# 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**

## 3057

Vragen van het lid **Kathmann** (PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat (een gedeelte) van de Belgische overheid plat lag door een DDoS aanval* (ingezonden 7 mei 2021).

Antwoord van Staatssecretaris **Knops** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens van Minister van Justitie en Veiligheid) (ontvangen 3 juni 2021).

Vraag 1
Kent u het artikel «Belgische overheden getroffen door grote cyberaanval»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe vaak is de Nederlandse overheid doelwit geweest van een cyberaanval, zoals een DDoS aanval?

Antwoord 2
Er is geen volledig beeld van het aantal aanvallen waarvan de Nederlandse overheid doelwit is geweest. In algemene zin is bekend dat Nederlandse instellingen, waaronder overheden, te kampen hebben met digitale aanvallen. Het jaarlijks gepubliceerde Cybersecuritybeeld Nederland (CSBN) geeft inzicht in de digitale dreiging in Nederland, waaronder tegen de overheid, en de belangen die daardoor kunnen worden aangetast.[2]
De meest gestructureerde statistieken die beschikbaar zijn over DDoS-aanvallen zijn afkomstig van de Nationale Beheersorganisatie voor Internet Providers (NBIP). NBIP rapporteert jaarlijks over de DDoS-aanvallen die gemeten zijn door de Nationale DDoS Wasstraat (NaWas).[3] Ik verwijs u voor meer informatie hierover door naar de beantwoording van eerdere Kamervragen over DDoS gericht aan de Staatssecretaris van EZK.[4]

---

[1] https://www.rtlnieuws.nl/tech/artikel/5228981/netwerk-belgische-overheid-getroffen-door-grote-ddos-aanval
[2] https://www.nctv.nl/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020
[3] NBIP-Rapport-DDoS-data-2020.pdf
[4] Kamerstuk 42 266, nr. 551


ah-tk-20202021-3057
ISSN 0921 - 7398
's-Gravenhage 2021

Vraag 3
Is Nederland voldoende weerbaar tegen cyberaanvallen, waaronder DDoS-aanvallen? Zo ja, waaruit blijkt dat? Zo nee, hoe verbeteren we de Nederlandse weerbaarheid tegen cyberaanvallen?

Antwoord 3
Het CSBN 2020 laat zien dat de weerbaarheid tegen digitale dreigingen nog niet overal op orde is.[5] Cyberincidenten hebben de potentie om grote schade aan te richten en in uiterste gevallen maatschappelijke ontwrichting te veroorzaken.
De afgelopen jaren is daarom ingezet op het versterken van cybersecurity. De kabinetsbrede aanpak van cybersecurity is vastgelegd in de Nationale Cybersecurity Agenda (NCSA).[6] De uitvoering daarvan wordt ondersteund met investeringen door het kabinet die oplopen tot 95 miljoen euro structureel. Om in te kunnen spelen op technologische en maatschappelijke ontwikkelingen, en actuele dreigingen en risico's zijn de maatregelen uit de NCSA in de loop van de tijd verder uitgewerkt en versterkt. Dit is sinds de verschijning van de NCSA meerdere keren gebeurd.[7, 8, 9, 10] De zeven ambities uit de NCSA blijven hierbij het uitgangspunt en over de voortgang op deze ambities wordt jaarlijks gerapporteerd aan uw Kamer. De NCSA is opgesteld onder leiding van en uitgevoerd onder coördinatie van het Ministerie van Justitie en Veiligheid en met de vakdepartementen vanuit hun eigen specifieke beleidsverantwoordelijkheden. De Minister van Justitie en Veiligheid is de coördinerend bewindspersoon op het gebied van cybersecurity.
Over het niveau van de digitale weerbaarheid in Nederland en de maatregelen die in dat kader zijn genomen, verwijs ik graag naar het CSBN 2021 en de begeleidende beleidsbrief die de Minister van Justitie en Veiligheid op korte termijn aan uw Kamer zal aanbieden.
Specifiek voor de overheid geldt de Baseline Informatiebeveiliging Overheid (BIO) sinds eind 2018 als basisnormenkader voor informatiebeveiliging waaraan alle overheden zich moeten houden.[11] Door implementatie van de BIO hebben overheidsorganisaties de basisbeveiliging op orde. Dit levert een bijdrage aan de weerbaarheid tegen cyberaanvallen, bijvoorbeeld door het verplicht minimaal jaarlijks testen op feitelijke veiligheid. Een voorbeeld hiervan is het uitvoeren van penetratietesten. Een penetratietest is een beveiligingscontrole die gericht is op een deel van het systeem. Bij een penetratietest wordt gekeken of het mogelijk is om kwetsbaarheden en risico's ook daadwerkelijk te gebruiken om de beveiliging op deze systemen te omzeilen, in te breken of te doorbreken.

