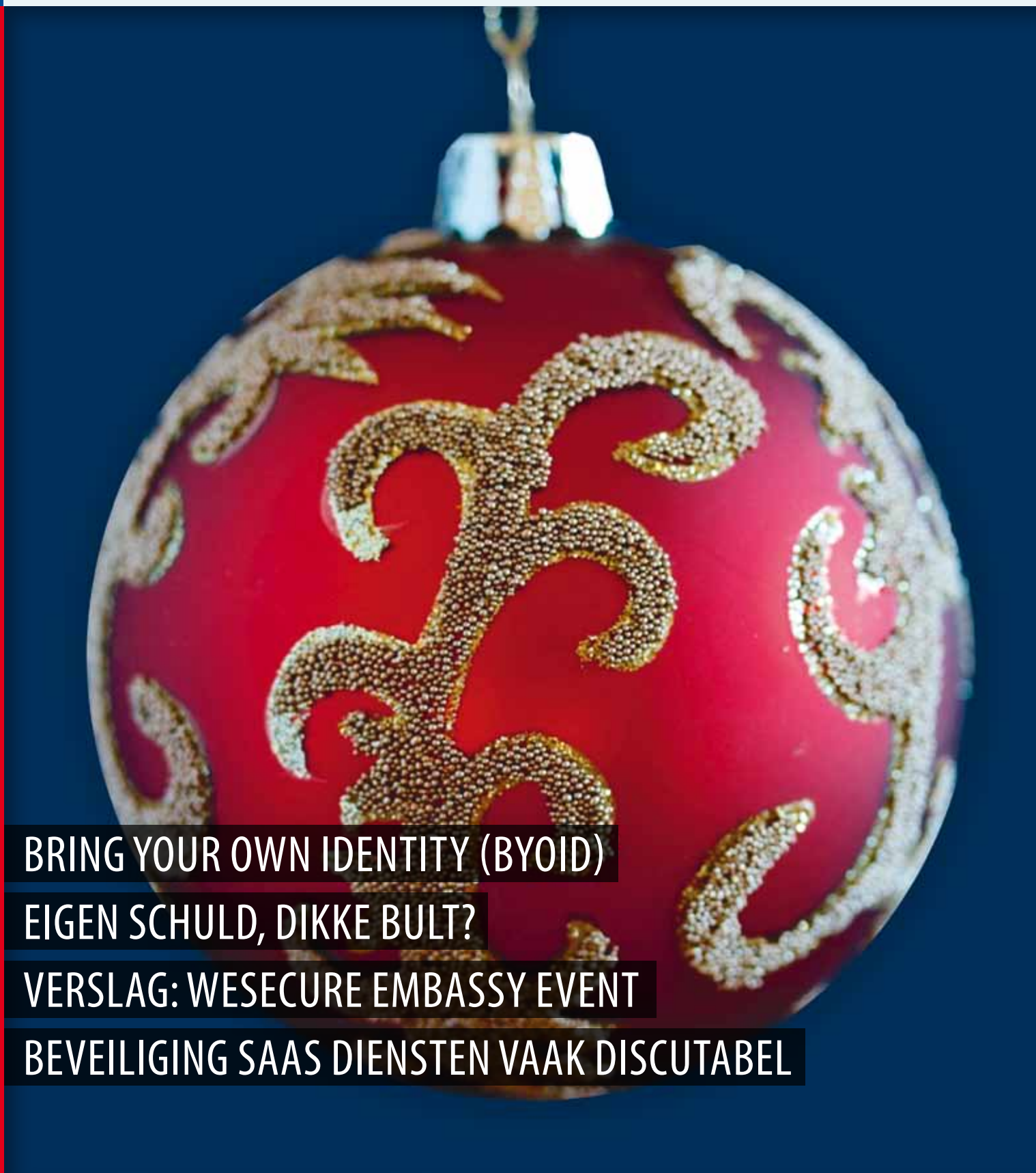
08/2012

INFORMATIE BEVEILIGING

PvIB Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 8 - 2012



BRING YOUR OWN IDENTITY (BYOID)

EIGEN SCHULD, DIKKE BULT?

VERSLAG: WESECURE EMBASSY EVENT

BEVEILIGING SAAS DIENSTEN VAAK DISCUTABEL

IMF
INTERNATIONAL MANAGEMENT FORUM

Cloud Security (CCSK)

CCSK™ Certificate of Cloud Security Knowledge

De 2-daagse training leidt op voor het wereldwijd erkende Certificate of Cloud Security Knowledge (CCSK) van de Cloud Security Alliance (CSA)

CCSK is de eerste leveranciersonafhankelijke Cloud Security certificering ter wereld. De certificering is ontwikkeld door CSA en ENISA.

Certified ISO 27005 Risk Manager

Deze 3-daagse training leidt u op tot Certified Risk Manager op basis van de internationale standaard voor informatiebeveiligingsrisicomanagement ISO 27005.

In deze 3-daagse training leert u de risico-elementen m.b.t. informatie te beheersen door vertrouwd te raken met hun levenscyclus.

CISM

CISM

3-daagse CISM training ter voorbereiding op het CISM examen van ISACA.

CISM® staat voor Certified Information Security Manager en is een titel van ISACA. Inmiddels hebben meer dan 13.000 cursisten wereldwijd de CISM titel behaald.

Meer informatie en inschrijven?
www.imf-online.com/partner/pvib

VOORWOORD

Ik kijk niet veel TV, maar als ik kijk ben ik een liefhebber van CSI. Regelmatig komen er scènes langs waarbij je als informatiebeveiligers wel even je zoutvaatje bij de hand moet hebben. Zoals een analyse van een iMac die ter plekke gedaan wordt, met slechts de hulp van een USB memorystick. Binnen vijf minuten is een wachtwoord gekraakt en springt men direct naar de interessante email. Een andere keer wordt een onderzoek gedaan in Second Life, waarbij andermans avatars gekraakt worden. En ik herinner me een aflevering waar vanuit het politielaboratorium een hele keten van computers gehackt wordt om het IP-adres van een dader te vinden, terwijl hij bezig is. Deze aflevering heeft Opstelten vast ook gezien. Maar nooit maakten ze het bij CSI zo bont als vorige week.
Eric Delko van CSI: Miami had twee minuten om een laptop te klonen naar een externe harde schijf via USB. Laten we even aannemen 500 Gb in grootte. Dat vergt een snelheid van 2Gb per seconde, de theoretische limiet van USB3 is 4,8 Gb per seconde. Dus dit zou nog kunnen. Horatio Caine drukt hem wel op het hart om 'protocol' te gebruiken. Hiermee moet het kennelijk authentieker lijken.
Het protocol voor een niet-verwijderbare schijf is de PC te booten in DOS en dan met een forensisch programma vanaf een andere computer de harde schijf laten lezen. Dit was duidelijk niet het geval, maar dat zal de leek niet opgevallen zijn. De originele laptop zijn ze daarna trouwens kwijt. Ook dat is volgens mij niet voorzien in het protocol.
In het laboratorium wordt de vercijferde harde schijf in verband gebracht met een vercijferde email bij een ander. Dat moet wel, want ze zijn beiden versleuteld... Sterker nog, de sleutel voor ontcijfering is een wachtwoord en die moet voor beiden gelijk zijn. Tja, al die encryptie lijkt ook zo op elkaar. En een keylogger die aan de andere PC zat biedt uitkomst, want deze bevat natuurlijk het wachtwoord.
Maar dat wachtwoord herken je niet zo maar. Bijkomend probleem is dat de forensische kopie zichzelf zal wissen als er twee keer een fout wachtwoord wordt ingevoerd. Hier laat mijn fantasie het afweten en blijf ik vastzitten in een zoektocht naar logica. Toch maar doorkijken, want ik begrijp dat dit gegeven het spannend moet maken voor de gewone kijker. De eerste keer raadt Eric fout en dan blijkt dat ze nog maar 30 seconden hebben om een tweede te proberen. Dit is pas sterke beveiliging, dat moeten we maar gelijk een standaard functie maken in Windows 9!
Natuurlijk raden ze de tweede keer het wachtwoord goed - en de criminelen blijken zelfs een goede smaak te hebben voor een sterk wachtwoord. Het heeft 8 posities en begint met een onderstreep en bevat een spatie, cijfers en letters. Echter... de letters blijken de initialen te zijn van de dader en vormen zo dus de doorbraak in de zaak.
Ik ben een realist en begrijp heel goed dat de show niet voor mij geschreven is, maar voor de leek, die van encryptie weet dat het leesbare tekst onleesbaar maakt en dat de leesbare versie nog teruggetoverd kan worden ook. Is het dus erg dat hier zo'n verdraaiing van de werkelijkheid gebracht wordt? Ik denk het wel. Één aspect wat ik belangrijk vind is het principe dat je zelf je wachtwoord moet kunnen kiezen, dat doet een ander niet voor je. Een ander is dat een wachtwoord en een cryptografische sleutel twee verschillende objecten zijn. Dan strijk ik nog even over mijn hart om ze de zelfwisselende kopie te vergeven in naam van spanning opbouwen, je moet het niet te moeilijk maken.
Ach, zoals Nikki Haley, de gouverneur van South Carolina eind oktober al zei als excuus voor het niet versleutelen van social security nummers: "Encryption is complicated." Zeker te veel CSI gekeken...

Lex Borger
hoofdredacteur

P.S. Wie van CSI: Miami en 'reality distortion' houdt, moet eens het adres 14600 Aviation Boulevard in Hawthorne opzoeken...

INHOUDSOPGAVE

Voorwoord 3

Bring your own Identity (BYOID) 4

Eigen schuld, dikke bult? 7

Column: 2012: Privacy is om te lachen! Of ook: Taarten bakken met Teeven 12

Kennismaking met: Alf Moens 13

Diepgaande kennis van software-ontwikkeling is cruciaal 14

Column: Collaborative 18

DNS, het 'laatste' onbeschermde protocol 19

Gevaar Cyberwar komt uit onverwachte hoek 20

Verslag: Wesecure embassy event 21

Beveiliging SAAS diensten vaak discutabel 24

Achter het nieuws 27

Ben je klaar voor cybercriminaliteit? 29

Column Berry: Sport en geld 31

Foto omslag:

BRING YOUR OWN IDENTITY (BYOID)

EEN UPDATE OVER DE STAND VAN ZAKEN VAN EEN OPENID VOOR DE CONSUMENT EN ONLINE DIENSTVERLENERS

Kick Willemse (Twitter: @papierloos) is identity expert en werkzaam als adviseur vanuit Evidos.

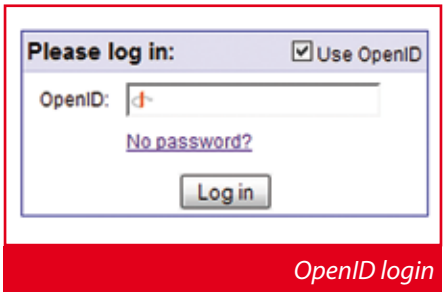
Het is alweer drie jaar geleden dat Hyves bekend maakte dat alle Hyvers hun account als OpenID konden gebruiken om op andere website(s) in te loggen. Ondersteund door grote aanbieders als Facebook, Google, Microsoft, PayPal zou OpenID de wereldwijde standaard worden om de consument van zijn grote hoeveelheid wachtwoorden te verlossen. Nu, 2012, maakt iedere consument nog altijd gebruik van veel verschillende wachtwoorden op verschillende website(s). Ondanks dat iedere consument het wachtwoordprobleem herkent en websites dagelijks wachtwoorden lekken [1], bieden weinig dienstverleners de mogelijkheid om je eigen identiteit te gebruiken om in te loggen. Tijd voor een update over de laatste stand van zaken en ontwikkelingen rondom OpenID, de mogelijkheid om je eigen identiteit te kiezen en hergebruiken op het web.

