Gespreksnotitie rondetafelgesprek met Tweede Kamerleden aangaande online betalingsverkeer

C. Verhoef

VU Amsterdam, Department of Computer Science,
De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands

x@cs.vu.nl

25 mei 2013

1 Achtergrond en aanleiding

De vaste commissie voor Financiën uit de Tweede Kamer der Staten-Generaal heeft besloten een rondetafelgesprek te organiseren met als onderwerp het online betalingsverkeer. Meer specifiek is het doel om beter zicht te krijgen in welke mate de beveiliging en beschikbaarheid van financiële transacties via Internet geborgd is. Over oorzaken van recente storingen en de informatievoorziening tijdens en na storingen zijn vragen gesteld.

Het rondetafelgesprek vindt plaats ter oriëntering van leden van de vaste commissie op de problematiek rond online betalingsverkeer. De agenda van deze ronde tafel kent een viertal blokken: Belanghebbenden, ICT, Banken en Toezichthouders. Tijdens het rondetafelgesprek willen de Kamerleden kennisnemen van mijn visie op de ICT-kant van de zaak.

2 Visie en advies

Als bedrijven onverantwoord handelen, gaan ze vroeg of laat failliet. Tegelijkertijd laat de Nederlandse overheid systeembanken niet failleren als hun financiële positie daartoe eigenlijk wel noopt. Dat betekent dat het bankwezen een speciale plaats in blijkt te nemen tussen andere bedrijven.

Betalingsverkeer is de smeerolie van onze economie. Dat wordt meer en meer online gedaan. Als banken financieel onverantwoord handelen, houdt de Nederlandse overheid ze het hand boven het hoofd. Als ze technisch onverantwoord handelen, laat de overheid ze dan wel vallen?

Als het antwoord daarop ontkennend is, dan is mijn advies om toezicht op de techniek bij banken in te stellen dan wel flink te versterken en proactief te maken, zodat transparant wordt hoe het staat met de technische kant van de bancaire systemen naast hun financiële houdbaarheid. Denk aan: welke verbetermaatregelen in welk tempo worden doorgevoerd. Toestemming voor verstrekkende technische besluiten behoort tot de mogelijkheden. Denk aan: alle IT gaat naar India. Of: we gooien 1500 IT-ers de deur uit. Het zal ongetwijfeld kosten besparen maar is het wel verantwoord? Of deze: we gaan 100 miljoen investeren in een geheel nieuw systeem. Is dat wel reëel?

Een toezichthouder (DNB) is hier al deels mee bezig, denk bijvoorbeeld aan het verbod om cloud diensten af te nemen zonder "the right to examine" door de DNB. Dit zou verder mogen worden uitgebreid met zaken die de technische kant in het algemeen betreffen en die verstrekkende gevolgen kunnen hebben op de operatie binnen de banken. Cyber security hoort daar nadrukkelijk bij.

Een volgend advies is om zich terdege af te vragen of de Nederlandse overheid wel genoeg investeert in de bestrijding van cyber-aanvallen op de kritische IT-infrastructuur (zowel privaat als collectief). De Israelische Nissim Bar-El (CEO van Comsec) geeft in een recente Brandpunt[1] uitzending aan dat de huidige investering van Nederland een lachertje is. Hij geeft aan dat Europese banken kwetsbaar zijn. Kwetsbaarder dan Amerikaanse banken en zeker kwetsbaarder dan Israelische banken. Volgens Nissim Bar-El is een aanpak vanuit de top van de Nederlandse overheid onontbeerlijk met voldoende fondsen. Nissim Bar-El lacht de 4 tot 5 miljoen Euro weg die Nederland investeert. In Isreal is het 750 miljoen dollar. In de VS doet Obama er dit jaar 225 miljoen dollar bovenop en voor het volgende fiscale jaar is het voorstel 13 miljard dollar uit te trekken voor cyber security ofwel 16% van het federale IT-budget[2].

