Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

773

Vragen van de leden **Amhaouch** en **Palland** (beiden CDA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over *de berichten «Bedrijfsleven start eigen alarmsysteem tegen hackers: «overheid te traag» & «Informatie over op handen zijnde hacks wordt grotendeels weggeooid»»* (ingezonden 6 oktober 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister van Economische Zaken en Klimaat (ontvangen 18 november 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 460.

Vraag 1
Bent u bekend met de berichten «Bedrijfsleven start eigen alarmsysteem tegen hackers: «overheid te traag» & «Informatie over op handen zijnde hacks wordt grotendeels weggeooid»»?[1, 2]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u de ontwikkelingen vanuit het bedrijfsleven waar men «niet meer wil wachten op de overheid» en zelf aan de slag gaat om een alarmsysteem dat waarschuwt voor aanstaande of bezig zijnde hacks?

Antwoord 2
Het is een positieve ontwikkeling dat private initiatieven op het gebied van cybersecurity, zoals het «alarmsysteem», zich ontwikkelen. Het initiatief past binnen de ambitie die het kabinet heeft om te komen tot een Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden zoals omschreven staat in de Nederlandse Cybersecurity Agenda (NCSA).[3] Om in Nederland op nationaal niveau voldoende slagkracht te kunnen organiseren tegen de toenemende digitale dreiging is publiek-private samenwerking noodzakelijk. De overheid stimuleert de totstandkoming van samenwerkingsverbanden zodat tussen hen informatie over digitale dreigingen en inciden-

[1] Het Financieele Dagblad, 28 september 2021, «Bedrijfsleven start eigen alarmsysteem tegen hackers: «overheid te traag»»
[2] De Volkskrant, 29 september 2021, «Informatie over op handen zijnde hacks wordt grotendeels weggeooid»
[3] Kamerstuk 26 643 nr. 625

ah-tk-20212022-773
ISSN 0921 - 7398
's-Gravenhage 2021

ten, die relevant is voor de verschillende doelgroepen, efficiënter en effectiever wordt gedeeld. Alle organisaties blijven zelf primair verantwoordelijk voor hun digitale veiligheid en het is van belang dat zij die verantwoordelijkheid ook nemen ongeacht of zij wel of niet een vitale aanbieder zijn of deel uitmaken van (rijks)overheid.

Vraag 3
Begrijpt u dat beide berichten waarover vragen worden gesteld een zekere samenhang lijken te hebben?

Antwoord 3
Ja.

Vraag 4
Kunt u aangeven of het Digital Trust Center (DTC) duurzaam is geborgd voor de toekomst? Heeft het Digital Trust Center haar waarde al bewezen? Zo nee, waarom (nog) niet?

Antwoord 4
Ja, het DTC is duurzaam geborgd. Het DTC is najaar 2019 geëvalueerd door onderzoeksbureau Kwink. De evaluatie is 18 februari 2020 aan de Tweede Kamer aangeboden.[4] Deze evaluatie gaf een positief beeld van de resultaten en het doelbereik van DTC. Op basis van deze evaluatie is besloten het DTC een vast onderdeel te laten worden van het Ministerie van EZK en hiervoor structureel budget beschikbaar te stellen. Per brief van 16 december 2020 bent u over de voortgang van de implementatie van de aanbevelingen geïnformeerd.[5] De aanbevelingen van het onderzoeksbureau zijn overgenomen. Dit heeft onder meer geleid tot uitbreiding van de diensten van het DTC, zoals het daadwerkelijk notificeren van individuele bedrijven indien de overheid informatie heeft over concrete kwetsbaarheden. Deze zomer is hiermee gestart, waarbij waar aangewezen zo veel mogelijk wordt samengewerkt met het Nationaal Cyber Security Centrum (NCSC).
Tevens heeft de Minister van Economische Zaken en Klimaat een wetsvoorstel in voorbereiding, dat de juridische basis van het DTC nader regelt. Hiermee ontstaan er nog meer mogelijkheden voor het DTC om informatie over digitale dreigingen en incidenten aan het Nederlandse niet-vitale bedrijfsleven te doen toekomen, ook als dit persoonsgegevens zoals IP-adressen bevat.

