De DDoS Paradox

Ontsluiten door Afsluiten

Bart Jacobs[1]

Als we van banken en andere essentiële dienstaanbieders verwachten dat ze binnen de huidige onbetrouwbare ICT-infrastructuur met een hoge graad van beschikbaarheid en betrouwbaarheid functioneren verdienen ze ook de ruimte om aantoonbare gevaren adekwaat te neutraliseren. Mogelijk gaat daar zelfs een heilzame werking van uit. In onderstaand artikel gaat Bart Jacobs in op de technische kant van de zaak; in het volgende artikel behandelt Eric Tjong Tjin Tai de juridische aspecten.

Een bedrijfsblokkade is een vorm van protest waarbij de toegang tot een bedrijf fysiek onmogelijk wordt gemaakt, bijvoorbeeld doordat demonstranten het toegangshek met een ketting en een zwaar slot vergrendelen of doordat ontevreden werknemers massaal op de toegangsweg gaan zitten. Mogelijk is dat aanleiding voor het bedrijf om te proberen via een juridische procedure opheffing van de blokkade te bewerkstelligen. Een rechter zal daarbij minder snel opheffing van de blokkade gelasten wanneer sprake is van een arbeidsconflict of van een politiek getint protest, en er juist sneller een einde aan maken wanneer het gaat om pure obstructie of vandalisme. Overigens kan de bedrijfseigenaar bij een blokkade zelf beslissen om het bedrijf te sluiten, in de hoop dat de betogers dan spoedig afdruipen. Zoals we zullen zien blijkt een dergelijke zelfgekozen afsluiting in een elektronische context een zeer effectief middel, indien selectief toegepast.

Een *distributed denial of service* (DDoS) aanval is een enigszins vergelijkbare blokkade op de elektronische snelweg van het internet, die ook wel verstikkingsaanval genoemd wordt. Daarbij wordt toegang tot een elektronische dienst, typisch aangeboden via een website, geblokkeerd door het veroorzaken van een verstopping via massale opvraging, en daarmee overbelasting, van de betreffende dienst. Het uitvoeren van zo'n DDoS aanval is een strafwaardige handeling, die omschreven wordt[2] als het belemmeren van de toegang tot of het gebruik van een geautomatiseerd werk door daaraan gegevens aan te bieden of toe te zenden (Sr. 138b).

In de praktijk wordt een DDoS aanval meestal gelanceerd vanuit een *botnet*: een samenwerkend stel besmette computers die centraal aangestuurd worden om eenzelfde website tegelijkertijd te benaderen. Degene die zo'n botnet aanval aanstuurt kan als de dader van de DDoS aanval aangemerkt worden. Het gevolg van een DDoS actie is vaak dat de aangevallen website het aangeboden verkeer niet aankan, 'omvalt', en onbereikbaar wordt voor regulier webverkeer. Daardoor kunnen bijvoorbeeld klanten van een bank hun financiële zaken niet regelen via het internet, of kunnen klanten van een webwinkel een beoogde bestelling niet plaatsen of een geplande reis niet boeken. Nu steeds meer transacties via internet plaatsvinden kan een geslaagde DDoS aanval leiden tot een ingrijpende verstoring van het economische verkeer, met potentieel maatschappelijk ontwrichtende gevolgen.

Een DDoS aanval kan leiden tot een ingrijpende verstoring van het economische verkeer