Nevenstaand is het advies om te voorkomen dat grote hoeveelheden persoonsgegevens bekend worden, bijvoorbeeld door slecht ontworpen systemen van aller aard. Zonder e-mailadressen of telefoonnummers van klanten van een bank heeft een DoS-aanval om hun rekeningen leeg te plunderen namelijk weinig zin. Het College Bescherming Persoonsgegevens doet wat ze kan, maar kennelijk is er meer nodig: meer mensen, meer geld, meer kennis, meer kunde. En zij zit aan de achterkant, dus het is dweilen met de kraan open. Die kraan moet dicht, en een keuringsinstituut vanuit de overheid zou een mogelijkheid kunnen zijn. Generieke regels zoals een IT-bouwbesluit zijn het overwegen waard. Waar een civiele constructie aan basale veiligheidsvoorschriften moet voldoen alvorens een omgevingsvergunning wordt verstrekt (vanuit het bouwbesluit), valt te denken aan een IT-bouwvergunning nadat is gebleken dat privacy, security, beschikbaarheid, safety en andere vitale generieke aspecteisen van een (deels) virtuele constructie voldoende zijn uitgewerkt.

3 Kernvragen

We behandelen een paar van de kernvragen die de vaste commissie heeft gesteld die de ICT kant het meeste raken.

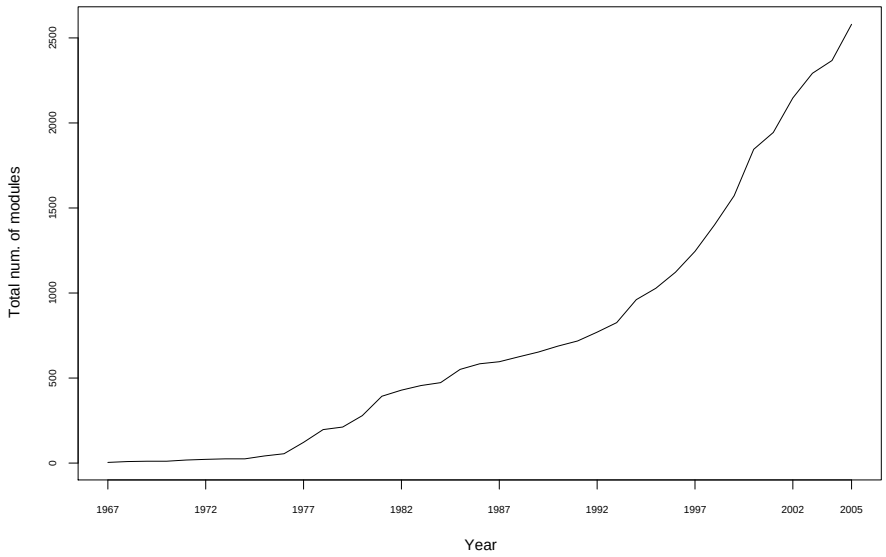
3.1 Ontwikkelingen online betalingsverkeer

vraag Wat zijn de laatste ontwikkelingen in het online betalingsverkeer? Welke nieuwe vormen van betalen worden ontworpen, welke ICT-ontwikkelingen vinden plaats en wat zijn de bijbehorende veiligheidsrisico's?

reactie Er zijn allerlei ontwikkelingen, zowel binnen als buiten de gebaande paden. We geven daarvan een schets weer plus kansen en risico's.

[1] http://brandpunt.kro.nl/seizoenen/2013/afleveringen/28-04-2013/fragmenten/veiligheid_uit_israel

[2] http://articles.washingtonpost.com/2013-04-14/business/38537681_1_budget-proposal-cyber-federal-agencies



Figuur 1: De groei van back-office modules over de jaren van een omvangrijke IT-portefeuille uit de financiële sector

