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

551

Vragen van het lid **Weverling** (VVD) aan de Staatssecretaris van Economische Zaken en Klimaat over *DDoS-aanvallen op internetproviders* (ingezonden 4 september 2020).

Antwoord van Staatssecretaris **Keijzer** (Economische Zaken en Klimaat), mede namens de Minister van Justitie en Veiligheid (ontvangen 26 oktober 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 67.

Vraag 1
Bent u bekend met het bericht «Netwerk Caiway opnieuw getroffen door DDoS-aanval»?[1]

Antwoord 1
Ja

Vraag 2
Kunt u aangeven, door middel van een overzicht, hoeveel DDoS-aanvallen op internetproviders of andere bedrijven in de vitale digitale infrastructuur er over de afgelopen jaren hebben plaatsgevonden? Hoeveel DD0S-aanvallen hebben er op het brede midden- en klienbedrijg (mkb) plaatsgevonden over de afgelopen jaren?

Antwoord 2
De meest gestructureerde statistieken die beschikbaar zijn over DDoS-aanvallen zijn afkomstig van de Nationale Beheersorganisatie voor Internet Providers (NBIP). NBIP rapport jaarlijks over de DDoS-aanvallen die gemeten zijn door hun Nationale DDoS Wasstraat (NaWas).[2] De NaWas is een privaat non-profit initiatief om DDoS-aanvallen te mitigeren. De NaWas heeft 90 deelnemers en beschermt 2,5 miljoen.nl domeinen, ongeveer 42,5% procent van het Nederlandse internet. In 2019 zijn 919 aanvallen geregistreerd door de NaWas, gemiddeld twee tot 3 per dag. Dit is een lichte daling ten opzichte van het aantal aanvallen in 2018, terwijl het aantal deelnemers groeide in dezelfde periode. De intensiteit van DDoS-aanvallen neemt al jaren gestaag toe. Daarin is geen uitsplitsing te maken naar sectoren.

[1] AD, 1 september 2020
[2] https://www.nbip.nl/wp-content/uploads/2020/05/NBIP-Rapport-DDoS-data-2019.pdf

ah-tk-20202021-551
ISSN 0921 - 7398
's-Gravenhage 2020

Vraag 3
Welke impact hebben dergelijke DDoS-aanvallen op internetgebruikers en het bedrijfsleven? Is een inschatting te maken van de economische schade als gevolg van de verstoring van het internet die DDoS-aanvallen veroorzaken?

Antwoord 3
DDoS-aanvallen zijn dagelijks aan de orde in het digitale domein. Om de impact te beperken nemen organisaties mitigerende maatregelen. Dat kan in eigen beheer, via commerciële partijen en men kan zich aansluiten bij de NaWas. Voor internetproviders geldt dat zij een zorgplicht hebben om maatregelen te nemen ten behoeve van de continuïteit van hun dienstverlening op basis van de Telecommunicatiewet. Aanbieders van essentiële diensten hebben een plicht om passende technische en organisatorische beveiligingsmaatregelen te nemen op basis van de Wet bescherming netwerk- en informatiesystemen (Wbni). Succesvol gemitigeerde aanvallen hebben niet of nauwelijks impact op de continuïteit van de dienstverlening van een bedrijf of voor internetgebruikers. Een inschatting van de economische schade als gevolg van een verstoring van het internet als gevolg van een DDoS-aanval is niet te maken omdat het afhangt van een groot aantal factoren zoals de omvang van de verstoring, de duur van de verstoring en welke diensten worden getroffen.

Vraag 4
Welke rol speelt het Digital Trust Center (DTC) in het voorkomen van DDOS-aanvallen en het beperken van de gevolgen van DDOS aanvallen voor het brede mkb? In hoeverre helpt het NCSC het brede mkb hierbij? Welke mogelijkheden bestaan er om het brede mkb hier bij te helpen?