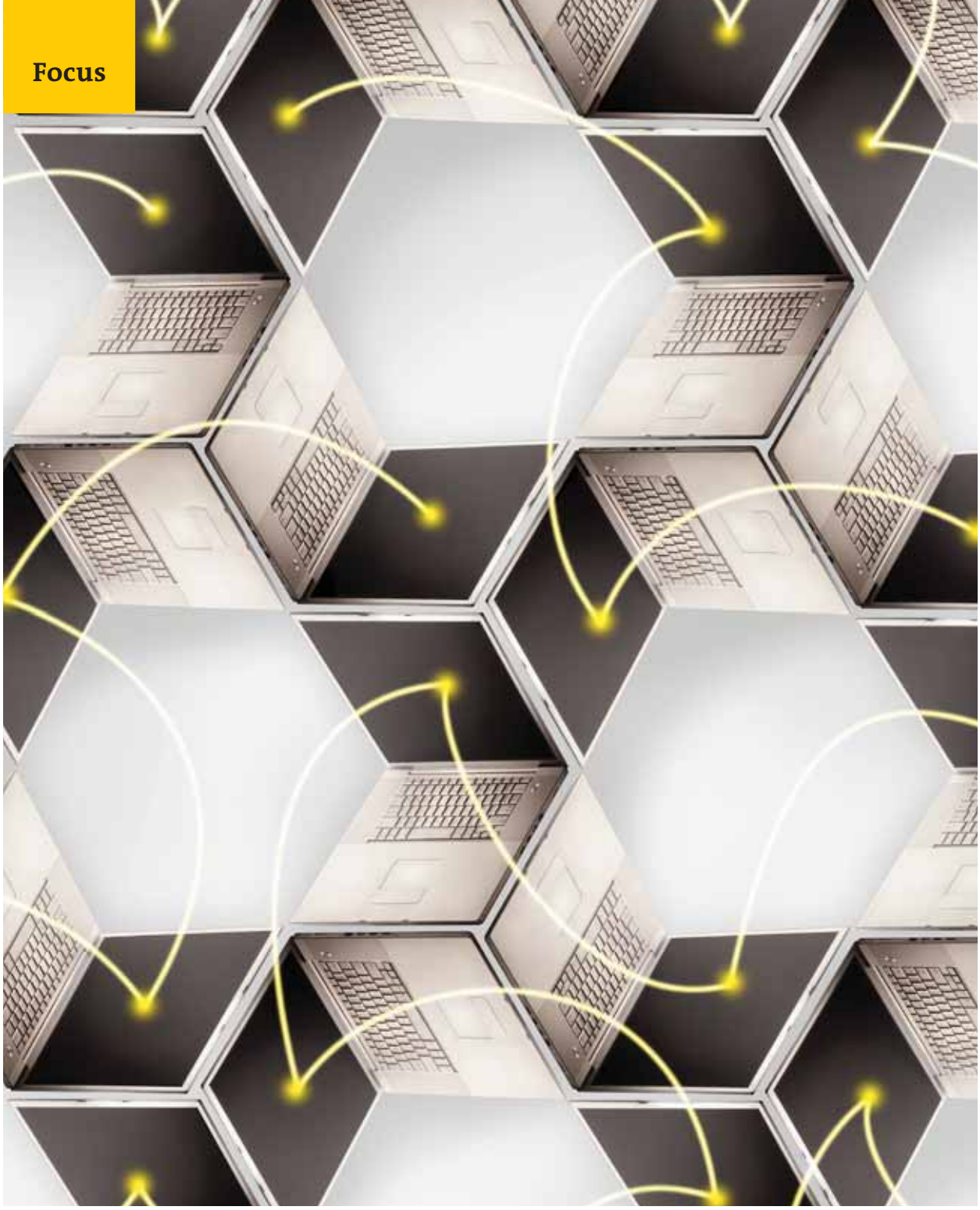
Sinds de grootschalige DDoS aanvallen van april 2013, gericht op banken maar ook op anderen zoals KLM en DigiD, bestaat er grote aandacht voor dit fenomeen. De gebleken kwetsbaarheid wordt breed onderkend, bij bedrijven en overheden (als mogelijke slachtoffers), en in de media en politiek. Algemeen wordt in afkeurende termen over DDoS aanvallen gesproken. Vermeldenswaard is daarbij dat binnen de politieke partij D66 in het voorjaar van 2012 nog serieus gedebatteerd is over een 'recht op DDoSsen'. In lijn met het hierboven genoemde mogelijke politieke/maatschappelijk karakter van bedrijfsblokkades werd het uitvoeren van een DDoS aanval voorgesteld als een vorm van protest die enige vorm van bescherming verdient. Deze kijk op de materie is inmiddels grotendeels verloren gegaan (en wordt ook binnen D66 uiteindelijk niet ondersteund). Toch zijn sommige DDoS aanvallen van de afgelopen jaren duidelijk politiek gemotiveerd. Een voorbeeld is de aanval van de hackersgroep *Anonymous* op de websites van verschillende creditcard bedrijven,

Auteur

1. Prof. dr. B.P.F. Jacobs is als hoogleraar verbonden aan het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen, webadres: www.cs.ru.nl/~bart.

Noten

2. Zie ook: B.J. Koops, *Strafrecht en ICT*, SDU, 2e druk, 2008.



Computernetwerk © Hollandse Hoogte

nadat zij, onder druk van de Amerikaanse overheid, weigerden contributies aan Wikileaks door te geven.