bancaire systemen Allereerst de bancaire systemen. Die bestaan over het algemeen uit front- & back-office systemen. De *achterkant* bestaat meestal uit een combinatie van oude en nieuwe gedeeltes waarbij de oude kern over het algemeen minder gevoelig is voor falen. Bij software geldt ruwweg: ouder is beter, omdat in de loop der decennia door falen, de fouten er meer en meer uitgehaald zijn. Om de vaste commissie een beeld te geven van de groei van dergelijke bancaire IT-portefeuilles geven we daarvan een indruk weer in Figuur 1. Deze figuur is overgenomen van een publicatie van Kwiatkowski en Verhoef getiteld *Recovering management information from source code*. Wat goed te zien is, is dat delen van de IT-portefeuille uit de zestiger jaren van de vorige eeuw stammen en dat door de jaren heen het aantal bestanden met broncode daarin een fikse groei door heeft gemaakt. Er is hier sprake van een evolutionair pad naar vernieuwing: voortbouwen op wat er is en dat verder uitbreiden. Probleem bij dat soort systemen is dat de beschrijving van wat ze precies doen vaker dan eens ontbreekt, dat documentatie die er (nog) is niet meer de huidige werkelijkheid reflecteert, kortom de bedrijfslogica is als het ware versleuteld in de broncode.

De voorkant is hetgeen dat soms revolutionair tot stand komt: geheel en al nieuw. Daar zitten meestal, maar niet altijd, de problemen waar de klant iets van merkt. De afhandeling van een betaling wordt veelal uitgevoerd door de back-office systemen waarbij vooral de aanleiding van een transactie door de jaren heen is veranderd. Een loketbeambte bij de bank, een acceptgiro vanuit het buitenland, een geld-automaat van de bank, een point-of-sale terminal in de supermarkt, een internet betaling via de bank's website, een iDeal betaling van een webwinkel, een mobiele betaling voor een kroketje uit de muur. Allemaal hebben ze gemeen dat ze uiteindelijk inprikken op diezelfde back-office systemen waar de uiteindelijke transactie mee uitgevoerd en geboekt wordt. Ze hebben ook gemeen dat het vaak om disruptievere innovaties gaat dan in de back-

office. Van loket naar automaat. Van acceptgiro naar Internet.

De risico's van bancair betalingsverkeer zitten zoals gezegd veelal aan de voorkant. Daar zit ook de nieuwigheid waardoor kwaadwillenden misbruik kunnen maken van fouten. Dat kunnen kinderziektes zijn, maar het kan ook gaan om onvoldoende kwaliteit van besluitvormer tot projectleider en van programmeur tot tester. Als die systemen worden uitbesteed bijvoorbeeld naar lage lonenlanden, dan kunnen kwaadwillenden kennis opdoen van de interne werking van die systemen en dat eventueel uitbuiten. En dan krijg je ook risico's aan de back-office kant. Zo is onlangs 35 miljoen dollar buitgemaakt door de limieten van een aantal betaalpassen uit het Midden-Oosten uit te zetten. Dat doe je meestal in de back-office systemen. De bende pinde binnen enkele uren wereldwijd 36000 keer[3].

Bitcoins Je kunt een gulden maar een keer uitgeven gaat het gezegde. Voor digitaal geld is dat niet vanzelfsprekend. Een Bitcoin is een alternatief en relatief nieuw betaalmiddel. Dat is werkelijk digitaal geld, waar geen bank of centrale instantie aan te pas komt. Bitcoins zijn voorgesteld om het zogenaamde *double-spending problem* op te lossen zonder een centrale toezichthoudende instantie. Digitaal geld kun je kopiëren zoals een file: dus je kunt het twee keer uitgeven! Een door iedereen vertrouwde centrale instantie kan bijhouden hoeveel er van wat is, zodat je je digitale gulden nog steeds maar een keer kunt uitgeven. Maar die instantie kan zelf falen, bijvoorbeeld door een DoS-aanval. Hoe decentraliseer je digitaal geld zonder dat je het twee keer kunt uitgeven? Bitcoins geeft daar een antwoord op. Er is een kleine gemeenschap begonnen met transacties in deze currency.

Q coins, Linden dollars Wie weet nog van Second Life? Daar heb je Linden Dollars, uitgegeven door de makers van Second Life. Je hoort niet veel meer van Second Life.

Q Coins zijn ook een betaalmiddel dat door een bedrijf wordt uitgegeven. In het westen kent niet iedereen deze currency, maar in China des te meer. QQ is een instant messaging systeem met bijna 800 miljoen actieve accounts rond maart 2013. Deze Q coins worden uitgegeven door het bedrijf dat de QQ software maakt. Dit virtuele geld wordt door QQers gebruikt om reële transacties te doen, maar was bedoeld om net als in Second Life virtueel zaken te doen. De Chinese Centrale Bank heeft deze vorm van digitaal geld aan banden gelegd omdat dit wel degelijk vormen ging aannemen: witwassen, criminaliteit, prostitutie, beïnvloeding van de reële munt.

