Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500EA Den Haag

De Voorzitter van de Tweede Kamer der Staten Generaal
Binnenhof 4
2513 AA 's-Gravenhage

DGOBR
Directie
Informatiseringsbeleid Rijk

Turfmarkt 147
's-Gravenhage
Postbus 20011
2500EA Den Haag
Nederland
www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2015-0000124417

Uw kenmerk
2015Z02555/2658/2763

Datum 5 maart 2015

Betreft Antwoorden op de vragen van Oosenbrug (PvdA), Dijkhoff (VVD) en Verhoeven (D66) over langdurige onbereikbaarheid van de website rijksoverheid.nl door een DDoS aanval

Hierbij zend ik u mede namens de minister-president en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie de antwoorden op de vragen van Oosenbrug (PvdA) met nummer 2015Z02555 (ingezonden 12 februari 2015), Dijkhoff (VVD) met nummer 2015Z02658 (ingezonden 13 februari 2015) en Verhoeven (D66) met nummer 2015Z02763 (ingezonden 17 februari 2015) over langdurige onbereikbaarheid van de website rijksoverheid.nl door een DDoS aanval.

De minister voor Wonen en Rijksdienst,

drs. S.A. Blok

2015Z02555

Datum
5 maart 2015

Kenmerk
2015-0000124417

Vragen van het lid Oosenbrug (PvdA) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en voor Wonen en Rijksdienst over langdurige onbereikbaarheid van overheidswebsites (ingezonden 12 februari 2015)

1
Is het waar dat op 10 februari 2015 de website www.rijksoverheid.nl meerdere uren onbereikbaar was? Zo ja, welke overheidssites zijn nog meer door deze storing getroffen?

Ja. De storing betrof in ieder geval de twee grote websites Rijksoverheid.nl en Defensie.nl, die een belangrijke functie hebben in het communiceren van informatie van de Rijksoverheid naar het algemeen publiek. Daarnaast zijn diverse kleine websites geraakt, die zijn gericht op de communicatie met specifieke groepen. De websites van Geenstijl en Telfort zijn ook getroffen.

2
Waardoor werd deze storing veroorzaakt en waarom duurde deze zolang?

De storing werd veroorzaakt door een DDoS aanval. De storing duurde zo lang, omdat deze vanwege de complexiteit door de leverancier in eerste instantie als een technische storing en niet als een DDoS aanval werd beoordeeld. Toen de conclusie was, dat het een DDoS aanval betrof, was deze binnen enkele uren afgeslagen.

3
Welke impact heeft deze storing gehad op het werk van de rijksoverheid en op mensen die overheidsinformatie zochten?

De impact op medewerkers van de Rijksoverheid is beperkt tot medewerkers die voor Rijksoverheid.nl of de andere getroffen websites werken. Redacteuren konden gedurende de storing geen informatie op de websites plaatsen. De publieksvoorlichters van het loket ‘Informatie Rijksoverheid’ konden gedurende de storing de website niet als bron gebruiken voor het beantwoorden van vragen per telefoon of e-mail

Mensen die tijdens de storing informatie van de Rijksoverheid zochten, hebben hiervoor Rijksoverheid.nl of de andere getroffen websites niet kunnen gebruiken. De vragen van mensen die de publieksvoorlichting ‘Informatie Rijksoverheid’ hebben gebeld zijn genoteerd. Na het oplossen van de storing zijn alle vragen, afhankelijk van de voorkeur van de vragensteller, per e-mail of telefoon alsnog beantwoord.

Voor informatie, zoals brieven van de ministers aan de Staten-Generaal, is Rijksoverheid.nl niet de enige bron. Deze zijn als kamerstukken bijvoorbeeld ook op de website van de Tweede Kamer te vinden.

4
Welke technische maatregelen zijn genomen om te voorkomen dat de centrale informatiesite van de rijksoverheid langdurig onbereikbaar is? Waardoor hebben deze maatregelen niet gewerkt?