De ontwikkeling dat consumenten de mogelijkheid krijgen om hun eigen iPad, iPhone of laptop te gebruiken op het werk krijgt steeds meer aandacht. Deze ontwikkeling staat algemeen bekend als de Bring your own device (BYOD) ontwikkeling. OpenID staat voor een vergelijkbare ontwikkeling waarbij de consument de mogelijkheid heeft om zijn eigen online identiteit (OpenID) te gebruiken op het web (BYOID). Oorspronkelijk is OpenID ontstaan als een techniek om eenvoudig een reactie op een blog te plaatsen. De bedenker, Brad Fitzpatrick [2], vond het handig als je niet bij iedere blogreactie opnieuw een registratie hoefde te doen. Al snel sloten grote partijen als Google, Microsoft en Facebook zich aan bij de technische standaard en werd OpenID het merk dat staat voor het eenvoudig inloggen op websites met je eigen Identiteit. De internationale OpenID stichting ontwikkelt de technologische standaarden en promoot het gebruik van OpenID.

Waar is OpenID gebleven?

Ondanks de populariteit en opkomst in 2007 nam het enthousiasme en de *buzz* rondom OpenID langzaam af. Vanuit de community ontstond kritiek op het feit dat bijvoorbeeld Google wel OpenID provider wil zijn, maar zelf geen andere OpenID's accepteert. Daarnaast tonen de OpenID providers liever hun eigen logo dan het OpenID logo. Consumenten begrepen het invoeren van een OpenID URL als gebruikersnaam niet en website(s) vonden het complex om het eenvoudig te integreren in hun diensten.

OpenID providers tonen liever hun eigen logo dan het OpenID-logo



OpenID login

Ondanks dat het OpenID-logo langzaam van website(s) verdween gingen steeds meer websites wel de mogelijkheid bieden om met je Facebook, Google of Paypal account in te loggen. De onderliggende techniek is nog altijd gebaseerd op OpenID en aanverwante technieken zoals oauth.

Belangrijk voor dit opvolgende succes zijn de aanvullende mogelijkheden van sociale netwerken en het delen van informatie met je vrienden of andere applicaties. Tegenwoordig kan je eenvoudig inloggen op bijvoorbeeld Spotify en AirBnB met één identiteit die je al hebt. Facebook Connect is verreweg de meest succesvolle implementatie met meer dan 250 millioen login's per maand. De vraag is of iedere consument het prettig vindt om zijn identiteit door Facebook te laten beheren. Door de dominante positie van deze grote partijen, hebben consumenten nog altijd niet de keuze met welke OpenID ze willen inloggen.

Met de ervaringen van de verschillende OpenID aanbieders en onine dienstverleners werkt de OpenID foundation aan twee verbeteringen voor 2012. Er wordt hard gewerkt aan de opvolger van de technische standaard; OpenID Connect en een oplossing voor de keuzeproblematiek van de OpenID provider met de Accountchooser.

OpenID en OAuth

De betrokkenen bij OpenID werkten ook aan de vraag hoe je uitwisseling van informatie uit een webapplicatie kunt toestaan aan andere website(s) zonder je login gegevens te delen. Bijvoorbeeld omdat je andere toepassingen eenvoudig toestemming wilt geven voor het gebruiken van je gmail adres, je twitterfeed of je online foto's. Een Application Programming Interface(API) voor het delegeren van toegang aan een derde applicatie, zonder je wachtwoord te delen was op dat moment niet beschikbaar.

Deze behoefte resulteerde in de ontwikkeling van het Oauth-protocol. Oauth (www.oauth.net) staat letterlijk voor open standaard voor autorisatie. Een zeer krachtig protocol dat zich in korte tijd heeft ontwikkeld tot internationale standaard en door bijvoorbeeld Twitter, LinkedIn, Facebook en vele andere online diensten wordt gebruikt. De insteek bij Oauth is het eenvoudig autoriseren van applicaties tot je persoonlijke data, zoals bijvoorbeeld je adresboek of foto's.

Door de hoge betrouwbaarheid van het Oauth protocol, de behoefte om met toestemming gegevens uit te wisselen en het feit dat dit ook op bijvoorbeeld het mobiele kanaal werkt, gaan steeds meer OpenID providers het Oauth-protocol gebruiken voor authenticatie in plaats van het OpenID protocol.

In principe is hier sprake van oneigenlijk gebruik van het protocol omdat je hiermee niet alleen jezelf authenticeert, maar ook direct autorisatie moet geven tot specifieke gegevens. Een gebruiker wil best inloggen met FaceBook of Twitter, maar mogelijk niet direct de website toegang geven tot al zijn FaceBook of Twitter gegevens. In veel gevallen is hier nu wel sprake van.

Daarom is er een nieuwe versie van het OpenID protocol ontwikkeld bovenop Oauth, dit is OpenID connect en inmiddels beschikbaar als implementers draft [1] OpenID connect maakt gebruik van Oauth en daarmee de autorisatie tot je identiteitsgegevens die bij een provider staan.

Met de ontwikkeling van Oauth en OpenID Connect zijn de bezwaren die er zijn tegen de beperkte betrouwbaarheid van versie 2.0 van het OpenID protocol komen te vervallen.

Accountchooser

OpenID accepteren op mijn website?

Door de behoefte om een betere relatie te hebben met bestaande gebruikers bieden steeds meer websites de mogelijkheid om je Facebook, Twitter of Google account te koppelen. Dit is waardevol vanwege de aanvullende gegevens die je als website krijgt over de gebruiker en om berichten te delen met zijn vriendennetwerk. Toch zijn er ook andere voordelen om andere OpenID providers te ondersteunen, ondanks dat je niet gelijk de sociale voordelen krijgt. Veel online webshops hebben er de afgelopen jaren voor gekozen om klanten de mogelijkheid te bieden om een online aankoop te doen zonder registratie. Funest vanuit het perspectief om een relatie met je klant op te bouwen, maar gedreven door het conversie verlies van registratie, e-mail verificatie en wachtwoord vergeten procedures. Het hergebruik van je identiteit door een OpenID kan webwinkels helpen om toch eenvoudig een relatie op te bouwen met de klant, zonder conversie verlies. Het is niet voor niks dat de Thuiswinkel.org een oproep heeft gedaan voor de ontwikkeling van een OpenID voor online winkelen [3].

Facebook Connect is de meest succesvolle implementatie

Als online aanbieder krijg je ook steeds vaker te maken met nieuwe kanalen zoals mobiel of televisie. Het is belangrijk dat je met de bestaande manier om gebruikers te herkennen ook deze kanalen kan ondersteunen. Externe OpenID providers zijn hierin gespecialiseerd, waardoor gebruikers niet eerst een registratie op je website moeten doen, voordat ze van je mobiele applicatie gebruik kunnen maken. Aan de andere kant kun je zonder meer de OpenID technologie implementeren voor je eigen accounts. Last but not least beschik je als online dienstverlener wellicht niet over de juiste kennis om wachtwoordbeheer op een goede wijze te organiseren. Met het accepteren van een OpenID is het opslaan van wachtwoorden niet meer nodig en voorkom je het risico dat deze gegevens in verkeerde handen komen.

Is dit waardevol voor de consument?

Iedere consument worstelt met zijn wachtwoordbeheer. Ondanks de verschillende suggesties en tips om een goed wachtwoord te bedenken, zijn er in de praktijk twee type gebruikers. Gebruikers die voor iedere website een ander wachtwoord bedenken en dit op een lijstje bijhouden en gebruikers die hetzelfde wachtwoord gebruiken op diverse websites. De eerste groep baalt ervan als de browser het wachtwoord niet vooraf invult op basis van wachtwoord-onthouden-feature of wanneer men moet inloggen vanaf een andere pc of mobiel. Tenslotte moet je dan op je lijstje controleren wat dat moeilijke wachtwoord ook alweer is. De verleiding is dan groot om toch een wachtwoord te kiezen dat je makkelijk kunt onthouden. In de praktijk heeft de grootste groep gebruikers een aantal favoriete wachtwoorden die ze standaard gebruikt op

verschillende websites. Hackers kennen ook dit gedrag en gaan steeds vaker op zoek naar websites die hun wachtwoordbeheer niet goed georganiseerd hebben. Op basis van de gegevens die ze daar eenvoudig achterhalen proberen ze toegang te krijgen tot zoveel mogelijk andere website(s). In sommige gevallen om bijvoorbeeld je vrienden of andere contacten om geld te vragen, omdat je zogenaamd ergens op reis gestrand bent. Wanneer een dergelijke hack bekend is, is deze groep consumenten erg druk om te bedenken op welke websites ze deze gegevens gebruikt hebben. Met een race tegen de klok moeten deze gegevens dan zoveel mogelijk gewijzigd worden. Een OpenID geeft gebruikers de mogelijkheid om een identiteit vanaf een centrale plek te beheren. Uiteindelijk kies je als gebruiker voor de manier waar of bij wie je deze OpenID wilt beheren. De keuze is afhankelijk van wat een gebruiker belangrijk vindt. Kies ik voor Google, een regionale aanbieder, een overheidsmiddel (zoals DigiD) of beheer ik liever mijn eigen OpenID? Gebruikersgemak, vertrouwen, kosten en eventuele verzekering bij verlies spelen hierbij een mogelijke rol. Het is belangrijk dat er eenvoudige oplossingen zijn die goed te gebruiken zijn voor de doorsnee internetgebruikers. Diverse partijen zoals banken, telecom, verzekeraars, Apple en Google kunnen hier mogelijk een rol spelen. Het centraal beheren van je identiteit levert mogelijk risico's op, omdat je dan erg afhankelijk bent van dit account. In de praktijk zal je dus wellicht een aantal OpenID's hebben om niet afhankelijk te zijn van één oplossing. Het geeft je echter ook de mogelijkheid om deze OpenID beter te beveiligen dan alleen een wachtwoord, bijvoorbeeld via aanvullende maatregelen als een code op je mobiel of biometrie. De volgende keer dat een website vraagt om een wachtwoord, vraag je dan af of deze website in staat is om je gegevens op een goede wijze te beschermen, zo niet, vraag ze waarom ze niet de mogelijkheid leveren voor het gebruik van een OpenID.

> Met OpenID voorkom je het risico van lekken van wachtwoorden

Conclusie

De ontwikkeling om je eigen identiteit mee te brengen (BYOID) en gebruiken op het web heeft zich in de afgelopen jaren verder ontwikkeld. Primair gedreven vanuit de aanvullende sociale interactie die partijen als Facebook, Twitter en Google hierbij bieden. OpenID biedt de verschillende technologieën om het hergebruik van een identiteit steeds beter mogelijk te maken, waarbij OpenID providers het belangrijk vinden om hun eigen merk te promoten. Op basis van de marktontwikkelingen is de verwachting dat consumenten steeds vaker hun eigen OpenID zullen meebrengen als ze van een online dienst gebruik willen maken. Als online dienstverlener is het belangrijk om je voor te bereiden op de mogelijkheden om OpenID's te accepteren. Wellicht gedreven door de vraag van je gebruikers, maar ook omdat er diverse voordelen aan verbonden zijn voor een betere online dienstverlening en klantrelatie.

Bronnen

[1] Zie rubriek Achter het Nieuws, Informatiebeveiliging 5 2012

[2] http://www.crunchbase.com/person/brad-fitzpatrick

[3] http://www.thuiswinkel.org/webwinkels-overheid-moet-pilot-online-leeftijdcheck-starten

EIGEN SCHULD, DIKKE BULT?

AANSPRAKELIJKHEID BIJ FRAUDE MET INTERNETBANKIEREN

Dr. Nicole S. van der Meulen is werkzaam als universitair docent Internet Governance bij de Faculteit Rechtsgeleerdheid van de Vrije Universiteit Amsterdam. Zij promoveerde in 2010 aan de Universiteit van Tilburg met een vergelijkend proefschrift naar identiteitsfraude in Nederland en de Verenigde Staten. Zij is te bereiken via n.s.vander.meulen@vu.nl.

Meerdere jaren geleden, in 2008, mocht ik een gesproken column voordragen tijdens een landelijke praktijk dag voor gemeenteambtenaren over privacy en gegevensuitwisseling. Destijds droeg mijn voordracht de titel 'Identiteitsfraude: U bent gewaarschuwd.' Specifiek zei ik daarover het volgende: "De Nederlandse Vereniging van Banken (NVB) heeft recent nog een campagne gehouden om burgers te waarschuwen voor de kenmerken van betrouwbare en onbetrouwbare websites voor internetbankieren. Mooie actie, zult u misschien denken. Bewustwording is een belangrijke eerste stap om identiteitsfraude tegen te gaan. De vraag is echter wat als men deze bewustwordingscampagnes gaat gebruiken als verdediging tegen slachtoffers van identiteitsfraude. Als een slachtoffer, nadat haar bankrekening leeg geroofd is door een vindingrijke fraudeur, bij de bank aanklopt zal de medewerker dan met een uiterst vriendelijke stem zeggen 'Maar mevrouw, wij hebben u toch gewaarschuwd?'

