Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

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

156

Vragen van het lid **Oosenbrug** (PvdA) aan de Minister van Veiligheid en Justitie over *de storing bij Ziggo ten gevolge van DDos-aanvallen* (ingezonden 21 augustus 2015).

Antwoord van Staatssecretaris **Dijkhoff** (Veiligheid en Justitie) mede namens de Minister van Economische Zaken (ontvangen 30 september 2015) Zie ook Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 26

Vraag 1
Kent u het bericht «Ziggo verwacht nog meer cyberaanvallen»?[1]

Antwoord 1
Ja.

Vraag 2 en 3
In hoeverre wordt door storingen bij grote internetbedrijven zoals Ziggo de publieke dienstverlening geraakt bijvoorbeeld omdat publieke dienstverleners waaronder de Belastingdienst, de Dienst Uitvoering Onderwijs, het Uitvoeringsinstituut Werknemersverzekeringen of gemeentelijke diensten voor miljoenen personen niet meer bereikbaar zijn?
Deelt u de mening dat vanwege die dienstverlening storingen bij particuliere internetbedrijven ook het publieke belang raken? Zo ja, op welke wijze draagt u bij aan het voorkomen en oplossen van genoemde problemen en het beschermen van de digitale infrastructuur? Zo nee, waarom niet?

Antwoord 2 en 3
De storingen bij Ziggo werden veroorzaakt door een Distributed Denial of Service (DDoS) aanval op de zogenaamde DNS-servers van Ziggo. DNS is het systeem dat op het internet gebruikt wordt om domeinnamen naar IP-adressen te vertalen en omgekeerd. Als dit niet werkt, zijn websites niet langer bereikbaar voor gebruikers van deze DNS-server. Hierdoor was het voor een groot aantal Ziggo-klanten niet mogelijk om gebruik te maken van het internet, dit laat onverlet dat alternatieven wel beschikbaar waren. Dergelijke storingen door digitale verkeersopstoppingen zijn nu en in de toekomst niet geheel te voorkomen.

[1] http://www.volkskrant.nl/tech/ziggo-verwacht-nog-meer-cyberaanvallen~a4124865/

ah-tk-20152016-156
ISSN 0921 - 7398
's-Gravenhage 2015

De storingen hebben geen gevolgen gehad voor de beschikbaarheid van de digitale publieke dienstverlening. Desalniettemin zorgde deze digitale verkeersopstopping er wel voor dat de getroffen klanten van Ziggo tijdelijk niet in staat waren om gebruik te maken van digitale diensten, waaronder digitale publieke diensten.
Partijen zijn, zowel binnen als buiten de overheid, zelf primair verantwoordelijk voor de beveiliging van de eigen netwerken en systemen. Voorts is er in de Telecommunicatiewet een zorg- en meldplicht opgenomen. De zorgplicht houdt in dat telecommunicatieaanbieders passende technische en organisatorische maatregelen nemen om risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen. De meldplicht houdt in dat aanbieders inbreuken op de veiligheid en integriteit melden bij het Loket meldplicht van Agentschap Telecom. Ziggo heeft dit ook in onderhavig geval gedaan. De initiële melding wordt gevolgd door een analyse van het incident door Ziggo. Ziggo zal de analyse bij Agentschap Telecom aanleveren. Als deze analyse daartoe aanleiding geeft, zal Agentschap Telecom dit incident verder onderzoeken.
Het Ministerie van Veiligheid en Justitie draagt bij aan de bescherming van de digitale infrastructuur middels een algehele verhoging van de digitale weerbaarheid aan de hand van acties uit de tweede Nationale Cybersecurity Strategie.

Vraag 4
In hoeverre neemt vanwege uw ambitie om uiterlijk vanaf 2017 bedrijven en burgers de mogelijkheid te bieden zaken met de overheid digitaal af te handelen, het belang van het voorkomen van DDos-aanvallen toe? Wat zegt dat over uw rol in het voorkomen van dergelijke aanvallen?

Antwoord 4
Zoals eerder door de Minister van Binnenlandse Zaken en Koninkrijksrelaties in de Visiebrief digitale overheid 2017 d.d. 23 mei 2013 is aangegeven, dienen het beveiligen van informatie en de beschikbaarheid van digitale dienstverlening urgent en blijvend op de agenda te staan.[2] In mijn brief aan de Tweede Kamer d.d. 14 mei 2013 is ingegaan op de het fenomeen van DDoS-aanvallen.[3] Hierin is aangegeven dat DDoS-aanvallen geen nieuw fenomeen zijn en helaas een wereldwijd probleem vormen dat op grote schaal plaatsvindt. Daarnaast kan dit type aanval iedere partij treffen die diensten aanbiedt op of via het internet.
Een storing van de bereikbaarheid van websites of het internet als geheel heeft een zichtbare impact, zoals de storingen bij Ziggo wederom laten zien. Daarbij is elektronische dienstverlening niet meer weg te denken uit onze informatiesamenleving en vergt dus constant aandacht. Zoals reeds is aangegeven bij de beantwoording van de vragen van de leden Dijkhoff (VVD), Oosenbrug (PvdA) en Verhoeven (D66) op 5 maart 2015 (kenmerk 2015Z02555/2658/2763) neemt het kabinet verschillende maatregelen om de weerbaarheid tegen DDoS-aanvallen te verhogen. Zo is er onder andere in publiek-private samenwerking sprake van een geïntensiveerde aanpak van botnets. Daarnaast deelt het NCSC beschikbare informatie over cyberaanvallen met overheidsorganisaties, zodat hier lering uit getrokken kan worden en bezien kan worden of (nieuwe) extra maatregelen moeten worden genomen.

Vraag 5
Kent u particuliere initiatieven voor de beveiliging tegen DDos-aanvallen zoals De Nationale anti-DDoS Wasstraat (NaWas)[4]? Acht u het wenselijk om met dergelijke particuliere initiatieven te overleggen over op welke manier u kunt bijdragen aan het beveiligen tegen DDos-aanvallen? Zo ja, op welke termijn gaat dit overleg plaatsvinden? Zo nee, waarom niet?

---

[2] Kamerstuk 26 643, nr. 280.
[3] Kamerstuk 26 643, nr. 278.
[4] http://www.nbip.nl/diensten/nawas-demand-beveiliging-tegen-ddos/

Antwoord 5
Ja, zowel marktpartijen als ik zijn bekend met particuliere initiatieven die zich richten op de beveiliging tegen DDoS-aanvallen. Er bestaan diverse en uiteenlopende initiatieven. Het NCSC staat daarbij reeds in contact met de partijen achter de diverse initiatieven Zoals reeds aangegeven is bij brief d.d. 24 november 2014, neemt het NCSC, daar waar private initiatieven bijdragen aan de beveiliging tegen digitale aanvallen, waar mogelijk en noodzakelijk, een faciliterende rol op zich.[5]

Vraag 6
Heeft het Nationaal Cyber Security Centrum (NCSC) een concrete taak in het beveiligen van internetbedrijven tegen DDos-aanvallen? Zo ja, welke taak? Zo nee, waarom niet?

Antwoord 6
Zoals reeds aangegeven in mijn beantwoording van de vragen 2 en 3 zijn partijen zelf primair verantwoordelijk voor de beveiliging van de eigen netwerken en systemen. Het NCSC is dan ook niet verantwoordelijk voor het beveiligen van de digitale systemen en infrastructuren van internetserviceproviders, zoals Ziggo. Wel levert het NCSC als informatieknooppunt en expertisecentrum voor cyber security, ondersteuning en advies aan getroffen partijen.

[5] Kamerstuk 26 643, nr. 337.