Herkomst van blokkades

Bij een bedrijfsblokkade is het niet vanzelfsprekend duidelijk welke individuen of groeperingen de blokkade uitvoeren. De demonstranten kunnen bivakmutsen of helmen dragen, maar via spandoeken hun opvattingen kenbaar maken. Evenmin hoeven bij een DDoS aanval de daders bekend te zijn. In de meeste gevallen zijn ze dat ook niet, tenzij het daderschap expliciet (en geloofwaardig) geclaimed wordt of duidelijke sporen achtergelaten worden. Bij de eerder genoemde recente aanvallen in Nederland was dat niet het geval. Het politieonderzoek heeft tot nu toe geen duidelijke dadersporen opgeleverd. Een ter zake deskundige kan zijn/haar handelingen op internet goed maskeren. In de fysieke wereld is dat een stuk moeilijker ... maar niet onmogelijk.

Ondanks deze (beperkte) overeenkomst is het verschil tussen een elektronsiche DDoS aanval en een fysieke blokkade aanzienlijk. Bijvoorbeeld, bij een fysieke blokkade zijn de gebruikte middelen direct herkenbaar: een kabel of slot om het hek, of een samengeschoolde menigte. Daardoor kan de blokkade ook met fysieke middelen ongedaan gemaakt worden, bijvoorbeeld door de kabel of het slot door te knippen, of door de menigte te verplaatsen of te verdrijven. Kortom, de door de blokkade getroffene partij heeft in principe de mogelijkheid om de reguliere toegang te herstellen.

Bij een DDoS aanval zijn de gebruikte middelen echter niet goed herkenbaar: het grote probleem bij het afslaan (of 'mitigeren') van een DDoS aanval is dat het

Het grote probleem bij het afslaan van een DDoS aanval is dat het kwaadaardige webverkeer niet of nauwelijks te onderscheiden is van het reguliere verkeer

kwaadaardige webverkeer niet of nauwelijks te onderscheiden is van het reguliere verkeer. Er is zijn op dit moment zo'n twintig verschillende soorten DDoS aanvalstechnieken bekend. Bij een geavanceerde aanval wordt een continu wisselende mix van deze technieken aangewend, om het scheiden van de 'goede' en 'foute' berichten te bemoeilijken. Het vergt op dit moment zo'n grote inzet van middelen om je hier tegen te wapenen dat slechts grote, kapitaalkrachtige partijen zich dit kunnen veroorloven. Bij de recente DDoS aanvallen zijn banken er toe overgegaan het internetverkeer dat op hun webpagina's binnenkomt om te leiden via een speciaal bedrijf dat, via een proces dat met *scrubbing* wordt aangeduid, de kwaadaardige pakketjes eruit filtert. Dit is gespecialiseerd (en kostbaar) werk, dat pas na enige tijd effect heeft. Dit filteren verloopt op weinig subtiele wijze. Een paardenmiddel, dat ook inderdaad gebruikt is, is om al het webverkeer uit het buitenland te blokkeren. Dit soort selectieve afsluitingen blijken zeer effectief: indien de DDoSser merkt dat zijn/haar verkeer tegengehouden wordt, stopt de aanval snel. Dit is de essentie van de DDoS-paradox: juist afsluiting leidt tot ontsluiting.[3]

Overigens leidt het omleiden van het eigen verkeer via een externe (Amerikaanse) *scrubbing* partij tot terechte zorgen met betrekking tot privacy en beveiliging. De voor de eigen website bedoelde gegevens komen hierbij onder andere, onbedoelde jurisdictie, waardoor ze mogelijk binnen het blikveld van buitenlandse diensten geraken. Hierdoor wordt aan het probleem van de beschikbaarheid van de eigen dienst het probleem van vertrouwelijkheid van klantgegevens toegevoegd.

Vragen en observaties

De recente DDoS aanvallen geven aanleiding tot een aantal nieuwe vragen, waarbij we ons hier vooral zullen richten op de bancaire sector. Wie is er aansprakelijk voor de geleden schade (bijv. bij webwinkels)? Waar liggen de verantwoordelijkheden en mogelijkheden voor het tegengaan van dergelijke aanvallen, en hoe kunnen die verantwoordelijkheden (en taken) het beste verdeeld worden tussen publieke en private partijen? Dit artikel pretendeert niet een definitief antwoord te presenteren, maar wil wel achtergrondinformatie en aanknopingspunten bieden voor het vervolg (zie ook het artikel van E. Tjong Tjin Tai elders in dit nummer).