De risico's van alternatieve volledig digitale betaalmiddelen ontstijgen beveiliging en beschikbaarheid. De reële economie kan erdoor worden geraakt bijvoorbeeld doordat het de koers van een munt gaat beïnvloeden zoals met de Q coin het geval was. Naast deze risico's is het nuttig om na te pluizen of de technologieën achter dit soort betaalmiddelen kunnen worden ingezet om de beveiliging van reëel geld dat online vloeit verder te kunnen borgen. Als transacties zonder centraal punt kunnen worden uitgevoerd dan heb je het probleem van de DoS-aanval opgelost. Zitten er weer andere nadelen aan gedecentraliseerd digitaal geld? Hoe dit allemaal zou kunnen werken moet dan worden uitgezocht.

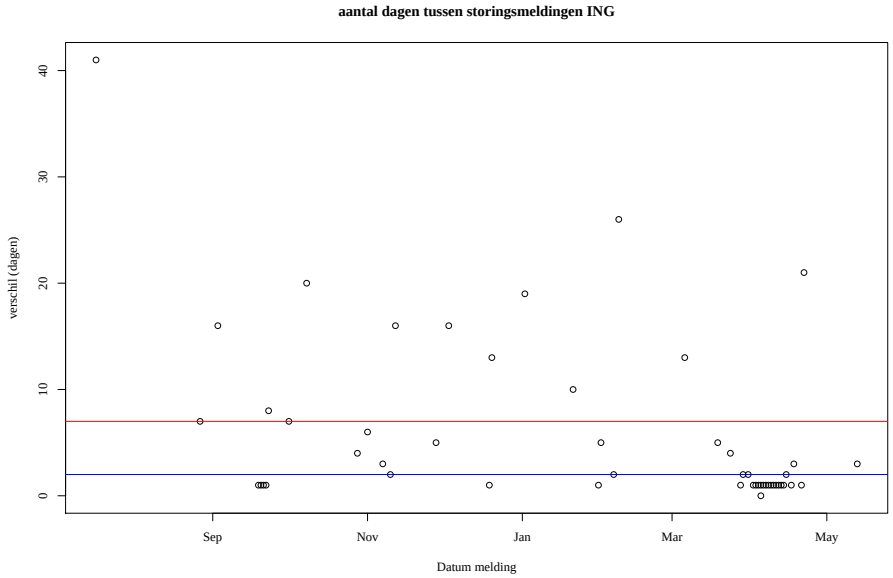
3.2 Recente storingen

vraag Welke oorzaken van storingen in het betalingsverkeer kunnen worden onderscheiden? Welke komen het meeste voor? En wat zijn de oorzaken van de recente

[3] urlhttp://nos.nl/op3/artikel/505253-bankoverval-20-roven-zonder-wapens.html

storingen in het bijzonder?

reactie Er is onvoldoende transparantie over de oorzaak van storingen in het betalingsverkeer. Er zijn sites die overal en nergens vandaan hun informatie verzamelen en op die manier te weten komen dat er sprake is van storingsmeldingen. Vervolgens is het onduidelijk hoe we—en of we—oorzaken te weten komen. Een issue dat van belang is voor de Tweede Kamerleden is om zich dit te realiseren. Ook frequenties van bepaalde storingen weten we alleen omdat er door klanten ruchtbaarheid aan gegeven wordt. Niet omdat de bedrijven in kwestie zelf alle kleine en grote storingen snel en vrijwillig melden.



