VOORSTEL VAN WET

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over netwerk- en informatiesystemen van andere aanbieders dan vitale aanbieders of aanbieders die deel uitmaken van de rijksoverheid te verstrekken aan deze andere 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, uit te breiden;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

De Wet beveiliging netwerk- en informatiesystemen wordt als volgt gewijzigd:

A

Artikel 3, tweede lid, wordt als volgt gewijzigd:

1. In onderdeel a wordt na "informeren" ingevoegd ", aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie".
2. Onder vervanging van de punt aan het slot van onderdeel d door een puntkomma wordt een onderdeel toegevoegd, luidende:
e. aanbieders, niet zijnde een vitale aanbieder of een andere aanbieder die onderdeel is van de rijksoverheid, indien een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening en voor de verstrekking van gegevens een onder a tot en met d bedoelde organisatie ontbreekt.

B

In artikel 20, tweede lid, wordt onder vervanging van de punt aan het slot van onderdeel c door een puntkomma een onderdeel toegevoegd, luidende:
d. organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie.

ARTIKEL II

Indien het bij koninklijke boodschap van [PM: datum Wet bevordering digitale weerbaarheid bedrijven van EZK] ingediende voorstel van wet [PM: opschrift en Kamerstuknummer Wet bevordering digitale weerbaarheid bedrijven van EZK] tot wet is of wordt verheven en artikel 5 van die wet:

a. eerder in werking treedt of is getreden dan artikel I van deze wet, komt artikel I van deze wet als volgt te luiden:

A

Artikel 3, tweede lid, wordt als volgt gewijzigd:

1. In onderdeel a wordt na "informeren" ingevoegd ", aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie".
2. Onder vervanging van de punt aan het slot van onderdeel e door een puntkomma wordt een onderdeel toegevoegd, luidende:
f. aanbieders, niet zijnde een vitale aanbieder of een andere aanbieder die onderdeel is van de rijksoverheid, indien een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening en voor de verstrekking van gegevens een onder a tot en met e bedoelde organisatie ontbreekt.

B

In artikel 20, tweede lid, wordt onder vervanging van de punt aan het slot van onderdeel d door een puntkomma een onderdeel toegevoegd, luidende:
e. organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie.

b. later in werking treedt dan artikel I van deze wet, komt artikel 5 van die wet als volgt te luiden:

Artikel 5 (wijziging Wet beveiliging netwerk- en informatiesystemen)

De Wet beveiliging netwerk- en informatiesystemen wordt als volgt gewijzigd:

A

Artikel 3, tweede lid, wordt als volgt gewijzigd:

1. Onder verlettering van onderdeel e tot f een onderdeel ingevoegd, luidende:
e. Onze Minister van Economische Zaken en Klimaat, ten behoeve van de uitvoering van de taken, bedoeld in artikel 2, eerste lid, van de Wet bevordering digitale weerbaarheid bedrijven;
2. In onderdeel f (nieuw) wordt "onder a tot en met d" vervangen door "onder a tot en met e".

B

In artikel 20, tweede lid, wordt onder vervanging van de punt aan het slot van onderdeel d door een puntkomma een onderdeel toegevoegd, luidende:
e. Onze Minister van Economische Zaken en Klimaat, ten behoeve van de uitvoering van de taken, bedoeld in artikel 2, eerste lid, van de Wet bevordering digitale weerbaarheid bedrijven.

C

In artikel 21, tweede lid, wordt onder vervanging van de punt aan het slot van onderdeel c door een puntkomma een onderdeel toegevoegd, luidende:
d. Onze Minister van Economische Zaken en Klimaat, ten behoeve van de uitvoering van de taken, bedoeld in artikel 2, eerste lid, van de Wet bevordering digitale weerbaarheid bedrijven.

ARTIKEL III

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven,

De Minister van Justitie en Veiligheid,

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel zorgt voor een uitbreiding van de bevoegdheid van het Nationaal Cyber Security Centrum (NCSC) om namens de Minister van Justitie en Veiligheid informatie over dreigingen en incidenten betreffende de netwerk- en informatiesystemen van aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, te verstrekken aan of ten behoeve van deze andere aanbieders. Deze aanbieders worden in deze toelichting *andere aanbieders* genoemd. Het voorstel bevat daartoe wijzigingen van twee artikelen uit de Wet beveiliging netwerk- en informatiesystemen (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 andere 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 hen 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 kan 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 dan vitale aanbieders of aanbieders die onderdeel zijn van de rijksoverheid verkrijgen. Het tweede lid van dit artikel bepaalt dat het NCSC de taak heeft om, ter voorkoming van nadelige maatschappelijke gevolgen, die informatie over 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 bijzondere gevallen deze informatie ook kan verstrekken aan genoemde andere aanbieders.

