Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Directie Cyber Security

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
386064

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 14 mei 2013
Onderwerp Reactie DDoS-aanvallen bij de Rijksoverheid

De Vaste Kamercommissie (VKC) voor Veiligheid en Justitie heeft de Minister van Veiligheid en Justitie op 8 mei jl. verzocht om te reageren op de berichten over de aanhoudende cyberaanvallen op de websites van de NOS en het Rijk. Deze brief geeft mede namens de Ministers van Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, voor Wonen en de Rijksdienst en de Staatssecretaris van Financiën invulling aan dit verzoek.

Van aanhoudende cyberaanvallen op de NOS, zoals aangegeven door de Vaste Kamercommissie, is ook bij navraag bij het Ministerie van OCW niets bekend. In de brief treft u: 1) de rollen en verantwoordelijkheden van de betrokken partijen, 2) een duiding en de opsporing en vervolging bij de aanvallen en 3) verdere informatie over de aanvallen op de Rijksoverheid en de ondernomen en aanvullende acties, zowel naar aanleiding van de aanvallen op de bancaire sector, als bij de Rijksoverheid.

Over de aanvallen op partijen binnen de bancaire sector en de naar aanleiding daarvan ondernomen en ingezette acties is de Tweede Kamer door de Ministers van Financiën en Veiligheid en Justitie d.d.16 april reeds geïnformeerd. Belangrijk onderdeel daarin is het plaatsen van een liaison van de bancaire sector in het Nationaal Cyber Security Centrum en het uitvoeren van een onderzoek naar de robuustheid van het betalingsverkeer. Voor de volledigheid treft u in de bijlage bij deze brief een overzicht van de DDoS-aanvallen (Distributed Denial of Service attacks) in de periode van 4 april (de eerste aanval op de Rabobank) tot 11 mei (de aanval op de Belastingdienst) op de Rijksoverheid en de vitale sectoren.

Rollen en verantwoordelijkheden

De minister van Veiligheid en Justitie is coördinerend bewindspersoon voor cyber security en de nationale veiligheid. De onder deze minister vallende Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) richt zich daarbij op de bescherming van vitale belangen en de weerbaarheid van vitale sectoren. Daarbij functioneert het onder de NCTV vallende Nationaal Cyber Security Centrum (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 richt zich op de

primaire doelgroepen: de Rijksoverheid en de vitale sectoren en fungeert tevens als informatiepunt voor de overige sectoren in Nederland.

Partijen, zowel binnen als buiten de overheid, zijn primair zelf verantwoordelijk voor de beveiliging van de eigen netwerken en systemen. Het gaat om de kern van de eigen dienstverlening en getroffen organisaties zullen er alles aan doen om hun klanten de dienstverlening te bieden die zij mogen verwachten.

Binnen de Rijksoverheid geldt de volgende verdeling: De website www.rijksoverheid.nl ressorteert onder de Minister van Algemene Zaken. De Staatssecretaris van Financiën gaat over de website www.belastingdienst,nl. De Minister voor Wonen en Rijksdienst is systeemverantwoordelijk voor de ICT bij de rijksoverheid. De Minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor DigiD en voor de basisinfrastructuur van de verschillende bestuurslagen ten behoeve van de e-dienstverlening aan burgers. Tevens wordt in het Informatie Strategie Overheden (ISO) overleg van de vier overheidssectoren (Rijk/ZBO's, provincies, gemeenten en waterschappen) informatie gedeeld tussen de Chief Information Officers (CIO's)' van alle bestuurslagen.

Aanvallen op vitale sectoren en de Rijksoverheid

In de periode vanaf 4 april tot 11 mei hebben meerdere aanvallen plaatsgevonden op organisaties vallend binnen de vitale sectoren en de Rijksoverheid. In de eerste helft van april was sprake van meerdere aanvallen op diverse onderdelen van de bancaire sector. Hierover is de Tweede Kamer d.d. 16 april door de Ministers van Financiën en Veiligheid en Justitie geïnformeerd.