Antwoord 4
DDoS-aanvallen zijn niet te voorkomen, het is wel mogelijk om de kwetsbaarheid voor en de impact van DDoS-aanvallen te verkleinen. Het DTC en het NCSC maken deel uit van het zogenaamde Landelijk Dekkend Stelsel van schakelorganisaties op het gebied van cybersecurity. Binnen dit stelsel kan, met inachtneming van de hiervoor geldende wettelijke kaders, informatie over bijvoorbeeld digitale kwetsbaarheden en DDoS-aanvallen worden gedeeld tussen publieke en private partijen, met als doel de slagkracht van de partijen te vergroten.
Het DTC informeert niet-vitale bedrijven via haar website over wat te doen voor, tijdens en na een DDoS-aanval, zoals het maken van afspraken met hun ICT-leveranciers.[3] Ook informeert het DTC bedrijven welke beschermingsmaatregelen zij kunnen nemen om minder kwetsbaar te zijn voor misbruik van digitale systemen.
Het NCSC heeft primair tot taak de rijksoverheid en vitale bedrijven te informeren en adviseren over voor hen relevante digitale dreigingen en incidenten. Daarnaast verstrekt het NCSC ook, binnen de daarvoor geldende wettelijke kaders, aan andere organisaties voor die organisaties of hun doelgroepen relevante dreigingsinformatie, die in het kader van de primaire taakuitoefening beschikbaar is gekomen. Verder draagt het NCSC bijvoorbeeld ook met haar kennis en expertise bij aan de publiek-private anti-DDoS coalitie en faciliteert het de Information Sharing and Analysis Centers (ISACs). Binnen de ISACs wisselen aanbieders onderling kennis en informatie uit over onder andere DDoS-aanvallen. Naar aanleiding van de recente toename van het aantal en de intensiteit van DDoS-aanvallen, heeft het NCSC gewaarschuwd om extra waakzaam te zijn. Op haar beurt heeft het DTC de aangesloten samenwerkingsverbanden van bedrijven hierover geïnformeerd.

Vraag 5
Hoe duidt u het feit dat, volgens cijfers van onder andere de nationale anti-DDoS-coalitie, de complexiteit en intensiteit van DDoS-aanvallen toeneemt? Welke consequenties voor de manier waarop er wordt samengewerkt om DDoS-aanvallen af te slaan dient deze observatie volgens u te hebben?

[3] https://www.digitaltrustcenter.nl/informatie-advies/ddos-aanval

Antwoord 5
Op basis van de gegevens van NBIP neemt de intensiteit van DDoS-aanvallen al een aantal jaren toe. In het Cyber Security Beeld Nederland 2020 kwam naar voren dat een toename van de complexiteit van DDoS-aanvallen volgens experts is uitgebleven. Met een toename van de intensiteit van DDoS-aanvallen neemt de noodzaak om samen te werken door kennis en technische mogelijkheden bij elkaar te brengen ook toe. De publiek-private anti-DDoS coalitie is hier een goed voorbeeld van. De anti-DDoS coalitie bestaat uit ongeveer vijfentwintig deelnemers vanuit overheidsorganisaties zoals het NCSC en Agentschap Telecom, internetproviders, internet exchanges, non-profit organisaties en universiteiten. De anti-DDoS coalitie is in 2018 gestart om Nederlandse organisaties beter te beschermen tegen DDoS-aanvallen door middel van kennisdeling, gezamenlijke oefeningen, het promoten van maatregelen tegen aanvallen en het ontwikkelen van technische oplossingen. Elk van deze onderdelen wordt ingevuld door een werkgroep van de coalitie waarin deelnemers kunnen plaatsnemen. De coalitie stelt zich ook tot doel om in brede zin organisaties te informeren over de ontwikkelingen en resultaten via hun website.[4]

Vraag 6
Kunt u aangeven of de wijze waarop er op dit moment tussen providers kennis gedeeld wordt over het afslaan van DDoS-aanvallen naar behoren functioneert?

Antwoord 6
Het delen van kennis en informatie tussen bedrijven vindt onder meer plaats in de ISACs en in de anti-DDoS coalitie. Mijn beeld is dat deze vormen van kennisdeling en samenwerking concreet bijdragen aan de aanpak van DDoS-aanvallen in Nederland. Een voorbeeld is dat in de anti-DDoS coalitie een zogenoemde *clearing house* wordt ontwikkeld waarbij in een technisch systeem de karakteristieken van een DDoS-aanval worden uitgewisseld tussen *clearing house* deelnemers. Dit project draagt ook bij aan de ontwikkelingen van *clearing houses* in Europa via het EU-project CONCORDIA. Tijdens de recente toename aan DDoS-aanvallen is ook informatie uitgewisseld tussen deelnemers in de coalitie om de kenmerken van de aanvallen scherper te kunnen duiden.

Vraag 7
Op welke wijze zijn overheidsinstellingen, zoals het NCSC, betrokken bij het tegengaan van DDoS-aanvallen? Welke instrumenten heeft het NCSC om DDoS-aanvallen te voorkomen en de gevolgen te verkleinen? Welke verbeterpunten signaleert u hierbij?