Vraag 5
Deelt u de signalen vanuit de praktijk dat het Nationaal Cyber Security Centrum (NCSC) de urgentie en het tempo volledig onderschat en daarmee in bepaalde gevallen niet van meerwaarde lijkt te zijn? Hoe gaat u dat verbeteren?

Antwoord 5
Het tempo in het digitale domein ligt hoog: digitale ontwikkelingen en dreigingen volgen elkaar in rap tempo op. De ernst en urgentie van de toename van digitale aanvallen wordt dan ook onderschreven in het Cyber Security Beeld Nederland (CSBN).[6] Wij delen daarom niet het perspectief dat het NCSC de urgentie en het tempo onderschat. Het is echter een constante uitdaging om deze digitale aanvallen het hoofd te bieden. Daar is de inzet vanuit onze ministeries ook volop op gericht.

Vraag 6
Op welke vlakken zorgt de Algemene verordening gegevensbescherming (AVG) voor knelpunten? Welke grondslagen zijn er nodig, bijvoorbeeld in de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI), om gegevens als IP-adressen te kunnen delen?

---

[4] Kamerstuk 26 643 nr. 668
[5] Kamerstuk 26 643 nr. 742
[6] Kamerstuk 26 643 nr. 767

Antwoord 6
De Wet beveiliging netwerk- en informatiesystemen (Wbni) regelt de taken en bevoegdheden die het NCSC namens de Minister van Justitie en Veiligheid op het terrein van cybersecurity uitvoert. Primair heeft het NCSC tot taak om vitale aanbieders en aanbieders die onderdeel zijn van de rijksoverheid te informeren en adviseren over digitale dreigingen en incidenten, en daartoe analyses en technisch onderzoek te verrichten. Het NCSC kan bij die analyses en dat technisch onderzoek ook informatie over digitale dreigingen of incidenten verkrijgen die andere aanbieders aangaat. Het NCSC kan die informatie, waaronder ook persoonsgegevens met inachtneming van de AVG, verstrekken aan krachtens de Wbni aangewezen schakelorganisaties, die andere aanbieders in hun doelgroep hebben. Gebleken is echter dat verstrekking van die informatie aan deze schakelorganisaties vanwege een leemte in de Wbni niet altijd mogelijk is en dat relevante dreigings- en incidentinformatie daardoor niet altijd voor die andere aanbieders beschikbaar komt. Om die reden is er deze zomer een voorstel tot wijziging van de Wbni in consultatie gebracht, dat ertoe strekt het NCSC de bevoegdheid te bieden om in ruimere zin dreigings- of incidentinformatie met of ten behoeve van andere aanbieders te delen. Daartoe regelt dit wetsvoorstel dat schakelorganisaties, die krachtens de Wbni zijn aangewezen als OKTT (organisatie die objectief kenbaar tot taak heeft om organisaties of het publiek te informeren over dreigingen en incidenten), in ruimere zin dreigings- en incidentinformatie, waaronder ook persoonsgegevens, verstrekt kunnen krijgen, zodat zij op basis daarvan andere aanbieders in hun doelgroep beter kunnen informeren en adviseren. Daarnaast regelt het wetsvoorstel dat in bepaalde gevallen het NCSC individuele andere aanbieders voor hen relevante dreigingsinformatie, met inbegrip van persoonsgegevens, kan verstrekken. Hiervan is sprake als er geen schakelorganisatie (zoals een OKTT of computercrisisteam) is die de aanbieder van de informatie kan voorzien én de informatie gaat over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de aanbieder. Naast dit wetsvoorstel is er, zoals hierboven aangegeven, een wetsvoorstel in voorbereiding dat de juridische basis van het DTC nader regelt.

