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

955

Vragen van de leden **Yesilgöz-Zegerius** en **Aartsen** (beiden VVD) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat over *het bericht «Providers gaan bedrijven waarschuwen voor beveiligingslekken»* (ingezonden 9 oktober 2020).

Antwoord van Minister Grapperhaus (Justitie en Veiligheid) en van Staatssecretaris Keijzer (Economische Zaken en Klimaat), mede namens de Minister van Economische Zaken en Klimaat (ontvangen 30 november 2020).

Vraag 1
Bent u bekend met bovenstaand bericht?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat de Nationale Beheersorganisatie Internetproviders (NBIP) binnenkort meldingen van het Nationaal Cyber Security Centrum (NCSC) kan gaan ontvangen over dreigingsrisico's omdat het NBIP als samenwerkingsverband is aangemerkt als objectief kenbaar tot taak (OKTT)? Zo ja, bent u bereid om de Kamer halfjaarlijks op de hoogte te houden van de uitbreidingen van het landelijk dekkend stelsel? Zo nee, waarom niet?

Antwoord 2
Het klopt dat de Nationale Beheersorganisatie Internetproviders (NBIP) eerder krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) is aangewezen als organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen dan die van vitale aanbieders of de rijksoverheid (OKTT). Dit maakt het voor het Nationaal Cyber Security Centrum (NCSC) mogelijk om de NBIP, met inachtneming van de wettelijke kaders, informatie over dreigingen en incidenten met betrekking tot systemen van de doelgroep van de NBIP te verstrekken, die het NCSC heeft verkregen bij analyses in het kader van de primaire taakvervulling (bijstand aan vitaal en Rijk, etc.). Zie het antwoord op vraag 7 voor een

[1] https://fd.nl/ondernemen/1358912/providers-gaan-bedrijven-waarschuwen-voor-beveiligingslekken

ah-tk-20202021-955
ISSN 0921 - 7398
's-Gravenhage 2020

nadere toelichting op de verstrekking van deze informatie. Meer in het algemeen publiceert het NCSC op haar website publiekelijke informatie over bekende kwetsbaarheden, beveiligingsadviezen en andere adviezen waarmee organisaties hun weerbaarheid kunnen vergroten. De inzet op de uitbreiding van het Landelijk Dekkend Stelsel (LDS) vindt plaats binnen de kaders van de Nederlandse Cyber Security Agenda (NCSA).[2] Over de voortgang van de NCSA, inclusief initiatieven die plaatsvinden in het kader van het LDS, wordt jaarlijks aan uw Kamer gerapporteerd. De volgende rapportage zal zijn voor de zomer 2021. Ik realiseer mij dat er nog veel werk moet worden verricht om te komen tot een daadwerkelijk LDS. Vandaar dat ik het WODC heb gevraagd onderzoek te doen naar de stand van zaken en de verbeterpunten van dit stelsel. Uw Kamer is hierover geïnformeerd op 17 november jl.

Vraag 3
Vanaf wanneer wordt voorzien dat de NBIP meldingen van het NCSC kan gaan ontvangen over dreigingsinformatie?

Antwoord 3
Zoals in het antwoord op vraag 2 aangegeven, kan het NCSC reeds aan de NBIP, een krachtens de Wbni als OKTT aangewezen organisatie, dreigings- en incidentinformatie, verstrekken met betrekking tot netwerk- en informatiesystemen van hun doelgroep. In verband met eerder gesignaleerde belemmeringen wordt thans onderzocht welke mogelijkheden tot informatiedeling binnen de bestaande wettelijke kaders nog verder ontwikkeld zouden kunnen worden.

Vraag 4
Deelt u de mening dat ondernemers die niet zijn aangesloten bij brancheorganisaties met een OKTT-status of een sectoraal expertisecentrum voor cybersecurity (CERT) adequate hulp moeten kunnen krijgen van het Digital Trust Center (DTC)? Zo ja, kunt u toelichten waarom het NBIP als OKTT wel binnenkort meldingen kan ontvangen van het NCSC terwijl het Digital Trust Center, waarvan meer dan een miljoen ondernemers in hun informatievoorziening afhankelijk zijn, dat nog steeds niet kan? Zo nee, waarom niet?