Figuur 2: Overzicht van de storingsmeldingen over de tijd uitgezet tegen het aantal dagen tussen meldingen op basis van allestoringen.nl

In Figuur 2 hebben we op basis van de website allestoringen.nl een overzicht gemaakt van alle storingsmeldingen van ING. We leggen de figuur uit. Horizontaal staat de tijd uitgezet. Die loopt van juli 2012 tot en met mei 2013. Verticaal staat het aantal dagen dat tussen storingen zit. Helemaal linksboven in de figuur zit een punt op 17 juli 2012 en dat staat 41 dagen hoog. Kortom: de storingsmelding daarna is pas 41 dagen later (op 27 augustus 2012). De blauwe lijn is de mediaan: 50% van het aantal dagen dat tussen storingsmeldingen zit is korter dan twee dagen en 50% is hoger dan twee dagen. De rode lijn is het derde kwartiel: in 75% van de gevallen zit maximaal zeven dagen tussen opeenvolgende storingsmeldingen. Dat is wekelijks. De vraag die je je als overheid moet stellen is of dergelijke niet geplande onbeschikbaarheid acceptabel is voor dergelijke virtuele bouwwerken.

paasweekend Wat opvalt aan Figuur 2 is dat er twee verdichtingen zijn in de laagte: dat zijn twee reeksen kort op elkaar volgende storingsmeldingen. We pakken de recente reeks aan storingsmeldingen bij de kop. Op goede vrijdag 29 maart 2013 wordt

op de website allestoringen.nl aan het einde van de werkdag om 18:02 een storing gemeld. Goede vrijdag is meestal een dag dat banken dicht zijn. Wellicht is men bezig met onderhoud waardoor een storing is ontstaan. We weten dat echter niet want er is onvoldoende transparantie.

Dan volgt op zondag 31 maart 2013 rond 00:48 nog een storingsmelding op de net genoemde site. Er is geen oorzaak bekend. Het kan om onderhoud gaan wordt gesteld op de site. Een feit is dat het een dag is dat banken dicht zijn en dat zijn uitgelezen dagen dat, als je geen boekingen doet, je een window hebt voor onderhoud en beheer. Op dinsdag 2 april en woensdag 3 april zijn er weer meldingen van storingen. Bij de melding op 3 april wordt opgemerkt dat er transacties niet zijn verwerkt op tweede paasdag (maandag). Dat laatste zou betekenen dat er inderdaad geen boekingen gedaan worden op tweede paasdag bij ING. We nemen op basis hiervan aan dat er vanaf goede vrijdag geen boekingen gedaan zijn, waardoor de betaalrun die na deze periode zal gaan lopen in de back-office veel omvangrijker dan normaal wordt. Alle boekingen van vrijdag, zaterdag, zondag en maandag (tweede paasdag) zijn opgespaard.

driemaal is scheepsrecht Van een ING-klant kreeg ik door dat hetzelfde bedrag drie keer afgeschreven was waar dat maar één keer had gemoeten. Daaruit is af te leiden dat er bij de waarschijnlijk bijzondere betaalrun minstens twee keer iets fout gegaan moet zijn. Immers, bij de eerste keer gaat iets fout en wordt het bedrag afgeschreven, dan gaat men het overnieuw doen, en dan gaat er weer iets fout, en tenslotte draait men de betaalrun nog eens. Dat veroorzaakt dan drie keer afschrijven. Het vermoeden is dat de omvang van de betaalrun bijzonder was en dat een in het verleden bepaalde drempelwaarde die normaliter altijd voldoet, door de bijzondere omvang ergens is overschreden. Denk aan een maximaal aantal computercycles dat wordt overschreden (MIPS), een maximale doorlooptijd per transactie (is het te lang dan zal er wel iets in kringetjes ronddraaien, denk aan AICA ABENDs), een maximale doorlooptijd voor het proces (als het om 1 uur in de middag nog runt zal er vast iets fout zijn en breken we het programma af), een maximaal aantal transacties per betaalrun, enzovoort.