Vraag 7
Welke stappen worden er gezet om het NCSC meer mogelijkheden te geven wanneer het gaat om niet-vitale onderdelen in de samenleving? Wordt er ook gekeken om de WBNI een ruimer bereik te geven?

Antwoord 7
Zoals in het antwoord op vraag 6 is vermeld is een wetsvoorstel tot wijziging van de Wbni opgesteld en in consultatie gebracht, dat ertoe strekt het NCSC de bevoegdheid te bieden om in ruimere zin dreigings- en incidentinformatie aan of ten behoeve van aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, te verstrekken.
Daarnaast is het Digital Trust Center (DTC) in juni gestart met het proactief informeren van individuele niet-vitale bedrijven over digitale dreigingen, zoals toegelicht in de brief aan uw Kamer over dit onderwerp op 2 juni jl.[7] Het DTC doet dit in eerste instantie nog op beperkte schaal in geval van ernstige dreigingen bij het niet-vitale bedrijfsleven.
In november 2021 start het DTC met het notificeren van bedrijven die deel uitmaken van een pilot. Deze pilot maakt het mogelijk voor DTC concrete dreigingsinformatie waar de overheid over beschikt te matchen met bedrijven die hun technische gegevens hebben doorgegeven aan het DTC. Er zijn 62 bedrijven uit negen sectoren geselecteerd, van groot tot klein, die deel kunnen gaan uitmaken van deze pilot. De pilot zal duidelijk maken of en hoe deze nieuwe dienst van het DTC verder kan worden opgeschaald en ook kan worden geautomatiseerd.
Het demissionaire kabinet zet daarnaast stappen om het cybersecuritystelsel door te ontwikkelen en te versterken, op korte termijn onder meer door middel van het genoemde wetsvoorstel tot wijziging van de Wbni. Op de lange termijn adviseren wij een volgend kabinet om een nieuwe integrale cyberstrategie te formuleren en het cybersecuritystelsel door te ontwikkelen,

[7] Kamerstuk 26 643 nr. 760

daarbij rekening houdend met de aankomende herziening van de netwerk- en informatiebeveiliging richtlijn (NIB-richtlijn). Onze digitale weerbaarheid zal immers de nodige aandacht en investeringen blijven vragen.

Vraag 8
Acht u het een meerwaarde dat er ook een private partij komt waar tevens meldingen van hacks en/of kwetsbaarheden kunnen worden gedaan?

Antwoord 8
Zie het antwoord op vraag 2.

Vraag 9
Kunt u aangeven waar er bij het NCSC behoefte aan is en in hoeverre u kunt zorgen dat het NCSC deze bevoegdheden, middelen en/of grondslagen ook krijgt? Welke obstakels liggen er in de weg?

Antwoord 9
In onder meer bovengenoemd CSBN valt te lezen dat de digitale dreiging alleen maar toeneemt, net als onze afhankelijkheid van digitale systemen. Om ervoor te zorgen dat de bij de overheid, meer in het bijzonder het NCSC, voorhanden zijnde informatie inzake digitale dreigingen en incidenten zo veel als mogelijk ter beschikking komt van organisaties waarvoor die informatie relevant is, is er zoals hierboven vermeld een wetsvoorstel tot wijziging van de Wbni in procedure gebracht. Daarnaast is het van belang dat met het oog op een zo optimaal mogelijk functionerend cybersecuritystelsel voortdurend door alle partijen in dat stelsel, waaronder het NCSC, nagedacht wordt over nodige doorontwikkelingen van dat stelsel. De Cyber Security Raad (CSR) schat in dat voor de benodigde verdere ontwikkeling van het gehele stelsel een totaal aan investeringen nodig is van ca. 833 miljoen euro, bestaande uit investeringen in de overheid, waaronder ook het NCSC en het DTC, en investeringen door private organisaties via bijvoorbeeld een fonds voor vitale aanbieders. Het is aan een volgend kabinet om invulling te geven aan de inzet van de rijksoverheid in dit verband.

Vraag 10
Bent u bekend met signalen dat er vanwege veel te stringente wettelijke beperkingen het NCSC genoodzaakt is om buiten de wet om te werken? Acht u dat acceptabel?