Voor de site Rijksoverheid.nl en de andere getroffen sites van de Rijksoverheid is een set aan beveiligingsmaatregelen (inclusief back-up) genomen, die normaliter afdoende is om DDoS aanvallen te weerstaan of binnen korte tijd op te lossen. Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek. Heel 2014 had Rijksoverheid.nl een uitval van 0%. Echter, in dit geval is dit niet afdoende gebleken omdat de leverancier eerst aan een andere oorzaak van de storing dacht (zoals in vraag 2 is vermeld).

5
Wat voor acties overweegt u om een urenlange onbereikbaarheid van de website van de rijksoverheid in de toekomst te voorkomen?

De leverancier zal een verbeterplan opstellen, waarbij het ministerie van Algemene Zaken en het Nationaal Cyber Security Centrum (NCSC) nauw betrokken zijn. De analysemethode zal daarvan onderdeel zijn.
Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen Het gaat erom om tegen aanvaardbare kosten de risico’s zo minimaal mogelijk te maken.

6
Worden voor dienstverlenende overheidswebsites waarbij onbereikbaarheid een zeer grote impact heeft, zoals de Rijksdienst voor het Wegverkeer (RDW) of de Belastingdienst, extra technische maatregelen genomen om de bereikbaarheid te waarborgen? Zo ja, welke? Hadden die deze storing kunnen voorkomen of verkorten? Zo nee, waarom niet?

Zowel de RDW als de Belastingsdienst hebben beveiligingsmaatregelen genomen om DDoS aanvallen te weerstaan of binnen korte te tijd af te slaan, een zg. anti-DDoS wasstraat, die verschillende technieken omvat. Zij hebben geen last van deze DDoS aanval gehad. De DDoS aanvallen zijn de laatste tijd tot nu toe zonder al te veel problemen voor de bereikbaarheid afgeweerd.
Het NCSC ondersteunt de overheid en de vitale sectoren onder andere door nieuwe beschikbare informatie over cyberaanvallen te delen met de overheidsorganisaties om er lering uit te trekken en te bezien of (nieuwe) extra maatregelen moeten worden genomen.
Gezien de rapportage van de leverancier zelf (zie vraag 2) heeft de duur van de storing niet gelegen aan de beveiligingsmaatregelen, maar aan de analyse van de storing.

2015Z02658

Datum
5 maart 2015

Kenmerk
2015-0000124417

Vragen van het lid Dijkhoff (VVD) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over het bericht 'Rijksoverheid.nl was dupe van DDoS-aanval' (ingezonden 13 februari 2015)

1
Bent u bekend met het bericht 'Rijksoverheid.nl was dupe van DDoS-aanval'? 1)

Ja.

2
Klopt het bericht dat rijksoverheid.nl en diverse andere websites plat werden gelegd door een DDoS-aanval? Is er meer bekend over de achtergrond van de aanval? Was er sprake van ingekochte 'pesterij' om de sites plat te leggen of was dit een mogelijk rookgordijn om een hack of andere besmetting te verhullen?

Ja, dat bericht klopt. Eventuele motieven of achtergronden bij deze aanval zijn vooralsnog niet bekend. Het ministerie van Algemene Zaken heeft aangifte gedaan.

3
In hoeverre behoren de getroffen websites tot de vitale infrastructuur? Is het essentieel dat websites als rijksoverheid.nl ten alle tijden beschikbaar zijn voor publiek? Of is het platleggen van de websites 'slechts' een hinderlijke overlast waar we eens in de zoveel tijd rekening mee moeten houden?

De getroffen websites maken geen deel uit van de vitale infrastructuur. Uiteraard zijn zij wel van groot belang voor het informeren van de burgers.
Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek. Heel 2014 had Rijksoverheid.nl een uitval van 0%.
Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen. Het gaat erom om tegen aanvaardbare kosten de risico's zo minimaal mogelijk te maken.

4
In hoeverre zou het bieden van een back-up in geval van een cyberaanval soelaas kunnen bieden aan het publiek? Wat zouden de kosten zijn van zo'n back-up en acht de regering die kosten proportioneel?

Voor de getroffen sites bestaat een back-upvoorziening, die echter ook getroffen bleek. De leverancier zal een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. Onderdeel van dat plan zal zijn te regelen, dat deze back-up voorziening bij een DDoS aanval wel kan worden ingeschakeld.
Zie ook het antwoord op vraag 3.