Een eerste observatie is van algemene, infrastructurele aard. De nadruk in de ICT-wereld ligt meer op functionaliteit dan op beveiliging. Een gevolg is dat de programmatuur (software) die gebruikt wordt om communicatie via internet te bewerkstelligen en om computers hun werk te laten doen relatief makkelijk misbruikt kan worden. Het is voor een kwaadwillende niet geweldig moeilijk om, door uitbuiting van fouten in software, een computer van een ander te 'besmetten' met kwaadaardige software en daarmee de controle over die computer, en over alle daarop opgeslagen gegevens, over te nemen. Wanneer deze controle over besmette computers centraal aangestuurd wordt spreekt men van een *botnet*. Er wordt geschat dat rond de 10% van alle PCs in Nederland onderdeel uitmaakt van een of ander botnet,[4] zonder dat de eigenaars zich daar van bewust zijn. Zo'n botnet wordt typisch gebruikt voor het verzamelen van inloggegevens voor fraude-doeleinden, het versturen van ongevraagde e-mail (spam), of het uitvoeren van een DDoS aanval. Het verminderen van de kwetsbaarheid van de software op onze computers is dus de meest fundamentele manier om zulke DDoS (en andere) aanvallen tegen te gaan. Het is echter niet realistisch veel verbetering op dit gebied te verwachten, onder andere omdat 1. aansprakelijkheid voor gebrekkige software in de praktijk niet functioneert, bijvoorbeeld via uitsluitingen in algemene voorwaarden, en omdat 2. de ICT-markt primair gericht is op het prematuur uitbrengen van producten om zo snel mogelijk een groot marktaandeel te verwerven en zo klanten aan zich te binden (het creëren van een *customer lock-in)*; verbetering en beveiliging van (de software van) deze producten is van secundair belang. Ondanks het feit dat op dit gebied weinig te verwachten valt, is het goed voor ogen te houden waar de werkelijke oorzaak van de problemen ligt.

Een tweede observatie betreft het bestrijden van botnets. Op dit gebied zijn enkele justitiële successen te melden, waarbij ook in Nederland botnets ontmanteld zijn (bijvoorbeeld in de zogenaamde BredoLab zaak van eind 2010). Echter, dit uit de lucht halen van botnets is een moeizame, arbeids- en kennis-intensieve aangelegenheid doordat botnets zich voortdurend ontwikkelen, bijvoorbeeld via gedistribueerde, versleutelde aansturing, en moeilijker verstoord of opgerold kunnen worden. Het *runnen* van een botnet heeft zich ontpopt als een eigen economische activiteit, waarbij botnet-capaciteit tegen betaling beschikbaar is. Als gevolg zullen opgerolde botnets snel hersteld of vervangen worden. Ook de daders, als het al lukt ze te achterhalen en op te pakken, zijn snel vervangen.

Een alternatieve benadering richt zich op de besmette computers in een botnet. Wanneer eenmaal ontdekt is dat een computer besmet is, bijvoorbeeld omdat die computer spam verstuurt of DDoS-aanvallen uitvoert, kan de computer 'in quarantaine' geplaatst wor-

3. Voor meer informatie, zie de factsheet *Continuïteit van onlinediensten* (mei 2013) van het Nationale Cyber Security Centrum, beschikbaar via de website ncsc.nl.

4. Zie de studie in opdracht van het Ministerie van Economische Zaken: M. van Eeten, H. Asghari, J. Bauer, S. Tabatabaie, *Internet Service Providers and Botnet Mitigation. A fact-finding study on the Dutch Market*. TU-Delft, jan. 2011. Dit rapport vermeldt een percentage van 5-10% besmettingen als onderschatting, op basis van een beperkt aantal besmettingsvormen. Commerciële partijen op het gebied van computerbeveiliging noemen vaak hogere percentages. Precieze cijfers zijn moeilijk te verkrijgen.