Antwoord 10
Wij zijn bekend met deze signalen en deze situatie is onwenselijk. Informatie over digitale dreigingen en incidenten kan vanuit het NCSC vanwege een leemte in de wet momenteel niet altijd worden verstrekt aan of ten behoeve van aanbieders, die geen vitale aanbieder zijn of deel uitmaken van de rijksoverheid. Daarom is, zoals hierboven ook vermeld, een wetsvoorstel tot wijziging van de Wbni opgesteld en in consultatie gebracht dat ertoe strekt dat het NCSC in ruimere zin de bevoegdheid heeft om genoemde informatie aan die andere aanbieders of hun schakelorganisaties te verstrekken. Daarnaast wordt voortdurend gewerkt aan de doorontwikkeling van het LDS. Daarvan deel uitmakende schakelorganisaties kunnen ook krachtens de Wbni als bijvoorbeeld OKTT worden aangewezen, en zo in bredere zin dreigings- en incidentinformatie verstrekt krijgen vanuit het NCSC ten behoeve van hun doelgroepen.

Vraag 11
Kunt u aangeven waarom het NCSC niet de mogelijkheden heeft om het internet te scannen om te kijken welke partijen er gevaar lopen voor bepaalde software of kwetsbaarheden? Welke mogelijkheden ziet u om ervoor te zorgen dat dit wel gaat gebeuren?

Antwoord 11
Het NCSC voert zoals vermeld technisch onderzoek uit ten behoeve van het informeren en adviseren van organisaties die deel uitmaken van de rijksoverheid en vitale aanbieders over voor hen relevante dreigingen en incidenten. In het kader van deze taakuitoefening scant het NCSC ook op kwetsbaarheden voor zover dit mogelijk is zonder daarbij de netwerk- en informatiesystemen

van organisaties binnen te dringen. Voor zover scannen naar kwetsbaarheden het zonder toestemming binnendringen van een netwerk- of informatiesystemen inhoudt, beschikt het NCSC niet over de daartoe benodigde wettelijke bevoegdheid.

Vraag 12
Kunt u een overzicht geven van alle initiatieven die er thans lopen om de cyberveiligheid bij (mkb-)bedrijven te vergroten? Wat is het bereik hiervan?

