Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

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

1409

Vragen van het lid **Alkaya** (SP) aan de Minister van Financiën over *DDoS-aanvallen op banken* (ingezonden 2 februari 2018).

Antwoord van Minister **Hoekstra** (Financiën) en Staatssecretaris **Snel** (Financiën) (ontvangen 8 maart 2018).

Vraag 1
Is er economische schade opgetreden als gevolg van het onbereikbaar zijn van internetbankieren door de DDoS-aanvallen op banken? Zo ja, hoe groot is de totale schade?[1]

Antwoord 1
Als gevolg van de DDoS-aanvallen (*distributed denial-of-service*) had een aantal Nederlandse banken gedurende enkele dagen last van tijdelijke verstoringen in of beschikbaarheid van hun dienstverlening (internetbankieren, mobiele bankapps en iDEAL-betalingen). Door de aanvallen raakten de webservers van enkele banken tijdelijk overbelast waardoor hun websites trager werden, of moeilijk of niet bereikbaar waren, wat met name tot ongemak voor klanten heeft geleid. In hoeverre er economische schade is opgetreden als gevolg van onbeschikbare internetdiensten, laat zich lastig bepalen. Het gegeven dat klanten die op het moment van de DDoS-aanvallen een betaling via internet- of mobielbankieren mogelijk niet konden uitvoeren, is daarbij op zichzelf niet voldoende. Zij konden hun betaling namelijk later alsnog doen. In geval van een verstoring in iDEAL konden zij voor hun betaling uitwijken naar een andere betaalmethode, waaronder betalen met creditcard of Paypal. Deze mogelijkheden om op een andere manier of op een ander moment alsnog te kunnen betalen, geven mij het vertrouwen dat de economische schade beperkt is.

Vraag 2
Klopt het dat gemiddeld genomen zo'n tien à elf miljoen betalingen per dag worden verricht? Hebben de DDoS-aanvallen invloed gehad op het aantal betalingen? Zo ja, in hoeverre is het aantal betalingen beïnvloed door de DDoS-aanvallen?

[1] https://nos.nl/artikel/2214177-derde-ddos-storing-abn-amro-binnen-24-uur-ook-ing-getroffen.html

ah-tk-20172018-1409
ISSN 0921 - 7398
's-Gravenhage 2018

Antwoord 2
Gemiddeld genomen worden er dagelijks zo'n 9,5 miljoen betalingen via internet-bankieren en mobiele bankapps verricht, waaronder ongeveer 1 miljoen iDEAL-betalingen.[2] De recente DDoS-aanvallen en de daaruit voortvloeiende tijdelijke beschikbaarheidsproblemen van de getroffen banken hebben volgens de Betaalvereniging geen zichtbare invloed gehad op het aantal via deze kanalen verrichte betalingen.

Vraag 3
Welke wettelijke vereisten worden gesteld aan banken om het betalingsverkeer te beveiligen tegen DDoS-aanvallen? Bent u van mening dat banken deze wettelijke vereisten in voldoende mate naleven? Kunt u uw antwoord toelichten?

Antwoord 3
DNB heeft normen gesteld voor de veiligheid en beschikbaarheid van het betalingsverkeer in Nederland, die in de *Regeling Oversight goede werking betalingsverkeer* zijn vastgelegd. Daarin zijn onder meer beschikbaarheidsnormen opgenomen en is bepaald dat een instelling haar systemen zo heeft ingericht dat deze een hoog niveau van beschikbaarheid en veiligheid waarborgen. Op basis van deze regeling houdt DNB toezicht op het retailbetalingsverkeer, en DNB beoordeelt of banken de normen in voldoende mate naleven. Alle instelling waarop de regeling van toepassing is, hebben maatregelen genomen om zich tegen DDoS-aanvallen te beveiligen. De modus operandi van DDoS-aanvallen wijzigt echter, en het kost tijd om mitigerende maatregelen aan te passen en om de beveiliging tegen nieuwe soorten DDoS-aanvallen in te regelen. DNB heeft hier aandacht voor in het kader van het toezicht dat zij op basis van de regeling houdt. Wanneer instellingen structureel niet aan de regeling voldoen, acteert DNB hierop.

Vraag 4
Zijn de DDoS-aanvallen van de laatste week geavanceerder dan eerdere DDOS-aanvallen op banken? Kunt u uitleggen in welk opzicht deze aanvallen geavanceerder zijn?

Antwoord 4
De DDoS-aanvallen van eind januari jl. waren omvangrijker en geavanceerder dan eerdere aanvallen op banken. De modus operandi die de aanvaller(s) toepaste, was anders dan voorheen. De DDoS-aanvallen waren niet alleen gericht op de zogeheten mijnbank- en iDEAL-omgevingen van de bank in kwestie, maar ook op de netwerkproviders en alle publieke IP-adressen van de bank. De aanvaller hield daarbij rekening met wat er met het aanvalsdataverkeer werd gedaan. Op basis van de reactie van de banken koos de aanvaller een andere methode, of werd de aanval in bandbreedte verzwaard.

