Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

2364

Vragen van het lid **Verhoeven** (D66) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over *het uitvallen van DigiD vanwege DDoS-aanvallen* (ingezonden 1 mei 2013).

Antwoord van minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 23 mei 2013).

Vraag 1
Heeft u kennisgenomen van het bericht «DigiD moeilijk te bereiken door een DDoS-aanval»?[1]

Antwoord 1
Ja.

Vraag 2 en 3
Kunt u bevestigen dat de kracht van de aanval beperkt was tot slechts 200 aanvragen per seconde?
Klopt het dat voor een dergelijke capaciteit geen botnet nodig is en dat een dergelijke aanval in theorie door een persoon thuis vanaf zijn laptop uitgevoerd zou kunnen worden?

Antwoord 2 en 3
Bij een DDoS-aanval (Distributed Denial of Service-aanval) worden grote hoeveelheden dataverkeer naar een website verstuurd waardoor deze onbereikbaar kan worden. DDoS-aanvallen bestaan in diverse varianten. Daarnaast bestaat de DoS-aanval (Denial of Service) aanval, hierbij is dus geen sprake van een netwerk aan betrokken systemen, maar van een enkele computer of server.
DigiD heeft te kampen gehad met meerdere DDoS-aanvallen die verschilden in aard en omvang. Elke aanval is met specifieke maatregelen bestreden.

[1] https://tweakers.net/nieuws/88702/digid-moeilijk-te-bereiken-door-ddos-aanval.html

ah-tk-20122013-2364
ISSN 0921 - 7398
's-Gravenhage 2013

Vraag 4
Is het niet schokkend dat een kritische overheidsdienst zo eenvoudig uit de lucht gehaald kan worden en zo lang uit de lucht gehouden kan worden?[2]

Antwoord 4
Gedurende de DDoS aanvallen is DigiD niet uit de lucht geweest. Er was sprake van een beperkte bereikbaarheid van deze voorziening. Om ongewenst dataverkeer zo veel mogelijk tegen te houden is DigiD voor gebruikers in het buitenland in de periode van 28 april tot 2 mei geblokkeerd geweest.
Het belang van de continuïteit en beschikbaarheid van DigiD is zeer groot en hier wordt veel geld en menskracht in geïnvesteerd. De actualiteit van de beveiligingsmaatregelen (waaronder de nodige afweermechanismen) wordt continue bewaakt en waar nodig worden passende aanvullende maatregelen ten uitvoer gebracht. Dit laat onverlet dat DDoS-aanvallen helaas een wereldwijd probleem zijn dat op grote schaal plaatsvindt. Dergelijke aanvallen en de ongewenste gevolgen van deze verkeersopstoppingen, zijn daarom nu en in de toekomst niet uit te sluiten.
Ik hecht eraan te benadrukken dat bij de aanvallen geen hacks hebben plaatsgevonden. De intrinsieke veiligheid van DigiD en de betrouwbaarheid van informatie en persoonsgegevens, zijn niet in het geding geweest.

Vraag 5
Is DigiD niet dezelfde kritische overheidsdienst waarvoor Microsoft ten tijde van het DigiNotar-incident was gevraagd een update uit te stellen?

Antwoord 5
Na het opzeggen van het vertrouwen in DigiNotar heeft Microsoft een update gemaakt die DigiNotar certificaten in de lijst van onbetrouwbare certificaten plaatste. DigiD was één van de vele overheiddiensten die gebruik maakte van DigiNotar certificaten.
Het uitstel van de update was in zijn algemeenheid bedoeld om organisaties meer tijd te geven om de certificaten van DigiNotar te vervangen. Hierdoor voorkwam men dat, door een abrupte beëindiging van de mogelijkheid om van DigiNotar-certificaten gebruik te maken, het communicatieverkeer tussen bijvoorbeeld machines onderling («server-to-server») zou worden verstoord. Hierdoor zouden websites en onderliggende systemen moeilijker of in het geheel niet meer bereikbaar zijn.
Overigens, zoals beschreven in het rapport «Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis» van de Inspectie Veiligheid en Justitie, zou de update van Microsoft op dinsdag 6 september 2011 om 19:00 uur plaatsvinden. In de middag van 6 september laat de rijksoverheid via de website rijksoverheid.nl echter al weten dat DigiD weer veilig kan worden gebruikt (http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/09/06/digid-weer-veilig.html).

Vraag 6
Hoe verhouden volgens u deze incidenten zich tot elkaar? Hoe kan het belang toen zo groot zijn geweest om de boel draaiende te houden, terwijl nu vrij simpel de dienstverlening alsnog stil gelegd kan worden?

Antwoord 6
Beide incidenten illustreren de toegenomen afhankelijkheid van informatiesystemen. De incidenten zijn evenwel van een andere orde. In het geval van DigiNotar was een derde partij erin geslaagd om ongeautoriseerde toegang te krijgen tot de servers van DigiNotar en vervalste digitale certificaten te genereren. Bij een DDoS-aanval is primair sprake van het verstoren van de bereikbaarheid en niet van het binnendringen in netwerken en toegang tot servers en bestanden. Zoals bij vraag 4 is vermeld, is DigiD alleen de voor gebruikers in het buitenland in de periode van 28 april tot 2 mei geblokkeerd geweest.

[2] http://www.nrc.nl/nieuws/2013/04/25/problemen-digid-nog-steeds-niet-opgelost/ en Volkskrant 26 april «Cyberaanval DigiD hardnekkig»

Vraag 7
Welke mogelijkheden ziet u om de afhankelijkheid van enkele systemen (single points of failure) te verkleinen? Wat betekent dit voor een ontwerp van een nieuw eID?

Antwoord 7
Eén van de ontwerpcriteria die bij de ontwikkeling van het eID-stelsel als uitgangspunt zal gelden is dat het stelsel geen single points of failure kent. Daarnaast biedt het keuzevrijheid voor burgers (en bedrijven) bij het gebruik van authenticatiemiddelen. Dit betekent dat als een voorziening, zoals DigiD, door een DDoS-aanval slecht bereikbaar is, men met andere middelen alsnog overheidsdienstverlening moet kunnen bereiken.

Vraag 8
Welke acties gaat u de komende periode ondernemen om de dienstverlening te verbeteren?

Antwoord 8
Gelet op het economisch en maatschappelijk belang van DigiD heeft Logius naar aanleiding van de aanvallen additionele en verscherpte maatregelen getroffen om de continuïteit en beschikbaarheid van DigiD, te kunnen blijven bewaken en te borgen. Logius is hierbij op het technisch vlak ondersteund en geadviseerd door het Nationaal Cyber Security Centrum (NCSC). Verder verwijs ik naar de brief van mijn ambtgenoot van het ministerie van Veiligheid en Justitie aan uw Kamer van 14 mei 2013 (Kenmerk 386064), waarbij, mede namens de Ministers van Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, voor Wonen en de Rijksdienst en de Staatssecretaris van Financiën, een reactie is gegeven op de DDoS-aanvallen bij de Rijksoverheid en de in dat verband genomen en voorgenomen maatregelen.