Antwoord 12
Eind 2020 heeft het DTC in samenwerking met leden van het CIO Platform Nederland de «Cybersecurity Wegwijzer» gelanceerd. Er zijn voor bedrijven veel cybersecurityinitiatieven in Nederland die zich ten doel stellen om een hoog niveau van cyberweerbaarheid in de keten, branche of regio te bereiken. De «Cybersecurity Wegwijzer» maakt het landschap aan dergelijke cybersecurity initiatieven in Nederland inzichtelijk.[8] Deze wegwijzer is met name relevant voor intermediaire organisaties. Tot nu zijn er 2.000 unieke bezoekers geweest. Daarnaast is er sprake van een sterke toename van het aantal bezoeken van de website van het DTC, naar verwachting zullen er dit eind van het jaar meer dan 200.000 bezoeken zijn. De website biedt bezoekers relevante informatie en tools om hun eigen weerbaarheid te verhogen. Ook het aantal op het DTC aangesloten samenwerkingsverbanden op het gebied van cybersecurity neemt sterk toe. Op dit moment zijn er 37 samenwerkingsverbanden van niet-vitale bedrijven, regionaal en/of sectoraal, aangesloten bij het DTC, en het aantal neemt verder toe. Hiermee wordt het mogelijk nog meer bedrijven, vaak mkb, vanuit het DTC bij te staan om de cyberweerbaarheid te vergroten van de deelnemers van deze samenwerkingsverbanden. Ook zorgt de interactie in dit nieuwe netwerk ervoor dat de leercurve van ieder samenwerkingsverband sneller doorlopen wordt. Naast de hiervoor genoemde initiatieven wordt door het DTC waar aangewezen zo veel als mogelijk samengewerkt met het NCSC, alsook met de Kamers van Koophandel, VNO-NCW/MKB-Nederland en een aantal gemeenten om zo nog meer bedrijven cyberbewust en -bekwaam te maken. De Minister van Economische Zaken en Klimaat zal uw Kamer begin 2022 een overzicht geven van de door het DTC bereikte resultaten en de concrete plannen voor 2022 en verder.
Een concreet voorbeeld van de initiatieven die lopen om de cyberveiligheid bij (mkb-)bedrijven te vergroten is de Citydeal «Lokale weerbaarheid Cybercrime», die op 28 oktober 2020 is ondertekend. In de City Deal «Lokale weerbaarheid Cybercrime» gaan gemeenten, ministeries (JenV, BZK en EZK/DTC), veiligheidsorganisaties en kennisinstellingen samen aan de slag om de cyberweerbaarheid te verhogen van burgers en bedrijven. De City Deal ondersteunt regionale samenwerkingsverbanden Veiligheid, gemeenten en Platforms Veilig Ondernemen en activeert hen om burgers en mkb-ondernemers bewust te maken van hun kwetsbaarheid en hun weerbaarheid tegen cybercrime te vergroten.
Een van de pijlers binnen de Citydeal is het versterken van de cyberweerbaarheid in het mkb. Het afgelopen jaar zijn binnen deze pijler projecten uitgevoerd gericht op het versterken van de cyberweerbaarheid van agrariërs, het inzetten van studenten om bedrijven te helpen, digitale ambassadeurs en een website met handelingskader. In de tweede fase van de Citydeal ligt de focus op het landelijk verspreiden van de resultaten uit de eerste fase en op nieuwe innovatieve projecten.
Daarnaast subsidieert JenV het project Samen Digitaal Veilig van MKB-Nederland. Met dit project wil MKB-Nederland, via een groot aantal branche- en ondernemersverenigingen, ondernemers helpen digitaal veiliger te worden.
De basis is een brancheaanpak, waarin met de branches wordt ingezet op een vorm van zelfregulering met een groeicurve. Door dat centraal te organiseren, worden bedrijven efficiënt en laagdrempelig stap voor stap veiliger.

Vraag 13
Bent u bereid om een evaluatie te laten uitvoeren over het functioneren van de instanties als het NCSC en het DTC in relatie tot relevante stakeholders.

[8] www.digitaltrustcenter.nl/Wegwijzer-cybersecurity-initiatieven

Antwoord 13
Tijdens ISIDOOR2021, Nederlands grootste nationale cyber-crisisoefening, werd er geoefend met het Nationaal Crisisplan Digitaal. Het COT Instituut voor Veiligheids- en Crisismanagement heeft het evaluatierapport van ISIDOOR2021 afgerond en deze is met uw Kamer gedeeld.[9] Het is belangrijk om lering te trekken uit deze lessen, ook met betrekking tot het NCSC, het DTC en daarmee in relatie staande andere partijen in het LDS.
Naast de evaluatie van ISIDOOR2021 is een evaluatie van de werking van het gehele LDS, waaronder deelname daaraan door het NCSC en het DTC, naar mijn mening ook waardevol. Het stelsel is echter sterk aan verandering onderhevig waardoor het eerst zinvol is om een evaluatie in gang te zetten als onder meer informatiedeling tussen het NCSC en het DTC verder op gang is gekomen en bovengenoemde pilot voor het vanuit het DTC notificeren van bedrijven gestart is en de resultaten van de eerdere pilot van het DTC hiervan opgetekend kunnen worden. Ook is het van belang om te kunnen bepalen of en in welke zin de herziening van de NIB-richtlijn, over het ontwerp waarvan de EU-onderhandelingen nog gaande zijn, en in vervolg daarop de implementatie daarvan gevolgen zal hebben voor de informatie-uitwisseling tussen organisaties die deel uitmaken van het LDS.

[9] Kamerstuk 26 643 nr. 781