Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

34 388 Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 23 juni 2016

Met belangstelling heb ik kennis genomen van het verslag van de vaste commissie voor Veiligheid en Justitie over het wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Graag maak ik van de gelegenheid gebruik om de gestelde vragen te beantwoorden en op enkele punten een nadere toelichting te geven. Bij de beantwoording heb ik zo veel mogelijk de volgorde van het verslag aangehouden. Waar dit de helderheid en overzichtelijkheid ten goede kwam, heb ik vragen samengenomen in de beantwoording.

Algemeen

1. Inleiding

De leden van de fracties van het CDA en D66 stellen vragen over de noodzaak en meerwaarde van de voorgestelde meldplicht, gezien andere recent ingevoerde meldplichten (zoals de meldplicht datalekken), de komende EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn) en de keuze van de regering om de onderwerpen toezicht en sancties nog niet te regelen. De leden van de CDA-fractie vragen onder meer of de regering hun mening deelt dat de noodzaak tot onderhavig wetsvoorstel substantieel is veranderd sinds de motie-Hennis-Plasschaert c.s. Zij verzoeken om een overzicht van het aantal meldplichten, per sector waarop het wetsvoorstel betrekking heeft, dat sinds 2011 in het leven is geroepen. De leden van de D66-fractie onderschrijven het belang dat ICT-inbreuken in de informatiesystemen van vitale aanbieders die gevolgen kunnen hebben voor de samenleving, actief worden gemeld, maar vragen wat de toegevoegde waarde is van de voorgestelde wettelijke meldplicht als deze voorlopig niet handhaafbaar is en waarom de regering er dan niet voor kiest om te wachten totdat de NIB-richtlijn geïmplementeerd is.
De leden van de VVD-fractie vragen of het, nu in dit wetsvoorstel een meldplicht opgenomen is, niet van belang is om tegelijkertijd ook het onderwerp sancties te regelen. De leden van de D66-fractie vragen wat het regelen van het toezicht en een sanctie nu precies zo lastig maakt. De

kst-34388-6
ISSN 0921 - 7371
's-Gravenhage 2016

leden van de SP-fractie vragen welke waarborgen er in de tussentijd zijn voor de naleving van de meldplicht.

De directe aanleiding voor de nu voorgestelde meldplicht is de in 2011 door de Tweede Kamer met algemene stemmen aangenomen motie-Hennis-Plasschaert c.s., waarin de Kamer de regering verzocht om te komen tot de wettelijke vastlegging van een «security breach notification» bij het Nationaal Cyber Security Centrum (NCSC) voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen. Sinds die motie zijn dreigingen op het gebied van cybersecurity niet afgenomen, zij worden veeleer sterker, zo blijkt uit het Cybersecuritybeeld Nederland 2015.[1] De risico's die daardoor voor informatiesystemen gelden en de behoefte aan hulpverlening vanuit het NCSC blijven daardoor onverminderd bestaan. Mijns inziens moet hulpverlening door het NCSC, zeker in gevallen waarin maatschappelijke ontwrichting door ICT-inbreuken dreigt, verzekerd zijn. De meerwaarde van de voorgestelde wettelijke regeling voor het melden van ernstige ICT-inbreuken is onder meer dat bij vitale aanbieders de twijfel wordt weggenomen of zij wel bevoegd zijn om gevoelige incidentinformatie aan het NCSC te verstrekken. Dat stimuleert naar verwachting de bereidheid tot melden, zeker in combinatie met de eveneens voorgestelde strikte regeling voor het verstrekken door het NCSC van vertrouwelijke gegevens waarover het NCSC beschikt (artikel 9). De wenselijkheid van een wettelijke meldplicht wordt onderstreept door de komende EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn), die de lidstaten verplicht om een dergelijke meldplicht in te voeren. Overigens regelt het wetsvoorstel behalve een meldplicht ook de taken en bevoegdheden van het NCSC en de vertrouwelijkheid van zich bij het NCSC bevindende gegevens.

Het is denkbaar dat sommige vitale aanbieders één incident aan meerdere overheidsinstanties zullen moeten melden. Die instanties worden immers vanuit een ander belang en op grond van andere taken en bevoegdheden betrokken bij een incident. Zo is de meldplicht bij het NCSC bedoeld om het NCSC in staat te stellen om met het oog op het waarborgen van de nationale veiligheid hulp te verlenen aan getroffen aanbieders bij het voorkomen of beperken van de negatieve gevolgen van een ICT-inbreuk. Daarnaast kan het NCSC met behulp van de melding andere organisaties die gelijksoortige risico's lopen tijdig informeren en adviseren over te nemen maatregelen om een vergelijkbare inbreuk te voorkomen of te beperken. De thans bestaande meldplichten bij sectorale toezichthouders hebben daarentegen veeleer tot doel hen in staat te stellen om toezichthoudend en handhavend op te treden. De meldplicht bij de Autoriteit Persoonsgegevens (AP) ziet specifiek op de bescherming van persoonsgegevens. De verschillende bij een meldplicht betrokken overheidsorganisaties zullen zo veel mogelijk de processen voor het doen van meldingen op elkaar afstemmen, zodat de sector niet onnodig wordt belast.

Naast de «meldplicht datalekken», die sinds begin 2016 voor alle sectoren geldt, zijn sinds 2011 alleen in de sectoren telecom (artikel 11a.2 Telecommunicatiewet) en financiën (uitbreiding reikwijdte artikelen 3:10, derde lid, en 4:11, vierde lid, Wet financieel toezicht) nieuwe meldplichten ingevoerd.

Ik verwacht dat de in het wetsvoorstel opgenomen meldplicht ook goed zal werken zonder toezicht en sancties op niet-naleving daarvan. Het NCSC werkt al geruime tijd samen met aanbieders van vitale producten en diensten en de verwachting is dat deze aanbieders ook zonder toezicht en sancties aan de meldplicht zullen voldoen. Van belang is in dit verband

[1] Kamerstukken II 2015/16, 26 643, nr. 369.

dat met de voorgestelde wettelijke regeling, inclusief de in artikel 5 bedoelde algemene maatregel van bestuur en de te maken richtsnoeren ter nadere uitwerking van de meldplicht, voor genoemde aanbieders buiten twijfel wordt gesteld in welke gevallen een ICT-incident van dien aard is dat daardoor maatschappelijke ontwrichting aan de orde is of kan zijn en betrokkenheid van het NCSC, gelet op dat maatschappelijk belang, in elk geval noodzakelijk is. Over de samenloop met de NIB-richtlijn merk ik op dat, gelet op het maatschappelijke belang van de in het wetsvoorstel bedoelde verplichte meldingen, het gerechtvaardigd is om de meldplicht bij het NCSC eerder in te voeren dan de richtlijn vereist. Toezicht op de naleving van de meldplicht bij het NCSC zal worden geregeld in het kader van de implementatie van de NIB-richtlijn, die de lidstaten onder meer hiertoe verplicht. Dit toezicht kan niet los worden gezien van dat op de naleving van de overige verplichtingen van de NIB-richtlijn, zoals de plicht voor aanbieders om informatiesystemen in voldoende mate te beveiligen en de plicht om incidenten mede met het oog daarop ook te melden bij toezichthouders. Daarom is ervoor gekozen om de wettelijke regeling van het toezicht op de naleving van de verschillende verplichtingen van de NIB-richtlijn, waaronder de aanwijzing van de organisaties die hiermee zullen worden belast, in onderlinge samenhang ter hand te nemen, en de meldplicht bij het NCSC, gelet op het maatschappelijke belang daarvan, geen vertraging te laten ondervinden en daarop vooruitlopend al met dit wetsvoorstel te regelen.

De leden van de PVV-fractie vragen hoe vaak ICT-inbreuken die een serieuze bedreiging voor de Nederlandse samenleving inhouden, naar schatting jaarlijks voorkomen. Worden deze ICT-inbreuken nu zonder meldplicht en hulp van het NCSC netjes opgelost of zijn er aanwijzingen waaruit blijkt dat dit niet of onvoldoende is gebeurd?

Voor zover er ICT-inbreuken zijn geweest bij in de toekomst onder de meldplicht vallende aanbieders, hebben die feitelijk niet geleid tot maatschappelijke ontwrichting. Bij het NCSC worden wel steeds meer incidenten gemeld, in 2015 waren dat er 675. Een deel van die meldingen komt overigens niet van de aanbieder zelf maar bijvoorbeeld van buitenlandse Computer Emergency Response Teams (CERT's). De zwaarte van de gemelde incidenten varieert van heel kleine kwetsbaarheden tot grotere inbreuken waarbij de continuïteit van een vitaal product of vitale dienst in het geding is of kan komen. Het NCSC ondersteunt in dergelijke gevallen de meldende organisatie bij het oplossen van het incident en het voorkomen of beperken van de negatieve gevolgen daarvan, bijvoorbeeld door het adviseren over te treffen maatregelen of het bieden van technische ondersteuning. Precieze cijfers over hoeveel van die incidenten onder de thans voorgestelde meldplicht zouden vallen zijn, mede omdat er thans nog geen daarbij behorende drempelwaarden zijn vastgesteld, niet voorhanden.

De leden van de fracties van D66 en de PvdA vragen op wat voor manier vitale aanbieders geholpen worden om ICT-inbreuken te voorkomen.

Het NCSC geeft preventieve hulp via verschillende kanalen en op verschillende manieren; te denken valt aan het faciliteren van samenwerking binnen sectoren in zogenoemde Information Sharing and Analysis Centres (ISAC's), het opstellen van beveiligingsadviezen[2] of het opstellen van factsheets over specifieke kwetsbaarheden.

[2] Zie https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen-toelichting.html.

De aan het woord zijnde leden vragen in hoeverre dit wetsvoorstel ook van toepassing is op de niet-vitale aanbieders die onderdeel zijn van de rijksoverheid.

De doelgroep van het NCSC is de rijksoverheid en vitale private organisaties. Rijksoverheidsorganisaties kunnen zowel vitaal als niet-vitaal zijn. De doelgroep ten behoeve waarvan het NCSC de in artikel 2, eerste lid, van het wetsvoorstel genoemde taken uitoefent, bestaat dus uit alle vitale aanbieders (privaat en publiek) en de overige, niet-vitale onderdelen van de rijksoverheid. De voorgestelde meldplicht geldt alleen voor aan te wijzen vitale aanbieders, dus ook alleen voor die onderdelen van de rijksoverheid die als vitaal worden aangemerkt.

De leden van de D66-fractie vragen of de regering voornemens is het wetsvoorstel te voorzien van een evaluatiebepaling.

