Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

28 684 Naar een veiliger samenleving

Nr. 379

BRIEF VAN DE MINISTERS VAN FINANCIËN EN VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 april 2013

In de Regeling van Werkzaamheden van 9 april jl. zijn de ministers van Veiligheid en Justitie en Financiën door het lid van Hijum (CDA) verzocht de Kamer binnen een week te informeren over de oorzaken van de problemen bij het internetbankieren, de veiligheid hieromtrent en hoe in de toekomst dergelijke storingen te voorkomen. Met deze brief geven wij gehoor aan dit verzoek en gaan wij in op de cyberaanvallen, de ondernomen acties, de rollen en verantwoordelijkheden en de ingezette en te ondernemen acties.

Tevens heeft de vaste commissie voor Financiën op 11 april 2013 een brief gestuurd aan de minister van Financiën over storingen en problemen in het online betalingsverkeer. Op deze brief zal binnenkort een aanvullende reactie komen.

Cyberaanvallen in de afgelopen periode

De afgelopen weken zijn verschillende instellingen getroffen door cyberaanvallen, meer specifiek door zogeheten DDOS-aanvallen (distributed denial-of-service-aanvallen). Dit zijn aanvallen waarbij grote hoeveelheden dataverkeer naar een website worden verstuurd, waardoor deze onbereikbaar wordt. Meerdere partijen van diverse aard zowel in het binnen- als buitenland en zowel binnen als buiten vitale sectoren zoals de bankensector, zijn hierdoor getroffen. De aanvallen op de als vitaal aangemerkte financiële sector hebben echter de meest zichtbare impact gehad.

Nederland beschikt al sinds enkele jaren over een sterk ontwikkeld elektronisch betalingsverkeer. Internetbankieren en iDeal maken hier deel van uit en worden op zeer grote schaal gebruikt. Dit draagt bij aan economische en maatschappelijke ontwikkeling en hiermee loopt Nederland voorop in Europa.

kst-28684-379
ISSN 0921 - 7371
's-Gravenhage 2013

De banken nemen het belang van een betrouwbaar en veilig betalingsverkeer zeer serieus en investeren hier veel geld en menskracht in. Zij hebben naar aanleiding van de omvangrijke DDOS-aanvallen de afgelopen weken op grond van hun eigen verantwoordelijkheid dan ook verschillende aanvullende (technische) maatregelen getroffen.

Hoewel de banken door middel van het omleiden van het dataverkeer in staat zijn gebleken aanvallen steeds sneller en effectiever af te slaan kan dit gepaard gaan met de tijdelijke onbereikbaarheid van websites. Helaas zijn technische problemen of incidentele verstoringen van het betalingsverkeer nooit helemaal uit sluiten. Dat is ook nu gebleken.

Feitenrelaas en duiding DDOS aanvallen

De eerste van de aanvallen is op donderdag 4 april door Rabobank geconstateerd. Naar aanleiding hiervan zijn de andere banken geïnformeerd via de daartoe bestemde geëigende kanalen. Op 5 april zijn Rabobank en ING getroffen door een DDOS-aanval. Rabobank heeft de aanvallen weten af te slaan. Bij ING heeft dit geresulteerd in een verstoring in de bereikbaarheid van haar website van enige uren.

Naar aanleiding van deze aanvallen zijn er door de banken additionele maatregelen getroffen. In de hierop volgende dagen zijn er meerdere aanvallen geconstateerd en deze zijn nog steeds gaande. De aanvallen variëren in intensiteit en duur en hebben ertoe geleid dat de websites van ING en Rabobank enkele malen onbereikbaar zijn geweest. Door de genomen maatregelen waren de storingen van de getroffen websites van korte duur.

Deze aanvallen volgden op een technische storing bij ING op woensdag 3 april waarbij banksaldi tijdelijk onjuist werden weergegeven. Deze technische storing ging dus aan de DDOS-aanvallen vooraf en is hier niet aan gerelateerd. Wel heeft dit geleid tot ongemak en zorgen bij klanten en ondernemers.

Bij een DDOS-aanval is sprake van het verstoren van de dienstverlening en niet van het binnendringen in netwerken. Het is dan ook belangrijk om te benadrukken dat bij de aanvallen geen hacks hebben plaatsgevonden. Het leverde weliswaar ongemak voor de klanten op, maar noch de intrinsieke veiligheid van internetbankieren en iDeal, noch de betrouwbaarheid van gegevens, zijn in het geding geweest. Er is dan ook geen sprake geweest van een verstoring van het gehele betalingsverkeer. Betalen in winkels en het pinnen bij geldautomaten was mogelijk, het bereiken van de betreffende websites was gedurende de aanval helaas soms niet mogelijk. Deze casus laat zien dat wij in grote mate afhankelijk van het digitale domein en dat ICT een essentiële rol vervult binnen de vitale sectoren, zoals de bancaire sector.

