Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2173

Vragen van het lid **Yesilgöz-Zegerius** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Justitie deelt kritieke informatie over hacks niet met bedrijven»* (ingezonden 8 maart 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 29 maart 2021).

Vraag 1
Bent u bekend met het bericht «Justitie deelt kritieke informatie over hacks niet met bedrijven»?[1]

Antwoord 1
Ja.

Vraag 2
Bent u bekend met de betreffende brief van de Cyber Security Raad? Zo ja, hoe beoordeelt u de zorgwekkende analyse van de Cyber Security Raad? Kunt u dit toelichten?

Antwoord 2
Ja, ik ben bekend met de adviesbrief van de Cyber Security Raad (CSR) inzake het versneld delen van incidentinformatie. Het Nationaal Cyber Security Centrum (NCSC) kan in het kader van analyses ten behoeve van de primaire taakuitoefening (informeren en adviseren van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid) ook gegevens over dreigingen en incidenten met betrekking tot de netwerk- en informatiesystemen van andere aanbieders verkrijgen. De CSR stelt terecht dat het voor het NCSC nog niet mogelijk is om deze gegevens telkens te doen toekomen aan die andere aanbieders. Zij zijn hierdoor niet altijd op de hoogte van deze dreigingen of incidenten. Ik deel de zorgen van de CSR hierover en ben van mening dat het zo veel als mogelijk delen van informatie over dreigingen en incidenten van groot belang is voor de Nederlandse digitale veiligheid en weerbaarheid. Ik werk daarom aan een wetsvoorstel om ervoor te zorgen dat

[1] Het Financieele Dagblad, 24 februari 2021, «Justitie deelt kritieke informatie over hacks niet met bedrijven», https://fd.nl/economie-politiek/1375016/justitie-geeft-kritieke-informatie-over-cyberhacks-niet-door-aan-kwetsbare-bedrijven-kxb1caBDYOtP.

ah-tk-20202021-2173
ISSN 0921 - 7398
's-Gravenhage 2021

meer van de hiervoor genoemde gegevens bij die andere aanbieders terecht kunnen komen.

Vraag 3
Klopt het dat nog veel dreigingsinformatie blijft hangen bij het National Cyber Security Centrum (NCSC) omdat de wettelijke basis voor het delen van deze informatie met betrokkenen nog niet op orde is? Zo ja, in hoeveel gevallen zijn bedrijven slachtoffer geworden van cyberaanvallen, terwijl het NCSC wel over relevante cruciale informatie beschikte en deze vervolgens niet kon delen?

Antwoord 3
In de Wet beveiliging netwerk- en informatiesystemen (Wbni) zijn de taken en bevoegdheden van het NCSC opgenomen. Op dit moment bestaat er nog niet in alle gevallen een wettelijke grondslag voor het NCSC om dreigings- en incidentinformatie over netwerk- en informatiesystemen van andere aanbieders dan die in de doelgroep van Rijk en vitaal, die is verkregen in het kader van de primaire taakuitoefening, aan of ten behoeve van deze aanbieders te verstrekken. Zoals ook aangeven in het antwoord op vraag 2, vind ik dit niet wenselijk en kom ik daarom met een wetsvoorstel om ervoor te zorgen dat deze aanbieders meer van de hiervoor genoemde informatie kunnen verkrijgen. Dit voorstel houdt in dat het NCSC ook aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren (OKTT's) vertrouwelijke herleidbare informatie over aanbieders kan verstrekken, zodat deze schakelorganisaties de niet-vitale aanbieders in hun doelgroep van relevante dreigings- en incidentinformatie kunnen voorzien (wijziging van artikel 20, tweede lid, van de Wbni). De verstrekking van deze gegevens is momenteel al mogelijk aan onder meer computercrisis-teams.
Daarnaast houdt dit voorstel in dat het NCSC in bijzondere gevallen informatie kan verstrekken aan individuele organisaties die geen deel uitmaken van de doelgroep Rijk en vitaal (wijziging artikel 3, tweede lid, van de Wbni).
Het NCSC ontvangt dagelijks veel data uit verschillende (internationale) bronnen en analyseert deze in het kader van de uitoefening van de wettelijke taak ten behoeve van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid. Ik beschik niet over concrete cijfers over aantallen slachtoffers van cyberaanvallen buiten deze doelgroep.

Vraag 4
Wordt er bij het NCSC actief gezocht naar alternatieven om toch cruciale dreigingsinformatie te kunnen delen met betrokkenen? Zo ja, op welke alternatieven wordt ingezet en op welke schaal? Zo nee, waarom niet en wat is de huidige status van het landelijk dekkend stelsel? Welke niet-vitale sectoren kunnen nog steeds geen dreigingsinformatie ontvangen?