Het digitale domein is van nature dynamisch. In aanvulling hierop ontstaan de komende jaren met de implementatie van de NIB-richtlijn aanzienlijke aanvullende wettelijke verplichtingen. Het ligt daarmee in de rede om te zijner tijd het volledige cybersecurity-pakket te evalueren en de evaluatie niet te beperken tot dit wetsvoorstel. Ik zeg dan ook graag toe dat ik de Staten-Generaal binnen drie jaar na inwerkingtreding van de wettelijke bepalingen ter implementatie van de NIB-richtlijn een verslag zal zenden over de werking van dit geheel van wettelijke regels.

2. Meldplicht

2.1 Inleiding

De leden van de VVD-fractie vragen hoe wordt vastgesteld of een vitale aanbieder had kunnen of moeten weten dat er sprake was van een ICT-inbreuk.

De vraag of een aanbieder op de hoogte had kunnen of moeten zijn van een ICT-inbreuk, heeft betrekking op de maatregelen die een aanbieder kan nemen om zijn ICT adequaat te beveiligen. In het kader van het onderhavige wetsvoorstel kan die vraag relevant zijn als het NCSC een getroffen aanbieder een advies geeft hoe hij herhaling kan voorkomen. Een hulpmiddel om inbreuken tijdig op te merken is het installeren van software die inbreuken detecteert. Deze vraag zal nader aan de orde komen bij het nog te maken wetsvoorstel ter implementatie van de NIB-richtlijn. Die richtlijn voorziet immers niet alleen in melding van ernstige incidenten maar ook in beveiligingsmaatregelen ter voorkoming van incidenten.

De leden van de PvdA-fractie vragen welke maatregelen de regering treft om een *just culture* te stimuleren, een cultuur waarin het gezamenlijk bijdragen aan veiligheid centraal staat.

Het NCSC voert structureel overleg met vitale partijen over de wijze waarop zij gevoelige informatie veilig aan het NCSC kunnen verstrekken. Deze publiek-private samenwerking heeft uitgewezen dat aanbieders in vitale sectoren in veel gevallen bereid zijn om incidentinformatie aan bijvoorbeeld het NCSC te verstrekken. Ook zien organisaties de meerwaarde die uitwisseling van incident-informatie kan hebben, omdat daarmee de sector als geheel weerbaarder wordt. Ook door samenwerking binnen sectoren te faciliteren, bijvoorbeeld door het secretariaat te voeren van verschillende ISAC's, stimuleert het NCSC het uitwisselen van informatie.

De aan het woord zijnde leden vragen verder wat de regering doet om aanbieders, zoals bijvoorbeeld softwareleveranciers in de telecomsector, te verplichten om de geleverde software te allen tijde bijgewerkt te houden en blijvend aan de hoogste («state of the art») veiligheidsnormen te laten voldoen. Deze leden zijn in algemene zin van mening dat een softwareleverancier nooit mag stoppen met het bieden van software-updates. Is de regering het met deze leden eens? Zo nee, waarom niet? Zo ja, welke maatregelen treft de regering om dit te bewerkstelligen bij de desbetreffende bedrijven?

Softwareleveranciers zijn essentieel voor de veiligheid van informatiesystemen alsook de continuïteit en privacy-bescherming van Nederlandse burgers. Hun producten worden immers veelvoudig gebruikt in netwerk- en informatiesystemen of in apparatuur zoals computers en mobiele telefoons. Ik merk op dat het bewustzijn van veiligheidsaspecten bij zowel opdrachtgevers (gebruikers) als opdrachtnemers (leveranciers) steeds meer doordringt. Het PPS-project «Secure Software» biedt een kader voor het ontwikkelen van aantoonbaar veilige software. Door de Stichting Secure Software wordt momenteel in nauwe samenwerking met het Ministerie van Economische Zaken, ECP (Platform voor de informatiesamenleving) en diverse marktpartijen intensief gewerkt aan een volgende publicatie «Normenkader Secure Software 2.0» met als doel de veiligheid van software, bewustwording van en kennisvergroting bij software-ontwikkelbedrijven te stimuleren. Van softwareleveranciers kan niet worden verwacht dat zij tot in lengte van dagen updates van verouderde software blijven aanbieden. Met betrekking tot het blijven aanbieden van software-updates ben ik van mening dat dit een verantwoordelijkheid is van zowel de aanbieder als de gebruiker van de software; organisaties kunnen contractueel afspraken maken over de termijn gedurende welke ondersteuning zal worden verleend.

De leden van de CDA-fractie informeren naar de in voorbereiding zijnde algemene maatregel van bestuur, waarin zal worden aangewezen welke aanbieders, producten en diensten onder de meldplicht vallen.

De hierna opgenomen tabel noemt de aanbieders, producten en diensten ten aanzien waarvan ik het voornemen heb om ze onder de meldplicht te brengen. Over de sectoren waarvoor die uitwerking nog niet beschikbaar is, zal ik de Kamer op een later moment informeren.

Sector	Vitale aanbieder als bedoeld in artikel 1, tweede streepje, wetsvoorstel gegevensverwerking en meldplicht cybersecurity	Product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving
Drinkwater	Drinkwaterbedrijf als bedoeld in artikel 1, eerste lid, van de Drinkwaterwet	Het leveren van deugdelijk drinkwater door middel van een openbare drinkwatervoorziening.
Energie	De netbeheerder van het landelijk hoogspanningsnet, aangewezen op grond van artikel 10, tweede lid, of 14 van de Elektriciteitswet 1998	Transmissie en distributie van elektriciteit.
	De regionale netbeheerders, aangewezen krachtens artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998	
	De netbeheerder van het landelijk gastransportnet, aangewezen op grond van artikel 2, eerste lid, van de Gaswet	Transmissie en distributie van gas.

Sector	Vitale aanbieder als bedoeld in artikel 1, tweede streepje, wetsvoorstel gegevensverwerking en meldplicht cybersecurity	Product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving
Mainport Rotterdam	Havenbedrijf Rotterdam N.V.	Het afwikkelen van scheepvaartverkeer.
Nucleair	Houder van een vergunning als bedoeld in artikel 15, onderdeel b, van de Kernenergiewet	Het vrijmaken van kernenergie en het vervaardigen, bewerken, verwerken en opslaan van splijtstoffen.
	Bedrijven vallend onder het Geheimhoudingsbesluit Kernenergiewet, Toepassingsbesluit 24 september 1971/ nr.671/524	Het vrijmaken van kernenergie en het vervaardigen, bewerken, verwerken en opslaan van splijtstoffen. Het beschikbaar houden van gegevens welke noodzakelijk zijn voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges en het produceren van hulpmiddelen en materialen, welke zijn benodigd voor het scheiden van verschillende in splijtstof voorkomende uraniumisotopen met gebruikmaking van gasultracentrifuges.
Mainport Schiphol	1 Schiphol Group/ Schiphol Telematics 2. Luchtverkeersleiding Nederland 3. Air Fuel Supply 4. Koninklijke marechaussee 5. elke luchtvaartmaatschappij met minimaal 25% van het totale aantal vliegbewegingen op Schiphol per jaar.	Een veilige en vlotte vlucht- en vliegtuigafhandeling.

De leden van de SP-fractie vragen of de meldplicht ook geldt als het handelen of nalaten van een eigen medewerker heeft gezorgd voor inbreuk op de veiligheid of verlies van integriteit, ongeacht of er nu wel of niet ongeoorloofd toegang is geweest. Moet het uiteindelijk niet uitsluitend gaan om de gevolgen van een bepaalde handeling?

Bij de vraag of de meldplicht van toepassing is op ICT-inbreuken zijn primair de gevolgen van die inbreuk bepalend. Het zal immers moeten gaan om incidenten waarbij de beschikbaarheid of betrouwbaarheid van een vitaal product of dienst in belangrijke mate wordt of kan worden onderbroken. Het maakt op zichzelf niet uit of een incident met een dergelijk gevolg is veroorzaakt door aanvallen van externe kwaadwillenden of door een fout van een eigen medewerker van de betrokken organisatie. Wanneer sprake is van een fout in laatstbedoelde zin, met een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een vitale dienst of een vitaal product als (mogelijk) gevolg, is de betrokken aanbieder, ook als er feitelijk geen ongeoorloofde toegang van buitenaf is geweest, tot het melden hiervan verplicht.

De leden van de fracties van de PvdA en D66 stellen enkele vragen over de keuze om DDoS-aanvallen niet onder de voorgestelde meldplicht te laten vallen.

DDoS-aanvallen vallen niet onder deze meldplicht, omdat zo'n aanval niet gepaard gaat met een inbreuk op of een verlies van integriteit van een informatiesysteem van een vitale aanbieder, maar alleen de bereikbaarheid aantast zonder aantasting van de systemen die voor het

aanbieden van een product of dienst worden gebruikt. Bij een DDoS-aanval heeft verplichte betrokkenheid van het NCSC bovendien niet voldoende meerwaarde, onder meer omdat zo'n aanval een relatief eenvoudig karakter heeft en de onderbreking van de bereikbaarheid, mede gezien de maatregelen die een aanbieder zelf kan nemen, niet lang duurt. De voorgestelde tekst van artikel 6, eerste lid, laat niet toe om de meldplicht in de toekomst eventueel wél te laten gelden voor een DDoS-aanval: bij zo'n aanval is immers geen sprake van een inbreuk of van een verlies van integriteit. Wel zal in het kader van de implementatie van de NIB-richtlijn worden bezien of DDoS-aanvallen alsnog meldplichtig moeten worden. Een en ander laat overigens onverlet dat partijen de mogelijkheid hebben om ook deze verstoringen van de bereikbaarheid op basis van vrijwilligheid aan het NCSC te melden.

De leden van de SP-fractie vragen hoe de regering aankijkt tegen de mogelijkheid om ook te kunnen leren van kleinere inbreuken of van zaken waarin men zogezegd langs de rand van de afgrond is gescheerd en die evengoed tot grote problemen hadden kunnen leiden. Heeft de regering overwogen om de verplichting tot melden te laten gelden voor alle ICT-inbreuken, zo vragen de leden van de D66-fractie.

Weliswaar kan ook informatie over kleinere inbreuken voor het NCSC waardevol zijn, maar het maatschappelijke belang daarvan is niet groot genoeg om een wettelijke meldplicht te rechtvaardigen. Wel geldt de meldplicht voor inbreuken die hadden kúnnen leiden tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een product of dienst. Daarnaast stimuleert het NCSC dat niet-meldplichtige incidenten op vrijwillige basis worden gemeld zodat het NCSC een zo breed mogelijke informatiepositie verkrijgt.

Deze leden vragen verder of de grootst mogelijke mate van transparantie niet juist de voorkeur verdient. Zou dit niet veel meer toekomen aan een goede werking van bijvoorbeeld de markt, omdat (potentiële) klanten van bedrijven dan een beter geïnformeerde keuze kunnen maken voor een bepaalde dienst of product?