5
Binnen hoeveel tijd kon de overheid de burger informeren over de problemen op de websites en zijn hiervoor alternatieve kanalen beschikbaar?

Datum
5 maart 2015

Kenmerk
2015-0000124417

De Rijksoverheid heeft per direct de telefonische (1400) en e-mail beantwoording van de dienst voor publieksvoorlichting 'Informatie Rijksoverheid' ingezet om burgers te informeren over de storing. Daarnaast is ook het Twitterkanaal 'Informatie Rijksoverheid' gebruikt om de volgers te informeren.

Na het oplossen van de storing zijn alle vragen die bij het loket zijn binnengekomen alsnog per mail of telefoon beantwoord.

1) Nos, 11 februari 2015, http://nos.nl/artikel/2018594-rijksoverheid-nl-was-dupe-van-ddos-aanval.html

2015Z02763

Datum
5 maart 2015

Kenmerk
2015-0000124417

Vragen van het lid Verhoeven (D66) aan de minister van Veiligheid en Justitie en de minister-president over het bericht dat de website van de Rijksoverheid plat lag door een DDoS-aanval. (ingezonden 17 februari 2015)

1
Bent u bekend met de berichten 'Ddos'ers wijzigden tijdens aanval Rijksoverheid hun aanvalsmethode' en 'Rijksoverheid.nl was dupe van DDoS-aanval'? 1)

Ja.

2
In 2013 heeft u een brief naar de Kamer gestuurd met een aantal maatregelen om de weerbaarheid tegen DDoS-aanvallen te vergroten; kunt u per punt aangeven wat de stand van zaken is ten aanzien van de implementatie? 2)

In de brief d.d. 14 mei 2013 en de eerdere brief over DDoS-aanvallen op de bancaire sector d.d. 16 april 2013 zijn de volgende acties aangekondigd:
1) Het nog dit jaar actualiseren van de Nationale Cyber Security Strategie; 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. 4) Plaatsen filters bij DigiD en het preventief door de Minister van BZK afnemen van aanvullende diensten om grote aanvallen af te slaan. 5) De Minister voor Wonen en Rijksdienst en de minister van Binnenlandse Zaken en Koninkrijksrelaties zullen samen met de Chief Information Officers (CIO's) van de departementen, de medeoverheden, de interne en externe ICT dienstverleners en het NCSC verder bezien wat er nog voor aanvullende acties mogelijk zijn om de cyber security te verhogen en de impact van DDoS aanvallen op de belangrijke voorzieningen van de overheid te beperken. 6) De minister van Algemene Zaken ziet toe op het op orde houden van de maatregelen tegen toekomstige DDos aanvallen van Rijksoverheid.nl. 7) Informatiedeling naar aanleiding van de ervaringen in 2013.

Hierbij per punt de stand van zaken:

1) In het najaar van 2013 is de Tweede Nationale Cyber Security Strategie gepubliceerd. Op 18 december 2014 is de eerste rapportage over de uitvoering hiervan aan de TK verzonden,
2) Naar aanleiding van het AO Cybersecurity d.d. 27 maart 2014 is de TK op 7 juli 2014 uitvoerig geïnformeerd over de geïntensiveerde aanpak van botnets. Een belangrijk onderdeel hiervan is de publiek-private samenwerking bij de bestrijding van botnets,
3) Over de versterking van het juridisch instrumentarium is in de eerdergenoemde rapportage d.d. 18 december aangegeven dat deze in de eerste helft van 2015 aan de Tweede Kamer zal worden aangeboden.
4) Naar aanleiding van de DDoS-aanvallen op DigiD in de periode van 23 april tot en met 27 april 2013 heeft Logius in opdracht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aanvullende maatregelen getroffen om uitval en/of verminderde beschikbaarheid te beperken en dergelijke aanvallen te kunnen mitigeren. Het gaat daarbij onder meer om het creëren van een grotere capaciteit in het verwerken van dataverkeer, en specifieke anti-DDoS tooling. Digitale voorzieningen van de overheid

staan regelmatig bloot aan DDoS-aanvallen die variëren in aard en omvang. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen,

