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

1408

Vragen van het lid **Nijboer** (PvdA) aan de Minister en Staatssecretaris van Financiën over *de aanhoudende DDoS-aanvallen op Nederlandse banken en de Belastingdienst* (ingezonden 1 februari 2018).

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

Vraag 1, 2 en 3
Bent u bekend met de berichtgeving over de DDoS-aanvallen op ABN AMRO, ING, Rabobank en de Belastingdienst?[1]
Kunt u uiteenzetten wat er is gebeurd? Houden deze aanvallen verband met elkaar?
Zijn gegevens van klanten en/of belastingplichtigen op straat gekomen? Is er bij deze aanvallen data gelekt? Kunnen klanten en belastingplichtigen er zeker van zijn dat hun gegevens en geld veilig zijn?

Antwoord 1, 2 en 3
De berichten over de recente DDoS-aanvallen zijn bekend en hier heb ik ook eerder met uw Kamer tijdens het Algemeen Overleg Bankensector op 7 februari jl. over gesproken. Eind januari had een aantal Nederlandse banken gedurende enkele dagen last van tijdelijke verstoringen in of onbeschikbaarheid van hun dienstverlening (internetbankieren, mobiele bankapps en iDEAL-betalingen) door omvangrijke en geavanceerde DDoS-aanvallen (*distributed denial-of-service*). De websites van een aantal Nederlandse banken zijn in die dagen regelmatig vanuit verschillende locaties bestookt met grote hoeveelheden data. Klanten van ABN AMRO, ING, Rabobank, Volksbank, Triodos en Bunq hebben in verschillende mate hinder ondervonden van de DDoS-aanvallen. Door de aanvallen raakten de webservers van deze banken tijdelijk overbelast waardoor hun websites tijdelijk trager werden, of moeilijk of niet bereikbaar waren. Elke digitale aanval die tot overlast leidt is vervelend voor de consument.
De DDoS-aanvallen op de Belastingdienst waren ook gericht op het onderbreken van de dienstverlening van de Belastingdienst. Tussen maandag 29 januari 2018 en woensdag 1 februari 2018 signaleerde het *Security Operations Center* (SOC) van de Belastingdienst meerdere aanvallen op de

[1] https://www.nrc.nl/nieuws/2018/01/29/ook-rabobank-slachtoffer-van-ddos-aanval-a1590162, https://nos.nl/artikel/2214339-ook-belastingdienst-getroffen-door-ddos-aanval.html

ah-tk-20172018-1408
ISSN 0921 - 7398
's-Gravenhage 2018

infrastructuur. Tijdens een aantal aanvalsgolven is er een periode geweest van ongeveer tien minuten waarin burgers en bedrijven de websites van de Belastingdienst niet konden benaderen. Dit heeft tot gevolg gehad dat burgers en bedrijven op dat moment tijdelijk geen aangifte konden doen of toeslagen aan konden vragen. Dat is voor burgers vervelend.
DDoS-aanvallen zijn geen fraudeaanvallen en leiden niet direct tot financiële schade. Er wordt niet in de systemen en netwerken van banken en de Belasting-dienst binnengedrongen. Er is geen gevaar voor de persoonsgegevens van klanten en/of belastingplichtigen of voor de veiligheid van hun gegevens en geld, en er is geen sprake geweest van een datalek.
Phishing (een vorm van oplichting via email) is bij een aantal banken meer waargenomen direct na de DDoS-aanvallen. De verwarring die de aanvallen zelf en de nieuwsberichten hierover veroorzaakte bij klanten, is mogelijk een voedingsbodem voor meer phishing geweest. DNB heeft in dit verband op 31 januari jl. een persbericht uitgebracht waarin zij waarschuwt voor phishing-emails.[2] Ook de banken zelf waarschuwen hun klanten voor phishing-berichten, via hun eigen websites en de gezamenlijke website https://www.veiligbankieren.nl/. Hier lichten zij klanten voor over wat zij tegen phishing kunnen doen en hoe zij valse berichten kunnen herkennen.

Vraag 4
Op welke manier wordt onderzocht wat er gebeurd is, en is het mogelijk te achterhalen wie de daders zijn? Zo ja, worden deze daders vervolgd? Welke straffen kunnen tegen hen worden geëist?

Antwoord 4
Nadat de politie in september 2017 informatie over de DDoS-aanvallen op Bunq bank had ontvangen, werd onder leiding van het Landelijk Parket door het Team High Tech Crime (THTC) van de Landelijke Eenheid een onderzoek gestart. Na de recente aanvallen heeft ook de Belastingdienst de bij haar bekende gegevens overgedragen aan THTC, en heeft aangifte gedaan. Zoals blijkt uit mediaberichten wees het opsporingsonderzoek daags na de recente DDoS-aanvallen in de richting van een 18-jarige man uit Oosterhout. Deze man werd op 1 februari jl. aangehouden. Het uitvoeren van een DDoS-aanval is strafbaar en wordt gestraft met een gevangenisstraf van maximaal zes jaar indien gemeen gevaar voor goederen of verlening van diensten te duchten is. Indien er levensgevaar voor een ander te duchten is of het feit de dood ten gevolge heeft, is de maximum gevangenisstraf negen respectievelijk vijftien jaar.