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 (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.

Het is niet wenselijk dat bovengenoemde 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 het 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 deze andere aanbieders bekend raakt, kan dit tot gevolg hebben dat één of meer van hun netwerk- en informatiesystemen kwetsbaar blijven. Hierdoor bestaat er 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.

Er is in toenemende mate sprake van (geslaagde) digitale aanvallen op andere aanbieders. Ook neemt de impact van die aanvallen door de toenemende mate van verwevenheid van de digitale wereld met de fysieke wereld toe. Een voorbeeld van zo'n geslaagde digitale aanval is de besmetting met Petya-*ransomware* bij een in de Rotterdamse haven gevestigd containeroverslagbedrijf, waardoor in 2017 de dienstverlening 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 die ertoe leidde dat er onder andere geen aktes gepasseerd konden worden. Als dreigings- of incidentinformatie over de netwerk- en informatiesystemen van deze 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.

Met bovenbedoelde wijzigingen wordt het in ruimere zin mogelijk om deze 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.

2. De inhoud van het voorstel

Dit wetsvoorstel strekt tot de volgende aanpassingen van de Wbni:
a. het in bijzondere 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 2.1 gaat in op de onder a. omschreven aanpassing, paragraaf 2.2 gaat in op de onder b. en c. omschreven aanpassingen.

2.1 Delen van dreigings- en incidentinformatie met andere aanbieders

2.1.1 Aanleiding en probleembeschrijving

Artikel 3, eerste lid, Wbni regelt, zoals vermeld in de inleiding, als 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) met betrekking tot netwerk- en informatiesystemen van andere aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, verkrijgen. 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 in de inleiding 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. Hieronder vallen onder meer bij ministeriële regeling aangewezen computercrisisteams en OKTT’s, die de hiervoor bedoelde andere aanbieders als doelgroep hebben en hen over de voor hen relevante dreigingen of incidenten kunnen informeren en adviseren. Een voorbeeld 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 2.2.1.

In de afgelopen periode is echter gebleken dat voor deze andere aanbieders een schakelorganisatie niet altijd aanwezig is. Hierdoor is het in die gevallen niet mogelijk gebleken 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 partijen en organisaties konden de hiervoor bedoelde gegevens niet worden gedeeld 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 in stand bleven, zoals risico’s op

sabotage of uitval van de logistieke processen in de vaccinatieketen, waardoor de omstandigheden waaronder de opslag plaats diende te vinden of de planning van de leveringen mogelijk niet langer geborgd zouden kunnen worden.

2.1.2 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 bijzondere gevallen de voor aanbieders, die geen vitale aanbieder zijn en evenmin onderdeel zijn van de rijksoverheid, relevante dreigings- en incidentinformatie 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 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 komt hierdoor immers in gevaar, met alle mogelijke nadelige maatschappelijke gevolgen van dien. Door het in bijzondere gevallen zo nodig ook verstrekken van belangrijke dreigings- en incidentinformatie aan andere aanbieders, worden zij in de gelegenheid gesteld om maatregelen te treffen om incidenten te voorkomen of de gevolgen daarvan te beperken.

Om die verstrekking 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 AVG vereiste grondslag voor rechtmatige verwerking voor deze verstrekkingen gecreëerd.

De voorgestelde bevoegdheid tot het verstrekken van restdata is beperkt tot bijzondere gevallen. Deze beperking tot bijzondere gevallen houdt ten eerste in dat informatiedeling door het NCSC met andere aanbieders alleen tot diens taak behoort, indien er geen schakelorganisatie 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 namelijk zo ingericht dat het verstrekken van bijvangst ten behoeve van andere aanbieders telkens door tussenkomst van een schakelorganisatie, indien deze aanwezig is, plaatsvindt. Op deze wijze kan de informatie via deze schakelorganisaties zo efficiënt en accuraat mogelijk aan belanghebbende andere aanbieders worden doorverstrekt. Deze schakelorganisaties hebben immers nadrukkelijk tot taak om aanbieders in hun achterban over hen aangaande digitale dreigingen en incidenten te informeren en mogelijk ook te adviseren. Zij zijn dan ook het meest bekend met de in hun achterban aanwezige netwerk- en informatiesystemen, bijbehorende belangen en risico’s en informatiebehoeften.