Vraag 4
Is de Nederlandse overheid proactief op zoek naar kwetsbaarheden in de beveiliging? Zo nee, waarom niet?

Antwoord 4
Alle overheden hanteren de overheidsbrede BIO als basis voor de inrichting van hun digitale veiligheid. De baseline is erop gericht om de weerbaarheid van overheidsorganisaties ten aanzien van cyberdreigingen en incidenten te vergroten. Het proactief monitoren op kwetsbaarheden en waar nodig verhelpen van deze kwetsbaarheden is een van de relevante maatregelen daarbij. Zoals ik op 18 maart jl. aan uw Kamer heb gemeld in mijn voortgangsbrief over informatieveiligheid bij de overheid[12], testen steeds meer overheden hun feitelijke veiligheid op verschillende manieren. Het overheidsbrede ondersteuningsprogramma BIO van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), dat overheden sinds 2019 helpt met de

---

[5] https://www.nctv.nl/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020
[6] https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda
[7] Kamerstuk 26 643, nr. 673.
[8] Kamerstuk 26 643, nr. 614.
[9] Kamerstuk 26 643, nr. 695
[10] Kamerstuk 26 643, nr. 738
[11] *Stcrt.* 2019, nr. 26526.
[12] Kamerstuk 26 643, nr. 749

implementatie van de BIO, besteedt ook aandacht aan het belang van testen. Eveneens vinden er bij de overheid ook verschillende cyberoefeningen plaats, die kwetsbaarheden in de beveiliging kunnen aantonen. De Nederlandse overheid is dus inderdaad proactief op zoek naar kwetsbaarheden in de beveiliging.
Specifiek voor het Rijk is geïnventariseerd bij de departementen op welke wijze het geautomatiseerd zoeken naar kwetsbaarheden gestalte krijgt. Uit deze inventarisatie blijkt dat dit breed wordt toegepast. In het kader van kennisdeling heeft het Ministerie van BZK in samenwerking met een groep experts binnen de rijksoverheid en de departementen een handreiking opgesteld en vastgesteld voor het inrichten van een doorlopende kwetsbaarhedenscan bij rijksoverheidsorganisaties. Daarnaast worden er door departementen diverse middelen ingezet om proactief naar kwetsbaarheden te zoeken, waaronder penetratietesten en red teaming oefeningen, en voert de Auditdienst Rijk in opdracht van de departementen en het Ministerie van BZK onderzoeken uit naar de feitelijke veiligheid van systemen en netwerken. Een belangrijk uitgangspunt is dat iedere private en publieke organisatie primair zelf verantwoordelijk is voor zijn eigen digitale beveiliging.
De computercrisisteams (CSIRTS)[13] van de overheden spelen een belangrijke rol om overheidsorganisaties te ondersteunen bij het voorkomen en verhelpen van digitale incidenten. Wel geldt voor organisaties die deel uitmaken van de rijksoverheid (en vitale aanbieders) dat het Nationaal Cybersecurity Centrum (NCSC) krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) tot taak heeft om hen bijstand te verlenen om hun digitale weerbaarheid te waarborgen en te versterken. Daarnaast deelt het NCSC in algemene zin informatie over kwetsbaarheden en daarbij behorende beveiligingsadviezen op zijn website.

Vraag 5
Is er een noodprotocol om de overheid te laten functioneren als de overheid te maken krijgt met een cyberaanval? Zo nee, vindt u het zinvol om een noodprotocol te ontwikkelen? Wilt u uw antwoord motiveren?