Vraag 5 en 6
In hoeverre hebben banken afdoende maatregelen getroffen om DDos-aanvallen te voorkomen, aangezien zij in het verleden daar vaker slachtoffer van zijn geweest? Hoe is het mogelijk dat zij nu toch weer slachtoffer zijn van dit soort aanvallen?
Welke stappen ondernemen de banken en de Belastingdienst om toekomstige aanvallen te voorkomen en/of af te slaan? Hoe wordt erop toegezien dat deze maatregelen afdoende zijn?

Antwoord 5 en 6
Banken zijn zelf verantwoordelijk voor de beveiliging van hun systemen en moeten storingen in de beschikbaarheid bij De Nederlandsche Bank (DNB) melden. DNB zet zich in voor een betrouwbaar en veilig betalingsverkeer en is aanspreekpunt van de financiële sector voor de cyberweerbaarheid van de financiële kerninfrastructuur.[3] Zo zijn DNB en de banken in 2017 het samenwerkingsverband *Threat Intelligence Based Ethical Red Teaming*(TIBER) gestart. Met dit programma wordt beoogd de cyberweerbaarheid van financiële kerninstellingen te verhogen, onder meer door aanvallen gecontro-

[2] https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/Persberichten2018/dnb372138.jsp.
[3] De financiële kerninfrastructuur (FKI) bestaat uit de financiële instellingen en marktinfrastructuren die van essentieel belang zijn voor het Nederlandse betalings- en effectenverkeer. De FKI-instellingen zijn verantwoordelijk voor de belangrijkste transactiestromen en betaal- en effectenafwikkelsystemen en daarmee voor de vitale processen van de financiële sector.

leerd na te bootsen op basis van actuele dreigingsinformatie.[4] Daarnaast toetst DNB als toezichthouder of financiële instellingen hun beveiligingseisen op orde hebben. Verder werken banken in het bestrijden van cybercriminaliteit, waaronder DDoS-aanvallen, onderling nauw samen, alsook met gespecialiseerde cybersecurity-bedrijven en met verschillende autoriteiten. Naast DNB gaat het onder meer om de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) die primair verantwoordelijk is voor het voorkomen en beperken van maatschappelijke ontwrichting door cybercriminaliteit, en het daaronder vallende Nationaal Cyber Security Centrum (NCSC) dat het centrale informatieknooppunt en expertise-centrum voor cyberveiligheid in Nederland is.
Tijdens en na de DDoS-aanvallen is op ambtelijk niveau direct contact geweest met de NCTV. Ook heeft het Ministerie van Financiën in het kader van het tripartiete crisismanagement geschakeld met DNB, de AFM en de Nederlandse grootbanken, en met die partijen de stand van zaken rond de operationele verstoringen besproken.[5] Ik vind het van belang om zorgvuldig en waakzaam te blijven om ongemak door verstoring en digitale vormen van criminaliteit zoveel mogelijk te voorkomen en bestrijden.
DDoS-aanvallen komen wereldwijd vaak voor en de modus operandi van aanvallers wijzigt voortdurend. Daardoor hebben instellingen, waaronder banken, dagelijks te maken met – kleine en omvangrijke – DDoS-aanvallen. De meeste aanvallen worden door de afweersystemen van banken succesvol afgeslagen voordat ze leiden tot overlast door tijdelijke uitval of onbeschikbaarheid van hun dienstverlening. Evenwel kunnen banken opnieuw worden getroffen door (omvangrijke) geslaagde DDoS-aanvallen, zoals eind januari het geval was.
Banken nemen dan maatregelen om de impact te minimaliseren en de aanvallen zo snel mogelijk af te slaan. Het gaat om maatregelen rond het versterken van IT-afweersystemen, en het vergroten van de dataverwerkingscapaciteit in combinatie met het plaatsen van filters, waardoor de getroffen webservers niet langer overbelast raken. Daarnaast wisselden de banken onderling en met het Nationaal Cyber Security Centrum (NCSC), onder meer via de in 2013 aangestelde bankenliaison,[6] continu informatie uit tijdens de aanvallen. Mede hierdoor werd de toegepaste DDoS-aanvalsmethode snel onderling gedeeld, wat heeft bijgedragen aan het wegnemen van de verstoringen.
De Belastingdienst heeft middels het SOC veel kennis en middelen om aanvallen succesvol af te wenden. Het volledig voorkomen van dergelijke aanvallen is niet mogelijk. Met haar Internet Service Providers (ISP's) neemt de Belastingdienst maatregelen die de negatieve gevolgen van aanvallen moeten verminderen. Het SOC zorgt ervoor dat het kennisniveau van haar medewerkers en de benodigde apparatuur ruimschoots toereikend en op niveau zijn, en dat deze gelijke pas houden met ontwikkelingen in het domein van cyberveiligheid. Voordat nieuwe diensten of apparatuur in gebruik worden genomen, ondergaan deze een zogeheten «*Aanval en Penetratietest*» en een kwetsbaarhedenonderzoek. Daarnaast vindt er tweemaal per jaar een DDoS-oefening plaats met medewerking van een groot aantal gekwalificeerde partners om de maatregelen te testen. Uit diverse kennisnetwerken haalt het SOC informatie om haar kennisniveau, en daarmee de weerbaarheid van de ICT-systemen van de Belastingdienst, te verhogen.