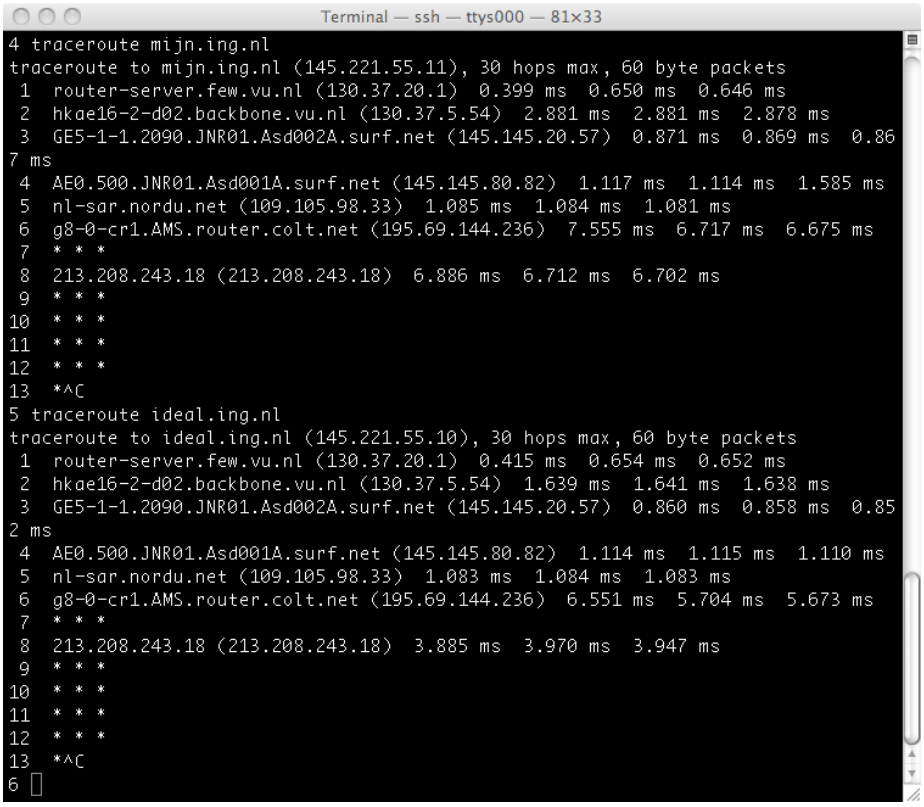
De tweede fout kan van alles en nog wat wezen, maar zal met aan zekerheid grenzende waarschijnlijkheid gecorreleerd zijn aan de eerste fout. Bijvoorbeeld een operator kent een bepaalde drempelwaarde niet, domweg omdat die nooit bereikt wordt. Of door paniek, onderbezetting of onvoldoend ervaren personeel is een herstelprocedure onvoldoende opgevolgd met dezelfde of een andere fout tot gevolg. Of de betaalrun is *even snel* handmatig herstart met een ongewenst effect. Hoe het ook zij, voor de Tweede Kamerleden is het van belang om zich te realiseren dat we in het duister tasten over de precieze gang van zaken omdat transparantie onvoldoende is afgedwongen.

flash crowd Omdat de storing via sociale media bekend werd, is als gevolg van dat lopend vuurtje een zogenaamde flash crowd opgetreden. Een flash crowd is een DoS-aanval maar dan van de eigen klanten. Doordat steeds meer mensen te horen kregen dat er saldi niet klopten, ging iedereen kijken op de eigen rekening. Met als gevolg dat de klanten van ING niet meer bij hun account konden. Een flash crowd schijnt vaker voor te komen dan een DoS-aanval aldus RFC4732 van de Internet Architecture Board uit november 2006:

> A general problem with DoS defense is that it is not in principle possible to distinguish between a flash crowd and a DoS attack. Indeed, having your site taken down by a flash crowd is probably a more common experience than having it DoS-ed – so common it has acquired its own names: being

> Slashdotted or Farked, after the web sites that are common sources of flash crowds. Thus, the first line of defense against DoS attacks must be to provision your service so that it can handle a foreseeable legitimate peak load. Underprovisioned sites are the easiest to take down.

In dit geval was het niet slashdot of fark.com die de aanleiding gaven tot onbeschikbaarheid, maar het waren de social media gevoed door de storing bij ING in de back-office. Kortom, die back-office storing heeft een probleem in de front-office geïnduceerd. De net aangehaalde RFC4732 die handelt over "Internet Denial-of-Service Considerations" geeft duidelijk aan dat je een legitieme peak load aan zou moeten kunnen. Hier is—klaarblijkelijk—ook weer een in het (recente) verleden bepaalde drempelwaarde van het maximale aantal simultane gebruikers van de website ingeschat waar aantoonbaar onvoldoende rekening is gehouden met een flash crowd.