Kassa

Deze 'voorspelling', hetzij op zeer beperkte schaal en met een minder cynische ondertoon, is inmiddels uitgekomen. Op zaterdag 15 september verwelkomde consumentenprogramma Kassa! enkele slachtoffers van fraude met internetbankieren. Deze slachtoffers, in tegenstelling tot de meeste anderen, waren door de Rabobank niet schadeloos gesteld. Enkele weken later, op 13 oktober, besteedde Kassa! wederom aandacht aan een slachtoffer van fraude die niet schadeloos gesteld was door een bank, ditmaal de ABN AMRO. Het tij ten aanzien van het schadeloos stellen van slachtoffers, wanneer hun bankrekening leeg geroofd is door een crimineel, lijkt te keren. En dat roept vragen op. Moeilijk te beantwoorden vragen voor de banken. Deze bijdrage beoogt daarom een overzicht te geven over de huidige ontwikkelingen op het gebied van aansprakelijkheid bij fraude met internetbankieren. Deze worden vervolgens kort in een bredere context geplaatst om na te gaan wat voor gevolgen de huidige tendens kan hebben voor internetbankieren in het algemeen en het vertrouwen daarin in het bijzonder.

"Maar mevrouw, wij hebben u toch gewaarschuwd?"

Achtergrond

Fraude met internetbankieren was in eerste instantie een probleem waar Nederlandse banken weinig tot geen last van leken te hebben. Helemaal in vergelijking met banken elders in de wereld welke uitsluitend gebruikmaakte van single factor authenticatie, veelal gebruikersnaam en wachtwoord, voor hun cliënten. De Verenigde Staten is daar het meest vooraanstaande voorbeeld van. Het Nederlandse systeem wat gebruikmaakt van de bekende twee factor authenticatie bleek robuuster, totdat de man-in-the-middle aanval arriveerde en roet in het eten gooide. Vraag naar de omvang van het probleem begon te groeien, maar bleef enige tijd onbeantwoord. Pas eind 2010 trad de NVB voor het eerst naar buiten met een kwantitatieve indicatie van het probleem (zie tabel 1).

Duidelijk wordt uit de cijfers van de afgelopen tijd dat de schade jaarlijks toeneemt. Deze stijging lijkt op het eerste oog zorgwekkend, maar relatief gezien blijft de schade uitermate beperkt. Zoals de NVB beschrijft in haar persbericht: "Per jaar vinden ongeveer 3 miljard transacties plaats via het internetbankieren, met een totale waarde van 3200 miljard euro. De schade van 27,3 miljoen betrof bijna 0,002% van de totale halfjaarlijkse transactieomzet." (NVB 2012) Reden tot paniek op basis van de cijfers blijft dus uit. En dat is terecht. De aansprakelijkheidskwestie daarentegen van individuele gevallen geeft wel reden tot zorg.

Jaar	Schade in euro's
2008	2,1 miljoen
2009	1,9 miljoen
2010	9,8 miljoen
2011	35 miljoen
2012 (eerste halfjaar)	27,3 miljoen

Tabel 1. Schadecijfers fraude internet bankieren

Aansprakelijkheid

Het beleid van banken in Nederland is vanaf het begin geweest dat zij in de regel de klant schadeloos stellen, maar henzelf voldoende ruimte gunnen

om per geval te beslissen. Doorgaans betekende dit concreet dat nagenoeg alle gevallen hun geld terugkregen. Een lange tijd bleef het aansprakelijkheidsfront daarom rustig. Dit was grotendeels totdat consumentenprogramma Kassa! in twee afleveringen aandacht wijdde aan slachtoffers die door de Rabobank en de ABN AMRO niet schadeloos gesteld zijn. Dit is een belangrijk teken dat de grens begint te verschuiven. Inmiddels wordt meer van de consument verwacht. Na jaren van voorlichtingscampagnes mag gerekend worden op een zeker bewustzijn aan de kant van de consument, volgens de banken. Deze verwachting geeft ook een andere invulling aan het begrip eigen schuld, hetgeen deel uitmaakt van de juridische aansprakelijkheid. De vraag is immers: In hoeverre is de schade te wijten aan 'eigen schuld' van het slachtoffer? Om deze vraag te beantwoorden worden twee maatstaven gebruikt, causaliteit en redelijkheid. Te beginnen met de tweede maatstaaf, "[d]e vraag die daarbij beantwoord dient te worden, is of [het slachtoffer] verwijtbaar of anders heeft gehandeld dan een zorgvuldig, redelijk handelend mens met het oog op zijn eigen belangen in de gegeven omstandigheden zou hebben gedaan…" (Timmer, 2012). Deze vraag is moeilijk te beantwoorden. Banken hebben ten alle tijde het recht behouden om consumenten die nalatig of onzorgvuldig gedrag hebben vertoond niet schadeloos te stellen. En daar zit de angel in het verhaal. De definitie van nalatig en onzorgvuldig gedrag is niet eenduidig. Gijs Boudewijn van de NVB bevestigd het gebrek aan eenduidigheid tijdens de uitzending van 15 september door te stellen dat: 'De termen onvoorzichtig en nalatig verschillen per geval, per klant en per bank.'

> Het Nederlandse systeem bleek robuuster, totdat de man-in-the-middle-aanval arriveerde

Gebrek aan eenduidigheid

Het gebrek aan eenduidigheid is bijzonder problematisch omdat consumenten op deze manier weinig houvast hebben. Het nodigt uit tot willekeur en enige vorm van transparantie is afwezig. In de uitzending van 15 september, bijvoorbeeld, kregen twee slachtoffers de gelegenheid om hun verhaal te vertellen. Het eerste slachtoffer, Helene Schrever, bankiert bij de ABN AMRO. Zij ontving een phishing email en werd vervolgens gebeld door 'Vanessa' van de ABN AMRO. Dirk Massink, gedupeerde klant van de Rabobank, ontving eveneens een email en een telefoontje van een nep bankmedewerker, Kimberly. In beide gesprekken werd naar de e-mails gerefereerd en gezegd dat de rekeningen doorgelopen moesten worden in verband met mogelijke 'fouten.' Daarvoor waren de e.dentifier of random reader codes nodig. De ABN AMRO stelde haar gedupeerde cliënt schadeloos. De Rabobank daarentegen niet. De Rabobank, zoals bleek uit de uitzending, acht het doorgeven van de random reader codes als onzorgvuldig en nalatig gedrag. Zelfs als klanten geloven dat zij met de bank in gesprek zijn. Ter verantwoording voor dit besluit refereert de Rabobank naar haar specifieke waarschuwingen om random reader codes nooit te delen. Volgens de Rabobank vertegenwoordiger heeft de bank gedurende een jaar een melding op het scherm van de internet bankierende klant geplaatst met dit bericht. In de ogen van de Rabobank is het geen gehoor geven aan deze melding dus onzorgvuldig en nalatig. Volgens Michel van Eeten, aanwezig bij de uitzending, zal de claim van de Rabobank voor de rechter geen stand houden. Op dat punt vrees ik dat hij ongelijk zou kunnen krijgen. En dat vergroot de onrust. Er is weinig jurisprudentie in Nederland en omringende landen over dergelijke zaken. In Duitsland is echter eerder dit jaar een soortgelijke zaak voor het hoogste gerechtshof verschenen. In die zaak was het slachtoffer evenmin schadeloos gesteld door zijn bank. Het slachtoffer diende daarom een aanklacht in tegen de Sparda bank (The Local, 2012). Daarin gaf de rechtbank het gelijk aan de bank. Een gevaarlijk precedent. De klant had geen recht op een vergoeding omdat hij de specifieke waarschuwingen van de bank, over het invoeren van meerdere tan-codes, onvoldoende had

> De grens van aansprakelijkheid begint te verschuiven

opgevolgd. Wederom geen vergoeding dus. Het bovenstaande introduceert een tweetal problemen. Het eerste probleem is de onduidelijkheid over de begrippen nalatig en onzorgvuldig gedrag.
Zonder definitie van onzorgvuldig en nalatig blijven deze aan verandering onderhevig. Door de individuele toepassing komt het beleid van de banken over als inconsequent en weten consumenten niet waar zij aan toe zijn. Dit tast het vertrouwen aan. Het tweede probleem is het gebruik van waarschuwingen als instrument om de aansprakelijkheid op consumenten af te schuiven.

Glijdende schaal

Hoewel in de zojuist beschreven aflevering van Kassa! de ABN AMRO nog de bank was welke haar klanten wel schadeloos stelde, bleek dit enkele weken later niet meer het geval te zijn. Op zaterdag 13 oktober kwam Kassa! wederom met een aflevering waarin een slachtoffer, Michel Moret, van fraude met internetbankieren het woord kreeg. In tegenstelling tot de zaak bij de Rabobank was bij het ABN AMRO slachtoffer uitsluitend sprake van gebruik van malware. Enige vorm van social engineering was afwezig. Dit is een belangrijk gegeven omdat bij social engineering de verwijtbaarheid van het slachtoffer sneller een onderwerp van discussie zou kunnen zijn. Dit is bij malware, door de beperkte detectiemogelijkheden, moeilijker te verantwoorden. In dit geval, werd de eerste poging van criminelen om de cliënt geld afhandig te maken door de bank gedetecteerd. Deze belde de cliënt om te verifiëren dat hij inderdaad 10.000 euro naar een Poolse rekening wilde overmaken. Dit was niet het geval. De ABN AMRO gaf aan dat de computer van Moret geïnfecteerd was en hij werd aangeraden om een goede anti-virus software te installeren. Deze had Moret al. Daarnaast raadde de ABN AMRO aan om de computer op te laten schonen door een deskundig bedrijf. Volgens de uitzending heeft dit plaatsgevonden. Enkele weken later loopt, tijdens een overboeking, de computer vast. De volgende dag wordt bekend dat 9.500 euro alsnog richting Polen is gegaan. De ABN AMRO verzocht de cliënt om de factuur van het bedrijf dat zijn computer had opgeschoond, hetgeen Moret weigert te overhandigen. Vervolgens stuurt het externe bedrijf alsnog een getuigschrift van de geleverde dienst, maar dat is voor de ABN AMRO niet voldoende. De bank weigert Moret schadeloos te stellen omdat hij de instructies onvoldoende zou hebben opgevolgd en omdat de bank onvoldoende inzicht heeft in de manier waarop Moret zijn computer heeft opgeschoond. Dit roept de vraag op of Moret dan ook gezien wordt als onzorgvuldig en nalatig? Daarover geeft de ABN AMRO geen duidelijkheid tijdens de uitzending. Hetgeen in ieder geval wel geconcludeerd kan worden is dat de toepasbaarheid van eigen schuld groeiende lijkt te zijn, waarbij deze niet alleen ter sprake komt bij slachtoffers van social engineering maar ook van malware. Dat lijkt toch een glijdende schaal te illustreren, waarbij waarschuwingen en instructies als glijmiddel worden ingezet.