5) Om het bewustzijn ten aanzien van informatieveiligheid bij de medeoverheden te versterken, heeft de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) in twee jaar tijd vele activiteiten verricht. Een rapportage van de activiteiten is op 18 december 2014 naar de Tweede Kamer verstuurd (vergaderjaar 2014-2015, Kamerstuk 26 643, nr. 344). In het overleg van de CIO's van de departementen komt informatiebeveiliging regelmatig op de agenda.
6) Het ministerie van Algemene Zaken ziet, geadviseerd door het NCSC, voortdurend samen met de leverancier toe of de genomen maatregelen nog toereikend zijn.
7) Het NCSC deelt beschikbare informatie over cyberaanvallen met de overheidsorganisaties om er lering uit te trekken en te bezien of (nieuwe) extra maatregelen moeten worden genomen. Dat gebeurt onder andere in zg. ISAC's (Information Sharing and Analysing Centres). In 2014 is de ISAC voor de overheid opgericht.

3
Volgens het bericht 'Ddos'ers wijzigden tijdens aanval Rijksoverheid hun aanvalsmethode' werd een type DDoS-aanval gebruikt waar het hostingbedrijf geen ervaring mee had; kunt u aangeven of de maatregelen uit de brief van 2013 voldoende zijn om DDoS-aanvallen van dit type in voldoende mate te kunnen afslaan? Of zijn er nieuwe maatregelen nodig?

Bij elke soort DDoS aanval is het van belang om te werken met een combinatie van technische maatregelen, waaronder filtering en additionele capaciteit. De leverancier zal hiertoe een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. (zie ook de verklaring van de leverancier bij vraag 2 van Oosenbrug)
De maatregelen uit de brief van 2013 blijven in grote lijnen ook nu nog relevant, maar op technisch niveau zullen telkens weer nieuwe maatregelen moeten worden genomen.
Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek.
Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen. Het gaat erom om tegen aanvaardbare kosten de risico's zo minimaal mogelijk te maken.

4
Kunt u aangeven door wie en/of waarvandaan de DDoS-aanvallen zijn uitgevoerd?

Eventuele daders, motieven of achtergronden bij deze aanval zijn vooralsnog niet bekend. Het ministerie van Algemene Zaken heeft aangifte gedaan

5
Staat weerbaarheid tegen DDoS-aanvallen op de agenda van de conferentie over cyber security in april 2015 in Nederland? Zo nee, bent u bereid het op de agenda

te zetten?

Nee, het specifieke onderwerp DDoS-aanvallen staat niet als dusdanig op de agenda. Wel komen maatregelen zoals normen en standaarden die bijdragen aan de weerbaarheid tegen dergelijke aanvallen prominent voor op de agenda. Over de nadere inhoud van de conferentie zal de Kamer nog deze maand geïnformeerd worden.

6
Waarom is ervoor gekozen geen tijdelijke noodwebsite te plaatsen waarmee mensen verwezen kunnen worden naar andere informatiekanalen?

Die keuze is een afweging tussen kosten en baten en de tijd, die nodig is om een omvangrijke site als rijksoverheid.nl elders op een veilige wijze in de lucht te krijgen. Gezien de kosten en de benodigde tijd is deze keuze niet gemaakt.
Voor de getroffen sites bestaat een back-upvoorziening, die echter ook getroffen bleek. De leverancier zal een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. Onderdeel van dat plan zal zijn te regelen, dat deze back-up voorziening bij een DDoS aanval wel kan worden ingeschakeld.

1) http://tweakers.net/nieuws/101329/ddosers-wijzigden-tijdens-aanval-rijksoverheid-hun-aanvalsmethode.html en http://nos.nl/artikel/2018594-rijksoverheid-nl-was-dupe-van-ddos-aanval.html
2) http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/15/reactie-ddos-aanvallen-bij-de-rijksoverheid/lp-v-j-0000003271.pdf

Toelichting:
Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Dijkhoff (VVD), ingezonden 13 februari 2015 (vraagnummer 2015Z02658)