Figuur 3: De routes naar mijn.ing.nl en ideal.ing.nl hebben een identiek verloop.

DoS-aanvallen ING en iDeal Mijn speculatie is dat vervolgens hackers bloed hebben geroken. Wellicht om te treiteren, wellicht om klanten te benaderen met phishing e-mails om ze gegevens te ontlokken zodat ze geld van rekeningen konden plunderen. De dagen erna waren er in ieder geval aanvallen op ING, dat is de puntenwolk in Figuur 2 rond begin april 2013. En volgens allestoringen.nl ook op iDeal. Om 13:10 uur was het raak bij ING en om 13:21 bij iDeal. Dat laatste is wat vreemd want iDeal is niet gecentraliseerd. Dat gaat meteen naar een bepaalde bank, dus er is iDeal van ING, van

Rabo, etc. Zit er een technische verbinding tussen de verschillende iDeal systemen? Wie zal het zeggen.

IP-pakketten naar mijn.ing.nl als ideal.ing.nl leggen op het moment van schrijven van deze notitie precies dezelfde weg af. Het UNIX commando traceroute vist de route uit die IP-pakketten afleggen. We geven het resultaat van die analyse weer in Figuur 3 om te zien waar mijn.ing.nl en ideal.ing.nl naar toe gaan. Daar is goed te zien dat de laatst bekende machine in beide gevallen het IP-adres 213.208.243.18 heeft. Wie weet is deze machine een of andere filtertunnel die normaal internet verkeer inclusief flash crowds probeert te onderscheiden van DoS aanvallen.

Maar als dat niet zo is of was, dan zou het kunnen dat de aanval op mijn.ing.nl automatisch heeft geleid tot onbeschikbaarheid van hun iDeal platform. Het kan ook zijn dat ten tijde van de aanvallen de configuratie anders in elkaar zat, dat heb ik niet gemeten destijds. Vooraf weten hoe dat precies zit of zat lijkt een taak voor een keuringsinstantie te zijn die vooraf keurt.

Wat bijvoorbeeld anders had kunnen zijn is dat er sprake was van servers in het buitenland voor de iDeal kant. Typisch zul je als eerste verdedigingslinie tegen een DoS-aanval buitenlands verkeer afknijpen. Dit doe je omdat een gedistribueerde aanval allerlei computers betreft van onwetende consumenten overal ter wereld. Als je dat verkeer afknijpt, ben je de facto (abusievelijk) zelf ook onbereikbaar geworden. Hoe dit feitelijk zit of gegaan is, weten we natuurlijk niet.

Hoe ook, is het wel nodig en/of verstandig om iDeal betalingen voor webwinkels en online bankieren dezelfde paden te laten bewandelen (zelfs als alles door hetzelfde DoS-filter gaat)? Is het slim om servers in het buitenland te zetten, mocht dat het geval zijn geweest? Nogmaals, het probleem is dat er onvoldoende transparantie is over de technische kanten van deze bancaire systemen.

opaakheid Waarom zien we deze problemen? Het echte probleem is dat we dat niet transparant krijgen. Banken zijn jaren geleden massaal gaan offshoren: ICT uitbesteden naar lage lonenlanden. Kostenbesparing was een veel gehoorde reden. Was dat altijd een goed idee? Wat heeft dat met de staat van het applicatielandschap gedaan? Is teveel kennis uit banken weggelopen? Krijgen kwaadwillenden zo toegang tot de broncode van de systemen waardoor men zwakheden kan exploiteren? Hebben banken te snel vernieuwd? Te langzaam? Te onvoorzichtig? Te conservatief? Is wel geld uitgegeven aan de juiste zaken?

Banken reorganiseren, ook als er flinke winsten gemaakt worden. Lean en mean moet het worden. Maar: kan dat technisch gezien allemaal wel? Is er wel genoeg capaciteit vooor beheer, onderhoud, operations? Allemaal vragen, geen antwoorden. Deze opaakheid is een probleem dat onder andere door proactief technisch toezicht kan worden ondervangen.