In de periode van 23 april tot en met 11 mei zijn DDoS-aanvallen op informatiesystemen van de Rijksoverheid uitgevoerd. Het gaat daarbij om aanvallen op: 1) DigiD, 2) de website www.Rijksoverheid.nl en 3) de website www.Belastingdienst.nl. Deze aanvallen hebben geresulteerd in tijdelijke uitval dan wel een verminderde beschikbaarheid van de getroffen systemen. Van de aanvallen is door de getroffen overheidspartijen aangifte gedaan en er zijn aanvullende maatregelen getroffen om uitval en/of verminderde beschikbaarheid nu en in de toekomst te beperken en de hersteltijd te verminderen. Een overzicht van de DDoS-aanvallen en de response treft u in bijlage 1.

Maatregelen

DDoS-aanvallen zijn geen nieuw fenomeen en vormen helaas een wereldwijd probleem dat op grote schaal plaats vindt. Deze aanvallen kunnen iedereen treffen die diensten aanbiedt op het internet. Ook de Rijksoverheid staat dagelijks bloot aan grotere en kleinere aanvallen. Een storing van de bereikbaarheid van websites heeft een zichtbare impact. Dergelijke storingen door digitale verkeersopstoppingen zijn nu en in de toekomst niet te vermijden. Het is echter wel mogelijk en van groot belang om maatregelen te treffen om de impact te beperken. Op dit vlak is het nodig de weerbaarheid tegen DDoS-aanvallen te verhogen. Het belang hiervan is des te groter waar het vitale sectoren, instellingen of voorzieningen betreft die een essentiële rol in de samenleving vervullen.

Daarbij speelt dat de elektronische dienstverlening niet meer weg te denken is uit onze informatiesamenleving. Duidelijk is dat geïnvesteerd moet worden in

beveiliging van ICT en alternatieve kanalen en infrastructuren voor e-dienstverlening om de veiligheid van vitale en essentiële voorzieningen in de dienstverlening te kunnen waarborgen. De aangevallen organisaties zijn daar zelf verantwoordelijk voor.

Duiding en opsporing en vervolging

Naar aanleiding van de aanvallen is door organisaties binnen de vitale sectoren en de Rijksoverheid aangifte gedaan. Op grond hiervan is op last van het Openbaar Ministerie door het Team High Tech Crime van de Nationale Politie een strafrechtelijk onderzoek opgestart. Op internet zijn meerdere en soms tegenstrijdige berichten verschenen waarin gerefereerd werd aan mogelijke daders en doelwitten van deze aanvallen. Deze zullen in het onderzoek worden betrokken. Gezien het feit dat het strafrechtelijk onderzoek nog loopt is het onmogelijk om uitspraken te doen over mogelijke dader(s), motieven en/of de relatie tussen de beschreven aanvallen.

Genomen acties n.a.v. de aanvallen op de vitale sectoren en de Rijksoverheid

Buiten de door de Minister van Financiën ingezette acties ten behoeve van de bancaire sector heeft de Minister van Veiligheid en Justitie in de brief d.d. 16 april reeds aangekondigd de volgende acties in gang te zetten: 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.

In reactie op de aanvallen op rijksoverheidssites zijn diverse acties in gang gezet. Bij de aanvallen op DigiD zijn filters geplaatst om ongewenst dataverkeer zo veel mogelijk tegen te houden. Daarnaast is DigiD voor gebruikers in het buitenland tijdelijk afgesloten. Deze blokkade is op 2 mei jl. opgeheven. De veiligheid en integriteit van DigiD zijn niet in het geding geweest. Als de veiligheid wel in het geding dreigt te komen, wordt DigiD preventief uit de lucht gehaald. De Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft besloten om als preventieve maatregel aanvullende diensten af te nemen van leveranciers om grote DDoS-aanvallen beter af te kunnen slaan. Het gaat daarbij onder meer om het creëren van een grotere capaciteit in het verwerken van dataverkeer, en een dienst waarbij tijdens een DDoS-aanval aanvullende scheiding plaatsvindt in het inkomende dataverkeer. Daarnaast is er sprake van versterkte alertheid om eventuele nieuwe aanvallen om deze op gepaste wijze te kunnen afslaan.