DDOS-aanvallen zijn helaas een wereldwijd probleem dat op grote schaal plaats vindt. Deze problemen kunnen niet alleen banken treffen, maar iedereen die deelneemt aan het internetverkeer. Een storing van de bereikbaarheid van websites heeft een zichtbare impact. Dergelijke storingen door digitale verkeersopstoppingen zijn niet altijd te vermijden. Het is echter wel mogelijk maatregelen te treffen om de impact te beperken. Het belang hiervan is des te groter waar het vitale sectoren of instellingen betreft die een essentiële rol in de samenleving vervullen.

Ondernomen acties

Naar aanleiding van de geconstateerde verstoringen is er terstond intensief contact gelegd tussen de banken en de betrokken instanties, onder meer met de ministeries van Veiligheid en Justitie, Financiën en De Nederlandsche Bank (DNB).

Om deze verstoringen tegen te gaan onderhouden banken veiligheidssystemen die verscheidene afweermechanismen bevatten. Naar aanleiding van de onderhavige aanvallen zijn bovendien additionele en verscherpte maatregelen getroffen. Zo is onder meer dataverkeer omgeleid om de websites snel weer bereikbaar te maken. Dit heeft er toe geleid dat latere DDOS-aanvallen sneller konden worden afgeweerd waardoor de impact op de beschikbaarheid van iDeal en internetbankieren is verkleind.

Op initiatief van de Nationaal Coördinator Terrorismebestrijding en Veiligheid zijn de afgelopen periode tevens meerdere bijeenkomsten georganiseerd met betrokken banken, Internet Service Providers (ISP's) en relevante (overheids-) partijen waar praktische afspraken zijn gemaakt om zo door een gezamenlijke aanpak de invloed van de aanvallen te beperken.

Banken zijn hierbij op technische vlak ondersteund en geadviseerd door het Nationaal Cyber Security Centrum (NCSC). Hiertoe staat het NCSC in nauw contact met nationale en internationale partners en heeft tevens een verbindende rol tussen partijen. Door de banken en de overheid wordt binnen de FI-ISAC (Financial Information Sharing and Analysis Centre), die verbonden zijn aan het NCSC en daardoor worden ondersteund, intensief informatie gedeeld over de aanvallen.

Opsporing en vervolging

ING heeft aangifte gedaan van de cyberaanval. Uiteraard zijn opsporing en vervolging van groot belang. Opsporing en vervolging hebben een belangrijke rol om herhaling in de toekomst te voorkomen. Het Team High Tech Crime van de politie voert op last van het Openbaar Ministerie een strafrechtelijk onderzoek uit.

Rollen en verantwoordelijkheden

De minister van Veiligheid en Justitie is coördinerend bewindspersoon voor cyber security en de nationale veiligheid. De NCTV richt zich daarbij op de bescherming van vitale belangen en de weerbaarheid van vitale sectoren. Daarbij functioneert het onder de NCTV vallende NCSC als informatieknooppunt en expertisecentrum voor cyber security. Het NCSC brengt de betrokken partijen bij elkaar en deelt actief de kennis uit het nationale en internationale netwerk van het NCSC. Daarbij levert het NCSC ondersteuning en advies aan de getroffen partijen. Het NCSC is gericht op de doelgroep van de Rijksoverheid en vitale sectoren, zoals de financiële sector.

Banken zijn primair zelf verantwoordelijk voor de beveiliging van de eigen netwerken en systemen. Het gaat om de kern van de bancaire dienstverlening en de banken zullen er alles aan doen om hun klanten de dienstverlening te bieden die zij mogen verwachten.

Daarnaast wordt de continuïteit van het betalingsverkeer nauwgezet gevolgd door DNB, die op dit terrein meerdere rollen vervult. Allereerst is zij wettelijk belast met de taak de goede werking van het betalingsverkeer te bevorderen. Deze taak valt uiteen in een aantal onderdelen, waarvan de

belangrijkste in dit kader het zogenoemde «oversight» is. Dit bestaat uit systeemtoezicht op belangrijke deelnemers aan het betalingsverkeer en is er onder meer op gericht de betaalketen en daarmee het betalingsverkeer in het algemeen, zo goed mogelijk te laten functioneren, waarmee wordt bijgedragen aan de stabiliteit van de financiële sector.

Overigens heeft DNB in het kader van het bevorderen van de goede werking van het betalingsverkeer ook een coördinerende rol. DNB is voorzitter en secretaris van het Maatschappelijk Overleg Betalingsverkeer (MOB). Het MOB is breed samengesteld uit partijen die aanbieders en gebruikers van het betalingsverkeer vertegenwoordigen, bijvoorbeeld de koepelorganisaties van winkeliers, banken alsook de Consumentenbond. Binnen het MOB vindt afstemming en overleg plaats over allerlei punten die spelen op het terrein van betalingsverkeer.