> De termen onvoorzichtig en nalatig verschillen per geval, per klant en per bank

> Er is weinig jurisprudentie over dergelijke zaken

Borgen van aansprakelijkheid

In ieder geval de ABN AMRO is van plan om per 1 januari 2013 enkele instructies ten aanzien van de beveiliging van de computer op te nemen. Deze houden bijvoorbeeld in dat gebruikers ten minste anti-virus software op hun computer dienen te hebben en alle updates geïnstalleerd hebben. Door deze instructies op te nemen in de algemene voorwaarden, krijgen zij een belangrijkere status. De cliënt gaat immers akkoord met de algemene voorwaarden van de dienstverlener. Dit zou dus kunnen betekenen dat als een slachtoffer niet heeft voldaan aan deze voorwaarden dat hij of zij mogelijk niet schadeloos gesteld wordt. Dit kan lei-

den tot een significante toename van het aantal gevallen slachtoffers die zelf de opdraaien voor de fraude. Daarnaast is er nog een ander punt van discussie. Het niet voldoen aan de voorwaarden kan aanleiding zijn voor de bank om de cliënt niet schadeloos te stellen. Dit is mogelijk problematisch omdat hier een oorzaak gevolg verondersteld wordt wat wellicht niet van toepassing is. Anti-virus software en het regelmatig installeren van updates maakt gebruikers immers veiliger, niet veilig in absolute zin. Causaliteit is echter wel de andere maatstaaf voor de bepaling van eigen schuld in het aansprakelijkheidsrecht. Zoals Jaap Timmer beschrijft, "Er moet in ieder geval sprake zijn van een conditio sine qua-non verband tussen de schade en het nalaten bepaalde beveiligingsmiddelen in te zetten. Indien in een specifiek geval kan worden vastgesteld dat de schade niet was ingetreden wanneer van bepaalde maatregelen gebruik was gemaakt, is er in beginsel sprake van een conditio sine qua non-verband." (Timmer 2012) Er moet dus sprake zijn van directe causaliteit en dat is een lastige kwestie met betrekking tot fraude bij internetbankieren. Dan moet bijvoorbeeld vastgelegd worden of de gebruikte malware voor de aanval gedetecteerd had kunnen worden door de anti-virus software. Dit is zeker niet altijd het geval.

Eigen risico

De beslissingen van de Rabobank en de ABN AMRO zijn controversieel, maar niet geheel onverwacht. De algemene tendens is om de grens van verantwoordelijkheid en aansprakelijkheid te verschuiven aangezien internetbankieren dermate ingeburgerd is dat meer van consumenten verwacht mag worden. In februari van dit jaar kwam het idee van een eigen risico bij fraude met internetbankieren al ter sprake. De NVB opperde destijds het idee tijdens een discussiebijeenkomst waarin onder andere de ABN AMRO aangaf al eerder het idee intern besproken te hebben (Security.nl, 2012). Met het eigen risico wil de NVB consumenten vooral wijzen op hun eigen verantwoordelijkheid. Dat kwam ook naar voren tijdens de uitzending van Kassa! waarin Boudewijn benadrukte dat fraude bij internetbankieren een gezamenlijke verantwoordelijkheid kent. Dat zal niemand ontkennen, maar de verantwoordelijkheid van de consument is beperkt. Deze beperkte verantwoordelijkheid heeft onder andere te maken met de beperkte mogelijkheden van consumenten om een aanval of een infectie te detecteren. Criminelen gaan immers steeds geavanceerder te werk waardoor hun aanvallen minder zichtbaar zijn. Zoals ik in het verleden heb beargumenteerd worden de mogelijkheden voor consumenten om zichzelf te beschermen steeds beperkter door deze dalende zichtbaarheid van aanvallen (Van der Meulen, 2011).

> De bank weigert schadeloosstelling omdat de instructies onvoldoende waren opgevolgd

Daarnaast heeft ook ENISA in juli nog het advies aan banken gegeven om er vanuit te gaan dat de computer van de consument geïnfecteerd is en daarop maatregelen te treffen (ENISA, 2012).

> De beslissingen van de banken zijn controversieel

Mogelijke gevolgen

Het niet schadeloos stellen van slachtoffers, hoe beperkt ook, gaat niet geheel zonder gevolgen. Het meest in het oog springende potentieel gevolg is een verlies van vertrouwen van consumenten in de banken en het internetbankieren. Hoewel de banken content zullen zijn met consumenten

die zorgvuldiger zijn, kan dit ook doorslaan. Dat wil zeggen, consumenten kunnen in het uiterste geval internetbankieren gaan mijden en terugkeren naar ouderwets bankieren. Internet bankieren an sich wordt namelijk een risico, zelfs wanneer beveiligingsmaatregelen getroffen zijn. Een verlies van vertrouwen zou vervolgens financiële gevolgen kunnen hebben voor de banken aangezien deze ontwikkeling met grotere kosten gemoeid zou gaan.

Slachtoffers schadeloos?

Een mogelijke tweede gevolg is de roep naar betere beveiliging van internetbankieren. Dit is een ongewenste ontwikkeling. Het huidige systeem voorziet grotendeels in een balans tussen gemak en beveiliging. De hoeveelheid schade is, zoals eerder aangegeven, relatief klein waardoor een investering in meer preventiemaatregelen economisch niet per se verantwoord zou zijn. Deze gevolgen zouden meer schade en kosten kunnen opleveren dan de schade die geleden is door de slachtoffers die niet schadeloos gesteld zijn. Het is daarom ook de vraag hoeveel een dergelijke beslissing waard is voor de bank. Als de omvang van de schade met internetbankieren relatief gezien meevalt, dan is het aantal gevallen waarvan de bank oordeelt dat het slachtoffer in kwestie onzorgvuldig heeft gehandeld nog beperkter. Daar valt financieel gezien weinig te halen.

> Consumenten kunnen in het uiterste geval internetbankieren gaan mijden

Een andere verklaring zou zijn om dit als waarschuwingssignaal richting de consument te sturen. Het altijd vergoeden van fraude met internetbankieren kan leiden tot onverschilligheid aan de kant van de consument, waardoor deze beveiliging in zijn geheel negeert. Maar dit roept wederom de vraag op hoeveel is dat signaal waard?

Conclusie

De grens van aansprakelijkheid bij fraude met internetbankieren is aan het verschuiven. De vrijblijvendheid van waarschuwingen lijkt inmiddels officieel ten einde te zijn gekomen. Deze ontwikkeling is niet geheel zonder gevolgen. De overheersende onduidelijkheid over de begrippen onzorgvuldig en nalatig is problematisch en kan leiden tot een verlies aan vertrouwen. Daarnaast is causaliteit in het geval van malware een lastige kwestie. De vraag is echter of andere banken zullen volgen. En zo ja, wanneer? Want hoewel banken het risico lopen dat consumenten digitale diensten gaan weigeren vanwege een gebrek aan vertrouwen, hangt de dreiging in de lucht. En wanneer het voorbeeld van de Rabobank en de ABN AMRO eerder regel dan uitzondering wordt zullen de zorgen voor consumenten aanzienlijk toenemen.

Referenties

ENISA (2012). 'Flash note: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps.' Beschikbaar op: http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps (laatst geraadpleegd 31 oktober 2012).

The Local (2012). Phishing victims' losses are own fault – court. Beschikbaar op: http://www.thelocal.de/money/20120425-42161.html (laatst geraadpleegd 31 oktober 2012).

Van der Meulen, N.S. (2011). Between Awareness and Ability: Consumers and Financial Identity Theft. Communications & Strategies, First Quarter 2011: 23 – 44.

Nederlandse Vereniging van Banken (2012). 'Fraude internetbankieren stijgt eerste halfjaar met 14 %.' Beschikbaar op: http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14_.html (laatst geraadpleegd op 31 oktober 2012).

Security.nl (2012). 'Banken willen eigen risico voor internetbankieren.' Beschikbaar op: http://www.security.nl/artikel/40507/1/Banken_willen_eigen_risico_voor_internetbankieren.html (laatst geraadpleegd op 31 oktober 2012).

Timmer, J. (2012). Aansprakelijkheid en schadevergoeding. Beschikbaar op: http://www.iusmentis.com/aansprakelijkheid/onrechtmatigedaad/ (laatst geraadpleegd op 31 oktober 2012).

COLUMN

2012: PRIVACY IS OM TE LACHEN! OF OOK: TAARTEN BAKKEN MET TEEVEN

"The current criticism is a little bit misinformed", sprak de altijd geweldig quotebare Schmidt van Google toen de eerste kritische noten gekraakt werden over de nieuwe algemene voorwaarden van het bedrijf. Toen hij dat liet volgen door "Google makes it very easy for you to be very private", wist ik precies weer waarom ik graag naar deze meneer luister. Als er twee zinnen uit zijn mond vandaan gekomen zijn, lig ik alweer gierend van het lachen op de grond. Overigens zal meneer Schmidt wel gelachen hebben als een boer met kiespijn, want het label 'a little bit misinformed' werd met een genadeloze kamikazeklap op Google zelf geplakt door alle Europese Data Protection Agencies.

Ik moest trouwens ook heel erg lachen om de topman van Amazon die in FD doodleuk riep dat al die discussie over privacy en de cloud "pure bangmakerij was". Dat wij toch vooral niet moesten denken dat de Amerikaanse overheid geïnteresseerd zou zijn in onze data. Het klonk als "rustig doorlopen mensen, er is hier niets aan de hand". De opmerking was zo uitermate ridicuul dat het grappig werd, want zo stelde hij ook nog, die Nederlandse wetenschappers die onderzoek hebben gedaan naar privacy en de cloud die zaaien echt alleen maar Fear Uncertainty & Doubt. Natuurlijk beste Amazon, dat is ook echt het wezenskenmerk van onafhankelijk onderzoek. Maar ik snap het best hoor, een niet fraaie boodschap die ook nog eens wetenschappelijk onderbouwd is, hoe pareer je dat in vredesnaam? Tsja, daar zou ik ook wel een beetje raar van gaan stotteren.

En wat te denken van het meest geweldige toegewezen patent van 2012? Jawel. Facebook heeft een jarenlange strijd gewonnen en heeft een heus patent toegewezen gekregen voor… haar privacyinstellingen! Die instellingen waren van dermate unieke aard dat de toekennende instantie niet anders kon dan oordelen dat dit wel degelijk patenteerbaar is. Ja, uniek zijn die instellingen zeker, ik ben tot op heden namelijk nog niemand tegengekomen die er echt wijs uit kon worden. Dus, chapeau voor het meest lollige patent van 2012. In de beschrijving staat trouwens de volgende prachtige zinsnede: "As social networking has grown more popular, users have realized a need for a certain amount of privacy." Nee, zou je denken?

En ach, misschien niet heel chique, maar ik moest ook zo gniffelen om onze eigen overheid en onze handhaver OPTA. Die met zoveel bombarie aankondigden dat de privacy van burgers beter beschermd zou gaan worden met de cookiewet. U weet wel, dat stukje prachtwet waardoor u nu niet meer het door publiekgeld betaalde 'Uitzending gemist' kunt kijken omdat u uiteraard net als ik niet-functionele cookies weigert. Nou, die overheid en die OPTA dus (die zelf groots aankondigden dat het handhaven van de cookiewet een van de grootste prio's is) die zelf op de dag dat de wet bewaarheid werd niet-functionele cookies lieten draaien zonder enige optie tot decline voor de bezoeker. Oeps. Oh! En dan die ochtend dat ik wakker werd, Twitter aanklikte en ik hele kuddes aluhoedjes ontwaarde in de timeline, allen op zoek naar het spreekwoordelijke 'Edwin-de-Rooij-van-Zuyde-wijn-schroefje' in de trams van de RET. Klaarblijkelijk luisterde de RET alle reizigers af ("dat is voor de veiligheid") door stiekem microfoontjes te plaatsen in de tram. Prachtige foto's zag ik van tramstoelen, banken, palen en plafonds met vermeende vreemde objecten daarin verborgen. Massaal waren we paranoide geworden en heel even ontwaarden wij ons overal bespied. Heel even hè, want u weet natuurlijk allemaal dat er verder in Rotterdam echt nergens mensen gevolgd worden en dat er daar al helemaal geen sprake van is dat Big Brother op elke straathoek meeloert.

Nog een uitsmijter dan. De prachtige meneer Teeven. Wat hij voor de privacy betekent is van ongekende heerlijkheid. Zo mag het CBP straks per jaar 60.000 datalekmeldingen ontvangen. Natuurlijk heeft het CBP daar geen geld en mankracht voor, volgens Teeven ook niet zo nodig, na een jaartje kijken we wel hoe het met jullie gaat, suste hij het CBP toe. Ik moest al een beetje lachen, want zouden die privacygekkies nu echt denken dat het meneer Teeven om privacy te doen is? Hij gaf privacyminnend Nederland een lolly en zei vervolgens "ja, sorry dat jullie het papiertje er niet kunnen afhalen, ik kan er ook niets aan doen dat jullie geen armen hebben". Het is ook een lastig vak dat privacygedoe, meneer Teeven. Ik snap dat. In augustus riep Teeven namelijk nog dat de privacy van inbrekers beter beschermd moet worden en dat het een grote "foei" is als iemand online foto's plaatst van het geboefte. Nog geen maand later heeft hij het alweer over het inbrekersvak. Als je betrapt wordt tijdens je werkzaamheden en je wordt daarbij doodgeknuppeld dan is dat een "inbrekersrisico". Ik zag het voor me. Op goede nacht wordt Rachel wakker van een inbreker, samen met haar Lief sluipt ze het bed uit. Lief pakt de honkbalknuppel en met een forse mep tikt hij de inbreker onderuit. Rachel heeft altijd haar iPhone in de aanslag en knipt als een razende foto's en zet die op Facebook. De volgende dag mag Lief een taart met een vijl gaan bakken voor Rachel, volledig volgens het privacyrecept van Teeven.