den door de betreffende internet (service) provider ('ISP'). Daarbij worden verbindingsmogelijkheden van deze computer tot een minimum beperkt, waarbij eigenlijk alleen nog een website bereikbaar is waar informatie (en software) beschikbaar is om de besmetting ongedaan te maken. Deze quarantaine-aanpak wordt hier en daar gebruikt, bijvoorbeeld in universitaire omgevingen (waaronder studentenflats, die vaak berucht zijn om hun creatieve computergebruik). De aanpak kan zeer effectief zijn, maar kan ook tot aanzienlijke frustratie aanleiding geven, met name bij de tijdelijk afgesloten gebruiker. Ook wordt de nodige inzet van de ISP vereist, in het omgaan met boze of niet-begrijpende klanten. ISPs zullen hierbij voorzichtig te werk willen gaan, want een onterecht in quantaine geplaatste klant kan mogelijk zo ontevreden zijn dat hij/zij overstapt naar een andere provider. De grote commerciële ISPs zijn daarom terughoudend over het in quarantaine plaatsen van de besmette computers van hun klanten. Het kost hen geld en moeite en leidt tot ontevreden klanten, terwijl de grote voordelen elders liggen. Toch valt hier veel verbetering te halen, temeer daar inmiddels duidelijk geworden is[5] dat er grote verschillen bestaan tussen de ISPs onderling, in de percentages besmettingen in hun netwerk (oplopend tot een factor vijf).

Naast zulke opschoningsoperaties bij eindgebruikers kunnen ISPs er zelf voor zorgen dat er geen 'onjuiste' berichten door hun netwerken stromen. Het blijkt dat veel van de nepberichten die bij DDoS aanvallen op het doel afgestuurd worden onjuist in elkaar steken. Typisch is er sprake van 'spoofing', waarbij het adres van de afzender dat in het DDos bericht staat niet overeenkomt met het daadwerkelijke adres van de (besmette) computer die het bericht verstuurd heeft. ISPs kunnen zulke onjuistheden herkennen en de onjuiste berichten blokkeren (dit heet 'egress' filtering). In Nederland doen alle grote providers dit inmiddels, maar in het buitenland zijn er nog veel providers die dergelijke onjuiste berichten wel doorlaten. Internationale druk en afspraken kunnen helpen de situatie te verbeteren, waarbij de overheid een belangrijke rol speelt.

Tenslotte mag van gewone computergebruikers verwacht worden dat zij gebruik maken van software die up-to-date is en van virusscanners. Echter, de effectiviteit van zulke scanners is beperkt doordat ze alleen bekende kwaadaardige software tegen kan houden, en doordat dergelijke software vaak in nieuwe, steeds wisselende vorm opduikt. Daarbovenop is er een markt ontstaan in nog-niet-bekende kwetsbaarheden, de zogenaamde *zero-day-exploits,* vanwege hun waarde bij het uitvoeren van criminele of strategische cyberaanvallen. Omdat de softwareproblemen van structurele aard zijn, zal het aanpakken van structurele oplossingen meer effect hebben dan het 'opvoeden' van gebruikers die in feite niks aan de problemen kunnen doen. Een basisregel is: leg de verantwoordelijkheid bij die partij die ook daadwerkelijk dingen kan bewerkstelligen. In lijn daarmee is een trend waarneembaar waarbij beveiliging vanuit de infrastructuur geregeld wordt, vaak zonder veel sturing of invloed van de individuele eindgebruiker.

Banken en DDoS

Met deze informatie in het achterhoofd zijn we bij de banken aangeland. Het verlies van de beschikbaarheid van (elektronische) bancaire diensten is bij de recente DDoS-aanvallen door de banken aangeduid als 'overmacht'. Dit is zonder meer een te eenvoudige voorstelling van zaken. Het is goed te bedenken dat internetbankieren veel voordeel oplevert voor banken: waar zij vroeger de handgeschreven bankoverschrijvingen moesten overtypen en in hun systemen moesten invoeren, verzorgen wij als klanten die invoer nu zelf. Dit alleen al levert een enorme kostenbesparing op. Voor banken heeft het gebruik van internet als communicatiekanaal met de klanten dus grote voordelen. Echter, in de loop van de jaren is de omvang van kwaadaardige activiteiten op internet gegroeid. Nu er feitelijk geen weg terug is naar de oude overschrijfkaart zullen banken hun verdedigingslinies adekwaat moeten versterken. Dit is een dynamisch proces, waarbij grote investeringen gemoeid zijn in detectie en responscapaciteit. Bij eerdere gelegenheid[6] zei auteur dezes hierover: wanneer je zelf besluit je eigen cruciale operaties naar het wilde westen van het internet te verplaatsen moet je natuurlijk wel zorgen dat je eigen pistolen groot genoeg zijn!