Antwoord 4
De digitale weerbaarheid is primair een eigen verantwoordelijkheid, ook 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. Daarnaast kan eenieder en dus ook niet-vitale bedrijven, zoals in antwoord 2 aangegeven, via de website, kennisnemen van algemene beveiligingsadviezen van het NCSC. Het NCSC en het DTC werken bovendien vanuit hun onderscheidenlijke taken nauw samen waar het gaat om afstemming in externe overheidscommunicatie. Ook wisselen het NCSC en het DTC als kenniscentra zo veel als wettelijk mogelijk informatie en kennis(producten) uit.
Zoals aangegeven in de beantwoording op vraag 2, is het voor het NCSC mogelijk om, met inachtneming van de wettelijke kaders, informatie over dreigingen en incidenten met betrekking tot systemen van de doelgroep van de OKTT aan een organisatie te verstrekken. Dit indien deze organisatie is aangewezen als organisatie die objectief kenbaar tot taak (OKTT) heeft andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen dan die van vitale aanbieders of de rijksoverheid. Hierbij gaat het om informatie die het NCSC heeft verkregen bij analyses in het kader van de primaire taakvervulling en die betrekking heeft op andere netwerk- en informatiesystemen dan die van vitale aanbieders of de rijksoverheid.
Het NCSC en het DTC werken nauw samen en zijn ook voortdurend, samen met de NCTV, in gesprek over de mogelijkheden om binnen het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden informatie te delen. Waar mogelijk, verbinden zij hier, voor de betrokken organisaties, handelingsperspectief aan. Alleen dan wordt de digitale weerbaarheid van Nederland immers daadwerkelijk verhoogd. Onderdeel van de samenwerking

[2] Kamerstuk 26 643, nr. 536.

tussen het NCSC en het DTC is ook het binnen de wettelijke kaders optimaliseren van de onderlinge informatie-uitwisseling. In het kader daarvan wordt ook een aanwijzing krachtens de Wbni van het DTC als OKTT bezien. Momenteel wordt door het Ministerie van EZK gewerkt aan het laten voldoen van het DTC aan, voor overheidsorganisaties vanwege de AVG meer strenge, voorwaarden waardoor het krachtens de Wbni aangewezen zou kunnen worden als organisatie waaraan het NCSC concrete dreigingsinformatie kan delen die betrekking heeft op het niet-vitale bedrijfsleven. Het DTC zou dan de bedrijven over de dreigingsinformatie kunnen informeren. Het Ministerie van EZK is bezig met de voorbereidende werkzaamheden hiervoor. Het streven is dat deze nieuwe dienstverlening begin volgend jaar kan starten.

Vraag 5 en 6
Deelt u de mening dat het voor de digitale veiligheid van Nederland van essentieel belang is dat zowel vitale als niet-vitale organisaties worden geïnformeerd over dreigingsinformatie? Zo ja, wat is de laatste stand van zaken omtrent het DTC te voorzien van een OKTT-status? Zijn er wettelijke barrières die voorkomen dat het DTC van deze status kan worden voorzien? Zijn er de afgelopen tijd gesprekken gevoerd om te werken aan een OKTT-status voor het DTC? Zo ja, wat waren de uitkomsten van deze gesprekken? Zo nee, waarom niet? Kunt u de Kamer informeren over de voortgang van deze gesprekken?

Antwoord 5 en 6
Ik deel de mening dat het de digitale veiligheid van Nederland vergroot als zowel vitale als niet-vitale organisaties worden geïnformeerd over relevante dreigingen, incidenten en kwetsbaarheden. Om die reden zijn algemene beveiligingsadviezen van het NCSC via de website openbaar beschikbaar en werkt het kabinet aan de totstandkoming van een landelijk dekkend stelsel (LDS) waarin, met inachtneming van de wettelijke kaders, relevante informatie breder, efficiënter en effectiever gedeeld kan worden. Binnen dat LDS spelen het NCSC en het DTC een belangrijke rol.
Zoals in het antwoord op vraag 4 is aangegeven, wordt door het Ministerie van EZK gewerkt aan het laten voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni aangewezen zou kunnen worden als organisatie waaraan, onder de bij de beantwoording van vraag 4 benoemde voorwaarden, het NCSC concrete dreigingsinformatie kan delen die betrekking heeft op het niet-vitale bedrijfsleven.

Vraag 7
Gelet op het feit dat vitale bedrijven, zoals KPN en VodafoneZiggo die ook onderdeel uitmaken van het NBIP, al informatie krijgen van het NCSC, kunt u aangeven welk type niet-vitale bedrijven voortaan dreigingsinformatie krijgen via het NBIP? Welke meldingen zal het NCSC wel of niet gaan doorsturen naar het NBIP? Wordt hierin, ondanks dat het NBIP een OKTT-status heeft ook nog onderscheid gemaakt tussen informatie voor vitale en niet-vitale bedrijven gezien het aantal niet-vitale bedrijven dat onderdeel is van het NBIP?

