Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

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)

B

MEMORIE VAN ANTWOORD

Ontvangen 25 april 2017

1. Inleiding

Met belangstelling heb ik kennisgenomen van het voorlopig verslag. Graag maak ik van de gelegenheid gebruik om de gestelde vragen te beantwoorden. 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.

2. Effectiviteit meldplicht

De leden van de fractie van **D66** stellen vragen over de meerwaarde van de voorgestelde meldplicht. Zij vragen waarom de huidige publiek-private samenwerking ontoereikend is, hoe vaak ernstige ICT-inbreuken niet gemeld worden en waarop de regering haar stelling baseert dat de meldingsbereidheid van vitale aanbieders wordt vergroot door een wettelijke meldplicht zonder toezicht en sancties. Ook de leden van de fractie van de **VVD** stellen vragen over de effectiviteit van een wettelijke meldplicht zonder toezicht en sancties.

De voorgestelde meldplicht zonder toezicht en sancties past in het bredere kader van publiek-private samenwerking, omdat zij een bijdrage levert aan de zogeheten *just culture*, een cultuur waarin het gezamenlijk bijdragen aan veiligheid centraal staat. De meerwaarde van de voorgestelde wettelijke regeling voor het melden van ernstige ICT-inbreuken is onder meer dat hiermee, en met de op te stellen richtsnoeren, voor aanbieders van producten en diensten buiten twijfel wordt gesteld in welke gevallen ICT-incidenten van dien aard zijn dat daardoor maatschappelijke ontwrichting aan de orde is of kan zijn en betrokkenheid van het NCSC, teneinde de uitval van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale producten en diensten te voorkomen of beperken, in elk geval noodzakelijk is. Daarnaast is van belang dat met de voorgestelde wettelijke meldplicht bij vitale aanbieders de twijfel wordt weggenomen of zij wel bevoegd zijn om gevoelige informatie over dergelijke

kst-34388-B
ISSN 0921 - 7371
's-Gravenhage 2017

incidenten 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). Ik beschik niet over cijfers over niet-gemelde incidenten. Mede blijkens de bevindingen in het meest recente Cybersecuritybeeld Nederland[1] is er in elk geval een aanzienlijke kans op ICT-incidenten die ook een serieuze bedreiging vormen voor vitale producten en diensten. Van belang is het derhalve dat het NCSC in dergelijke situaties tijdig betrokken is en door advisering en overige bijstand de schadelijke gevolgen hiervan kan helpen voorkomen of beperken.

3. Melding inbreuk

De leden van de **VVD**-fractie benadrukken het belang van de voortgang van het wetsvoorstel en vragen wanneer de meldplicht naar verwachting in werking zal treden.

De wet kan in werking treden op 1 juli 2017, de meldplicht – waarvoor nog een algemene maatregel van bestuur (amvb) in voorbereiding is – naar verwachting op 1 oktober 2017.

Deze leden vragen aan de hand van welke criteria de in de memorie van toelichting bedoelde drempelwaarden (om te bepalen of sprake is van «in belangrijke mate» in artikel 6, eerste lid, van het wetsvoorstel) zullen worden vastgesteld en zij ontvangen graag het betreffende beleidsbesluit.

De criteria aan de hand waarvan de drempels om te melden worden vastgesteld, verschillen per sector. Deze criteria kunnen onder meer zien op het aantal getroffen gebruikers, de geografische reikwijdte van het incident en de duur van de uitval van de betrouwbaarheid of beschikbaarheid van de dienst of het product. Deze criteria zullen door middel van vastlegging in richtsnoeren bekend worden gemaakt aan de betrokken aanbieders, maar zullen niet openbaar worden gemaakt, aangezien de veiligheid van deze producten en diensten in het geding kan komen als derden van deze criteria kennis kunnen nemen.

Verder stellen deze leden vragen over de situatie dat voor een bij het NCSC te melden incident ook een of meer andere meldplichten gelden, bijvoorbeeld als bij het incident ook persoonsgegevens betrokken zijn. Moet het incident dan ook worden gemeld bij de Autoriteit persoonsgegevens? Hoe wordt ervoor gezorgd dat steeds voldoende bekend is wie welke incidenten waar moet melden? En hoe wordt voorkomen dat de meldplicht een «administratief circus» wordt?