De oversight-taak van DNB moet worden onderscheiden van de prudentiële toezichtstaak die DNB heeft. Het prudentiële toezicht is gericht op de soliditeit van financiële instellingen als zodanig (en draagt daarmee tevens bij aan de stabiliteit van de financiële sector). Belangrijk daarbij is onder andere dat banken en betaalinstellingen beschikken over een beheerste en integere bedrijfsvoering, in het kader waarvan ook eisen worden gesteld aan de ICT-omgeving. Dit raakt dus ook het beveiligingsniveau van een individuele bank. Een andere eis in dit verband is dat banken incidenten aan DNB dienen te melden. Incidenten zijn gedragingen of gebeurtenissen die een ernstig gevaar vormen voor de integere bedrijfsuitoefening. Verstoringen in het betalingsverkeer die zijn te kwalificeren als incident moeten derhalve aan DNB worden gemeld.

Ingezette en te ondernemen acties

Naar aanleiding van de cyberaanvallen heeft op maandag 15 april jl. een overleg plaatsgevonden gevoerd tussen de Ministers van Financiën en Veiligheid en Justitie en DNB, de NVB, ING, Rabobank en ABN-AMRO.

Tevens heeft er op 15 april jl. naar aanleiding van de recente verstoringen van het betalingsverkeer en in aanloop naar de vergadering van het Maatschappelijk Overleg Betalingsverkeer op 15 mei (waar dit onderwerp al door DNB op de agenda is geplaatst) een speciale vergadering plaatsgevonden van de Kerngroep van het Maatschappelijk Overleg Betalingsverkeer. Hier hebben o.a. MKB Nederland, de Consumentenbond, Detailhandel NL, Thuiswinkel.org alsook de banken aan deelgenomen. Deze overleggen waren erop gericht te bespreken hoe dit soort storingen in het betalingsverkeer tot een minimum beperkt kunnen worden en hoe de digitale weerbaarheid van een vitale sector zoals de financiële sector, kan worden versterkt. Naar aanleiding van deze overleggen is tot de volgende acties besloten:

1) Er zal door de banken een liaison in het NCSC worden geplaatst om de intensieve samenwerking te bestendigen.
2) Er is afgesproken dat bij storingen in het betalingsverkeer, ongeacht welke oorzaak, er door de banken zo snel mogelijk zal worden gecommuniceerd richting klanten en organisaties die gebruikers in het betalingsverkeer vertegenwoordigen.
3) Naast verbetering van de actuele informatie zal de transparantie over storingen en onderbrekingen worden vergroot door het inrichten van een centrale plek waar informatie hierover te vinden is.
4) Het MOB zal een analyse maken welke alternatieven er zijn bij (onverwachte) storingen in het betalingsverkeer. Hieruit moet duidelijk worden of er nog alternatieven ontbreken en hoe die eventueel ondervangen kunnen worden om zo de robuustheid van het betalingsverkeer verder te versterken.

De Minister van Veiligheid en Justitie heeft vanuit de coördinerende verantwoordelijkheid voor cyber security de afgelopen periode de Kamer reeds geïnformeerd over ingezette acties om dreigingen in het digitale domein tegen te gaan. Het gaat daarbij onder andere om:

1) Het nog dit jaar actualiseren van de Nationale Cyber Security Strategie, met als belangrijk onderdeel daarvan het op- en uitbouwen van een Nationaal Detectie en Response Netwerk;
2) Een geïntensiveerde aanpak van «Botnets» (netwerken van geïnfecteerde computers die gebruikt kunnen worden bij een (DDOS) aanval); en
3) Het aanpassen van het juridisch instrumentarium aan de ontwikkelingen in het digitale domein om middels gepaste opsporingsbevoegdheden cybercrime effectief te bestrijden.

Slot

ICT is een belangrijke drijvende kracht achter economische en maatschappelijke groei. Tegelijkertijd is onze samenleving ook steeds afhankelijker van ICT. DDOS-aanvallen en andere ICT-gerelateerde dreigingen raken ons allemaal. Dergelijke aanvallen en de storingen die deze veroorzaken zijn nu en in de toekomst niet uit te sluiten. Daarom is het van belang dat alle publieke en private partijen gezamenlijk op blijven trekken en de noodzakelijke maatregelen nemen. De ingezette en te ondernemen acties sluiten aan op ontwikkelingen in het digitale domein en dragen gezamenlijk bij aan de digitale veiligheid van de bancaire sector en andere vitale sectoren.

De minister van Financiën,
J.R.V.A. Dijsselbloem

De minister van Veiligheid en Justitie,
I.W. Opstelten