Banken zijn zich hier terdege van bewust en investeren voortdurend en systematisch in de beveiliging van hun internetdiensten. Ook hebben zij onderling regelmatig overleg over beveiligingsrisico's (het zogenaamde FI-ISAC beraad) waarin ze elkaar informeren en waarschuwen. Banken hebben een direct belang bij adekwate beveiliging en hoge beschikbaarheid van hun diensten. Nederlandse banken behoren met hun niveau van beveiliging tot de internationale voorhoede, bijvoorbeeld in het vroege gebruik van *two-factor* authenticatie bij internetbankieren, waarbij login en wachtwoord niet voldoende zijn, maar een eenmalige code, liefst gerelateerd aan de transactie, via een apart kanaal of apparaatje gebruikt dient te worden. Dat wil echter niet zeggen dat banken altijd de juiste besluiten nemen en dat zij altijd een evenwichtige afweging maken tussen hun eigen belang en het belang van hun klanten (zowel particulier als zakelijk). De dynamiek van het proces maakt ze echter moeilijk aanspreekbaar op de details ... die er terdege toe doen.

Ter illustratie van zulke details: de infrastructuur van het iDeal systeem dat in Nederland veelvuldig gebruikt wordt voor betalingen bij webwinkels was aanvankelijk vervlochten met de infrastructuur voor internetbankieren. Het gevolg was dat bij verschillende aanvallen op internetbankieren, ook iDeal onderuit ging, met schade voor webwinkeliers tot gevolg. Inmiddels zijn deze twee systemen, zover bekend, ontvlochten. Het lijkt erop alsof aanvankelijk over deze, op zich verstandige, scheiding onvoldoende nagedacht is door de ICT-architecten van de banken. Maar mogelijk ook is het nut van zo'n scheiding wel gezien, maar werden de kosten ervan in eerste instantie te hoog geacht. Een ander voorbeeld: zoals eerder genoemd is het afsluiten van webverkeer uit het buitenland een effectieve manier om een DDoS aanval te mitigeren. Dit is wel gedaan bij een aanval op DigiD, maar niet bij aanvallen op banken. De reden is dat banken hiermee ook de communicatie zouden afsluiten met hun eigen buitenlandse kantoren, waardoor bijvoorbeeld actuele informatie van de internationale beurzen niet goed verwerkt kan worden. Een oplossing hiervoor is conceptueel

simpel: communiceer met je filialen via een eigen afgesloten netwerk dat niet kwetsbaar is voor DDoS aanvallen. Zulke besloten netwerken bestaan, zoals GemNet voor de gemeentelijke overheden in Nederland, maar vereisen extra investeringen.

(Overigens leidde de afsluiting van buitenlands verkeer bij de DDoS aanval op DigiD ook tot verbreking van communicatie met verwerkingskantoren buiten Nederland, maar die uitwisseling werd minder (tijd)kritisch geacht dan bij banken en kon mogelijk ook via andere kanalen opgevangen worden.)

Bescherming tegen DDoS

Gegeven het grote belang van de beschikbaarheid van snelle, betrouwbare elektronische verrekeningen mogen we verwachten dat de banken zeer ver gaan in het bewerkstelligen van die beschikbaarheid. Het is daarvoor zinvol om de 'up-time' van voldoende capaciteit onafhankelijk te meten en te publiceren, zoals heel gebruikelijk is in bijvoorbeeld de elektriciteitssector. Tegelijkertijd moeten we ons realiseren dat internet een zeer dynamisch, slecht voorspelbaar speelveld vormt. Dat is voor iedereen een probleem en kan dus geen excuus vormen voor een specifieke sector. Hieronder worden de twee belangrijkste algemene (niet-technische) regels[7] genoemd die van belang zijn bij het tegengaan van DDoS-aanvallen, niet alleen voor banken.

1) Zorg dat de eigen infractuur robuust is, niet alleen in de zin dat een flinke fluctuatie in het webverkeer niet tot instabiliteit leidt, maar ook dat onderlinge systeemafhankelijkheden tot een minimum beperkt zijn. Hierdoor kan voorkomen worden dat de overbelasting en uitval van de ene dienst de uitval van een ander dienst tot gevolg heeft.
2) Zorg dat het inkomende webverkeer selectief en dynamisch afgeknepen kan worden, zonder dat dit effect heeft op de eigen noodzakelijke interne communicatie (mogelijk door daarvoor een apart gesloten netwerk te gebruiken). Voor de hand liggend selectiecriteria bij het afsluiten zijn 'verkeer uit het buitenland' of 'verkeer van buiten Europa'. Hiervoor moeten de eigen fire-walls, of die van ingehuurde partijen, voldoende flexibel ingesteld staan.