De beperking tot bijzondere gevallen houdt ten tweede in dat er tevens sprake dient te zijn 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 ook hieraan toetsen, mede met het oog op de voor verstrekking van persoonsgegevens vereiste noodzakelijkheidstoets uit de AVG.

De bevoegdheid tot het verstrekken van restdata met de hiervoor bedoelde andere aanbieders wordt beperkt tot enkel bijzondere gevallen 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.

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

2.2.1 Aanleiding en probleembeschrijving

Artikel 20, tweede lid, Wbni biedt de grondslag voor het NCSC om, 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) te 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[1] (CSIRT's), de AIVD en MIVD, en bij ministeriële regeling aangewezen computercrisisteams. Voor OKTT's geldt dat zij niet in de opsomming van organisaties in artikel 20, tweede lid, Wbni zijn opgenomen, en dat verstrekking van genoemde gegevens thans dus niet aan OKTT's kan plaatsvinden.

Ten aanzien van OKTT's is echter gebleken dat zij een in belangrijke mate vergelijkbare rol hebben als computercrisisteams. Zij zijn een schakelorganisatie voor een achterban van aanbieders die (grotendeels) geen vitale aanbieder zijn en ook geen deel uitmaken van de rijksoverheid, en kunnen die rol slechts beperkt uitvoeren zonder ook over genoemde vertrouwelijke herleidbare gegevens te 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 nu 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. Zoals hiervoor is vermeld kan bij de voor andere aanbieders relevante informatie bijvoorbeeld gedacht worden informatie over *ransomware*-besmettingen. Ook kan worden gedacht aan informatie waarover het NCSC beschikt over kwetsbaarheden in systemen vanwege het gebruik van (versies van) VPN-software.[2]

2.2.2 Probleemaanpak

In verband met het hiervoor omschreven probleem, dat in de afgelopen periode ook aandacht heeft gekregen in de media[3] en politiek[4], wordt voorgesteld om in artikel 20, tweede lid, Wbni OKTT's toe te voegen aan de opsomming van organisaties waaraan vertrouwelijke herleidbare gegevens met

[1] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).
[2] *Kamerstukken II* 2019/20, 26643, nr. 666.
[3] Zie onder meer de berichtgeving hierover in de Volkskrant van 12 december 2020 ('Informatie over lekken in computernetwerken wordt niet gedeeld') en in het Financieel Dagblad van 14 december 2020 ('Hackers manifesteren zich extra aan einde coronajaar').
[4] Zie de vragen van het lid Yesilgöz-Zegerius (VVD) aan de Minister van Justitie en Veiligheid over het bericht «Justitie deelt kritieke informatie over hacks niet met bedrijven» (ingezonden 8 maart 2021), https://zoek.officielebekendmakingen.nl/ah-tk-20202021-2173.html.

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 wordt naar mijn oordeel de kring van organisaties waaraan de in artikel 20, tweede lid, Wbni bedoelde informatie kan worden verstrekt, niet te groot. Ook wordt ondanks deze uitbreiding van genoemde kring 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, omdat het van groot belang wordt geacht dat de vertrouwelijkheid van deze voor het NCSC beschikbaar gekomen gegevens zo veel mogelijk wordt gewaarborgd. 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 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 een toetsing plaats waarin wordt vastgesteld dat uitwisseling van gegevens over dreigingen of incidenten verantwoord en gerechtvaardigd is. De criteria die daarbij onder meer gelden, zijn of voldoende is gebleken dat de organisatie gegevens op een zorgvuldige en rechtmatige wijze verwerkt, en dat delen van gegevens bijdraagt aan het voorkomen van nadelige gevolgen voor het maatschappelijk verkeer.[5] Vóór aanwijzing van een organisatie als OKTT vindt thans ook al, aan de hand van grotendeels dezelfde criteria, een toetsing plaats waarin wordt vastgesteld dat uitwisseling van gegevens over dreigingen of incidenten verantwoord en gerechtvaardigd is.