Vraag 7 en 8
Het gebruikmaken van bankrekeningen is een nutsfunctie; is er voldoende voor gezorgd dat deze functie goed functioneert? Houdt De Nederlandsche Bank (DNB) daar toezicht op?
Heeft DNB de afgelopen jaren maatregelen afgedwongen om ervoor te zorgen dat de nutsfunctie van het betalingsverkeer door banken goed wordt vervuld? Zo ja welke? Zo nee, waarom niet?

---

[4] https://fd.nl/ondernemen/1226787/dnb-gaat-proberen-de-banken-te-hacken.
[5] Zie MoU sector crisismanagement: https://zoek.officielebekendmakingen.nl/blg-111937.pdf.
[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/.

Antwoord 7 en 8
Het is van belang dat de toegang tot geld op orde is en blijft. De toegang tot geld, inclusief de infrastructuur van het betalingsverkeer en het gebruik kunnen maken van een bankrekening, is nodig voor het functioneren van de Nederlandse economie en daarmee van belang voor iedereen in Nederland. DNB heeft tot taak om de goede werking van het betalingsverkeer te bevorderen. Zij heeft normen gesteld voor de veiligheid en beschikbaarheid van het betalingsverkeer in Nederland. Op basis van deze regeling houdt DNB toezicht op het retailbetalingsverkeer. Op verzoek van DNB hebben de relevante instellingen 2016 een plan van aanpak opgesteld waarin zij lieten zien hoe zij kunnen voldoen aan de veiligheids-en beschikbaarheidseisen.
De Betaalvereniging Nederland publiceert op haar website actuele beschikbaarheidscijfers van het internet- en mobielbankieren voor de meeste banken. Uit deze cijfers blijkt dat de beschikbaarheid hoog is: over 2017 >99,75% voor internetbankieren en >99,73% voor mobiel bankieren.[7]

Vraag 9 en 10
Wat gaat u doen om ervoor te zorgen dat mensen gewoon bij hun geld kunnen, hun bankzaken kunnen doen, belastingaangifte kunnen doen en dat hun gegevens veilig zijn bij banken en de Belastingdienst?
Deelt u de mening dat er na dit weekend verscherpte waakzaamheid en alertheid nodig is bij banken, DNB en de Belastingdienst? Zo nee, waarom niet?

Antwoord 9 en 10
De ICT-systemen van de Belastingdienst worden beschermd door diverse maatregelen, en er wordt op gelet dat deze optimaal blijven functioneren. De waakzaamheid bij de Belastingdienst voor de DDoS-aanvallen en andere risico's voor de cyberveiligheid was, is en blijft op het hoogste niveau. Het SOC monitort voortdurend en behoudt haar verscherpte waakzaamheid en alertheid.
Het is voor rekeninghouders vervelend als zij tijdelijk niet bij hun bankgegevens of geld kunnen. De actuele beschikbaarheidscijfers van het internet- en mobielbankieren laten gelukkig zien dat de beschikbaarheid van het betalingsverkeer hoog is. Dit, tezamen met de maatregelen die banken in samenwerking met elkaar, cybersecuritybedrijven en overheidsinstanties nemen, geeft mij het vertrouwen dat de toegang tot het betalingsverkeer voldoende op orde is. Tegelijk laten de recente DDoS-aanvallen zien dat dergelijke aanvallen blijven voorkomen en aan verandering onderhevig zijn. Dit maakt het van belang dat banken, DNB en andere betrokken waakzaam en alert zijn en zich voortdurend blijven inspannen voor een weerbaar betalings-verkeer zodat cyberaanvallen zoveel mogelijk kunnen voorkomen dan wel tijdig kunnen worden gedetecteerd, zodat de impact ervan relatief laag blijft.

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