Uiteraard acht ik transparantie een groot goed en zal dit ook daar waar mogelijk onderdeel laten zijn van mijn beleid. Niet-gevoelige informatie, bijvoorbeeld geaggregeerde data over aantallen incidenten, zal breed kunnen worden gedeeld. De informatie die het NCSC verkrijgt over dreigingen, kwetsbaarheden en incidenten wordt in eerste instantie door het NCSC gebruikt voor het uitoefenen van zijn taken. Dat wil zeggen dat het NCSC de informatie gebruikt om rijksoverheids- en private vitale aanbieders te informeren over dreigingen en kwetsbaarheden en te adviseren over maatregelen die zij kunnen treffen om inbreuken te voorkomen of beperken. Voorts kan het NCSC informatie over dreigingen en kwetsbaarheden, zonder vertrouwelijke tot een aanbieder herleidbare gegevens, ook verstrekken aan andere partijen, zoals CERT's. Verder heeft het NCSC op grond van artikel 9 van het wetsvoorstel de bevoegdheid om, in gevallen waarin dit noodzakelijk is ter voorkoming of beperking van ernstige maatschappelijke gevolgen, ook vertrouwelijke herleidbare gegevens te verstrekken aan bijvoorbeeld andere vitale organisaties of het publiek. Volledige transparantie van incidentinformatie is niet gewenst. Zolang het incident nog niet is verholpen kan openbaarheid een oplossing bemoeilijken en vertragen. Daarnaast moet worden voorkomen dat aanbieders beducht worden, vanwege risico's als reputatieschade en toegenomen kwetsbaarheid voor toekomstige aanvallen, om incidenten, ook de niet-meldplichtige, aan het NCSC te melden. Met een combinatie van het breed delen van niet-gevoelige informatie en een beperkte

openbaarheid van gevoelige incidentinformatie kan een bijdrage worden geleverd aan het ontstaan van een *just culture*, een veilige meldcultuur.

De leden van de SP-fractie vragen hoe de regering het risico inschat dat dienstverleners kunnen trachten om een onwelgevallig incident, dat publicitair onopgemerkt is gebleven en dat reputatieschade zou veroorzaken bij bekendwording, onder de pet te houden.

Het kan niet worden uitgesloten dat organisaties geen melding doen. Ik vertrouw erop dat vitale aanbieders, juist omdat het vitale processen betreft, het belang en de toegevoegde waarde onderkennen van het verstrekken van informatie aan het NCSC. Melding van een incident aan het NCSC moet overigens niet worden gelijkgesteld met het in de publiciteit komen ervan. Het voorgestelde artikel 9 bevat immers een strikte regeling voor de verstrekking door het NCSC aan derden van vertrouwelijke gegevens met betrekking tot een aanbieder.
De bereidheid tot melden zal nader aan de orde komen bij het nog te maken wetsvoorstel ter implementatie van de NIB-richtlijn. De richtlijn schrijft immers voor dat er ook toezicht wordt gehouden op de naleving van de meldplicht en dat sancties worden opgelegd bij overtreding.

De leden van de fracties van SP, VVD, D66, CDA en PvdA stellen diverse vragen over het criterium «in belangrijke mate» in het voorgestelde artikel 6, eerste lid. Onder meer vragen zij of dat criterium voldoende duidelijkheid en rechtszekerheid biedt, of de in de memorie van toelichting genoemde richtsnoeren er daadwerkelijk gaan komen, wat de visie van het Ministerie van Veiligheid en Justitie zelf is, of het criterium betekent dat een inbreuk niet gemeld hoeft te worden als een inbreuk alleen ontwrichtend is in individuele gevallen, of de Tweede Kamer van de richtsnoeren op de hoogte wordt gebracht en hoe vitale aanbieders moeten inschatten of een inbreuk wel of niet gevolgen heeft voor de beschikbaarheid of betrouwbaarheid van het product of dienst.

Het begrip «in belangrijke mate» zoals bedoeld in artikel 6 van het wetsvoorstel zal per sector nader worden uitgewerkt in richtsnoeren, waarmee per product of dienst duidelijk wordt welke incidenten meldplichtig zijn. In de richtsnoeren worden voor alle onder de meldplicht vallende producten en diensten nadere criteria geformuleerd, zo veel mogelijk in de vorm van concrete drempelwaarden. Deze drempelwaarden zien bijvoorbeeld op het aantal gebruikers dat door de onderbreking van de beschikbaarheid of betrouwbaarheid van het vitale product of de vitale dienst getroffen is of de duur van deze onderbreking. De drempelwaarden worden zodanig geformuleerd dat bijvoorbeeld incidenten waarbij slechts een klein aantal gebruikers gedurende korte tijd negatieve gevolgen ondervindt van een onderbreking, niet onder de meldplicht vallen. De richtsnoeren zijn momenteel in voorbereiding. Daarbij wordt rekening gehouden met de uitkomsten van overleg met betrokken sectoren en departementen. Ik zal uw Kamer te zijner tijd nader informeren.

De leden van de D66-fractie vragen of de melder van een ICT-inbreuk verplicht is om het advies van het NCSC op te volgen.

Een advies van het NCSC is niet bindend. Het staat aanbieders in beginsel vrij om andere maatregelen dan door het NCSC geadviseerd te treffen om (de negatieve gevolgen van) een ICT-inbreuk te voorkomen of te verhelpen. Wel kan ik, als een aanbieder onvoldoende gevolg geeft aan een advies en het risico op maatschappelijke ontwrichting nog steeds bestaat, de sectorverantwoordelijke bewindspersoon op de hoogte brengen van het incident en het gegeven advies, zodat deze desgewenst

op grond van zijn eigen bevoegdheden maatregelen kan (laten) nemen om naleving van het advies alsnog af te dwingen of het incident anderszins te verhelpen (zie het voorgestelde artikel 9, derde lid). Ook zal ik de sectorverantwoordelijke bewindspersoon onverwijld op de hoogte stellen als dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken, bijvoorbeeld als een crisissituatie dreigt die voor die bewindspersoon aanleiding kan zijn om maatregelen te nemen ter beheersing daarvan (artikel 9, vierde lid, onder a).

Ook vragen deze leden wanneer de regering verwacht dat de Europese NIB-richtlijn gereed zal zijn voor implementatie.

De richtlijn wordt naar verwachting in juni 2016 geplaatst in het Publicatieblad van de Europese Unie. De lidstaten hebben na die publicatie een periode van 21 maanden voor de implementatie en een additionele zes maanden voor het aanwijzen van de «essentiële aanbieders» waarop de verplichtingen van de richtlijn van toepassing zullen zijn.

Verder vragen deze leden of erin wordt voorzien dat toezichthouders op andere meldplichten een notificatie sturen aan het NCSC, om te ondervangen dat de voorliggende wettelijke regeling vooralsnog niet voorziet in toezicht en sancties op naleving van de meldplicht.

Het onderhavige wetsvoorstel voorziet op dit moment niet in een regeling op grond waarvan toezichthouders op andere meldplichten het NCSC kunnen informeren over meldingen die zij hebben ontvangen. Eventueel voorziet reeds bestaande sectorale wetgeving wel al hierin. Uiteraard zal de informatie-uitwisseling tussen toezichthouders en het NCSC in het kader van de implementatie van de NIB-richtlijn in ogenschouw worden genomen.

De aan het woord zijnde leden vragen de regering verder hoe dit wetsvoorstel zich verhoudt tot het wetsvoorstel Computercriminaliteit III (Kamerstuk 34 372).

Dit wetsvoorstel introduceert een meldplicht voor ICT-inbreuken en stelt regels over het verwerken van gegevens ten behoeve van de taken van het NCSC. De melding stelt het NCSC in staat om hulp te verlenen aan de getroffen aanbieder en om andere aanbieders te waarschuwen, met als uiteindelijke doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken. Het wetsvoorstel Computercriminaliteit III (34 372) beoogt de opsporing en vervolging van computercriminaliteit te versterken, onder meer door middel van de introductie van de bevoegdheid voor de officier van justitie om, na voorafgaande machtiging van de rechter-commissaris, een bevel af te geven tot het op afstand (online) binnendringen in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Beide wetsvoorstellen beogen de samenleving te beschermen tegen ICT-inbreuken, waarbij het functioneren van computers of ICT-systemen van burgers en bedrijven wordt aangetast of misbruik wordt gemaakt van gegevens die in die computers of ICT-systemen zijn opgeslagen.

De leden van de D66-fractie vragen wat er gebeurt als de politie bedoeld of onbedoeld een ICT-systeem van een vitale aanbieder hackt.

Op dit moment bevat het Wetboek van Strafvordering niet de bevoegdheid tot het op afstand binnendringen in een geautomatiseerd werk. Het voorstel voor een dergelijke bevoegdheid is opgenomen in het wetsvoorstel Computercriminaliteit III. Die bevoegdheid zal alleen worden

gebruikt na een zorgvuldige afweging, waarin onder meer het risico voor het geautomatiseerde werk wordt betrokken. Het binnendringen in een geautomatiseerd werk van een dienstverlener van vitale infrastructuur zal die afweging niet snel doorstaan. In beginsel zal het meer voor de hand liggen samen met de dienstverlener te bezien welke activiteiten mogelijk zijn voor de opsporing en hoe het risico daarvan kan worden geminimaliseerd.
Bij het binnendringen in een geautomatiseerd werk zal de politie schade aan systemen en processen zo veel mogelijk voorkomen. Dat geldt des te meer voor vitale producten of diensten. De politie zal na het binnendringen het geautomatiseerde werk zo veel mogelijk in de staat terugbrengen waarin het voordien was. Afhankelijk van het belang van geheimhouding voor het onderzoek kan contact met de aanbieder worden opgenomen om de risico's na de inzet verder te beperken.

Ten slotte vragen deze leden of de mogelijkheid bestaat dat de politie een bij het NCSC gemelde kwetsbaarheid eerst misbruikt in het kader van haar hackbevoegdheid.

Het wetsvoorstel staat niet toe dat het NCSC gegevens over een kwetsbaarheid in relatie tot een specifieke aanbieder aan de politie verstrekt. Wel is denkbaar dat de politie door het verkrijgen van algemene dreigingsinformatie op de hoogte raakt van een kwetsbaarheid en deze kennis gebruikt voor het op afstand binnendringen in een informatiesysteem.

2.2 Te melden ICT-inbreuken

De leden van de SP-fractie vragen hoe wordt omgegaan met ICT-inbreuken die slechts zeer negatieve gevolgen hebben voor een kleinere groep betrokkenen.