Antwoord 4
Het NCSC beziet voortdurend op welke manier zij het beste informatie en adviezen over digitale dreigingen en incidenten kan delen met de primaire doelgroep (vitale aanbieders, organisaties die deel uitmaken van de rijksoverheid) en andere organisaties in Nederland. Zo wordt er met inachtneming van de wettelijke kaders actief gewaarschuwd middels beveiligingsadviezen, nieuwsberichten op de website en berichten aan doelgroepen en andere partners.
Ten behoeve van een zo breed mogelijke uitwisseling en verstrekking van voor aanbieders relevante dreigings- en incidentinformatie zet het kabinet sinds 2018 in op de ontwikkeling van het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden. Binnen dit LDS wordt informatie over cybersecurity breder, efficiënter en effectiever gedeeld tussen publieke en private partijen. Dit moet leiden tot een netwerk van schakelorganisaties die organisaties binnen hun onderscheidenlijke doelgroepen zo goed mogelijk kunnen adviseren en ondersteunen op het gebied van digitale veiligheid. Zoals aangegeven in de Kamerbrief van 3 februari jl.[2] wordt, gebaseerd ook

[2] Kamerstukken II 2020/21, 26 643, nr. 738.

op aanbevelingen van het WODC, nog steeds gebouwd aan dit stelsel zodat zo veel mogelijk sectoren bereikt kunnen worden.
Over de voortgang van het LDS zal uw Kamer worden geïnformeerd in de voortgangsrapportage over de Nederlandse Cybersecurity Agenda (NCSA).

Vraag 5
Heeft het Digital Trust Center (DTC) inmiddels een OKTT-status (objectief kenbaar tot taak) mogen ontvangen zodat zij niet-vitale bedrijven kunnen voorzien van dreigingsinformatie? Zo nee, wat is de status, waarom is dit nog steeds niet gebeurd en wat zorgt voor de vertraging? Bent u het met de mening eens dat er snelheid gebaat is bij het toekennen van de OKTT-status aan het DTC, gezien de enorme veiligheidsrisico's die bedrijven nu lopen?

Antwoord 5
Het Digital Trust Center (DTC) van het Ministerie van EZK is op dit moment nog niet krachtens de Wbni als OKTT aangewezen. Door het Ministerie van EZK wordt momenteel gewerkt aan het laten voldoen van het DTC aan de voorwaarden voor die aanwijzing, waaronder het versterken van de juridische basis door middel van een wetsvoorstel. Na aanwijzing zal het DTC gaan beschikken over meer dreigings- en incidentinformatie die met het niet-vitale bedrijfsleven kan worden gedeeld.

Vraag 6
Gelet op deze veiligheidsrisico's voor duizenden ondernemers, wat is er op korte termijn (wettelijk) nodig om niet-vitale bedrijven toch te kunnen voorzien van dreigingsinformatie?

Antwoord 6
De eigen digitale weerbaarheid is primair een eigen verantwoordelijkheid van bedrijven. Het DTC biedt informatie, advies en tools aan om niet vitale bedrijven in staat te stellen invulling te geven aan deze eigen verantwoordelijkheid. Voor de stappen die het DTC verder zet, verwijs ik u naar de brief van de Staatsecretaris van EZK aan uw kamer van 16 december jl.[3].
Daarnaast kunnen niet vitale bedrijven ook kennisnemen van de algemene beveiligingsadviezen van het NCSC. Ook kunnen deze bedrijven ervoor kiezen om bijvoorbeeld een computercrisisteam in het leven te roepen, of zich bij een al bestaand computercrisisteam of andere schakelorganisatie aan te sluiten, die deze bedrijven voorziet van voor hen relevante dreigings- en incidentinformatie. Deze schakelorganisaties kunnen bijvoorbeeld ook krachtens de Wbni als computercrisisteam of OKTT worden aangewezen en daardoor informatie van het NCSC ontvangen. Het NCSC en het DTC werken bovendien nauw samen en zijn voortdurend, samen met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), telkens in gesprek over de mogelijkheden om binnen het LDS zo veel als mogelijk informatie te delen.
Voorts werk ik, zoals ook aangegeven bij de antwoorden op de vragen 2 en 3, aan een wetsvoorstel om ervoor te zorgen dat de bevoegdheid van het NCSC om dreigings- en incidentinformatie over de beveiliging- en informatiesystemen van niet-vitale aanbieders aan of ten behoeve van die aanbieders te verstrekken wordt uitgebreid en wordt, zoals in het antwoord op vraag 5 gegeven, gewerkt aan het door het DTC voldoen aan de voorwaarden voor een aanwijzing krachtens de Wbni als OKTT.

