Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

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

Nr. 5 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 mei 2022

Op 21 april jl. is een voorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) ingediend bij uw Kamer (Kamerstuk 36 084). Dit wetsvoorstel strekt ertoe het Nationaal Cyber Security Centrum (NCSC) een ruimere bevoegdheid te geven om dreigings- en incidentinformatie, die relevant is voor andere aanbieders dan vitale aanbieders of rijksoverheidsorganisaties (hierna: andere aanbieders), aan die andere aanbieders of hun schakelorganisaties te verstrekken. Met de vaste commissie Digitale Zaken van uw Kamer heb ik in een vergadering van 7 april jl. over Online veiligheid en cybersecurity gesproken over een spoedige indiening van dit wetsvoorstel en de eventuele mogelijkheden voor het NCSC om met andere aanbieders of hun schakelorganisaties vóór inwerkingtreding van dit wetsvoorstel al in ruimere zin dreigings- en incidentinformatie te delen.[1]

In het licht van het bovenstaande stel ik uw Kamer hierbij, nu bovenbedoeld wetsvoorstel bij uw Kamer is ingediend, op de hoogte van het dilemma waarvoor ik mij geplaatst zie en schets ik de omstandigheden die er naar mijn oordeel vóór en tegen pleiten om, in de periode dat het wetsvoorstel in behandeling is bij uw Kamer en de Eerste Kamer, het NCSC al in uitzonderlijke gevallen overeenkomstig het wetsvoorstel dreigings- en incidentinformatie aan andere aanbieders of hun schakelorganisaties te laten verstrekken.

[1] Kamerstuk 26 643, nr. 849.

kst-36084-5
ISSN 0921 - 7371
's-Gravenhage 2022

De urgentie om in genoemde komende periode in uitzonderlijke gevallen overeenkomstig het wetsvoorstel aan of ten behoeve van andere aanbieders informatie over digitale dreigingen en incidenten te verstrekken is actueel door de oorlog in Oekraïne. Vanwege deze oorlog is sprake van een reële digitale dreiging die ook voor de dienstverlening van andere aanbieders mogelijk grote gevolgen kan hebben en daarmee mogelijk grote impact voor de Nederlandse samenleving kan hebben. Na de uitbraak van de oorlog in Oekraïne hebben meerdere organisaties zich gemeld bij het NCSC met het verzoek om meer informatie in relatie tot deze digitale dreiging te ontvangen. Hierbij gaat het zowel om andere aanbieders zelf als schakelorganisaties van andere aanbieders. Daarnaast kunnen zich in de nabije toekomst ook andere digitale dreigingen en incidenten voordoen, die ook in relatie tot de dienstverlening van andere aanbieders grote impact en daarmee grote nadelige maatschappelijke consequenties kunnen hebben. Door bijvoorbeeld de Cyber Security Raad[2] is eerder al aangegeven dat het delen van informatie over dergelijke digitale dreigingen en incidenten met belanghebbende aanbieders urgent is. Voor zover het NCSC relevante informatie hierover heeft, kan het deze informatie nu niet altijd met deze partijen delen, waardoor mogelijke veiligheidsrisico's in stand blijven. Door het NCSC nu al, in relatie tot voornoemde dreigingen, in ruimere zin dan wettelijk mogelijk dreigings- en incidentinformatie te laten verstrekken, kunnen andere aanbieders maatregelen treffen om de continuïteit van hun dienstverlening te waarborgen en daarmee nadelige maatschappelijke gevolgen in sterkere mate te voorkomen of verhelpen. Dit pleit voor het anticiperen op het wetsvoorstel.

Daar staat tegenover dat ieder overheidshandelen moet plaatsvinden met inachtneming van de daarvoor geldende wetgeving. Voor het in het kader daarvan verwerken van met name persoonsgegevens moet een wettelijke grondslag aanwezig zijn. In het geval van het NCSC is die laatstbedoelde grondslag, als het gaat om het verstrekken van dreigings- en incidentinformatie aan andere aanbieders of hun schakelorganisaties, nu niet altijd aanwezig. Met het oog daarop is dan ook juist bovengenoemd wetsvoorstel, dat wel in die grondslag voorziet, opgesteld en inmiddels bij uw Kamer ingediend. Anticiperen op het wetsvoorstel betekent het zonder wettelijke grondslag verstrekken van persoonsgegevens en andere vertrouwelijke gegevens (IP-adressen, emailadressen, namen van aanbieders, etc.) aan andere aanbieders of hun schakelorganisaties, in de periode dat het wetsvoorstel in behandeling is bij uw Kamer en de Eerste Kamer. De Autoriteit Persoonsgegevens is bevoegd om de naleving van de Algemene verordening gegevensbescherming te handhaven. Bovendien is uiteraard nog niet duidelijk of de Tweede en Eerste Kamer met het wetsvoorstel zullen instemmen. Dit pleit tegen het anticiperen op het wetsvoorstel.

Alles afwegende ben ik voornemens om in zeer uitzonderlijke gevallen te anticiperen op bovenbedoeld wetsvoorstel. Dit betekent dat het NCSC mogelijk in die gevallen in ruimere zin dan nu wettelijk mogelijk dreigings- en incidentinformatie, met inbegrip van onder meer persoonsgegevens, aan andere aanbieders of hun schakelorganisaties kan verstrekken. Van belang is daarbij dus wel dat ruimere verstrekking enkel en alleen plaatsvindt in gevallen van zwaarwegende redenen van maatschappelijke aard, waarin het noodzakelijk is om dreigings- en incidentinformatie te verstrekken om nadelige maatschappelijke ontwrichting te voorkomen of te beperken. Om dat vast te stellen zal onder mijn verantwoordelijkheid aan de hand van een vast afwegingskader worden beoordeeld of in relatie

[2] https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/02/22/csr-adviesbrief-inzake-het-versneld-delen-van-incidentinformatie.

tot specifieke dreigings- of incidentinformatie sprake is van een uitzonderlijk geval. Bij de beoordeling aan de hand van genoemd afwegingskader zal onder meer worden gekeken naar de aard en ernst van een dreiging, de kans op manifestatie daarvan, de (mogelijke) impact voor andere aanbieders, en of er andere mogelijkheden zijn dan het verstrekken van informatie door het NCSC om andere aanbieders op adequate wijze over een dreiging in te lichten. Ik voeg hierbij voor uw Kamer het volledige afwegingskader bij[3].

Indien er naar mijn oordeel sprake is van een uitzonderlijk geval, zal ik uw Kamer daarover zo spoedig mogelijk vertrouwelijk informeren nadat in een dergelijk geval overeenkomstig het wetsvoorstel dreigings- of incidentinformatie is verstrekt zodat andere aanbieders zo snel mogelijk in staat worden gesteld om maatregelen te treffen.

Indien gewenst ga ik hier graag met uw Kamer over in gesprek, bijvoorbeeld tijdens het aankomende debat op hoofdlijnen over digitale zaken.

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

[3] Raadpleegbaar via www.tweedekamer.nl.