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.
De uitgebreide set maatregelen die al getroffen was voor de (alleen informatie verstrekkende) website www.rijksoverheid.nl heeft voor een relatief korte hersteltijd

gezorgd. De minister van Algemene Zaken ziet toe op het op orde houden van de maatregelen tegen toekomstige DDos aanvallen.

De technische maatregelen bij de Belastingdienst waren effectief en resulteerden in een relatief korte hersteltijd. Door de Staatssecretaris van Financiën zullen de procedures worden geëvalueerd en waar nodig aangepast. Reeds enkele weken worden zowel initiële maatregelen als evaluatieresultaten in het kader van de Manifestgroep (samenwerkende publieke uitvoeringsorganisaties) uitgewisseld binnen de landelijke uitvoeringsorganisaties. Via het NCSC en partner- en schakelorganisaties zoals de InformatieBeveiligingsDienst voor Gemeenten zal deze informatie ook beschikbaar worden gesteld aan andere publieke en private partijen

De lessen naar aanleiding van DigiNotar, Lektober en de recente cyberaanvallen benadrukken het belang van een adequate beveiliging van de overheid. Naar aanleiding van het DigiNotar- incident heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties de Taskforce Bestuur en Informatieveiligheid Dienstverlening ingesteld. De Taskforce heeft als doel bestuurders en topmanagers in het openbaar bestuur te doordringen van het belang van informatieveiligheid. De komende twee jaar gaat de Taskforce de ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen bijstaan bij het verbeteren van hun bewustzijn ten aanzien van informatieveiligheid (Kamerstuk 26 643, nr. 269).

Slot
De bancaire sector heeft reeds maatregelen ter versterking van die digitale weerbaarheid n.a.v. de eerdere aanvallen aangekondigd. Ook de overheden zijn, als essentiële sectoren in de samenleving zoals in deze brief beschreven, continu alert op cybercrime en op het bestendigen van de continuïteit van de dienstverlening in onze van ICT afhankelijke maatschappij. Hiertoe wordt samen met de private sector opgetrokken en continu bekeken welke maatregelen nodig zijn om cyberaanvallen af te kunnen wenden.

De DDoS-aanvallen die o.a. de Rijksoverheid hebben getroffen zijn ernstig. De dienstverlening aan burgers en bedrijven is op meerdere momenten onderbroken geweest en vervolgens hersteld. Daarbij is de dienstverlening veelal via andere kanalen beschikbaar gebleven. Het is van belang om te benadrukken dat het om een tijdelijke verstoring van de dienstverlening gaat en niet om een inbreuk op de veiligheid ofwel hack waarbij gegevens zijn ontvreemd of gelekt. Desalniettemin is het van groot belang om de weerbaarheid tegen en het herstelvermogen na geslaagde DDoS-aanvallen te versterken. De ingezette en aanvullende acties voorzien in het treffen van de benodigde extra maatregelen om de beschikbaarheid van websites van de Rijksoverheid en de continuïteit van dienstverlening te borgen.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Bijlage 1: DDoS-aanvallen op de Rijksoverheid en de vitale sectoren

DDoS-aanvallen op de bancaire sector

Op 4 en 5 april vond een eerste aanval plaats op Rabobank en ING. Hierna zijn ook andere banken en IDEAL getroffen door DDoS-aanvallen. Over deze aanvallen en de ondernomen acties is de Kamer per brief d.d. 16 april geïnformeerd door de Ministers van Financiën en Veiligheid en Justitie. Naar aanleiding van deze aanvallen zijn door de Minister van Financiën en Veiligheid en Justitie en de bancaire sector de volgende acties ondernomen: 1) het plaatsen van een liaison van de bancaire sector in het Nationaal Cyber Security Centrum (NCSC), 2) het verbeteren van de communicatie en de transparantie bij verstoringen in de bancaire sector en 3) het uitvoeren van een analyse door het Maatschappelijk Overleg Betalingsverkeer (MOB) om de robuustheid van het betalingsverkeer te versterken.