Inbreuken die slechts een kleine groep burgers treffen, vallen buiten de meldplicht van dit wetsvoorstel maar kunnen, mits zij plaatsvinden bij rijksoverheids- of private vitale organisaties, op vrijwillige basis aan het NCSC worden gemeld. Wanneer een dergelijke inbreuk wordt gemeld zal het NCSC eveneens hulpverlenend, informerend en adviserend optreden.

2.3 Verhouding tot sectorale meldplichten

De leden van de SP-fractie vragen hoe de betrokken sectoren aankijken tegen de administratieve lasten door samenloop met sectorale meldplichten.

In de consultatiefase zijn weliswaar zorgen geuit over de administratieve lasten met betrekking tot meerdere meldplichten, maar omdat de meldplicht beperkt blijft tot ernstige incidenten en voor meerdere meldplichten grotendeels hetzelfde soort gegevens moet worden verstrekt, blijven de administratieve lasten beperkt. Zie ook mijn antwoorden op de vragen van de leden van de CDA-fractie over paragraaf 8 (Regeldruk) van de memorie van toelichting.

Ook vragen deze leden of er bij het aanwijzen van meldplichtige aanbieders gekeken wordt of zij aan deze (extra) meldplicht kunnen voldoen en wat zij moeten ondernemen om hier wel aan te kunnen voldoen.

De keuze voor categorieën aanbieders die onder de meldplicht komen te vallen, zal worden gebaseerd op het belang van hun producten of diensten voor het goed functioneren van de Nederlandse samenleving. Er

zijn geen aanwijzingen dat deze aanbieders niet kunnen voldoen aan de meldplicht.

De aan het woord zijnde leden begrijpen dat, als het advies van het NCSC afwijkt van de aanwijzing van de sectorale toezichthouder, deze aanwijzing prevaleert, maar zij vragen of vervolgens wordt onderzocht waar het verschil in inzicht vandaan komt en hoe dat eventueel kan worden opgelost.
Uiteraard zal na afloop van dergelijke voorvallen – binnen de kaders die de wet biedt voor informatie-uitwisseling – contact tussen NCSC en toezichthouder plaatsvinden om hier lering uit te kunnen trekken.

De leden van de CDA-fractie vragen om een overzicht van alle bestaande sectorale toezichthouders en daaraan gelieerde organisaties die ook onder de reikwijdte van onderhavig wetsvoorstel vallen.

Een compleet overzicht van betrokken toezichthouders kan worden gegeven als duidelijk is welke aanbieders, producten en diensten onder de meldplicht vallen. Voor zover nu bekend gaat het in elk geval om (de desbetreffende ambtelijke diensten van) de Ministers van Economische Zaken, Infrastructuur en Milieu en Binnenlandse Zaken en Koninkrijksrelaties, en om de zelfstandige sectorale toezichthouders Autoriteit Consument en Markt en De Nederlandsche Bank N.V.

Deze leden vragen ook of is overwogen het wetsvoorstel op zo'n manier in te richten dat de sectorale toezichthouders meldingen die zij ontvangen van vitale aanbieders, doorspelen naar het NCSC in plaats van aanbieders een dubbele meldplicht en in sommige gevallen een driedubbele meldplicht op te leggen.

Ik ben geen voorstander van een dergelijke getrapte melding. Melding aan het NCSC via de toezichthouder brengt het risico met zich mee dat het NCSC minder snel op de hoogte is van incidenten. Ook als de toezichthouder, net als het NCSC, 24 uur per dag bereikbaar en beschikbaar is om binnenkomende meldingen te beoordelen op belang en urgentie, zal hij een ontvangen melding immers eerst inhoudelijk moeten beoordelen op de vraag of het incident van dien aard is dat het moet worden doorgegeven aan het NCSC. Dit terwijl het NCSC nu juist, ter voorkoming of beperking van maatschappelijke ontwrichting, zo snel mogelijk in staat moet worden gesteld om hulp te verlenen aan de getroffen vitale aanbieder en om relevante informatie over de bij het incident gebleken kwetsbaarheid te kunnen verstrekken aan andere vitale organisaties, die ook getroffen zouden kunnen worden. Wel zullen, ter beperking van de regeldruk, voor elkaar overlappende meldplichten de wijze waarop moet worden gemeld en de daarbij te verstrekken gegevens zo veel mogelijk onderling worden afgestemd.

De leden van de CDA-fractie vragen of het niet logischer zou zijn, uitgezonderd de informatievoorziening aan inlichtingen-, veiligheids- en opsporingsdiensten, dat de sectorale toezichthouder beslist over het verstrekken van gegevens aan derden en niet het NCSC.

Voor het NCSC geldt dat het ten aanzien van de verstrekking van meldingsgegevens aan derden, gelet op zijn verantwoordelijkheid voor de versterking van de digitale weerbaarheid van de Nederlandse samenleving, en meer in het bijzonder die van de rijksoverheid en vitale private aanbieders, een eigen afweging moet kunnen maken en daarbij, met name in situaties waarbij nadelige maatschappelijke gevolgen dreigen, niet afhankelijk moet zijn van de betrokkenheid van organisaties met andersoortige taken, zoals toezichthouders. Waar mogelijk zal het NCSC

overigens voorafgaand contact over dergelijke verstrekkingen hebben met in het bijzonder de betrokken aanbieder waarvan het meldingsgegevens betreft.

De leden van de fracties van CDA en D66 vragen hoe de stellingname dat de Staatssecretaris van Veiligheid en Justitie «een eigen verantwoordelijkheid heeft om de digitale weerbaarheid van de samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen» zich verhoudt tot de beperkte mogelijkheden die het NCSC worden toegekend. Immers, het NCSC heeft geen handhavingsbevoegdheid en ingeval van tegenstrijdige adviezen prevaleert het advies van de sectorale toezichthouder. Is de Staatssecretaris daarmee geen tandeloze tijger?

Ik heb een coördinerende rol op het terrein van cybersecurity.[3] Mijn verantwoordelijkheid ligt in het versterken van de digitale weerbaarheid van de Nederlandse samenleving en in het bijzonder in het voorkomen van maatschappelijke ontwrichting als gevolg van het door ict-incidenten uitvallen van de beschikbaarheid en betrouwbaarheid van voor de samenleving vitale producten en diensten. Met dit wetsvoorstel worden de hiermee samenhangende (NCSC-)taken vastgelegd, zoals advisering, waarschuwing en andere hulpverlening. Ook wordt de hiermee gemoeide verwerking van gegevens hierdoor van een stevige grondslag voorzien en de bevoegdheid gecreëerd voor het NCSC om organisaties ten behoeve van de taakuitoefening om gegevens te verzoeken. Voorts wordt, naast de regeling van de meldplicht, met onder meer ook de verplichting om aan het NCSC gevraagde gegevens te verstrekken, met dit wetsvoorstel voorzien in een regeling van de vertrouwelijkheid van, al dan niet verplicht, aan het NCSC gemelde informatie, teneinde nader te waarborgen dat vitale aanbieders niet beducht zullen hoeven te zijn om incidentinformatie met het NCSC te delen. Daarmee kan ik in voldoende mate invulling geven aan mijn verantwoordelijkheid. Dat laat onverlet dat naast het NCSC, gelet op de eigen verantwoordelijkheden van andere bewindspersonen, bijvoorbeeld ook een rol is weggelegd voor sectorale toezichthouders als het gaat om de naleving van in wetgeving voor vitale organisaties vastgelegde vereisten op het terrein van ICT-beveiliging.

De leden van de D66-fractie lezen dat de voorziene meldplicht van het NCSC wezenlijk verschilt van de sectorale meldplichten gericht op toezicht op een wettelijke zorgplicht. Zij vragen of dat wezenlijke verschil een keuze is van de regering zelf of voortvloeit uit de NIB-richtlijn. Onderschrijft de regering dat toezicht en hulpverlening elkaar niet hoeven te bijten en beide georganiseerd kunnen en moeten worden?

Het is een keuze van de regering om ernstige ICT-inbreuken te laten melden bij het NCSC ten behoeve van de hulpverlening en het daardoor voorkomen of beperken van maatschappelijke ontwrichting. De NIB-richtlijn laat het aan de lidstaten over om te bepalen bij welke overheidsinstanties belangrijke incidenten gemeld moeten worden en welke instantie of instanties wordt of worden belast met hulpverlening, toezicht en handhaving. Ik ben er geen voorstander van om het NCSC ook met toezichtstaken te belasten. Vitale aanbieders kunnen terughoudend worden om het NCSC te betrekken bij incidenten als zij er rekening mee moeten houden dat het NCSC de verstrekte gegevens niet alleen gebruikt voor hulp en bijstand maar wellicht ook voor (dwingende) interventie. Toezicht en handhaving zullen daarom elders worden ondergebracht. Naar mijn oordeel kunnen toezicht en hulpverlening gelet op het voorgaande goed naast elkaar worden georganiseerd.

---

[3] Kamerstukken II 2011/12, 26 643, nr. 247, p. 6.

Verder vragen deze leden of vitale aanbieders te maken kunnen krijgen met een samenloop van meldplichten. Welke meldplicht-instantie is dan leidend in de behandeling daarvan? Is in kaart gebracht in hoeverre daarbij sprake kan zijn van conflicterende aanwijzingen en adviezen?

Het is denkbaar dat voor vitale aanbieders meerdere meldplichten zullen gelden, dat is inherent aan het bestaan van meerdere overheidsinstanties met elk hun eigen taken en bevoegdheden en de noodzaak van normering en begrenzing van gegevensverstrekking tussen overheidsinstanties onderling. Wat betreft de samenloop van melding bij het NCSC met andere meldplichten wijs ik erop dat het NCSC waar mogelijk en mits de betrokken organisatie daar toestemming voor geeft, zal overleggen met toezichthouders om adviezen van het NCSC en aanwijzingen of ander handhavend optreden van de toezichthouder zo veel mogelijk op elkaar af te stemmen. Als een getroffen organisatie in een concreet geval wordt geconfronteerd met een bindende aanwijzing van een toezichthouder die tegenstrijdig is aan het advies van het NCSC, bijvoorbeeld omdat in een concreet geval onvoldoende tijd beschikbaar is voor onderling overleg of omdat de betrokken organisatie voor dat overleg geen toestemming heeft gegeven, dan prevaleert de aanwijzing van de toezichthouder.

De aan het woord zijnde leden vragen of het NCSC als enige hulp kan en zal aanbieden bij ICT-inbreuken bij vitale aanbieders die tot maatschappelijke ontwrichting kunnen leiden. Of is een hulp biedende taak ook belegd bij andere instanties die uitvoering geven aan een meldplicht?