Vraag 5, 6, 7 en 8
Waaruit blijkt dat Nederlandse banken er om bekend staan hun cyberveiligheid goed op orde te hebben?[3]
Wat is uw reactie op de bewering dat banken laks zijn en dat ons land alles in huis heeft om onaantastbaar te blijven voor DDoS-aanvallen?[4]
Hebt u, net als techneut Erik Bais, twijfels over de strategie van ABN AMRO ten aanzien van het afslaan van deze aanvallen?
Kunt u uitleggen waardoor ABN AMRO vaker is getroffen dan andere banken?[5]

Antwoord 5, 6, 7 en 8
DDoS-aanvallen komen wereldwijd vaak voor en de modus operandi van de aanvallers wijzigt voortdurend. Daardoor hebben instellingen, waaronder banken, dagelijks met dergelijke veranderlijke aanvallen te maken en dit maakt volledige onaantastbaarheid voor DDoS-aanvallen onmogelijk. De

[2] Gebaseerd op https://statistiek.dnb.nl/downloads/index.aspx#/details/retailbetalingsverkeer-kwartaal/dataset/9aa3c704–8e00–40b2-b075-b17e2a63de30.
[3] https://www.ad.nl/economie/banken-en-belastingdienst-slaan-cyberaanvallen-af~a1ec22e5/
[4] https://www.telegraaf.nl/nieuws/1608419/opstelling-banken-over-d-do-s-schandalig
[5] https://fd.nl/economie-politiek/1239501/banken-getroffen-door-dd-os-aanvallen

meeste aanvallen worden evenwel succesvol door de afweersystemen van banken afgeslagen voordat ze leiden tot overlast door tijdelijke uitval of onbeschikbaarheid van dienstverlening. Eind januari bleek dat banken bovendien in staat zijn om ook op nieuwe geslaagde aanvallen direct te reageren en ze af te slaan, onder meer door het nemen van maatregelen rond het versterken van hun IT-afweersystemen. In het bestrijden van cybercriminaliteit werken banken onderling nauw samen[6], alsook met bedrijven gespecialiseerd in cybersecurity en met verschillende autoriteiten, waaronder DNB, de NCTV en het NCSC. De NCTV gaf daags na de aanvallen aan dat de situatie goed en professioneel door de (financiële instellingen) is opgepakt.[7] Uit cijfers die de Betaalvereniging Nederland jaarlijks publiceert, blijkt dat de beschikbaarheid van het internet- en mobielbankieren voor de meeste banken hoog is: over 2017 >99,75% voor internetbankieren en >99,73% voor mobiel bankieren.[8] Daarnaast is de fraude in het betalingsverkeer de afgelopen jaren structureel gedaald. Verschillende maatregelen op het gebied van preventie, voorlichting van consumenten en samenwerking tussen partijen, hebben aan die daling bijgedragen. Waar de totale schade als gevolg van fraude in het betalings-verkeer in 2012 nog bijna 82 miljoen euro betrof, was dit bedrag in 2016 gedaald naar iets meer dan 10 miljoen euro.[9]
Ik heb geen signalen ontvangen dat de website van ABN AMRO vaker is getroffen dan andere banken. De beschikbaarheids- en fraudecijfers, alsook de directe reactie van de banken op DDoS-aanvallen en de uitspraken van de NCTV, geven mij het vertrouwen dat de banken voortdurend werken aan hun cyberveiligheid om de beschikbaarheid van het betalingsverkeer goed op orde te houden.

Vraag 9
Zijn DDoS-aanvallen in deze orde van grootte ook op buitenlandse banken voorgekomen? Zo ja, wanneer?

Antwoord 9
Mij zijn geen signalen bekend dat de recente DDoS-aanvallen ook waren gericht op buitenlandse banken. Dat laat onverlet dat ook buitenlandse banken met dergelijke aanvallen te maken hebben. DDoS-aanvallen komen wereldwijd vaak voor.

Vraag 10
Welke lessen kunnen worden getrokken uit de recente DDoS-aanvallen op banken? Hoe ziet u er op toe dat deze lessen ook leiden tot concrete actie van zowel de overheid als van de banken?

Antwoord 10
De veranderlijkheid van de DDoS-aanvallen noopt ertoe dat banken voortdurend werken aan hun cyberveiligheid en de beschikbaarheid van het betalingsverkeer, opdat deze goed op orde blijft. Hiervoor is nauwe samenwerking van belang, tussen banken onderling maar ook van banken met bedrijven gespecialiseerd in cybersecurity en met verschillende autoriteiten. Die publiek-private samenwerking vindt al plaats. De in 2013 aangestelde bankenliaison fungeert daarbij als permanente verbindingsofficier tussen de banken en overheidsinstanties, en draagt eraan bij dat snel informatie over de cyberveiligheid tussen die partijen kan worden uitgewisseld. Ik span mij ervoor in om de kwaliteit en intensiteit van deze samenwerking op peil te houden, opdat ook op toekomstige DDoS-aanvallen adequaat kan worden gereageerd.

---

[6] Banken en het NCSC hebben in 2013 besloten hun samenwerking verder te bestendigen. Onderdeel hiervan was het aanstellen van een bankenliaison. Zie https://www.betaalvereniging.nl/veiligheid/cybersecurity/.

[7] https://www.nctv.nl/actueel/nieuws/2018/ddos-aanvallen.aspx.

[8] https://www.betaalvereniging.nl/betaalproducten-en-diensten/beschikbaarheid-internet-en-mobiel-bankieren/.

[9] https://www.betaalvereniging.nl/actueel/persberichten/fraude-betalingsverkeer-wederom-forslager/; https://www.betaalvereniging.nl/actueel/nieuws/fraude-internetbankieren-gedaald/.

Vraag 11
Bent u bezig met het creëren van een back-upmogelijkheid voor directe digitale betalingen, bijvoorbeeld decentraal, voor het geval er op grote schaal aanvallen blijven plaatsvinden?

Antwoord 11
Gelet op de zeer hoge beschikbaarheid van het Nederlandse betalingsverkeer en de beperkte invloed daarop van de recente DDoS-aanvallen vertrouw ik erop dat banken ook in de toekomst in staat zullen zijn om een goede beschikbaarheid van hun digitale betaaldienstverlening zullen waarborgen. Hierbij acht ik het inrichten van een back-upmogelijkheid voor directe digitale betalingen niet proportioneel.