Mr. Rachel Marbus, @RachelMarbus op Twitter

KENNISMAKING MET: ALF MOENS

Als IT-er krijg je al gauw te maken met beveiligingsvraagstukken. Dat is nu zo en dat was ook zo toen ik in de IT begon in 1985. Tot 2000 waren dat voor mij nog incidentele projecten, al had ik bij IVEV ook al te maken met het hacken van inbel-accounts en misbruik van X.25-connecties. Vanaf 2002 is beveiliging mijn dagtaak, eerst als security officer voor TU Delft, sinds dit jaar coördineer ik beveiligings-, privacy en identity management initiatieven voor de bedrijfsvoering en de onderwijsondersteuning in het hele Hoger Onderwijs. Ik ben geen hardcore beveiliger, ik ben vooral bezig met het regelen, organiseren en coördineren. Wel wil ik het overzicht houden en ook probeer ik zo goed mogelijk op de hoogte te blijven van dreigingen, van nieuwe technieken. Lastig zat.

Bijzonder interessant was het om, op latere leeftijd, terug te gaan naar school en een master opleiding te doen. Ik had eerder eigenlijk mijzelf beloofd dat ik nooit meer tentamens of proefwerken zou hoeven maken. In de praktijk in de opleiding viel dat wel mee, al krijg je wel flink kramp in de vingers als je drie uur achter elkaar aan het pennen bent voor onmogelijke juridische opgaven. De TIAS-master was in meerdere opzichten een waardevolle investering. Uiteraard vakinhoudelijk maar ook voor het opdoen van blijvende goede contacten. De collega MSITs en MISM-ers kom ik heel veel tegen in 'het veld'. In de afronding van mijn master heb ik de basis gelegd voor

mijn werk nu bij SURF, het meten van volwassenheid van beveiliging.

Wonen en werken in de trein

Na mijn repatriëring naar het zuiden van het land in 2000 hebben wij thuis besloten niet meer te gaan verhuizen voor het werk. Dat betekent dat ik al tien jaar een flink deel van de dag in treinen woon en werk. Dat is op zich niet zo erg (in de tijd dat ik in Delft werkte heb ik alle 8 seizoenen van 24 gezien, precies een aflevering per terugreis); minder leuk is al het wachten, bij overstappen of bij uitval van treinen. Ik woon met veel plezier in Midden Brabant en kan me lekker uitleven op groot onderhoud in de tuin. Soms, niet vaak genoeg, pak ik de racefiets en maak een tocht van 2, 3 uur door bos en hei op de grens van België en Nederland.

Zelf iets bijdragen aan de ontwikkelingen

In het bestuur van het PvIB vervul ik nu de rol van vice-voorzitter. Ik zal me daarbij hoofdzakelijk richten op interne aangelegenheden van de vereniging: zorgen dat alles reilt en zeilt. Daarnaast pik ik er zo nu en dan wat leuke dingen uit om me ook inhoudelijk mee te bemoeien. De belangrijkste reden voor mij om een bestuursfunctie in te vullen is dat ik vind dat ik zelf iets moet bijdragen aan de ontwikkelingen in het vakgebied, buiten wat ik via mijn werk al doe. Daarnaast stelt het mij in staat een van mijn contactnetwerken te verstevigen. Ik merk in de praktijk dat vooral het combineren van verschillende netwerken, Hoger Onderwijs, PvIB, CIO Platform, ISACs, zeer waardevol is in het proces van informatie geven en nemen.

DIEPGAANDE KENNIS VAN SOFTWARE-ONTWIKKELING IS CRUCIAAL

INTERVIEW MET GARY MCGRAW

Gary McGraw is de CTO van Cigital, Inc., een software security adviesbedrijf gevestigd in Dulles, Virginia, vlak bij Washington D.C. Cigital heeft ook een vestiging in Amsterdam aan de zuidas. Gary is de auteur van meerdere boeken over software security en heeft meer dan 100 wetenschappelijke artikelen op zijn naam staan. Hij is te bereiken via gem@cigital.com. Opmerkingen of vragen naar aanleiding van dit interview kunnen gestuurd worden naar lex.borger@domustechnica.com.

Op 8 mei had ik het genoegen om een gesprek te hebben met Gary McGraw. Hij was in Nederland voor een OWASP presentatie en de BSIMM European Community Conference, twee verschillende doelen dacht ik, maar in het gesprek kwamen die twee nader tot elkaar. Ik kwam er al snel achter dat Gary een drukke agenda heeft. Hij schrijft veel - boeken en artikelen. Soms komt het verzoek voor een artikel van ver buiten het securityveld. Ook dit overweegt hij altijd. "Het helpt om naar een nieuw publiek uit te reiken."

Gary reist ook veel. "Ik geef ongeveer 35 presentaties per jaar, waarvan 10 tot 15 keynotes zijn voor meer dan duizend mensen. Dat is gewoon een deel van wat ik doe. Maar weet je, ik kijk geen TV. Nooit." Verder woont hij landelijk en speelt in een band. Zijn bedrijf hem al in bescherming genomen tegen een te druk schema. "Vier jaar geleden hebben ze tegen mij gezegd: Je bent jong, maar je kunt niet aan een stuk blijven reizen de komende 10 jaar, je put jezelf uit. Stel voor jezelf een leefpatroon in dat wél werkt, dat je vol kunt houden. Dat was een prachtadvies. Zo hebben we 'no-fly-July' ingesteld. In juli zit ik niet in een vliegtuig. Ik blijf thuis, zit op mijn steen in de rivier. Als mensen mij willen zien dan zitten ze bij mij op de steen in de rivier. Ik lees dan veel en denk na. Dat is zo'n waardevolle gewoonte voor mij geworden dat ik het nu ook in december toepas, 'no-fly-Noel'. Ik blokkeer een week per maand waarin ik niet op pad ga en ben ieder weekend thuis. In de overige tijd, wie weet waar ik ben… Mijn agenda is het komende jaar al gevuld."

Silver Bullet Security podcast

Ik luister veel naar podcasts en heb een abonnement op de podcast van Gary, de Silver Bullet Security podcast, maar ik hoor hem ook op andere podcasts langskomen als gast. Ik maakte de opmerking dat hij het in zijn eigen podcast nooit heeft over zaken als BSIMM. Gary is daar simpel en direct over: "Mijn podcast gaat niet over mijn werk."

Harde gegevens verzamelen

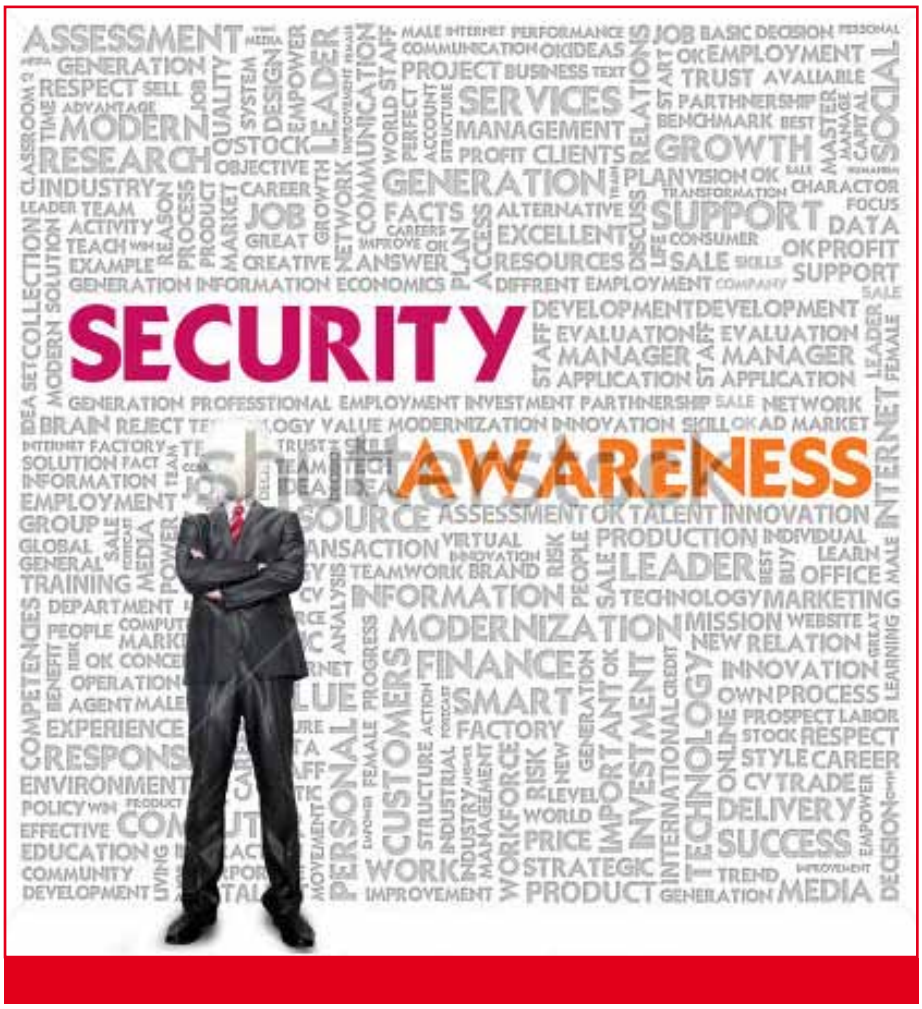
Zo gaan we naadloos over in het ontstaan van BSIMM. "Het is organisch gegroeid. Er zit een leuk verhaal achter. Toen ik voorzitter was van de technical advisory board bij Fortify hadden ze een jonge ingenieur de opdracht gegeven een software security methode te ontwikkelen. Hij presenteerde deze methode aan de directie en hij werd aan stukken gereten. Ze vroegen waarom er een nieuwe methode nodig was, "we hebben de zeven Touchpoints, Microsoft's SDL, OWASP CLASP en hier voeg jij er wéér een aan toe!" We hadden hier een discussie over en ik kreeg de ingeving om eens in de buitenwereld echte gegevens te verzamelen en dáár een model omheen te bouwen dat de data beschrijft. Ik heb negen vrienden gebeld bij bedrijven en ze gevraagd of ze mee wilden doen aan wetenschappelijk onderzoek voor software security. We verzamelden een heleboel gegevens en Brian Chess, Sammy Migues en ik hebben drie dagen bij mij thuis doorgebracht met ploeteren door de gegevens, argumenteren over wat er gezegd was, structureren van de informatie, samenstellen van het raamwerk en alle activiteiten benoemen. Het was een zeer creatieve bezigheid, inmiddels drie jaar geleden. Nu hebben we het aantal

BSIMM is organisch gegroeid

BSIMM

BSIMM (spreek uit als "biesim") staat voor "Building Security In Maturity Model". Het BSIMM is opgezet om een software security programma binnen een bedrijf begrijpelijk en meetbaar te maken. Het model kan gebruikt worden als uitgangspunt bij het opzetten of evalueren van zo'n programma. Het BSIMM is het resultaat van observatie en analyse van bestaande software security programma's bij meer dan 50 vooraanstaande bedrijven. In September 2012 is BSIMM versie 4 gepubliceerd.

bedrijven in de dataset vervijfvoudigd en de data zelf vertienvoudigd. Er zijn bedrijven die meerdere malen gemeten zijn, sommige bedrijven hebben deelmetingen gedaan. Wij publiceren alleen de globale resultaten, maar de hele dataset bevat een verbazingwekkende hoeveelheid informatie."