Vraag 7
Hoe staat het met de samenwerking tussen het NCSC en samenwerkingsverbanden met een OKTT-status zoals de Nationale Beheersorganisatie Internetproviders? In hoeveel gevallen heeft het NCSC al dreigingsinformatie gedeeld met bedrijven die onderdeel uitmaken van het Nationale Beheersorganisatie Internetproviders?

[3] Kamerstukken II 2020/2021, 26 643, nr. 742.

Antwoord 7
Het NCSC deelt met organisaties met een OKTT-status binnen de wettelijke kaders, zoals eerder beschreven, gegevens over dreigingen en incidenten, voor zover deze gegevens betrekking hebben op en relevant zijn voor netwerk- en informatiesystemen van organisaties in hun respectievelijke doelgroepen. Daarbij kan het in elk geval ook persoonsgegevens aangaande actoren betreffen, zodat organisaties aan de hand daarvan dreigingen beter kunnen detecteren in hun netwerken. Voor zover de te delen informatie, en in het bijzonder persoonsgegevens, vertrouwelijke herleidbare gegevens met betrekking tot een aanbieder betreffen, is verstrekking hiervan aan een OKTT zoals de Nationale Beheersorganisatie Internetproviders (NBIP) momenteel niet mogelijk zonder toestemming van de betrokken aanbieders. Gelet hierop heeft de NBIP in de afgelopen periode tot nu toe in een aantal gevallen informatie over dreigingen en incidenten ontvangen.

Vraag 8 en 9
Het bovenstaande overwegende, hoe beoordeelt u het huidige vermogen van de Nederlandse overheid om actief dreigingsinformatie te delen met Nederlandse bedrijven? Bent u het met de mening eens dat Nederland achterloopt op dit vlak wanneer wij kijken naar landen om ons heen zoals het Verenigd Koninkrijk?
Bent u het ook met de mening eens dat dit onacceptabel is gezien de serieuze veiligheidsrisico's voor onze hoogontwikkelde kenniseconomie? Zo ja, bent u bereid om in gesprek te gaan met uw collega's uit het Verenigd Koninkrijk? Zo ja, kunt u de Kamer op de hoogte houden van deze gesprekken?

Antwoord 8 en 9
Voor het goed functioneren van het Nederlandse cybersecuritystelsel is – zoals ik ook heb aangegeven in voornoemde Kamerbrief van 3 februari jl. – een optimale uitwisseling van informatie over digitale dreigingen, kwetsbaarheden en incidenten tussen de overheid, vitale organisaties en niet-vitale organisaties van groot belang. De in voorgaande antwoorden genoemde wetswijziging zal hieraan bijdragen. Daarbij kijk ik ook steeds naar de wijze waarop andere landen, zoals het VK, hun cybersecuritystelsels hebben ingericht, met als doel lessen daarvan te leren, en te kijken hoe die zouden passen in de Nederlandse bestuurlijke context. In het WODC-rapport over het Landelijk Dekkend Stelsel, dat ik in november 2020 aan uw Kamer heb aangeboden, is bijvoorbeeld een landenstudie opgenomen, waarin is gekeken hoe andere landen informatiedeling hebben vormgegeven, waaronder het Verenigd Koninkrijk.[4] Veel landen hebben ook, net als Nederland, documenten als hun nationale cyberstrategie openbaar beschikbaar gemaakt. Naast bilaterale contacten ben ik permanent met Europese lidstaten in gesprek over versterking van de digitale weerbaarheid o.a. in het kader van de besprekingen over de voorgenomen herziening van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen en de Europese cybersecurity strategie. Indien daar aanleiding toe is, zal ik uw Kamer informeren over de bevindingen naar aanleiding van deze contacten.

Vraag 10
Bent u bereid om op de korte termijn, gezien de actuele en reële dreiging van cyberaanvallen, maatregelen te nemen die het delen van dreigingsinformatie tussen overheid en niet-vitale bedrijven mogelijk maakt? Zo nee, waarom niet? Zo ja, kunt u de Kamer zo spoedig mogelijk informeren over de te nemen stappen en het bijbehorende tijdspad? Zo nee, waarom niet?

Antwoord 10
Ik werk, zoals hierboven is vermeld, aan een wetsvoorstel tot wijziging van de Wbni, om ervoor te zorgen dat meer dreigings- en incidentinformatie met betrekking tot de netwerk- en informatiesystemen van andere aanbieders dan die in de doelgroep van Rijk en vitaal bij deze aanbieders terecht kan komen. Ik streef ernaar om dit voorstel rond de zomer in consultatie te brengen.

[4] Kamerstukken II 2019/20, 26 643, nr. 717.