3.3 Hackers, DoS-aanvallen

vraag We zien voorbeelden in het nieuws van hoe hackers geld buitmaken bij banken. Het gaat daarbij om forse bedragen waarbij soms DOS aanvallen als afleidingsmanoeuvre gebruikt worden (om phishingmails te sturen, zogenaamd vanuit de helpdesk) en soms wordt er direct gehackt op de systemen van een bank. Is dat in Nederland ook mogelijk? Werken banken, DNB en overheid samen met internationale partijen om deze problemen in kaart te brengen en remedies te implementeren Zo ja, sinds wanneer en op welke schaal? Zijn er banken die dat nog niet doen? Zo ja, waarom niet?

reactie Dit zijn heel wat vragen. Hackers, lees criminelen, zijn uiterst spitsvondig. De vragen zijn heel legitiem, en wederom is het probleem dat individuele banken hier onvoldoende transparant over zijn.

internetfraude neemt vormen aan De NVB publiceerde vorig jaar maart dat fraude in het betalingsverkeer het jaar daarvoor was gestegen naar 92 miljoen euro[4].

In de Verenigde Staten beheert de Federal Trade Committee een online database van klachten van consumenten. Dit heet het Consumer Sentinel Network. Vele organisaties brengen daar hun klachten naar toe zodat een omvangrijk beeld ontstaat van wat zich afspeelt. In het jaar 2010 kreeg CSN meer dan 1.3 miljoen klachten binnen[5]. We citeren wat hoofdpunten uit het FTC rapport.

> The CSN received over 1.3 million complaints during calendar year 2010: 54% fraud complaints; 19% identity theft complaints; and 27% other types of complaints.
>
> Identity theft was the number one complaint category in the CSN for calendar year 2010 with 19% of the overall complaints, followed by Debt Collection (11%); Internet Services (5%); Prizes, Sweepstakes and Lotteries (5%); Shop-at-Home and Catalog Sales (4%); Impostor Scams (4%); Internet Auction (4%); Foreign Money Offers and Counterfeit Check Scams (3%); Telephone and Mobile Services (3%); and Credit Cards (2%).

Identiteitsfraude was nummer één, en Internet services nummer drie. Deze vorm van criminaliteit heeft in de VS flinke vormen aangenomen. Uit de CSN database is af te leiden hoe het initiële contact verliep bij fraude:

> Sixty percent of all fraud-related complaints reported the method of initial contact. Of those complaints, 45% said email, while another 11% said an Internet website. Only 10% of those consumers reported mail as the initial point of contact.

Kortom: voornamelijk via e-mail of via een website, samen 56%. Internet wordt hiermee een startpgaina voor fraude, dat kan niet de bedoeling zijn. Het zou goed zijn om in Nederland beter zicht te krijgen op de mate van problemen vanuit de overheid en niet volledig te bouwen op wat de sector er zelf van zegt.

hoe komen ze toch aan die e-mailadressen? Een nevenvraag is hier: hoe komen die fraudeurs toch aan al die e-mailadressen? De Kamerleden stellen namelijk wel dat hackers e-mail sturen, maar de vraag is: hoe komen ze toch aan al die adressen? Immers, als je die niet hebt, heeft een DoS-aanval ook geen zin als afleidingsmanoeuvre.

E-mailadressen worden bijvoorbeeld geoogst door het hacken van onvoldoend beveiligde sites waar consumenten denken veilig te zijn. Neem als voorbeeld babydump.nl waar gehackte persoonsgegevens van gebruikt werden om KPN te stangen. Naam, adres, woonplaats, e-mail, mobiel nummer, bankrekening, creditcard nummers, en meer informatie is op allerlei plekken opgeslagen in de virtuele wereld. De zwakke

[4] http://www.nvb.nl/nieuws/2012/1021/betalingsverkeer-veilig-ondanks-toename-fraude.html

[5] http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

broeders hebben hun systemen onvoldoend integraal ontworpen en missen de beveiliging als integraal onderdeel van hun systemen. Via die zwaktes kom je een hoop te weten, en dat kun je weer uitbuiten op een andere manier.

Een IT-bouwvergunning voor bepaalde diensten die vitaal zijn voor onze virtuele infrastructuur zou te overwegen zijn.