Antwoord 7
Zoals aangegeven bij de beantwoording van de voorgaande vragen verrichten verschillende overheidsinstellingen activiteiten ten behoeve van het bevorderen van de weerbaarheid met betrekking tot het tegengaan van DDoS-aanvallen via kennis, informatie en samenwerking. Het NCSC heeft krachtens de Wbni bijvoorbeeld NBIP aangewezen als organisatie waaraan in het kader van bovenvermelde taakuitoefening dreigingsinformatie kan worden verstrekt. Ook de Politie zet in het kader van haar taakuitoefening in op preventie, verstoring, opsporing en vervolging van daders en het uit de lucht halen van botnets die voor onder meer DDoS-aanvallen worden ingezet. Daarnaast wordt door Logius en CIO-Rijk afgestemd met internetproviders hoe directe koppelingen (peering) voor overheidsorganisaties behulpzaam kunnen zijn om de impact van DDoS-aanvallen te minimaliseren.

Vraag 8
Deelt u de mening dat samenwerkingsverbanden gericht op het tegengaan van DDoS-aanvallen een belangrijke rol hebben in het versterken van onze digitale weerbaarheid? Op welke wijze neemt u deel aan dergelijke samenwerkingsverbanden?

[4] https://www.nomoreddos.org/

Antwoord 8
Ik deel de mening dat samenwerking cruciaal is om de digitale weerbaarheid in Nederland te versterken. Het bundelen van kennis en krachten is een hoeksteen van de Nederlandse cybersecurity aanpak in de Nederlandse Cyber Security Agenda. De anti-DDoS coalitie is een goed voorbeeld van samenwerking op een specifiek gebied waarbij kennis vanuit publiek, privaat en wetenschap bij elkaar komt om de weerbaarheid in Nederland te verhogen tegen DDoS-aanvallen.

Vraag 9
Deelt u de mening dat het wenselijk is als, naast internetproviders met een landelijk netwerk, ook regionale providers, zoals Caiway of Delta, toetreden tot (publiek-private) samenwerkingsverbanden gericht op het afslaan van DDoS-aanvallen? Zo ja, bent u bereid deze providers hiertoe aan te sporen?

Antwoord 9
Op basis van de Telecommunicatiewet hebben aanbieders van openbare elektronische communicatienetwerken of -diensten de plicht om passende technische of organisatorische maatregelen te nemen om de continuïteit van hun dienstverlening te waarborgen. Ik vind het van belang dat internetaanbieders een oplossing kiezen die het beste aansluit bij hun bedrijfsvoering om de continuïteit te waarborgen. Zoals aangegeven in het antwoord op vraag 3 kunnen mitigerende maatregelen voor DDoS-aanvallen op verschillende manieren worden geïmplementeerd, namelijk in eigen beheer, via een commerciële partij of door zich aan te sluiten bij de NaWas.

Vraag 10
Wordt er, bijvoorbeeld in het kader van de stresstest digitale ontwrichting, geoefend op scenario's van (grootschalige) verstoring van het internetverkeer als gevolg van DDoS-aanvallen? Op welke wijze komen de lessen die uit deze oefeningen getrokken worden terecht bij de providers?

Antwoord 10
Binnen de anti-DDoS coalitie worden publiek-private oefeningen georganiseerd waar in een gecontroleerde omgeving een aantal partijen een DDoS-aanval inzet en aantal partijen de DDoS-aanval mitigeert. De lessen uit deze oefeningen worden gedeeld met de verschillende partners zodat zij verbetering door kunnen voeren in hun netwerken. De anti-DDoS coalitie wil deze lessen in de toekomst via hun site delen zodat meer partijen de opgedane lessen kunnen benutten. Deze oefeningen sluiten aan op de inzet van het kabinet voor een structureel oefen- en testprogramma conform de motie Weverling. [5]

Vraag 11
Worden «normale» internetgebruikers op dit moment voldoende voorgelicht over de noodzaak beschermingsmaatregelen te nemen om daarmee te voorkomen dat hun apparaten misbruikt worden voor het uitvoeren van een DDoS-aanval?

Antwoord 11
Voor vergroten van de bewustwording van burgers op het gebied van digitale veiligheidsmaatregelen is informatie en handelingsperspectief beschikbaar op veiliginternetten.nl en er vinden campagnes plaats, zoals «Doe je updates». Door apparaten te updaten beschermen eindgebruikers niet alleen zichzelf. Ze zorgen er ook voor dat apparaten minder kwetsbaar zijn om onderdeel te worden van een botnet waarmee onder meer DDoS-aanvallen worden uitgevoerd.

[5] Vergaderjaar 2019/20, Kamerstuk 24 095, nr. 496, ingediend op 6 februari 2020.