Antwoord 5
Alle overheden kennen herstel- en continuïteitsplannen voor wanneer er sprake is van digitale verstoring. Ook worden er diverse maatregelen getroffen om de continuïteit van de digitale overheid te kunnen waarborgen. Zo verplicht de BIO dat overheidsorganisaties hun informatiebeveiligingscontinuïteit plannen, implementeren, verifiëren, beoordelen en evalueren.[14] Voor bedrijfskritische onderdelen in de bedrijfsvoering geldt de eis van herstel binnen een week. Op die manier voorzien overheden in de continuïteit van processen en systemen van de digitale overheid.
Voor situaties waarvan sprake is van maatschappelijke ontwrichting kan in het uiterste geval de nationale crisisstructuur in werking treden. Deze is door het kabinet vastgelegd in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbesluitvorming. Het Nationaal Crisisplan Digitaal (NCP-Digitaal) is een specifieke uitwerking voor de aanpak van een crisis veroorzaakt in het digitale domein.[15]
Ten slotte wordt er ook geoefend bij de overheid. Omdat de ketenafhankelijkheid een gegeven is op de digitale snelweg, wordt er jaarlijks sinds 2019 geoefend met gesimuleerde hackaanvallen op processen en systemen van de overheid. Deze jaarlijkse Overheidsbrede Cyberoefening[16] wordt georganiseerd door het Ministerie van BZK. Met alle overheden wordt het oefenscenario zo realistisch mogelijk uitgewerkt waarbij een digitale verstoring merkbaar zichtbaar is bij meerdere overheidslagen. Juist door ketens heen, interbe-

---

[13] Het Nationaal Cybersecurity Centrum (NCSC) is het CSIRT voor het Rijk en vitale organisaties. Provincies verkennen, met subsidie beschikbaar gesteld door het Ministerie van BZK, momenteel de inrichting van een CSIRT-functie voor het provinciaal domein. De waterschappen hebben sinds april 2017 samen met Rijkswaterstaat een CERT Watermanagement en de gemeenten hebben sinds 2013 een eigen CERT, de Informatiebeveiligingsdienst (IBD)

[14] Zie hoofdstuk 17.1 van de BIO: *Stcrt*. 2019, nr. 26526.

[15] https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie

[16] Informatie over de Overheidsbrede Cyberoefening is te vinden op https://www.weerbaredigitaleoverheid.nl/

stuurlijk en met een brede doelgroep (van IT-professional tot aan de bestuurder van een overheidsorganisatie).

Vraag 6
Heeft u contact gehad met uw Belgische ambtgenoot over de DDoS-aanval? Zo ja, wat is er besproken en wat heeft het gesprek opgeleverd?

Antwoord 6
Internationaal wordt op continue basis met partners op operationeel niveau zoveel als mogelijk informatie over dreigingen en incidenten uitgewisseld. Het NCSC heeft op dinsdag 4 mei en donderdag 6 mei jl. contact opgenomen met het Belgische Collectief Computer Security Incident Response Team (CSIRT), CERT-BE, voor het opvragen van technische details van de DDoS-aanval.
In EU-verband en bilateraal werkt Nederland overigens ook goed samen met België aan de versterking van cyberweerbaarheid. De Nederlandse ambassade in België heeft op dinsdag 4 mei jl. contact gehad met de Belgische federale overheid over de DDoS-aanval en de maatschappelijke impact hiervan. De ontvangen informatie is direct gedeeld met het Ministerie van Buitenlandse Zaken en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Vraag 7
Welke lessen zijn er te leren aan de hand van de cyberaanvallen in België?

Antwoord 7
Digitale incidenten zijn niet gebonden aan landsgrenzen. Incidenten of dreiging daarvan in andere landen kunnen ook op organisaties in Nederland effect hebben. Internationale samenwerking is daarom van groot belang. Door snelle informatie-uitwisseling wordt bijvoorbeeld het NCSC in de gelegenheid gesteld organisaties binnen de doelgroep tijdig te waarschuwen en te informeren.
In Nederland wordt snelle informatie-uitwisseling over DDoS-aanvallen ook bevorderd door de Anti-DDoS-Coalitie.[17] Dit is een samenwerkingsverband van publieke, private en wetenschappelijke partijen waarbinnen informatie en kennis over DDoS-aanvallen gedeeld kan worden om de weerbaarheid tegen aanvallen te verhogen.
In algemene zin tonen de cyberaanvallen in België wederom het belang van het op orde hebben van de digitale weerbaarheid aan.

[17] www.antiddoscoalitie.nl