Dingen die iedereen doet

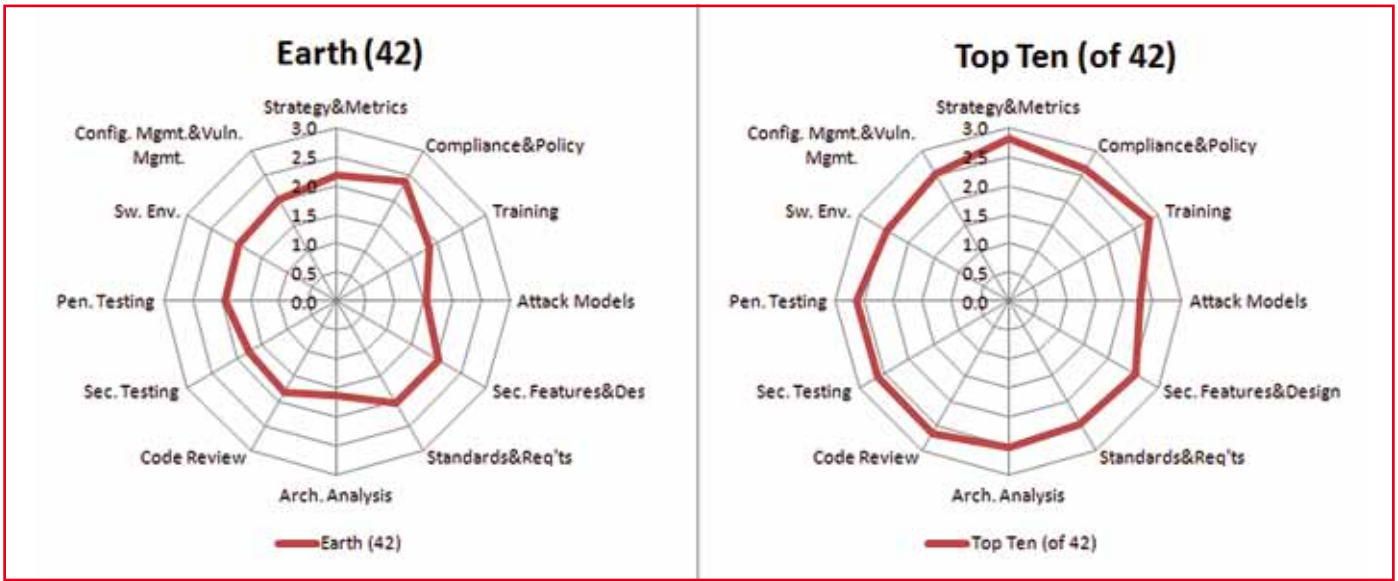
Ik had als voorbereiding uiteraard BSIMM versie drie doorgenomen en ik maakte de opmerking dat het softwareproject waar ik in zat niet alles deed uit de lijst 'Stuff everybody does'. "Er is een voorbehoud: 'iedereen' slaat maar op 67% van de bedrijven. Soms zijn activiteiten niet zinvol in de (bedrijfs)cultuur of de organisatie en dat is OK. We zijn daarom ook erg voorzichtig in onze presentatie van de BSIMM activiteiten en geven duidelijk aan dat dit is wat andere bedrijven doen. Je kunt hier naar kijken en beoordelen of het voor jou zinvol is. Wij zeggen niet dat je dit moet doen. BSIMM is een beschrijvend model. Er zijn critici die vinden dat bepaalde activiteiten niet thuishoren in het model en kraken het daarom af. Voor hen heb ik het advies: Lees het document, dat is niet wat we gezegd hebben. Ga de bron, bijvoorbeeld Microsoft, vertellen dat ze activiteit X niet moeten doen en kijk of ze naar je willen luisteren."

"Een probleem wat we hadden in het werkveld van software security is dat er een aantal mensen werken die een opinie hebben die niet gebaseerd is op feitelijke gegevens. Nu hebben we een hoop informatie waar we naar kunnen verwijzen. Bijvoorbeeld, ik heb in een blog geschreven dat je een software security team moest hebben in je organisatie. Want als je dat niet hebt, hoe weet je dan wie hiervoor verantwoordelijk is? Dus, richt een security team in. En ik kreeg commentaar op mijn blogpost van mensen die aangaven in hun IT-afdeling van zeven man alle security erbij te doen. Een discussie volgde. Nu kan ik uit de BSIMM-data zeggen dat ieder bedrijf uit de BSIMM-dataset een bestuurder heeft die verantwoordelijk is voor software security en er is ongeveer één software security teamlid per vijftig ontwikkelaars."

Security team

Security is veranderd

Al filosoferend komen we op de veranderingen in het vakgebied. "De toplevel security managers van nu sturen informatiebeveiliging totaal anders aan dan tien jaar geleden. En dat is goed.



Ze vragen om meer informatie, ze eisen een meetbaar resultaat, ze besturen het meer als een bedrijf. Die managers zijn voor ons fijn om mee te werken. Bij Cigital proberen we niet security budget af te snoepen van een grote hoop. In plaats daarvan benoemen we problemen die opgelost moeten worden en wijzen daar budget aan toe. Een strategische aanpak vanuit de top is te verkiezen boven het veranderen van IT-systemen aan de onderkant. Je moet wel je zaak bepleiten met gegevens die dat ondersteunen. Wanneer je een spider-chart maakt voor een bank, waarbij je het bedrijf vergelijkt met alle andere banken, geeft het voldoening wanneer je het laat zien aan de CIO, een machtige man binnen de bank. Hij vraagt dan gelijk door over de aspecten in de tabel waarbij ze achterblijven ten opzichte van de concurrentie. Ze willen weten of dat een slecht teken is en wat ze in dat geval eraan kunnen doen. "Het werken aan BSIMM is een plezier. We hopen nu dat we in Europa ook een gemeenschap kunnen opzetten die even sterk is als in de VS. Een gemeenschap van mensen die informatie uitwisselen en samen willen werken. Over drie dagen weet ik het." Gary doelt hierbij op de BSIMM European Community Conference, die ten tijde van het gesprek nog moest plaatsvinden. "We hebben twaalf grote bedrijven doorgelicht in Europa. Ik zou graag zien dat dit doorgroeit naar dertig in de komende twee jaar. Als we in London kunnen doorbreken zoals we in New York hebben gedaan, dan zal dit zo bereikt zijn. En veel bedrijven in London hebben ook een kantoor in New York…"

> Mijn podcasts gaan niet over mijn werk

Wie moet software security leiden?

"Over het algemeen komen mensen in IT security uit operationeel beheer, netwerkbeheer of systeembeheer en ze weten veel van de infrastructuur van security. Ze weten wat een SOC (security operations center) is en hoe dat werkt. Maar het zijn niet de beste mensen om met software security bezig te gaan. Zo iemand met ontwikkelaars laten werken om ze software security bij te brengen is als een hond voor de wolven gooien. De hond overleeft het niet."

"Mijn indruk is - en ik heb geen wetenschappelijke onderbouwing hiervoor - dat in Europa de eerste generatie software security professionals operationele security mensen waren. Ze liepen tegen de ontwikkelaars en de top-managers op zonder voortgang te boeken. Dus we hebben nu mensen nodig met een gedegen software ontwikkelingsachtergrond die de strekking van het verhaal kunnen bijsturen. Penetration testing is alsof je stenen gooit naar je vrienden. De software ontwikkelaars willen niet

Bugs

geraakt worden door stenen. Je maakt op die manier geen vrienden."

Vooruitgang…

"Er zijn mensen die zeggen dat software security helemaal geen vooruitgang boekt. We hebben nu vijf, tien jaar gewerkt aan beveiliging en de software ziet er nog steeds problematisch uit. Waarom moeten we nog geld spenderen aan software security? Het antwoord is complex. Eigenlijk boeken we goede vooruitgang, de defect-density-ratio (het aantal problemen per regel code) daalt. De trend gaat de goede kant op. Het lijkt alsof we geen vooruitgang boeken omdat de hoeveelheid software nog sneller groeit. De hoeveelheid bugs groeit dus, ondanks de vooruitgang. Als we stoppen krijgen we een exponentiële explosie van bugs. Je moet daarom door blijven gaan."

"Ik houd er niet van om incidenten hiervoor te gebruiken. BSIMM geeft me de mogelijkheden om een manager te overtuigen zonder incidenten te gebruiken. Zijn concurrenten hebben we al geanalyseerd. Nu kun je hem gelijk laten zien hoe hij daarmee verschilt, dat hij de langzaamste zebra in de kudde is. Je wilt die zebra niet zijn, want de cheeta's jagen al op je. Dat is veel beter dan stenen laten gooien door pen-testers. Pentesting is nodig, maar gebruik het niet om de aandacht van het management te trekken."

Where's Aubrey?

Aan het eind van het gesprek vraag ik Gary nog iets wat hij zijn gasten ook vaak vraagt, ik vraag hem om zijn muzikale voorkeuren en activiteiten. "Ik speel in meerdere bands. De belangrijkste band waar ik in speel is 'Where's Aubrey', al onze muziek is online te krijgen en we hebben 6 CD's uitgebracht. 'Luminous' is de meest recente, uitgekomen in december 2011. Ik speel al viool sinds ik drie jaar oud ben. Een andere band waar ik net mee begonnen ben is 'The Bitter Liberals'. Daar zal je binnenkort meer over horen. Een derde band is een Django Reinhardt coverband, 'Hot Club Millwood'. Muziek is belangrijk voor mij. Toen ik er voor koos om naar de universiteit te gaan en niet naar het conservatorium, kwam ik er achter dat ik moeilijker in het leven stond omdat ik geen muziek meer speelde…"

Gary on stage

> Security wordt nu anders aangestuurd dan 10 jaar geleden

Gary is een expert met enthousiasme en passie. Experts hebben we genoeg, maar in ons vakgebied wordt het nogal snel mat en droog. Ik bewonder zijn energieke enthousiasme en passie. Die werken om management te overtuigen. En voeg daar een instrument als BSIMM bij om het inhoudelijk af te maken.

Links

- *OWASP: https://www.owasp.org/*
- *BSIMM: http://bsimm.com*
- *Gary McGraw: http://www.cigital.com/~gem/*
- *Silver Bullet Security podcast feed: http://feeds.feedburner.com/silverbulletsecurity*
- *7 Touchpoints: http://www.buildingsecurityin.com/concepts/touchpoints/*
- *Microsoft SDL: http://www.microsoft.com/security/sdl/default.aspx*
- *OWASP CLASP: https://www.owasp.org/index.php/Category:OWASP_CLASP_Project*
- *Where's Aubrey: http://www.wheresaubrey.com/*

COLLABORATIVE

For the last time this year we look at Business Attributes from the SABSA Business Attributes Taxonomy, looking at each from new perspectives. At this time of the year when we celebrate the passing of the winter solstice and Christmas it is traditional to feast on rich meats, and so in this Issue we shall look at something very 'meaty' – the attribute 'collaborative'.

Let's dwell for a moment on what drives life – human life, any life form, life itself. The answer is, not surprisingly, risk. Without the uncertainty of risk there would be no such thing as life. Life is all about survival, not just in one generation, but also in all future generations – passing on the DNA against the competition from other life forms, both intra-species and inter-species. Competition means winners and losers – the game of life is full of risks. That means opportunities to win and threats of loss. Being in business is just another thread of life – a competitive sport in everyone's experience.

How did human life succeed in dominating life on earth? Answer – collaboration. We see rudimentary forms of collaboration in other species – for example, wolves that hunt in packs and ants that create organized colonies, but it is humans who have made collaboration their specialization. So, at one and the same time we compete fiercely, but we do it best by forming ourselves into collaborative groups that represent common DNA and common goals. At the primeval level there are families, tribes and nations. Translated into modern human culture we see the same, but now with more sophisticated group structures such as teams, companies, international alliances, joint ventures, and many more. The secret of success is collaboration with the right people on the right activities.

One might even create a Business Attributes Taxonomy that has at its root this one single attribute of 'collaborative', and from that single root one could argue that all other more granular attributes can be seen to flow. Let's look at some that are obviously sub-atomic components of an atom called 'collaborative'. Trusted, trusting and trustworthy come to mind immediately, and from these flow all of the operational-risk-related attributes with which we are familiar – the entire taxonomy.

What are the enablers of collaboration? They include many things but here are a few that are essential: intellectual property that can be shared but at the same time protected and leveraged for its value; shared processes that can be used to create end-to-end value chains; shared culture and socio-economic values; semantics of a common language for describing business scenarios and architectural responses; organizational structures and governance models; and above all, relationship management, since collaboration is all about relationships.