Dit afknijpen van bepaalde verkeersstromen hoeft niet noodzakelijkerwijs in de vorm van totale afsluiting. Het kan bijvoorbeeld ook plaatsvinden door gebruikers eerst een zogenaamde *captcha*[8] te laten beantwoorden, waarbij een paar woorden overgetypt moeten worden. De voorbeeldtekst wordt daarbij op een zodanige wijze vervormd dat automatisch lezen door een computer (van de aanvaller) praktisch onmogelijk is.

Een aanvullende, nieuwe optie is om bij hevige aanvallen en uitval van dienstverlening ook binnen Nederland selectief inkomend verkeer af te sluiten, door bijvoorbeeld al het verkeer van provider X of Y af te knijpen, terwijl het verkeer van andere providers de eigen systemen wel kan bereiken. Zulke vergaande stappen zullen, indien toegepast, op transparante wijze uitgevoerd moeten worden, op basis van heldere, toetsbare criteria. Een hoog aantal besmette computers in het netwerk van provider X kan bijvoorbeeld een goede reden zijn voor een hoge positie in de volgorde van af te knijpen providers. Dit zou kunnen leiden tot nieuwe incentives, waardoor providers er belang bij hebben om hun netwerk zo veel mogelijk vrij van besmettingen te houden, bijvoorbeeld via quarantaine, en waardoor klanten bereid zijn wat meer te betalen voor een 'goede' provider,

Als we banken willen aanspreken op hun zorgplicht, zullen we moeten accepteren dat ze ook streng voor ons zijn

die zijn netwerk schoon probeert te houden en daardoor niet zo snel afgesloten wordt. Dergelijke selectieve afsluitscenario's voor noodgevallen bestaan overigens al lang in andere sectoren, zoals de telecom. Kortom, als we banken willen aanspreken op hun zorgplicht, zullen we moeten accepteren dat ze ook streng voor ons zijn.

Vanuit civielrechtelijk perspectief speelt de driehoek van banken-webwinkels-providers een rol. Zelfs als een bank alle maatregelen heeft genomen die op dit moment vanuit het oogpunt van beveiliging en beschikbaarheid redelijk zijn, dan nog moet er bij een zware DDoS aanval rekening mee gehouden worden dat zo'n bank minstens enkele uren nodig heeft om de aanval te kunnen pareren en de eigen diensten (weer) beschikbaar te hebben voor een groot deel van de klanten. Van een webwinkel mag daarom verwacht worden dat daar in de eigen bedrijfsvoering rekening mee gehouden wordt, bijvoorbeeld door verschillende betaalmogelijkheden te ondersteunen (niet aleen iDeal, maar ook credit cards, PayPal en mogelijk nog meer) en door bij een DDoS aanval op die betaalmiddelen de eigen klanten de mogelijkheid te bieden om betalingen van bestellingen enige tijd uit te stellen. Ondertussen neemt de maatschappelijke druk op providers toe om actie te ondernemen tegen besmette computers in hun eigen netwerken. Omdat de grote voordelen van zulke actie elders liggen zullen providers hierin zowel aangespoord als geholpen moeten worden. In verschillende landen (Duitsland, Australië, Japan, Korea) bestaat een actieve vorm van publiek-private samenwerking, bijvoorbeeld in de vorm van een *clearing house*, dat zorgt voor detectie, melding en opschoning van besmette computers.[9] De ernst van de DDoS incidenten in het voorjaar van 2013 toont het belang van vergelijkbare Nederlandse initiatieven, in de vorm van de eind 2012 gestartte *Abuse Information Exchange*. •

5. Zie het Delftse rapport in de vorige voetnoot.
6. In de uitzending van *Nieuwsuur* op 25 april 2013.
7. Zie de eerder genoemde NCSC factsheet voor meer gedetailleerde aanbevelingen.
8. De term captcha is een afkorting van: computer animated picture for telling computers and humans apart.
9. Zie het in een eerdere voetnoot genoemde Delftse rapport.