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 nu ook in juridische zin op dezelfde manier te laten plaatsvinden als de aanwijzing van organisaties als computercrisisteam. Meer concreet houdt dit in dat de aanwijzing van een organisaties als OKTT voortaan, net als de aanwijzing van een computercrisisteam, bij ministeriële regeling geschiedt. In de praktijk leidt deze wijziging van de artikelen 3 en 20 Wbni niet tot veranderingen voor OKTT's, anders dan de (juridische) wijze waarop zij worden aangewezen.

3. Verhouding tot hoger recht

3.1 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 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 wijziging van artikel 3, tweede lid,

[5] *Kamerstukken I*, 2017/18, 34883, nr. C, p. 2.

voortaan in bijzondere gevallen ook verstrekken van persoonsgegevens, als onderdeel van dreigings- en incidentinformatie, aan aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid.

3.2 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, aan andere aanbieders. 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 bijzondere gevallen ook aan bovenbedoelde aanbieders verstrekken van persoonsgegevens geldt dat hiervoor met de toevoeging van het nieuwe onderdeel aan artikel 3, tweede lid, in samenhang met artikel 17, eerste lid, Wbni, een specifieke wettelijke grondslag wordt geboden en deze verwerking daarmee bij wet voorzienbaar wordt.

De verstrekking van "restdata", met inbegrip van persoonsgegevens, aan genoemde aanbieders heeft (net als de thans al in artikel 3, tweede lid, Wbni mogelijk gemaakte verstrekkingen daarvan) tot doel om nadelige maatschappelijke gevolgen te voorkomen. Door bovengenoemde andere aanbieders in het bezit te laten komen van voor hen relevante dreigings- en incidentinformatie worden die 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. De verstrekking van deze persoonsgegevens (IP-adressen, e-mailadressen en domeinnamen) aan deze aanbieders 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 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. Daarbij geldt bovendien dat deze verstrekking van persoonsgegevens aan genoemde aanbieders enkel plaatsvindt in bijzondere gevallen, namelijk indien er geen schakelorganisatie 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. De verstrekking geschiedt alleen voor zover dat noodzakelijk is voor het uitvoeren van de in artikel 3, tweede lid, Wbni genoemde taak. Verwerking vindt uiteraard 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 nieuw voorgestelde verstrekking van persoonsgegevens door het NCSC een gerechtvaardigde beperking is van de persoonlijke levenssfeer.

4. Gevolgen voor burgers en bedrijven

De in paragraaf 2.1 bedoelde aanbieders en de in paragraaf 2.2 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.

5. Uitvoering

Dit voorstel heeft wat betreft de uitvoering daarvan gevolgen voor het NCSC. Deze wijzigingen betekenen namelijk dat er aan OKTT's in ruimere zin dan tot nu toe het geval is, gegevens kunnen worden verstrekt en dat voortaan in bijzondere gevallen aan aanbieders, die geen vitale aanbieder en geen onderdeel van de rijksoverheid zijn, restinformatie 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 bijzondere 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.

6. Toezicht en handhaving

Dit voorstel leidt niet tot verplichtingen voor de aanbieders en OKTT's bedoeld in paragraaf 2.1 en 2.2. Van toezicht op en handhaving van de naleving van verplichtingen is dan ook geen sprake.

7. 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 bijzondere 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.

8. Advies en consultatie

[PM]

9. Inwerkingtreding

[PM]

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, tweede, vierde en zesde lid de doeleinden van die taken.

Artikel I, onderdeel A, eerste lid, 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 2.2.2.

Artikel I, onderdeel A, derde lid, 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 bijzondere gevallen aan aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, de in dit voorstel bedoelde "restdata" te verstrekken. Het ingevoegde onderdeel e bevat hiertoe twee beperkingen. Ten eerste is deze informatieverstrekking aan genoemde aanbieders alleen dan een taak, als er geen schakelorganisatie is die de aanbieder van die informatie kan voorzien. Ten tweede dient er sprake te zijn van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder. Voor een nadere toelichting hierop wordt verwezen naar paragraaf 2.1.2.

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.[6]

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, 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 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 het voorstel van wet van de Minister van Economische Zaken en Klimaat getiteld *Wet bevordering digitale weerbaarheid bedrijven*. 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. In dat kader regelt deze samenloopbepaling dat beide wetten op elkaar zijn afgestemd.

De Minister van Justitie en Veiligheid

[6] *Kamerstukken II* 2017/18, 34883, nr. 3, p. 45-51.