Anders dan bijvoorbeeld een toezichthouder is het NCSC, zoals ook vastgelegd in dit wetsvoorstel, belast met de taak van het, ter voorkoming van maatschappelijke ontwrichting, hulp verlenen aan de rijksoverheid en vitale private aanbieders. Een interventie van de toezichthouder is erop gericht een situatie waarin een aanbieder niet voldoet aan verplichtingen die voortvloeien uit (sectorale) wetgeving te verhelpen. Het NCSC maakt daarentegen geen afweging met betrekking tot het al dan niet voldoen aan verplichtingen in wet- en regelgeving, maar adviseert en ondersteunt aanbieders bij het treffen van maatregelen ter voorkoming van de uitval door een ict-incident van de beschikbaarheid van voor de samenleving vitale producten en diensten, ongeacht of die aanbieders wettelijk verplicht zijn tot het treffen van dergelijke maatregelen.

De leden van de D66-fractie vragen of uit de wettekst blijkt dat het advies van het NCSC ondergeschikt is aan het advies van de sectorale toezichthouder.

Anders dan de memorie van toelichting wellicht suggereert, regelt het wetsvoorstel niet dat bij tegenstrijdige adviezen het advies van de toezichthouder voorgaat. Geen van beide adviezen is als zodanig bindend. Het verschil zit in het vervolg: de aanbieder weet dat de toezichthouder hem zo nodig kan dwingen om diens advies te volgen, bijvoorbeeld door hem een bindende aanwijzing te geven of jegens hem een sanctiebesluit te nemen.

2.4 Verhouding tot meldplicht datalekken

De leden van de SP-fractie vragen wat er precies gebeurt als een toezichthouder of een instantie als het NCSC of de AP bij het onderzoek naar een melding erachter komt dat verkeerd gemeld is. Zullen zij de melding dan actief doorgeleiden naar de juiste instantie? Als het NCSC er bijvoorbeeld achter komt dat er ook persoonsgegevens in het geding zijn, zal het de zaak dan ook actief doorgeven aan de AP? Betrokken instanties

zullen namelijk niet altijd kunnen inschatten wat de gevolgen zijn van een inbreuk.

In veel gevallen zal het in zo'n geval de voorkeur hebben dat de overheidsinstantie contact opneemt met de melder en hem daarbij in overweging geeft om de melding zelf alsnog bij de bevoegde instantie in te dienen. Op die manier reikt de overheidsinstantie de melder de helpende hand, maar blijft de melder wel zelf verantwoordelijk om bij de juiste instantie te melden.

De leden van de CDA-fractie vragen de regering in te gaan op de ministeriële verantwoordelijkheid die geldt ten aanzien van de bescherming van persoonsgegevens. In het bijzonder vragen zij om een reactie op de wijze waarop de Minister van Volksgezondheid, Welzijn en Sport onlangs heeft gereageerd op de berichtgeving dat Belgische gevangenen gewerkt hebben met Nederlandse patiëntendossiers. Kan de regering verduidelijken hoe de ministeriële verantwoordelijkheid haar uitwerking krijgt in relatie tot de meldplicht datalekken en het onderhavige wetsvoorstel, ook voor wat betreft andere ministeries dan het Ministerie van Veiligheid en Justitie?

Dit wetsvoorstel brengt geen verandering in de ministeriële verantwoordelijkheid ten aanzien van de bescherming van persoonsgegevens. Elke Minister is politiek aanspreekbaar op de bescherming van persoonsgegevens binnen zijn portefeuille. Op het terrein van de gezondheidszorg vertaalt die politieke verantwoordelijkheid zich onder meer in de taak van de Inspectie voor de Gezondheidszorg (IGZ) om toe te zien op de naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging in de zorg, voor zover die raakt aan kwaliteit en veiligheid van zorg (Wet kwaliteit, klachten en geschillen zorg en NEN 7510, 7512 en 7513). De AP is bevoegd om toe te zien op de naleving van de Wet bescherming persoonsgegevens (Wbp) en om handhavend op te treden tegen overtredingen van die wet. De IGZ en de AP hebben afspraken gemaakt over de wijze van samenwerking voor het uitoefenen van toezicht op de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer binnen de gezondheidszorg.[4]
Meer specifiek ten aanzien van de door deze leden bedoelde berichtgeving wijs ik erop dat de AP onderzoek doet naar deze kwestie en dat ook de Minister van Volksgezondheid, Welzijn en Sport vanuit haar politieke verantwoordelijkheid onderzoek laat doen naar de vraag op welke wijze zorginstellingen in de dagelijkse praktijk omgaan met de beveiliging van hun patiëntgegevens en hoe hierin verbetering kan worden aangebracht.[5]

2.5 Naleving

De leden van de PvdA-fractie verzoeken om voorbeelden van de situatie dat het advies van de NCSC niet (voldoende) wordt opgevolgd door de getroffen organisatie en de voor de sector verantwoordelijke bewindspersoon op de hoogte wordt gebracht. Welke criteria gelden dan en welke maatregelen kunnen vervolgens worden getroffen, vooral richting de niet-coöperatieve organisatie, om escalatie te voorkomen? Wat verstaat de regering onder «passend invulling geven aan zijn sectorale verantwoordelijkheid»? Hoe is in dergelijke gevallen de aansprakelijkheid geregeld? En welke maatregelen kan een bewindspersoon vervolgens nemen, vragen deze leden en de leden van de PVV-fractie.

---

[4] Stcrt. 2006, 233.
[5] Kamerstukken II 2015/16, 31 765, nr. 196, Aanhangsel Handelingen II 2015/16, nr. 2172 en 2275.

De bevoegdheid om de eerstverantwoordelijke bewindspersoon te informeren, beoogt te voorkomen, bij wijze van stok achter de deur, dat de getroffen organisatie het NCSC-advies zonder goede reden naast zich neerlegt. Het uiteindelijke oogmerk is het voorkómen of beperken van maatschappelijke ontwrichting. Het blijft primair de eigen verantwoordelijkheid van de aanbieder zelf om passende maatregelen te nemen om uitval of verstoring van zijn product of dienst te voorkomen of te beperken. De aansprakelijkheid voor eventuele schade blijft dus liggen bij de aanbieder.

Het is aan de sectoraal verantwoordelijke bewindspersoon om al dan niet actie te ondernemen naar aanleiding van het aan hem verstrekte NCSC-advies. Welke actie dat is, hangt af van de interventiemogelijkheden die hij krachtens de toepasselijke sectorale wetgeving heeft. Het kan bijvoorbeeld gaan om een bindende aanwijzing, een last onder bestuursdwang, een last onder dwangsom of een bestuurlijke boete.

Een voorbeeld van het mogelijk handelen van een bewindspersoon na bovenbedoeld informeren door het NCSC is de situatie waarin een aanbieder in de telecomsector wordt getroffen door een omvangrijke hack. Als de aanbieder de adviezen van het NCSC naast zich neerlegt, en daardoor naar het oordeel van het NCSC het risico van maatschappelijke ontwrichting aanwezig blijft, kan de Minister van Economische Zaken, nadat hij hierover is geïnformeerd, bijvoorbeeld de telecomaanbieder op grond van artikel 11a.1, vijfde lid, van de Telecommunicatiewet verplichten een technische of organisatorische maatregel te treffen met betrekking tot de veiligheid of integriteit van het openbare elektronische communicatienetwerk of de openbare elektronische communicatiedienst. De leden van de D66-fractie vragen de regering toe te lichten op wat voor manier gerapporteerd wordt aan de Tweede Kamer door het NCSC over de meldplicht. Is de regering bereid de Kamer een overzicht toe te sturen van het aantal meldingen en in hoeverre de adviezen van het NCSC zijn opgevolgd?

Jaarlijks publiceert het NCSC het Cybersecuritybeeld Nederland (CSBN). Het CSBN komt in nauwe samenwerking met publieke en private partners tot stand. Doel is het bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. Het NCSC zal in elk geval jaarlijks rapporteren over de aan het NCSC gedane meldingen. Zo mogelijk zullen bovendien ook periodieke publieksmededelingen door het NCSC worden opgesteld over bijvoorbeeld voor sectoren geldende aantallen meldingen en typen incidenten. Uw Kamer zal hieromtrent via dezelfde kanalen worden geïnformeerd. Ook ben ik bereid uw Kamer, bijvoorbeeld via het CSBN, in algemene zin te informeren over de opvolging van NCSC-adviezen.

3. Wettelijke grondslag voor taken en gegevensverwerking NCSC

De leden van de VVD-fractie vragen in hoeverre het NCSC informatie kan delen met de inlichtingen- en veiligheidsdiensten, de politie en het Openbaar Ministerie (OM)?

Voor zover het niet gaat om persoonsgegevens en evenmin om vertrouwelijke, tot een aanbieder herleidbare gegevens kan het NCSC onbeperkt informatie verstrekken aan de inlichtingen- en veiligheidsdiensten, de politie en het OM. Daarnaast kan het NCSC persoonsgegevens die niet herleidbaar zijn tot een aanbieder verstrekken met inachtneming van de Wbp.
Voor vertrouwelijke, tot een aanbieder herleidbare gegevens geldt het volgende:

– als de betrokken aanbieder ermee instemt, mag het NCSC dergelijke gegevens aan derden verstrekken;
– zonder instemming van de betrokken aanbieder mag het NCSC dergelijke gegevens verstrekken aan bijvoorbeeld de inlichtingen- en veiligheidsdiensten (voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer, zie het voorgestelde artikel 9, tweede lid) en aan bijvoorbeeld de politie en het OM (voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken; dit mag alleen na raadpleging van de betrokken aanbieder, zie het voorgestelde artikel 9, vierde lid, onder b). Overigens kan de officier van justitie gegevens vorderen bij het NCSC op grond van artikel 126nc e.v. van het Wetboek van Strafvordering.

De leden van de PvdA-fractie vragen in hoeverre de regering de eigen verantwoordelijkheid van aanbieders voor de veiligheid van hun informatiesystemen kan en wil afdwingen.

Voor aanbieders in bepaalde vitale sectoren is thans al in sectorale wetgeving vastgelegd dat zij met het oog op de continuïteit van vitale processen passende voorzieningen moeten treffen en dat op de naleving daarvan toezicht wordt gehouden. Krachtens de NIB-richtlijn zullen dergelijke regels gaan gelden voor alle aan te wijzen aanbieders van essentiële en digitale diensten in de zin van de richtlijn.

Verder vragen deze leden of het NCSC ruimte ziet om jongeren met een stoornis in het autistisch spectrum in te zetten voor het verrichten van analyses en technisch onderzoek.