One of the fundamentals of SABSA Business Attribute Profiling is the ability to set performance targets and measure actual performance against target. So how shall we approach performance measurement for this attribute 'collaborative'? When you look at Google's search results on the phrase 'measuring collaboration' you get a lot of research papers popping up. One in particular, [Zutshi 2010], has interesting insights that are paraphrased here.

The key driver for collaboration is not idealism, but economic or value reciprocity, the willingness for sharing value when expecting or hoping to get something in return. Apes share bananas with the threat of hunger, but with the opportunity to get more bananas in return. So the key is exchange of value. There are three aspects: the willingness for sharing value; the value itself and the capability to do so.

From a SABSA point of view the willingness can be expressed as drivers; value can be expressed in terms of performance targets, and the capabilities are the logical services. The eight parameters and sub-parameters discussed in [Zutshi 2010], which address collaboration performance, can be regarded as control and enablement areas.

According to the laws of nature, willingness to share appears to be the greatest when there is an optimal match between 'genes' of collaborating organisms or between Business Attributes Profiles (BAPs) of two corporate entities. This influences the overall performance. The better the match, the better the performance. So, collaboration comes 'naturally' and is a matter of comparing BAPs. This willingness also depends on the amount of bananas expected to be hidden in the trees (expressed as business drivers).

Collaboration performance is also determined by capabilities. These capabilities are not only technical but rather socio-technical (people, process and technology). Depending on the number of bananas and the willingness for creating a match, there is some operational risk in the exchange of value, both opportunities and threats. The relationship itself becomes the asset, but is still driven by the same value drivers – the desire for more bananas. We wish you a Happy Christmas with nice rich meat and plenty of bananas too.

The Attributer

Link

[Zutshi 2010]: http://run.unl.pt/bitstream/10362/2646/1/Zutshi_2010.pdf

Dit artikel is mogelijk gemaakt door:

SIDN

https://www.sidn.nl/

DNS, HET 'LAATSTE' ONBESCHERMDE PROTOCOL

Marco Davids, technisch adviseur bij SIDN en bereikbaar via Marco.davids@sidn.nl of Twitter: @marcodavids

De geschiedenis van het internet mag fascinerend worden genoemd. Ontstaan in een academisch klimaat, waar men elkaar kende en vertrouwde, is het uitgegroeid tot een gigantische, globale infrastructuur met miljarden gebruikers. Talloze ondernemingen zijn voor hun voortbestaan afhankelijk van het internet. Maar uiteraard zijn er ook criminelen, die een graantje (vaak meer) mee proberen te pikken van het geld dat in 'cyberspace' is te verdienen. Logisch dus, dat er op het gebied van beveiliging veel moest worden verbeterd. In een poging om de slechteriken buiten de deur te houden, surfen we steeds vaker via SSL/TLS verbindingen, zijn we gewend geraakt aan VPN's en hebben we 'Telnet' al jaren geleden verruild door SSH. In dat licht bezien was het opmerkelijk dat de beveiliging van één van de meest essentiële internetprotocollen, het DNS, lange tijd op zich liet wachten.

Het DNS (Domain Name System) kan worden beschouwd als het telefoonboek van het internet. Vrijwel elke applicatie vertrouwt er blindelings op. En dat maakt het voor kwaadwillenden een aantrekkelijk doelwit. Immers; wie in staat is het DNS te manipuleren, kan argeloze gebruikers eenvoudig naar malafide websites leiden, zoals een nagemaakte bankwebsite, met alle nare gevolgen van dien. Maar dat is slechts een voorbeeld. Wie het DNS in zijn macht heeft, kan wachtwoorden en e-mail onderscheppen, (advertentie)inkomsten stelen, antivirussoftware om de tuin leiden, beurskoersen beïnvloeden en tal van andere obscure activiteiten ontplooien. En dat het geen 'rocket science' is om dit daadwerkelijk te doen en de dreiging dus reëel is, werd in 2008 nog eens feilloos aangetoond door veiligheidsonderzoeker Dan Kaminsky.

Toenemende dreiging

Naarmate kwetsbaarheden steeds vaker worden aangepakt en de mogelijkheden van misbruik zodoende beperkter worden, komt het DNS als aanvalsvector meer in beeld bij internetcriminelen. Het is dus niet verwonderlijk dat het redelijk gedateerde DNS (het protocol stamt uit 1983), uiteindelijk ook een beveiligingsuitbreiding heeft gekregen. DNSSEC, wat staat voor 'DNS SECurity extensions', kende een moeizame start - maar wint de laatste tijd gestaag aan populariteit. Daar staat tegenover dat het oude vertrouwde DNS-protocol, hoewel misschien niet veilig, wel erg stabiel is. Het vergt weinig onderhoud. DNSSEC is complexer en dat weerhoudt nog altijd veel organisaties ervan om over te schakelen. Desondanks is er een redelijk groot draagvlak voor DNSSEC ontstaan. De kennis over de materie is steeds meer gemeengoed geworden en er is inmiddels prima ondersteuning voor in software. Daarnaast wordt het volop toegepast in de kern van de 'DNS name space'. De 'rootzone' (daar waar de wereldwijde DNS-hiërarchie begint) is al sinds 2010 beveiligd en ook steeds meer toplevel domeinen, zoals .com en .org zijn beveiligd met DNSSEC. Ook het Nederlandse landendomein (.nl), dat beheerd wordt door SIDN, is al sinds 2010 beschermd. Ruim 1,2 miljoen .nl-domeinamen zijn inmiddels voorzien van digitale handtekeningen ten behoeve van DNSSEC.

Pas-toe-of-leg-uit

SIDN heeft daarnaast ook een belangrijk aandeel gehad bij het onder de aandacht brengen van DNSSEC bij de Rijksoverheid, dat een beleid hanteert voor het stimuleren van 'open standaarden'. Sinds enkele maanden zijn (semi-)overheidsorganisaties verplicht om DNSSEC te implementeren volgens het 'pas-toe-of-leg-uit' regime, en sinds dat moment zijn domeinnamen zoals 'rijksoverheid.nl', 'kabinetsformatie2012.nl' beschermd met DNSSEC.

Samenvattend

DNSSEC draagt dus bij aan een betere bescherming van het internet. En dit effect wordt groter, naarmate meer partijen overschakelen van DNS naar DNSSEC. Met DNSSEC worden ook nieuwe toepassingen mogelijk. Wanneer DNS-antwoorden weer 100% betrouwbaar zijn (en dat is waar DNSSEC voor zorgt), kunnen we

De uitloop van dit artikel staat op pagina 21

GEVAAR CYBERWAR KOMT UIT ONVERWACHTE HOEK

Erik Remmelzwaal is CEO van DearBytes, specialist in IT-beveiliging. DearBytes helpt bedrijven de regie te houden over de beveiliging van hun dierbare informatie én zakelijke systemen, zoals computers, servers, hypervisors, en mobiele apparaten. Erik is bereikbaar via erik.remmelzwaal@dearbytes.nl

De term 'cyberwar' wordt te pas en te onpas gebruikt. Vaak voor gebeurtenissen of incidenten die eigenlijk niets met oorlog te maken hebben. Bruce Schneier stelt zelfs dat dit verkeerd gebruik bewust gebeurt en dat de dreiging van een cyberoorlog zwaar wordt overdreven. En met die stelling krijgt hij bijval uit het Witte Huis. Howard Schmidt, voormalig Cyber Security coördinator van de eerste Obama regering, stelt dat cyberwar vaak wordt gebruikt om gevallen van online criminaliteit, sabotage of identiteitsfraude aan te geven. Fear sells, door bij elk incident van cybercrime weer te wijzen op de dreiging van een cyberwar, stijgen de zorgen. Wat vervolgens de weg vrij maakt voor verruiming van budgetten en wetswijzigingen waarmee de overheid het internet steeds meer probeert te bewaken (lees: monitoren). Commerciële partijen en overheidsorganen in de hoek van 'cyber intelligence' en opsporing profiteren hiervan, ten koste van onze (online) privacy. Een heel onwenselijke gang van zaken, als je het mij vraagt. Het zet namelijk de geweldige verworvenheid van het open internet en vrije informatie onder druk.

Door het foutief gebruik van de term cyberwar dreigen organisaties afgeleid te worden van wat er werkelijk moet gebeuren. Waar wij als samenleving en in onze economie écht last van hebben, zijn cyberspionage en -criminaliteit. Deze twee problemen vereisen een hele andere aanpak dan het opbouwen van een digitale krijgsmacht waar met cyberwar op in wordt gezet. Wat in de strijd tegen cybercrime hard nodig is, is dat wij allemaal onze eigen verantwoordelijkheid nemen om onze 'digitale kroonjuwelen' proactief te verdedigen. Dat organisaties ervoor zorgen dat ze de baas zijn over de beveiliging van hun IT-systemen en dierbare informatie. Ik ben van mening dat wanneer de bestuurders van deze wereld in de basis gaan inzien dat ze hun kritische data en systemen moeten koesteren, de samenleving vanzelf minder kwetsbaar wordt. Dat leidt vervolgens tot minder incidenten en zullen we zien dat het wel meevalt met die cyberwar.

Verantwoordelijkheid nemen

Laten we ons dus niet van de wijs brengen door oorlogsretoriek en vooral onze eigen verantwoordelijkheid nemen! Hoe? Door onze eigen risico's in kaart te brengen en het gebruik van gevoelige informatie binnen onze eigen omgeving te reguleren. Welke informatie en systemen zijn kritisch voor mijn voortbestaan, en hoe zorg ik ervoor dat ze niet in verkeerde handen komen? Is het dan allemaal onzin, die zogenaamde cyberwar? Nee dat niet. Naties zijn, zo kunnen we allemaal lezen, hun cybercapaciteiten aan het opbouwen. Zodat zij in het geval van een oorlog via het internet aanvallen kunnen uitvoeren of af slaan. Dergelijke cyberaanvallen zullen echter altijd onderdeel uitmaken van een groter geheel met ook conventionele wapens en diplomatie. Dat landen elkaar alléén via het internet bestoken en daarmee een ruzie kunnen beslechten, is echt uitgesloten. We hebben het wel over 'oorlog', en dat middel wordt niet zomaar ingezet.

WESECURE EMBASSY EVENT

VOLGT NOG OP 26 NOVEMBER

Hier staat de uitloop van de kennis-reportage van SIDN

Graag het artikel inkorten, zodat het passend wordt.

het gebruiken bij de beveiliging van andere toepassingen. Zo kunnen we met de nieuwe DANE-standaard (RFC6698) het PKI-systeem beter beveiligen. Met DANE (en DNSSEC) had het Diginotar-debacle zodoende kunnen worden voorkomen. Wilt u meer weten over DNSSEC, kijkt u dan op www.dnssec.nl.

Links

http://en.wikipedia.org/wiki/Dan_Kaminsky

Pas-toe-of-leg-uitregime:
www.forumstandaardisatie.nl/
open-standaarden/voor-overheden/
pas-toe-of-leg-uit-regime/

Meer informatie over DSNSEC:
www.dnssec.nl

WESECURE EMBASSY EVENT

VERVOLG

WESECURE EMBASSY EVENT

VERVOLG

BEVEILIGING SAAS DIENSTEN VAAK DISCUTABEL

Maarten Hartsuijker is beveiligingsconsultant en ethisch hacker bij Classity en bereikbaar via @classityinfosec.

De afgelopen maanden zijn we opgeschrikt door vele datalekken. Eind 2011 maakte Cheaptickets één foutje en de gegevens van 715.000 klanten konden eenvoudig gestolen worden. Begin 2012 stond KPN volop in het nieuws met een inbraak in de IT-omgeving die wordt gebruikt voor haar DSL en InternetBelDiensten.

Datalekken onvoorstelbaar

Voor veel mensen is het onvoorstelbaar om te lezen hoeveel er op het beveiligingsvlak mis blijkt te zijn bij een grote partij als bijvoorbeeld KPN. Naast het bedienen van miljoenen klanten heeft het bedrijf immers tevens de verantwoordelijkheid over een stuk vitale infrastructuur. Bij de meeste informatiebeveiligers oogsten de incidenten van de afgelopen maanden een hoop herkenning. Het is geen verrassing dat KPN niet anders blijkt te zijn dan de rest van corporate Nederland (en de rest van de wereld). Wat wel bijzonder is aan een inbraak bij een grote IT-dienstverlener is de impact die zo'n inbraak heeft op andere bedrijven en consumenten. Door de enorme hoeveelheid klanten heeft een enkele fout grote consequenties.