Een ICT-incident dat bij het NCSC dient te worden gemeld, moet ook worden gemeld bij de Autoriteit persoonsgegevens als door het incident tevens inbreuk wordt gemaakt op de beveiliging tegen verlies of onrechtmatige verwerking van persoonsgegevens met (aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van die gegevens (artikel 34a Wet bescherming persoonsgegevens (Wbp)). Als een incident onder meerdere meldplichten valt, is het aan de getroffen organisatie om het incident bij de juiste overheidsinstanties te melden, zoals het NCSC, de Autoriteit persoonsgegevens of een (sectorale) toezichthouder. Uiteraard zullen de betrokken overheidsinstanties – gevraagd en ongevraagd – hierover ook voorlichting geven. Ook zullen zij zo veel mogelijk de processen voor het doen van meldingen op elkaar afstemmen, zodat de sector niet onnodig wordt belast. Door zo veel

[1] Kamerstukken II 2015/16, 26 643, nr. 420.

mogelijk gelijke gegevenssets van aanbieders te vragen, wordt de aanbieder in staat gesteld met het eenmalig verzamelen en vastleggen van de gegevens, zonder significante inspanning, te voldoen aan verschillende meldplichten.

4. Vitale aanbieders

De leden van de fracties van de **VVD** en **D66** vragen welke vitale aanbieders en welke producten en diensten onder de meldplicht gaan vallen.

De aanbieders, producten en diensten die onder de meldplicht gaan vallen, worden aangewezen bij amvb. Deze amvb is vrijwel gereed en zal naar verwachting in april 2017 in consultatie worden gebracht. Ik zal u de tabel met de aan te wijzen aanbieders, producten en diensten toesturen zodra de consultatie is gestart.

5. Verhouding tot Wet bescherming persoonsgegevens

De leden van de **PvdA**-fractie vragen waarom in artikel 4 is gekozen voor vrijwillige verstrekking terwijl de bepaling gaat over gegevens die het NCSC nodig heeft voor de vervulling van zijn taken en de regering die noodzaak ook aanvoert als reden voor afwijking van het doelbindingsvereiste van de Wbp.

Het voorgestelde artikel 4 beoogt om organisaties bevoegd te maken om het NCSC desgevraagd de persoonsgegevens te verstrekken die het NCSC nodig heeft voor de vervulling van zijn taken. Die bevoegdheid is bedoeld voor de gevallen waarin die persoonsgegevens niet verkregen kunnen worden op grond van artikel 7 (verplichte verstrekking door vitale aanbieder van door het NCSC gevraagde gegevens naar aanleiding van een door die aanbieder verplicht gemeld incident). Dit betreft dus situaties waarin het NCSC op andere wijze dan door een verplichte melding (dus door een vrijwillige melding of informatie uit andere bronnen) van een dreiging of incident op de hoogte is gekomen en het voor het NCSC, juist ook ter voorkoming van grotere incidenten waarbij sprake zal zijn van maatschappelijke ontwrichting, nodig is daarover nadere informatie te verkrijgen. Ik heb tot nu toe geen signalen dat organisaties in dergelijke situaties niet bereid zijn om vrijwillig persoonsgegevens te verstrekken aan het NCSC. Een vorderingsbevoegdheid is daarom niet nodig. Wel wijzen organisaties erop dat zij het NCSC (uiteraard) alleen persoonsgegevens willen verstrekken als zij daartoe bevoegd zijn. Die bevoegdheid ontbreekt met name als het NCSC de persoonsgegevens nodig heeft ter bescherming van informatiesystemen van vitale aanbieders die niet behoren tot de rijksoverheid.[2] Met artikel 4 wordt erin voorzien dat organisaties die bevoegdheid ook in dergelijke gevallen hebben.

6. Netwerk- en informatiebeveiligingsrichtlijn

De leden van de **VVD**-fractie vragen wanneer het wetsvoorstel tot implementatie van de NIB-richtlijn wordt aangeboden aan de Tweede Kamer.

Ik verwacht dat het implementatiewetsvoorstel in het najaar van 2017 zal worden ingediend bij de Tweede Kamer.

---

[2] Zie de memorie van toelichting, Kamerstukken II 2015/16, 34 388, nr. 3, p. 26–27, en punt 2 van het nader rapport, Kamerstukken II 2015/16, 34 388, nr. 4, p. 3–5.

De **D66**-fractieleden vragen op welke punten de wettelijke meldplicht, zoals vervat in dit wetsvoorstel, afwijkt van de wettelijke meldplicht zoals vervat in de NIB-richtlijn.