Het NCSC heeft zeker oog voor deze groep jongeren, zoals reeds aan de orde is geweest in het algemeen overleg op 20 januari 2016. In antwoord op vragen van het lid Gesthuizen wees ik er toen op dat het NCSC constructief samenwerkt met deze jongeren. Onder andere zijn deze jongeren betrokken bij de NCSC One Conference en daarnaast biedt het NCSC hun ook stagemogelijkheden. Zoals in de genoemde beantwoording ook naar voren kwam, tracht het NCSC de vaardigheden van deze jongeren onder de aandacht te brengen bij het CyberSecurity Research and Education Platform om zo vraag en aanbod bij elkaar te brengen.

De leden van de CDA-fractie vragen of het wenselijk is, ook gelet op de verantwoordelijkheid die de regering bij de Minister van Veiligheid en Justitie wil neerleggen om de maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen, dat het NCSC niet bevoegd wordt gesteld om de identiteit van bijvoorbeeld hackers te achterhalen. Deze leden erkennen dat het strafrechtelijke opsporingsonderzoek is belegd bij politie en justitie, maar zij vragen of de regering de mening deelt dat medewerkers van het NCSC in elk geval hun ogen niet kunnen sluiten als zij op de identiteit van personen stuiten die (mogelijk) strafbare feiten hebben gepleegd of nog zullen plegen. Verder vragen deze leden wat de regering voornemens is hierover te regelen bij amvb.

Het NCSC heeft, anders dan inlichtingen- en veiligheidsdiensten en opsporingsdiensten, niet tot taak om de identiteit van aanvallers te achterhalen. Het NCSC heeft die informatie, anders dan bijvoorbeeld de betrokken IP-adressen, niet nodig om de in het wetsvoorstel vastgelegde taken (versterking digitale weerbaarheid, voorkoming maatschappelijke ontwrichting) te kunnen uitoefenen. Voor zover bepaalde gegevens die bij het NCSC berusten wellicht toch relevant zijn in het kader van bijvoorbeeld de opsporing, kan worden bezien of binnen de daarvoor geldende

wettelijke kaders (met name de Wbp) verstrekking daarvan aan bijvoorbeeld opsporingsdiensten mogelijk is. Het wetsvoorstel geeft geen grondslag voor het hierover bij amvb stellen van regels.

In dat kader maken deze leden zich zorgen over de opmerking dat indien aan het NCSC een dataset is overhandigd waarin bijzondere persoonsgegevens blijken te zijn opgenomen, deze onmiddellijk dient te worden vernietigd. Hoe verhoudt zich dit tot de effectiviteit van opsporing en vervolging dat uit NCSC-onderzoek naar datalekken kan voortvloeien?

Een dataset waarin bijzondere persoonsgegevens voorkomen, wordt niet in zijn geheel vernietigd, doch slechts de bijzondere persoonsgegevens die zich daarin bevinden.[6] Desgewenst kan de aanbieder, mits hij daartoe bevoegd is ingevolge de Wbp, de dataset rechtstreeks zelf aan de politie verstrekken. Daarnaast kan de officier van justitie gebruikmaken van zijn bevoegdheden om gegevens te vorderen.

Ook vragen deze leden of de regering de mening deelt dat ook het OM en de politie geschaard kunnen worden onder organisaties die tot taak hebben om andere organisaties of het publiek over dreigingen of incidenten te rapporten. Zo nee, waarom niet? Beschikt de regering over indicaties dat vitale aanbieders hier bezwaren tegen zouden hebben?

Het voorgestelde artikel 2, tweede lid, onder a, ziet op organisaties die tot taak hebben (objectief kenbaar, bijvoorbeeld blijkend uit een wettelijk voorschrift of uit statuten) om andere organisaties te informeren over ICT-dreigingen en incidenten. OM en politie voldoen niet aan die voorwaarde. Een voorbeeld van een organisatie waarop genoemde bepaling wel betrekking heeft, is de Stichting Internet Domeinnaamregistratie Nederland (SIDN). Uit de consultatiereacties blijkt inderdaad dat organisaties bezwaren hebben tegen het zonder meer door het NCSC kunnen doorverstrekken van (in elk geval de meest gevoelige onderdelen van) incidentinformatie. Overigens zal het NCSC daar waar nodig de betrokken organisaties aansporen om informatie zelf aan het OM en de politie te geven.

4. Verstrekking van vertrouwelijke gegevens

De leden van de PvdA-fractie verzoeken om voorbeelden van situaties waarin herleidbare gegevens moeten worden verstrekt aan andere organisaties of aan het publiek.

Een hypothetisch voorbeeld kan zijn dat een bepaalde bank gebruikmaakt van een identificatiemiddel van een derde partij. Indien het valt vast te stellen dat het gebruik hiervan ontegenzeggelijk voor een groot maatschappelijk risico zorgt, behoort het NCSC bevoegd te zijn om het publiek, onder vermelding van de betrokken bank, hiervoor te waarschuwen. Dat het NCSC deze bevoegdheid heeft, kan bijvoorbeeld ook een stimulans zijn voor organisaties om zelf het publiek te informeren over de kwetsbaarheid.

Deze leden vragen verder welke rol specifieke organisaties met bijzondere expertise kunnen hebben, zoals de Fraudehelpdesk.

---

[6] Bijzondere persoonsgegevens zijn persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (zie artikel 16 Wbp).

Of en aan welke andere organisaties genoemde herleidbare gegevens zullen moeten worden gedeeld, zal telkens afhangen van de omstandigheden van het geval. Van de zijde van het NCSC zal in elk geval telkens moeten worden bezien of het verstrekken aan een andere organisatie van dergelijke gegevens noodzakelijk is uit een oogpunt van voorkoming of beperking van ernstige maatschappelijke gevolgen. Daarbij zal in elk geval ook steeds worden beoordeeld of het in dergelijke situaties, ter voorkoming van ernstige maatschappelijke gevolgen, niet ook al voldoende is als incidentinformatie aan een andere organisatie wordt verstrekt zonder de daartoe behorende herleidbare gegevens.

De aan het woord zijnde leden vragen hoe de regering ervoor gaat zorgen, anders dan het streng houden aan het criterium «voorkómen van ernstige maatschappelijke gevolgen», dat toepassing van artikel 9, vierde lid, niet ten koste gaat van de privacy.

Artikel 9 ziet in beginsel niet op de verstrekking van persoonsgegevens, maar op de verstrekking van vertrouwelijke gegevens die herleidbaar zijn tot een aanbieder. Hierbij moet worden gedacht aan bijvoorbeeld de naam van de aanbieder of andere voor die aanbieder unieke kenmerken. In sommige gevallen kan het bij die herleidbare vertrouwelijke gegevens gaan om persoonsgegevens, zoals de naam of het zakelijk e-mailadres van een medewerker in relatie tot een incident. Ten aanzien van die gegevens geldt naast artikel 9 ook de Wbp en zal verstrekking alleen geschieden voor zover die wet dat toestaat.

Ook vragen deze leden hoe in het algemeen het publiek op de hoogte wordt gebracht en gehouden van de publieksmededelingen en voorlichting van het NCSC. Wordt daarvoor een apart medium en/of alert-systeem overwogen?

Het NCSC heeft verschillende informatiekanalen om informatie over dreigingen en kwetsbaarheden te delen met het publiek. Zo is er primair de website (www.ncsc.nl), waarop bijvoorbeeld ook alle algemene beveiligingsadviezen van het NCSC te vinden zijn. Juist in het licht van publieksvoorlichting is samen met ECP de website veiliginternetten.nl ingericht en werkt het NCSC mee aan de publiekscampagne «Alert Online». Deze websites worden daarnaast ondersteund door het gebruik van sociale media en andere (technische) mogelijkheden om op de hoogte gehouden te worden van nieuws. Daarmee acht de regering het niet noodzakelijk om in aanvulling hierop een apart alerteringskanaal in te richten.

De leden van de D66-fractie stellen enkele vragen over de reactie van de regering op de kritiek van de Afdeling advisering en de AP op de afwijking van het doelbindingsvereiste van de Wbp (artikel 9, eerste lid, Wbp) in het voorgestelde artikel 4, tweede lid.

De afwijking van het doelbindingsvereiste beoogt zeker te stellen dat een organisatie die bereid is om aan het NCSC vrijwillig persoonsgegevens te verstrekken (zoals IP-adressen), daartoe ook bevoegd is. Zonder die afwijking zou zij die bevoegdheid alleen hebben als de verstrekking aan het NCSC niet onverenigbaar is met de doeleinden waarvoor zij de persoonsgegevens heeft verkregen (artikel 9, eerste lid, Wbp) dan wel voor zover de verstrekking noodzakelijk is ter bescherming van de in artikel 43 Wbp genoemde belangen. Zoals in de memorie van toelichting en het nader rapport is uitgelegd, biedt artikel 43 Wbp onvoldoende ruimte om het doelbindingsvereiste buiten toepassing te laten in alle gevallen waarin het NCSC de persoonsgegevens nodig heeft voor de

vervulling van de taken, genoemd in artikel 2, eerste lid, van dit wetsvoorstel.
In haar advies merkt de Afdeling advisering van de Raad van State op: «Indien niettemin een wettelijke uitzondering zou worden overwogen dan zou in het voorstel moeten worden gepreciseerd in welke categorieën van gevallen van het doelbindingsvereiste kan worden afgeweken.» In het voorgestelde artikel 4, eerste lid, is de bevoegdheid van het NCSC om gegevens te vragen, gebonden aan de in artikel 2, eerste lid, genoemde NCSC-taken. Ingevolge het tweede lid van artikel 4 is de bevraagde organisatie alleen dan niet gebonden aan het doelbindingsvereiste als het NCSC-verzoek voldoet aan het eerste lid van artikel 4, dus voor zover het gaat om gegevens die het NCSC nodig heeft ter vervulling van zijn in artikel 2, eerste lid, genoemde taken. Op die manier doet het wetsvoorstel wat de Afdeling advisering voorstelt, namelijk preciseren (begrenzen) in welke gevallen de bevraagde organisatie mag afwijken van het doelbindingsvereiste.

5. Totstandkoming van dit wetsvoorstel

5.1 Bespreking van de reacties op hoofdlijnen

5.1.1 Zorgplichten en handhaving

De leden van de CDA-fractie vragen of de regering heeft overwogen in geval er geen sprake is van publiek-private samenwerking maar alleen van publiekrechtelijke organisaties, wel nadere interventiebevoegdheden voor het NCSC mogelijk te maken.

Ik heb ervoor gekozen om in dit wetsvoorstel geen interventiebevoegdheden op te nemen, ook niet jegens publiekrechtelijke organisaties. Het onderwerp interventiebevoegdheden zal nader aan de orde komen bij het nog te maken wetsvoorstel ter implementatie van de NIB-richtlijn.

