de algemene en artikelsgewijze toelichting bij de Wbni.[12]

Artikel I, onderdeel B, strekt tot de toevoeging van een onderdeel aan artikel 20, tweede lid, Wbni. Hiermee wordt mogelijk gemaakt dat de Minister van Justitie en Veiligheid vertrouwelijke gegevens, die herleid kunnen worden tot een aanbieder, zonder instemming van die aanbieder, voortaan in het kader van de in artikel 3, tweede lid, Wbni, bedoelde verstrekking van dreigings- en incidentinformatie kan verstrekken aan OKTT's.

Voor deze aanvulling van artikel 20, tweede lid, Wbni geldt dat die enkel strekt tot een beperkte uitbreiding van de kring van partijen die de in dit lid bedoelde vertrouwelijke gegevens van het NCSC kunnen ontvangen. Deze wijziging behelst nadrukkelijk geen verandering in de aard van de gegevens die krachtens dit lid zonder toestemming van de betrokken aanbieder met de in dit lid bedoelde kring van partijen kan worden gedeeld. Deze wijziging brengt evenmin verandering in hetgeen is bepaald in de andere leden van artikel 20 Wbni. Ook heeft de wijziging van het tweede lid geen consequenties voor de reikwijdte van de in

[12] *Kamerstukken II* 2017/18, 34 883, nr. 3, p. 45–51.

artikel 20, zevende lid, Wbni, vanwege de bijzondere openbaarmakingsregeling in het tweede tot en met zesde lid, geregelde uitzondering op de toepasselijkheid van de Wet openbaarheid van bestuur (Wob). Voor de wijziging van het tweede lid geldt, zoals gezegd, dat die de aard van de in dat lid bedoelde gegevens niet wijzigt, maar alleen een beperkte uitbreiding van de kring van partijen die die informatie kunnen ontvangen behelst. Er zullen dus geen extra categorieën gegevens onder deze uitzondering op de Wob komen te vallen.

Artikel II

Dit artikel ziet op de samenloop van dit voorstel met de voorgestelde Wet bevordering digitale weerbaarheid bedrijven van de Minister van Economische Zaken en Klimaat. In het laatstgenoemde voorstel wordt, net als in dit voorstel, voorzien in wijzigingen van artikel 3, tweede lid, en artikel 20, tweede lid, van de Wbni. Gelet daarop voorziet artikel II in een samenloopbepaling met betrekking tot de wijzigingen in beide wetsvoorstellen van laatstbedoelde artikelen in de Wbni.

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