DDoS-aanvallen op overige vitale sectoren

Naast de aanvallen op de bancaire sector is er sprake geweest van aanvallen op de NS en de KLM. Op 12 april heeft een DDoS-aanval plaatsgevonden op de website van de NS waardoor deze beperkt bereikbaar werd. Op 19 april jl. werd de website van de KLM getroffen door een DDoS-aanval. Hierdoor waren de elektronische diensten zoals het aanschaffen van tickets en inchecken gedurende enige uren beperkt of niet beschikbaar. Naar aanleiding van deze aanvallen zijn door de betrokken partijen aanvullende maatregelen getroffen om de impact van huidige en toekomstige aanvallen te beperken.

DDoS-aanvallen op de Rijksoverheid

In de periode van 23 april tot en met 13 mei is de Rijksoverheid op diverse vlakken geconfronteerd met DDoS-aanvallen op systemen die door de overheid gebruikt worden. Van deze aanvallen is aangifte gedaan bij het Team High Tech Crime van de Nationale Politie. Het gaat daarbij om de volgende 3 aanvallen:

1) *DDoS-aanvallen op DigiD*

In de periode van 23 april tot en met 27 april jl. hebben diverse aanvallen op de website van DigiD plaatsgevonden. DigiD is hierdoor beperkt bereikbaar geweest.. De beperkte bereikbaarheid ontstond met name aan het begin van de aanvallen daar op dat moment de additionele beschermingsmaatregelen op de aanval dienden te worden afgestemd. Daarnaast is in de periode van 28 april tot 2 mei het verkeer vanuit het buitenland geblokkeerd. Voor gebruikers in Nederland was DigiD in deze periode beschikbaar. Sinds 2 mei is DigiD ook weer beschikbaar vanuit het buitenland.

2) *DDoS-aanvallen op de website www.rijksoverheid.nl*

Op 7 en 8 mei jl. vond een tweetal aanvallen op www.rijksoverheid.nl plaats. Het effect van de aanval nam in de loop van de tijd af en vanaf woensdagochtend 8 mei jl. was de website weer goed bereikbaar. Direct tijdens de aanval al is de informatievoorziening per telefoon opgeschaald om via aanvullende kanalen bereikbaar te blijven (Informatie van de Rijksoverheid via telefoonnummer 1400)

en is een multidisciplinair crisisteam ingezet. Daarnaast zijn er aanvullende technische maatregelen getroffen. De technische maatregelen waren direct effectief en hebben de eerste aanval afgeweerd. De tweede aanval was na nieuwe aanpassingen snel onder controle, waarna de site weer beschikbaar was. Ook zijn maatregelen getroffen om te garanderen dat de andere kanalen voor publieksvoorlichting (telefoon en mail) doorgang vonden.

3) DDoS-aanvallen op de Belastingdienst

Op donderdagavond 9 mei jl. kreeg het Security Operation Center (SOC) van de Belastingdienst een signaal dat er een DDoS-aanval op www.belastingdienst.nl gestart was. Hierdoor was een groot gedeelte van de diensten onbereikbaar. Daarop zijn vervolgens direct uitwijk- en beschermingsmaatregelen genomen die ertoe hebben geleid dat in het begin van de nacht alle externe stromen, zoals aangiftestromen bij Douane, weer beschikbaar waren. De websites www.belastingdienst.nl, www.douane.nl, www.toeslagen.nl, en mijn.toeslagen.nl waren na een verminderde bereikbaarheid in het begin van de ochtend ondanks de aanhoudende aanval weer goed bereikbaar.