Deze leden vragen met betrekking tot de advisering omtrent installatie van detectiesoftware of ingeval van tegenstrijdige adviezen of het advies van de sectorale toezichthouder altijd prevaleert boven dat van het NCSC. Immers, de keuze de installatie van dergelijke programmatuur wel of niet te eisen van de betreffende vitale aanbieder, kan verstrekkende gevolgen hebben bij (latere) ICT-inbreuken. De leden van de CDA-fractie vragen de regering daarom op dit punt nader aandacht te besteden aan de verhouding tussen het NCSC en de sectorale toezichthouders.

Zoals ik in mijn antwoord op een vraag van de leden van de D66-fractie heb verduidelijkt (aan het slot van paragraaf 2.3), is geen van beide adviezen als zodanig bindend. Wel kan de toezichthouder, anders dan het NCSC, desgewenst afdwingen dat zijn advies wordt gevolgd.

Ook vragen deze leden of de regering kan verzekeren dat momenteel alle bekende vitale aanbieders in Nederland beschikken over een detectiesoftware.

Detectiesoftware kan helpen om inbreuken eerder te detecteren, doch daarmee worden niet noodzakelijkerwijs alle inbreuken gedetecteerd, bijvoorbeeld als een voor de detectiesoftware nog onbekende aanvalsvector (manier waarop een hacker toegang kan verkrijgen tot een informatiesysteem) wordt gebruikt. De beslissing om deze software te installeren, is in eerste instantie een eigen verantwoordelijkheid van aanbieders. Hierbij valt op te merken dat voor een deel van de aanbieders het gebruik van detectiesoftware mogelijk door toezichthouders met betrekking tot wettelijke voorschriften die tot het treffen van beveiligings-

maatregelen verplichten, aangewezen wordt geacht. Met de implementatie van de NIB-richtlijn zal worden voorzien in een wettelijke verplichting tot het treffen van genoemde passende technische en organisatorische maatregelen voor alle op grond van de NIB aangewezen aanbieders van essentiële diensten.

5.1.2 Administratieve lasten

De leden van de VVD-fractie vragen wat een melding van een ICT-inbreuk in de praktijk precies behelst voor de betrokken vitale aanbieder.

De aanbieder kan aan de hand van de voorgestelde wet, de op grond daarvan vast te stellen amvb en de te maken richtsnoeren zelf concluderen dat de inbreuk meldplichtig is en meteen een melding doen, maar vaak zal de aanbieder eerst telefonisch contact zoeken met het NCSC. Naar aanleiding van de gedane melding kan het NCSC hem om aanvullende informatie vragen. Op basis hiervan zal het NCSC advies geven en eventueel ook andere hulp bieden.

5.1.3 Reikwijdte meldplicht

De leden van de VVD-fractie vragen hoe gezondheidsinstellingen, zoals ziekenhuizen, zich verhouden tot de definitie van vitale aanbieders. Waarom wordt (hooggespecialiseerde) ziekenhuiszorg niet als voor de samenleving vitale dienst gekwalificeerd? Ook uitval van zorg door ICT-problemen kan toch leiden tot maatschappelijke ontwrichting?

De gezondheidszorg wordt niet als vitale sector beschouwd vanwege het geringere risico van cascade-effecten van een zorgincident. Die cascade-effecten zijn beperkt omdat de zorgverlening in Nederland en de ICT-ondersteuning daarvan grote spreiding en redundantie (mogelijkheid van vervanging) kent. De zorg is wel gevoelig voor kwetsbaarheden in andere sectoren, zoals energie en drinkwater. Die sectoren vallen wel onder de meldplicht.

5.1.4 Te melden ICT-inbreuken

De vraag van de leden van de SP-fractie over DDoS-aanvallen is beantwoord in paragraaf 2.1.

5.1.5 Vertrouwelijkheid

De leden van de SP-fractie vragen wie controleert of het NCSC zijn geheimhoudingsplicht naleeft en wat er gebeurt bij schending hiervan.

Het zal in eerste instantie de betrokken aanbieder zelf zijn die zich bij het NCSC vervoegt als hij van mening is dat het NCSC zich niet heeft gehouden aan zijn geheimhoudingsplicht. Schending daarvan is een strafbaar feit (artikel 272 van het Wetboek van Strafrecht). De aanbieder kan aangifte doen. Hij kan ook bij de burgerlijke rechter een actie tegen de Staat beginnen uit onrechtmatige daad. Overigens is het ook in het belang van het NCSC om zelf te voorkomen dat het aan derden gegevens verstrekt die vertrouwelijk dienen te blijven. Een dergelijke verstrekking zal de aanbieder immers terughoudend maken om het NCSC vertrouwelijke gegevens te blijven verstrekken.

6. Grondrechtentoets

De leden van de SP-fractie vragen hoe het NCSC op basis van sec de IP-adressen nader onderzoek kan doen zonder daarbij ook bijzondere persoonsgegevens te verwerken?

Over het algemeen ontvangt het NCSC geen bijzondere persoonsgegevens. De informatie die wordt gedeeld bevat voornamelijk IP-adressen en context informatie. IP-adressen zijn bijvoorbeeld nodig om uit te zoeken of en zo ja welke individuele computers betrokken zijn bij een ICT-inbreuk. Voor dergelijk onderzoek is het werken met persoonsgegevens in de vorm van onder meer IP-adressen onvermijdelijk. Het NCSC ontvangt met regelmaat van andere partijen, waaronder bijvoorbeeld Computer Emergency Response Teams (CERT's) die deel uitmaken van het internationale CERT-netwerk, gegevens over Nederlandse partijen in relatie tot ICT-incidenten. Het NCSC analyseert deze gegevens op relevantie voor de veiligheid en betrouwbaarheid van de ICT-systemen van de rijksoverheid en de vitale private sectoren. Het NCSC kan niet altijd voorkomen dat de informatie afkomstig van andere partijen bijzondere persoonsgegevens bevat. Wanneer een partij hierover vooraf contact zoekt met het NCSC, dan kan het NCSC erop aandringen dat het alleen de gegevens krijgt die nodig zijn voor het voorkomen van schade. Zodra het NCSC ongevraagd een dataset ontvangt met hierin bijzondere persoonsgegevens, zal het NCSC laatstbedoelde gegevens vernietigen. In een dergelijke situatie wordt aantekening gemaakt van het vernietigen van de bijzondere persoonsgegevens en met de resterende (persoons)gegevens wordt het incident verder verholpen.

De leden van de CDA-fractie vragen de regering waarom persoonsgegevens onmiddellijk vernietigd worden wanneer deze door het NCSC worden aangetroffen in datasets. Gelet op de mogelijke dreiging van een ICT-inbreuk, zou de focus van het NCSC toch vooral moeten zijn het oplossen hiervan en niet het uitkammen van datasets op de aanwezigheid van bijzondere persoonsgegevens? Is bij een voorgenomen verstrekking aan het NCSC van een dataset altijd vooraf duidelijk voor zowel de vitale aanbieder als het NCSC welke daarin aanwezige persoonsgegevens noodzakelijk zijn voor het uitvoeren van de NCSC-taken?

Het NCSC dient in een ontvangen dataset niet alle persoonsgegevens onmiddellijk te vernietigen, doch slechts de *bijzondere* persoonsgegevens. De verwerking van persoonsgegevens is op grond van de Wbp voor organisaties als het NCSC in beginsel alleen toegestaan wanneer dit noodzakelijk is met het oog op de publiekrechtelijke taak. Voor het NCSC is de verwerking van *bijzondere* persoonsgegevens niet noodzakelijk om zijn taken, zoals omschreven in artikel 2 van het wetsvoorstel, te kunnen uitoefenen. Met het oog daarop is daarom het uitgangspunt dat het NCSC geen datasets in ontvangst neemt als bekend is of vermoed wordt dat daarin ook bijzondere persoonsgegevens voorkomen, en wordt aan de aanbieder verzocht laatstgenoemde persoonsgegevens daar eerst uit te filteren alvorens de dataset wordt verstrekt aan het NCSC. Worden in een ontvangen dataset onverhoopt bijzondere persoonsgegevens aangetroffen, dan zullen die, bij afwezigheid van een wettelijke grondslag om ze te verwerken, onmiddellijk worden vernietigd.

De leden van de fracties van D66 en de SP vragen naar het oordeel van de AP over de uiteindelijke versie van de memorie van toelichting.

Ingevolge artikel 51 Wbp wordt de AP om advies gevraagd over voorstellen van wet (en ontwerpen van algemene maatregelen van bestuur) die geheel of voor een belangrijk deel betrekking hebben op de

verwerking van persoonsgegevens. Het is niet gebruikelijk om ook wijzigingen die naar aanleiding van het AP-advies worden aangebracht, weer aan de AP voor te leggen, en dat is ook hier niet gebeurd. Na inwerkingtreding van de voorgestelde wet is het aan de AP om toe te zien op de naleving van de Wbp en om zo nodig handhavend op te treden.

7. Privacy impact assessment

De leden van de SP-fractie hebben enkele vragen over de passage in de memorie van toelichting waarin wordt gesteld dat een betrokkene inzicht kan verkrijgen in de persoonsgegevens die het NCSC (heeft) verwerkt door een verzoek in te dienen bij het Ministerie van Veiligheid en Justitie.

Deze passage doelt op artikel 35 Wbp, dat betrokkene het recht geeft zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. Tegen de afwijzing van een verzoek staat bestuursrechtelijke rechtsbescherming open.

Ik voldoe graag aan het verzoek van de leden van de D66-fractie om toezending van het privacy impact assessment en stuur dat gelijktijdig met deze nota aan de Kamer[7].

8. Regeldruk

De leden van de CDA-fractie vragen om een indicatie van de administratieve lasten die aanbieders kwijt zijn in geval zij een dubbele of driedubbele melding van een inbreuk moeten maken. Zijn de lasten dan niet veel hoger dan de genoemde 17.000 euro per jaar? Zijn de kosten zeker voor het midden- en kleinbedrijf niet te hoog? Ook vragen deze leden om een reactie op het risico dat aanbieders bij invoering van de meldplicht veel tijd en middelen kwijt zijn aan het managen van processen in plaats van het oplossen van de betreffende ICT-problemen. Waarop baseert de regering de verwachting dat dit wetsvoorstel ondanks de administratieve lasten zal leiden tot een verdere vergroting van de meldingsbereidheid?