Antwoord 7
Het NCSC kan, binnen de wettelijke mogelijkheden, gegevens over dreigingen en incidenten delen met de NBIP, voor zover deze gegevens betrekking hebben op en relevant zijn voor netwerk- en informatiesystemen van organisaties uit de doelgroep van NBIP. Daarbij kan het in elk geval persoonsgegevens aangaande kwaadwillende actoren betreffen, zodat organisaties door tussenkomst van de NBIP aan de hand daarvan bijvoorbeeld dreigingen kunnen detecteren in hun netwerken. Voor zover de te delen informatie (tevens) vertrouwelijke herleidbare gegevens met betrekking tot een aanbieder betreffen, is verstrekking hiervan aan een OKTT zoals de NBIP, vanwege de toepasselijkheid van de Wbni[3], niet mogelijk. In de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting»[4] is als een van de verschillende maatregelen opgenomen dat wordt geïnventariseerd

[3] Artikel 20, lid 2
[4] Kamerstuk 26 643, nr. 673

welke wettelijke bevoegdheden de overheid heeft bij digitale crisissituaties, zodat kan worden bezien waar eventuele aanvullingen nodig zijn. Het type niet-vitale bedrijven dat dreigingsinformatie kan ontvangen via de NBIP zijn de bedrijven die behoren tot de achterban van de NBIP.
Als organisaties in de doelgroep van de NBIP eveneens vitale aanbieders zijn, zullen zij informatie die relevant is voor de netwerk- en informatiesystemen die de vitale dienstverlening betreffen, direct van het NCSC ontvangen. Het kan dus zijn dat een vitale aanbieder ook (algemene) informatie via organisaties zoals de NBIP ontvangt als deze informatie relevant is voor vitaal en niet-vitaal.

Vraag 8
Overwegende dat het NBIP een informatiestatus heeft dat aansluit op het uitganspunt van het realiseren van een landelijk dekkend stelsel en dat ook recent het Cyber Weerbaarheidscentrum Brainport Eindhoven informatie mag ontvangen van het NCSC[5], kan worden toegelicht welke sectoren er nu wel zijn afgedekt via OKTT's en andere sectorale cybersecurity expertisecentra en welke nog niet? Kunt u een overzicht geven van het huidige landelijk dekkend stelsel? Zo nee, waarom niet?

Antwoord 8
Het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden heeft tot doel om ervoor te zorgen dat, met inachtneming van de wettelijke kaders, informatie over cybersecurity zo breed, effectief en efficiënt mogelijk wordt gedeeld. De totstandkoming van een landelijk dekkend stelsel en het aansluiten van steeds meer sectoren is een verantwoordelijkheid van de verschillende vakdepartementen. Daarnaast zijn het NCSC en de NCTV in contact met sectoren om hen te stimuleren zich te organiseren.
De organisaties binnen het landelijk dekkend stelsel, bijvoorbeeld het NCSC en het DTC, hebben diverse samenwerkingsverbanden, zoals onder andere Information Sharing and Analysis Centers (ISAC's), computercrisisteams en andere sectorale- en brancheorganisaties, waar ze in het kader van de vervulling van hun onderscheidenlijke taken mee samen werken. Bij het DTC zijn inmiddels al 30 samenwerkingsverbanden van bedrijven uit niet-vitale sectoren aangesloten en dit aantal zal verder toenemen. Dit landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden is jong, divers, dynamisch en voortdurend in ontwikkeling. Een overzicht hiervan, zoals gevraagd, is daardoor al snel ofwel incompleet en achterhaald, ofwel groot en complex. Mede daarom heb ik via het WODC onderzoek laten doen naar de stand van zaken en de verbeterpunten voor dit stelsel. Dit onderzoek schetst ook een overzicht van het huidige stelselUw Kamer is hierover op 17 november jl. geinformeerd.

Vraag 9
Bent u bereid om zich de komende maanden, gezien de reële en actuele dreiging van cybercriminaliteit, in te zetten voor het versneld uitbreiden van het landelijk dekkend stelsel? Zo ja, kunt u de Kamer zo spoedig mogelijk informeren over de te nemen stappen en het bijbehorende tijdspad? Zo nee, waarom niet?

Antwoord 9
De digitale dreiging die uitgaat van criminelen, maar ook van statelijke actoren heeft volgens het Cybersecuritybeeld Nederland 2020 een permanent karakter.[6] Deze dreiging wordt het hoofd geboden langs de prioriteiten zoals uiteengezet in de NCSA en recente Kamerbrieven waarin de versterkte aanpak cybersecurity wordt beschreven,[7] de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting»[8] en de beleidsreactie op het CSBN 2020, die tevens de voortgangsrapportage over de NCSA bevat.[9] Bij de beleidsreactie op het WODC-rapport over Cybersecurity informatie-

[5] https://www.ed.nl/eindhoven/cyberaanval-op-vdl-bedrijf-afgeweerd-brainport-strijdt-tegen-computercriminaliteit~a673a56a/?referrer=https%3A%2F%2Fwww.google.com%2F
[6] Bijlage bij Kamerstuk 26 643, nr. 695.
[7] Kamerstuk 26 643, nr. 614 / Kamerstuk 26 643, nr. 647.
[8] Kamerstuk 26 643 en 308 21, nr. 673.
[9] Kamerstuk 26 643, nr. 695, inclusief bijlage.

uitwisseling zoals genoemd onder vraag 8 zal ik u nader informeren over recente ontwikkelingen binnen het landelijk dekkend stelsel.

Vraag 10
Bent u bereid deze vragen te beantwoorden voorafgaande aan de behandeling van de begroting van Justitie en Veiligheid?

Antwoord 10
Ja.