De meldplichten in het onderhavige wetsvoorstel en in de NIB-richtlijn komen goeddeels overeen. Afgezien van een wat andere terminologie is een verschil wel dat eerstgenoemde meldplicht ook geldt voor incidenten waardoor de beschikbaarheid of betrouwbaarheid van vitale diensten in belangrijke mate kán worden onderbroken, terwijl de NIB-richtlijn alleen een meldplicht bevat voor incidenten met aanzienlijke gevolgen voor de continuïteit van dergelijke diensten. De richtlijn staat overigens expliciet toe (artikel 3) dat de lidstaten in dit opzicht verder gaan dan de richtlijn voorschrijft.

7. Toezicht en handhaving

Op de vragen van de leden van de fracties van de **VVD** en **D66** over de effectiviteit van een wettelijke meldplicht zonder toezicht en sancties ben ik ingegaan in paragraaf 2 van deze memorie.

De leden van de fractie van **D66** vragen waarom de adviezen van het NCSC niet bindend zijn.

Ik hecht eraan om het NCSC te positioneren als hulpverlener en adviseur en niet als toezichthouder. Een bevoegdheid voor het NCSC om een bindend advies of een bindende aanwijzing te geven, ligt dan ook niet in de rede. Ik verwacht overigens wel dat de NCSC-adviezen, onder meer gelet op de kennis en expertise van het NCSC, in het algemeen door betrokken organisaties zullen worden opgevolgd. Als een aanbieder naar mijn oordeel desalniettemin onvoldoende gevolg geeft aan een NCSC-advies en daardoor het risico op maatschappelijke ontwrichting aanwezig blijft, dan kan ik de betrokken vakminister informeren. De vakminister kan dan zo nodig en waar mogelijk besluiten, vanuit zijn sectorverantwoordelijkheid, of interventie nodig is.

Verder vragen deze leden waarom het wetsvoorstel niet voorziet in een regeling op grond waarvan toezichthouders het NCSC kunnen informeren over meldingen die zij hebben ontvangen uit hoofde van andere meldplichten.

Gegevensverstrekking door toezichthouders aan het NCSC is een onderwerp dat aan de orde komt bij het opstellen van het wetsvoorstel ter implementatie van de NIB-richtlijn, die de lidstaten immers opdraagt om te voorzien in toezicht en samenwerking op nationaal niveau (door betrokken overheidsinstanties).

8. Overige

De leden van de **VVD**-fractie vragen hoe de leden van de in het voorgestelde artikel 9 genoemde computercrisisteams tot geheimhouding worden gehouden.

Op grond van het voorgestelde artikel 9 kan het NCSC ter uitvoering van zijn taken vertrouwelijke gegevens over een aanbieder, ook als die herleid kunnen worden tot die aanbieder, verstrekken aan een computercrisisteam dat bij ministeriële regeling als zodanig is aangewezen. Voorafgaand aan de aanwijzing van een computercrisisteam in deze zin wordt ook nadrukkelijk getoetst of een computercrisisteam voldoende maatregelen heeft getroffen om de geheimhouding van genoemde gegevens te waarborgen.

De leden van de **D66**-fractie vragen of de voorgestelde wettelijke grondslag voor het verwerken van persoonsgegevens door het NCSC met voldoende waarborgen omkleed is.

De voorgestelde artikelen 2 en 3 bieden een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door het NCSC ten behoeve van zijn publiekrechtelijke taken. Die verwerking moet voldoen aan de vereisten die krachtens de Wet bescherming persoonsgegevens aan de verwerking van persoonsgegevens worden gesteld, en staat onder toezicht van de Autoriteit persoonsgegevens en de functionaris voor de gegevensbescherming van het Ministerie van Veiligheid en Justitie. In de memorie van toelichting (paragraaf 6 en 7) en in het privacy impact assesment (zie de bijlage bij de nota naar aanleiding van het verslag) is uiteengezet dat en hoe de verwerking van persoonsgegevens door het NCSC is omkleed met voldoende waarborgen (gegevensminimalisering, beveiliging, etc.).

Tot slot wensen de **PvdA**-fractieleden van de regering te vernemen hoe het voorliggende wetsvoorstel zich verhoudt tot het initiatiefvoorstel Wet open overheid, zoals dat inmiddels in de Tweede Kamer is aangenomen.

Artikel 9.60a van het wetsvoorstel Wet open overheid (Woo) regelt de wetstechnische samenloop met het onderhavige wetsvoorstel, door de afwijking van de Wet openbaarheid van bestuur in artikel 9, zesde lid, van het onderhavige wetsvoorstel te converteren in een afwijking van de Woo (toevoeging aan de bijlage bij artikel 8.8 Woo).

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