De voorgestelde meldplicht is alleen van toepassing op de bij algemene maatregel van bestuur aangewezen aanbieders van voor de Nederlandse samenleving vitale producten of diensten. Naar verwachting behoort het midden- en kleinbedrijf niet tot de in de toekomst meldplichtige vitale aanbieders. De administratieve lasten voor vitale aanbieders als gevolg van dit wetsvoorstel zullen bescheiden zijn. Een concrete raming kan pas worden gemaakt als vaststaat voor welke vitale aanbieders en voor welke producten en diensten de meldplicht zal gelden en als voor de meldplichtige producten en diensten is bepaald welke drempelwaarden zullen worden gehanteerd ter nadere uitwerking van «in belangrijke mate» in het voorgestelde artikel 6, eerste lid. Om toch een indicatie te geven van de te verwachten administratieve lasten, heb ik in de memorie van toelichting gekeken naar de in 2010 geraamde administratieve lasten van een andere wettelijke meldplicht, namelijk die van artikel 11a.2 Telecommunicatiewet, die is ingevoerd in 2012.[8] Het bedrag van 17.000 euro dat ik

---

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

[8] «Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten stellen Onze Minister [van Economische Zaken] onverwijld in kennis van:
a. een inbreuk op de veiligheid,
b. een verlies van integriteit,
waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke mate werd onderbroken.»

daarbij noemde, zag echter op de totale lasten van de 80 meldingen per jaar waarvan bij de raming in 2010 is uitgegaan. De verwachte lasten per melding bedroegen toen dus 212,50 euro. Aangezien het soort gegevens dat moet worden verstrekt bij de meldplicht van artikel 11a.2 Telecommunicatiewet[9] deels hetzelfde zal zijn als bij de nu voorgestelde meldplicht (zie artikel 6, tweede lid), verwacht ik niet dat de lasten per melding van de nu voorgestelde meldplicht veel hoger zullen zijn. Alleen incidenten die «in belangrijke mate», en dus op grote schaal, de beschikbaarheid en betrouwbaarheid van een vitaal product of een vitale dienst doen onderbreken, en zodoende maatschappelijke ontwrichting tot gevolg (kunnen) hebben, dienen te worden gemeld. Ik verwacht dan ook niet dat de meldplicht van dit wetsvoorstel vele incidenten per jaar zal betreffen.

Tegenover de bescheiden lasten van de meldplicht staan voor de betrokken organisaties potentieel grote baten: advisering en bijstand door het NCSC dragen immers bij aan het zo snel mogelijk verhelpen van gebleken ICT-inbreuken. De werkwijze van het NCSC is erop gericht dat de aanbieder toekomt aan het herstellen van de continuïteit van de eigen dienstverlening en het oplossen van het incident en het NCSC daarbij zo veel mogelijk hulpverlenend optreedt in zijn hoedanigheid van CERT.

De leden van de D66-fractie vragen of het NCSC voldoende capaciteit heeft om bij een potentieel grote stroom aan meldingen daadwerkelijk hulp te bieden aan vitale aanbieders.

Het NCSC verwacht de meldingen te kunnen behandelen met zijn huidige bezetting, ook omdat de uit de meldplicht voortvloeiende werkzaamheden nauw aansluiten bij zijn huidige rol als CERT voor de rijksoverheid en vitale private organisaties. Uiteraard blijf ik volgen of het NCSC voldoende op sterkte is.

Artikelsgewijze toelichting

Artikel 1

De leden van de CDA-fractie vragen in verband met de herijkte lijst vitale infrastructuur (Kamerstuk 30 821, nr. 23) of gemeenten ook onder de reikwijdte van onderhavig wetsvoorstel vallen, dit omdat digitale overheid ook op deze lijst staat (onder categorie B).

De herijking van de vitale digitale overheid – of in dit geval is het, omdat het de eerste keer is, beter om van ijking te spreken – is nog niet afgerond. Bij deze ijking wordt het Nationaal Beraad Digitale Overheid betrokken. Gemeenten en andere overheden zijn daarin op directieniveau vertegenwoordigd via hun koepels. Als deze ijking oplevert dat bepaalde processen of systemen van de digitale overheid die ook bij of ten behoeve van gemeenten plaatsvinden respectievelijk gebruikt worden, van vitaal belang zijn voor de Nederlandse samenleving, dan vallen de desbetreffende aanbieders, producten en diensten ook onder de reikwijdte van dit wetsvoorstel. Denk daarbij vooral aan gezamenlijke infrastructurele componenten.

---

[9] Zie artikel 7, tweede lid, van het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten: «De melding bevat in ieder geval:
a. het tijdstip van aanvang van de inbreuk of het verlies;
b. de aard en de omvang van de inbreuk of het verlies;
c. op welk netwerk of bij welke dienst de inbreuk of het verlies heeft plaatsgevonden;
d. een prognose van de hersteltijd.»

Ook vragen deze leden hoe gemeenten zich hebben voorbereid op de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp, die op januari 2016 in werking is getreden.

De Informatiebeveiligingsdienst voor Gemeenten (IBD), een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING), heeft gemeenten met een factsheet actief geïnformeerd over de meldplicht. Het is de verantwoordelijkheid van de individuele gemeente om daar passend inhoud aan te geven.

Verder vragen deze leden of de regering het beeld herkent dat de digitale infrastructuur van gemeenten nog onvoldoende is toegerust op voorkomen van datalekken door gebrek aan expertise en financiële middelen. Hoe ondersteunt de regering gemeenten hierin, juist nu gemeenten door onder meer de transities in de zorg steeds meer bijzondere persoonsgegevens verwerken? Kan de regering aangeven in hoeverre gemeenten de adviezen van de Informatie Beveiligingsdienst (IBD) hebben opgevolgd om voorbereid te zijn op deze nieuwe meldplicht omtrent het datalekken?

Het geschetste beeld wordt niet herkend. Datalekken kunnen zo veel mogelijk worden voorkomen door het nemen van passende technische en organisatorische maatregelen. Deze maatregelen zijn beschreven in het gemeenschappelijk normenkader van de *Baseline Informatiebeveiliging Nederlandse Gemeenten* (BIG).[10] Gemeenten hebben de BIG als normenkader vastgesteld in de *Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente* [11] en zijn los van en ruim voor de inwerkingtreding van de meldplicht datalekken voortvarend aan de slag gegaan met de implementatie hiervan. De IBD is opgericht door gemeenten zelf en ondersteunt hen bij de implementatie van de BIG en faciliteert kennisdeling tussen gemeenten. Een gebrek aan expertise is bij gemeenten derhalve niet aan de orde.

De meldplicht datalekken is een aanscherping van de Wbp, het wettelijk kader waaraan gemeenten gehouden zijn. De adviezen van de IBD ter voorbereiding op de meldplicht datalekken hangen nauw samen met de BIG. Gemeenten voeren een gefaseerde en gedifferentieerde implementatie van de BIG door die gebaseerd is op lokale (risico)afwegingen. In algemene zin zijn gemeenten zich terdege bewust van de verantwoordelijkheid voor beveiliging van (bijzondere) persoonsgegevens en gaven zij hieraan reeds voor de inwerkingtreding van de meldplicht datalekken prioriteit.

De aan het woord zijnde leden vragen of gemeenten hierbij aanlopen tegen (financiële) problemen. Zij sommen daarbij diverse te nemen maatregelen op.

De plicht om persoonsgegevens te beschermen is niet nieuw en is niet ontstaan ten gevolge van de recente wijziging van de Wbp. Het College bescherming persoonsgegevens (de huidige AP) stelde al in 2013 richtsnoeren vast om invulling te geven aan het begrip «passende technische en organisatorische maatregelen» in artikel 13 Wbp zoals het toen al luidde. Het grootste deel van de maatregelen die door deze leden als voorbeelden worden genoemd van de adviezen van de IBD, is onderdeel van de wijze waarop de AP de beveiligingsnormen uit de Wbp

[10] www.ibdgemeenten.nl/producten/strategische-en-tactische-big
[11] www.ibdgemeenten.nl/wp-content/uploads/2014/04/20131031_resolutie-informatieveiligheid.pdf

toepast bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen. Het advies om een baselinetoets BIG uit te voeren is een logische consequentie van de implementatie van de BIG, waaraan gemeenten zich gecommitteerd hebben.

Artikel 4

De leden van de CDA-fractie vragen of het niet verstandig zou zijn om te voorzien in een vangnetconstructie, bijvoorbeeld in de vorm van een beoordeling door de betrokken sectorale toezichthouder, om te voorkomen dat het NCSC altijd aan het kortste eind trekt omdat de gegevensverstrekking op vrijwillige basis geschiedt.

Voor organisaties geldt op grond van artikel 4 geen plicht om het NCSC desgevraagd gegevens te verstrekken. Maar omdat het NCSC desgevraagd kan uitleggen waarom het de gevraagde gegevens nodig heeft voor de uitoefening van de in artikel 2, eerste lid, van het wetsvoorstel, genoemde taken, verwacht ik dat organisaties in veel gevallen bereid zullen zijn om de gevraagde informatie te verstrekken. Voor hen is het vooral van belang om te weten dat zij *bevoegd* zijn om de gevraagde (persoons)gegevens te verstrekken. Voor de door deze leden in overweging gegeven vangnetconstructie zie ik dan ook geen noodzaak.

Artikel 5

De leden van de PvdA-fractie vragen hoe buiten Nederland gevestigde meldplichtige aanbieders op de hoogte komen en blijven van de meldplicht en de daaraan verbonden eisen en verantwoordelijkheden.

Vooropgesteld zij dat communicatie over de meldplicht een belangrijke pijler voor het NCSC was en zal zijn bij totstandkoming van deze meldplicht. Het NCSC is in het kader van publiek-private samenwerking bekend met aanbieders die op Nederlands grondgebied een vitaal product of vitale dienst aanbieden. Van deze aanbieders mag worden verwacht dat zij op de hoogte zijn van in Nederland geldende wet- en regelgeving. Ik verwacht ook niet dat communicatieproblemen zullen opdoemen tussen het NCSC en aanbieders die niet in Nederland gevestigd zijn. Het NCSC is goed uitgerust om bijvoorbeeld ook in het Engels met aanbieders te communiceren over ICT-inbreuken, dreigingen en kwetsbaarheden.

Artikel 10

De leden van de fracties van de VVD en de PvdA vragen welke redenen er zouden kunnen zijn om te besluiten tot gedifferentieerde inwerkingtreding van onderhavige wet.

De mogelijkheid van gedifferentieerde inwerkingtreding zou bijvoorbeeld van pas kunnen komen als de bepalingen over de meldplicht nog niet in werking kunnen treden, bijvoorbeeld omdat de uitvoeringspraktijk op dat moment nog niet voldoende is voorbereid, terwijl er geen reden is om te wachten met de inwerkingtreding van de overige bepalingen, over de NCSC-taken en de verwerking van gegevens. Overigens ga ik ervan uit dat de wet als één geheel in werking zal kunnen treden.

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