SAAS vaak aantrekkelijk alternatief

Ditzelfde zien we terug bij SAAS diensten (al dan niet uit de cloud). Ook bij SAAS dienstverlening verzamelen grote groepen klanten zich in een centrale omgeving. Op basis van de aanname dat een grote service provider in staat is om een betrouwbare dienst te leveren, worden vertrouwelijke persoonsgegevens, bedrijfsgegevens en transactionele gegevens ondergebracht bij een derde partij. Op het moment dat een informatiebeveiliger het overeen te komen beveiligingskader ter sprake brengt is een vaak gehoorde opmerking: "het bedrijf bedient veel grote klanten. Als het voor hen goed genoeg is, is het dat voor ons toch ook?" En met dit uitgangspunt is de verleiding groot om de noodzaak om eens goed naar de inhoudelijke kwaliteit van de dienst te kijken voor ons uit te schuiven. En dat is niet vreemd als je je bedenkt dat de keuze voor SAAS niet zelden voortkomt uit onvrede over de leveringssnelheid en de kosten van de eigen IT-afdeling. En als SAAS dan een oplossing lijkt, moet je over "the next best thing" natuurlijk niet te kritisch zijn.

SAAS staat voor Software as a Service. Binnen dit model neem je een applicatie als een dienst of van een derde partij, waarbij deze partij je idealiter wat ICT betreft volledig ontzorgt en daarbij de hosting, het beheer en het onderhoud van de applicatie voor zijn rekening neemt.

Legacy in een nieuw jasje

Als informatiebeveiliger test ik regelmatig diensten van derden die verkocht zijn als "software uit de cloud" of SAAS. Met name een goede scheiding van klantdata bij zakelijke SAAS blijkt een ondergeschoven kindje. Dit geldt vooral voor Legacy pakketten die voorheen altijd op de klantlocatie draaiden en nu snel centraal aangeboden moeten worden om aan een klantvraag te voldoen. Omdat de vraag naar SAAS diensten toeneemt, haasten veel leveranciers zich om hier een oplossing voor te verzinnen. De makkelijkste

oplossing is dan om snel een paar servers in een datacenter neer te zetten, er een SAAS en/of Cloud label op te plakken, en klanten uit te nodigen om er gebruik van te maken. Vervolgens wordt vergeten dat er een compleet ander beveiligingsmodel nodig is om meerdere klanten veilig vanuit één IT-infrastructuur te bedienen.

Traditionele beveiligingsoplossingen onvoldoende

Binnen een multi-customer infrastructuur gaan traditionele beveiligingsconcepten over het algemeen niet meer op. Hierdoor is het resultaat van de beveiligingsaudits die op dit soort omgevingen voor klanten worden uitgevoerd vaak zo bedroevend dat je met weinig inspanning vaak bij de gegevens van alle SAAS gebruikers kunt. Omdat de impact van een inbraak

in zo'n infrastructuur de optelsom van de waarde van alle klantdata is, zijn op dat moment miljoenen persoonsgegevens of administraties van honderden miljoenen feitelijk toegankelijk voor iedereen die dezelfde dienst afneemt. En hier zit ook meteen het grote verschil met het voorbeeld van KPN waar ik in de introductie mee begon. Om connectiviteitspartijen als KPN kun je als klant niet heen, maar consolidatie in een gedeelde infrastructuur is een keuze. Je bepaalt als bedrijf zelf of de impact van misbruik van beveiligingsfouten in software en infrastructuur beperkt blijft tot het eigen personeel, of zich uitstrekt naar iedereen die voor een paar euro toegang tot het platform aanschaft.

Klein beginnen

Als we de berichten mogen geloven kunnen we niet meer om de Cloud heen. De industrie doet ons geloven dat we als we kosten willen besparen en schaalgrootte willen creëren alleen de Cloud nog een oplossing is. Maar het kan verstandig zijn om deze nieuwe hype eerst eens uit te proberen met data met een beperkte vertrouwelijkheid en een niet al te hoge integriteitsclassificatie.

IT-prioriteiten

Soms komt de keuze voor SAAS voort uit onvrede over de IT afdeling. De interne ICT afdeling is vaak druk of heeft geen prioriteit voor aandachtspunten die de business op dat moment erg belangrijk vindt. Hoewel business en IT-alignment vaak wel plaatsvindt en de basis is voor jaarbudgetteringen, is er op nieuwe initiatieven gedurende het jaar vaak slecht in te spelen (de pot met geld is verdeeld). De business besluit de IT-afdeling te passeren omdat er zich een goed alternatief aandient en financiert dit vervolgens uit andere potjes. Software uit de Cloud lijkt dan vaak te zorgen voor een goed beheersbare investering. De IT lijkt nog steeds goedkoop, omdat het niet uit het centrale budget wordt gefinancierd, maar de feitelijke stijging van IT-kosten blijft bestaan.

Kostenbesparing?

Maar besparen we op dat moment echt investerings- en exploitatiekosten? Als je een bedrijfsapplicatie zonder veel interfaces in een SAAS omgeving kunt onderbrengen, is de kans groot dat de leverancier goedkoper kan leveren dan je IT-afdeling. De aanschafkosten van een applicatie in de Cloud ligt vaak veel lager dan de traditionele "on-premise" installatie van dezelfde of vergelijkbare software. Veel bedrijven verslikken zich vervolgens echter in de interfaces die nodig zijn om de software te laten integreren met andere bedrijfsapplicaties. SAAS wordt vaak verkocht als eenvoudig en voordelig, maar pas op dat je met alle consultancy uren, het maatwerk aan de interfaces en nieuwe functionaliteit waarbij je als "launching customer" optreedt niet toch een grotere investering moet doen dan je vooraf had verwacht.

Afspraken en controle

Om de beveiliging van een SAAS oplossing uit een gedeelde infrastructuur onder controle te krijgen, is het verstandig om al voor de contractering een goed, op SAAS uit de Cloud toegespitst, beveiligingskader af te stemmen. Vaak resulteert alleen de discussie over dit kader al in verbeteringen van de dienst omdat er aspecten besproken worden waar de leverancier van de dienst nog niet aan had gedacht. En op het moment dat we als afnemers hier allemaal aandacht voor vragen wordt dat effect natuurlijk nog verder versterkt. Geïnteresseerden in specifieke aandachtspunten nodig ik uit om contact op te nemen. Daarnaast is het belangrijk om tijdens de acceptatietest dit kader mee te nemen als onderdeel van een beveiligingscontrole. Op deze manier heb je meer zekerheid over de beveiliging van je data, voordat je dit naar de Cloud van een derde kopieert.

Juridisch

Naast de feitelijke kwetsbaarheden die in meer dan de helft van de geteste omgevingen wordt aangetroffen, zitten er belangrijke juridische consequenties aan het gebruik van SAAS. De WBP

staat het immers niet toe om persoonsgegevens zonder meer te exporteren naar derden landen (landen die niet op de lijst van het CBP staan). Hoewel er sinds februari geen vergunning meer voor dataexport hoeft te worden aangevraagd, dienen er met de afnemer op basis van een modelcontract van de EU wel de juiste afspraken te worden vastgelegd. Dit geldt voor de plaatsing van data op servers in die landen, maar ook voor beheertoegang vanuit die landen. Als bedrijf weet je vaak niet waar de servers achter de SAAS oplossing zich bevinden of waar de beheerders van de SAAS dienst zich bevinden. Ik vermoed dat de Cloud ontwikkelingen er momenteel voor zorgen dat veel bedrijven zonder het zich te beseffen in strijd met de privacy wet handelen.

In control blijven

SAAS wordt te makkelijk gezien als het uitbesteden van je problemen. Gelet op de risico's zou je bijna kunnen stellen dat SAAS alleen geschikt is voor bedrijven met een grote mate van volwassenheid, waardoor ze de impact van de keuzes goed kunnen overzien. Zoek je een nieuwe applicatie en overweeg je SAAS? Beoordeel dan nog eens goed of je als organisatie voor de data in deze specifieke omgeving de extra risico's wilt lopen. En vergeet niet om tevens te beoordelen hoe de software gaat integreren in de rest van de IT-omgeving en hoe de data (en indien van toepassing, de processen) waar nodig weer terug naar de eigen organisatie gehaald kan worden.

ACHTER HET NIEUWS

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

MEER BEVOEGDHEDEN VOOR DE POLITIE TEGEN CYBER CRIME

Jochem Aart

Minister Opstelten heeft, vlak voor het nieuwe kabinet bekend gemaakt werd, nog een brief aan de Tweede Kamer gestuurd. Hierin breekt hij een lans voor het verruimen van de bevoegdheden van de politie in cyberspace. Cybercriminelen switchen met hun infrastructuur van land naar land terwijl de politie nog bezig is met de papierwinkel om de eerste server te mogen onderzoeken. En wat als de politie stuit op een computer waarvan niet bekend is waar hij staat? Als voorbeeld dient het kinderpornonetwerk dat pedofiel Robert M. gebruikte en verborgen lag in het anonieme TOR-netwerk. Opstelten vindt dat de politie ruimere bevoegdheden moet krijgen om een systeem te kunnen binnendringen, desnoods zonder internationaal rechtshulpverzoek. Eindelijk stappen maken of moeten we bang zijn voor Big Brother?

Gerrit Post

Meer bevoegdheden voor de politie tegen cybercrime… Wie kan daar nou tegen zijn? Deze vraag valt in de categorie "have you given up beating your wife?". Toch ben ik van mening dat we hiermee een heilloze ontwikkeling in gang zetten om een flink aantal redenen. Een goede definitie van cybercrime ontbreekt. Waar willen we ons nu exact tegen wapenen? Misschien is de wijze waarop Facebook met onze gegevens omgaat ook wel te kwalificeren als cybercrime. Gaat onze overheid binnenkort Facebook hacken? En de overheid. Is de overheid erop ingericht? Kort gezegd: neen. De overheid kampt al jaren met het probleem dat ze 'goede' mensen niet kan vasthouden, zeker niet de ICT-ers. Het lijkt een utopie om te veronderstellen dat het voorgestelde hacken dan gaat gebeuren door mensen met de kwaliteit van professionele hackers. Het zal toch niet gebeuren dat er een stagiaire de opdracht gaat krijgen "maar even die server in Verweggistan te hacken"? De overheid gaat zichzelf hiermee aanbieden als schietschijf. Opstelten wil criminelen hacken, die criminelen moeten echt wel in staat geacht worden een 'pre-emptive strike' uit te voeren. De overheid functioneert digitaal al echt niet groots maar als ze ook nog eens in de wielen gereden gaat worden door criminelen is het hek van de dam. Voordat je eigen huis op orde is moet je zeker niet zoiets gaan doen. In het voorstel is sprake van goedkeuring vooraf door het OM en van opslag van gegevens en controle achteraf. Het wordt er daarmee niet beter op. Wie gaat die goedkeuring geven? Mr. Tonino? Kan het OM deze verantwoordelijkheid dragen? Wie gaat de opslag van die gegevens uitvoeren en, niet onbelangrijk, waar gaat dat plaatsvinden? In de Cloud? Hoe gaat de controle hierop plaatsvinden? Dat zal allemaal ongetwijfeld betekenen dat er massa's gegevens heen en weer gesleept worden over de digitale snelweg en het toezicht daarop is, zoals bekend, nihil. Bedenk wel dat de afstandelijke

term cybercrime wel mede betrekking zal hebben op het op criminele wijze omgaan met gegevens die van u en mij zijn, het gaat echt niet alleen over kinderporno. Een vergissing is gauw gemaakt en de overheid is heel goed in het bewaren van gegevens. Er lijkt sprake van een trend, ik noem de discussie over voertuiggegevens, vingerafdruk in paspoort, DNA-informatie. Onze overheden zien in rap tempo hun greep op de wereld verslappen en nemen daar geen genoegen mee. Het zou ze overbodig maken en tot nu toe zijn ongeveer alle discussies over afslankende overheden stuk gelopen op de realiteit. We gaan hiervoor een flink apparaat optuigen waarvoor ongetwijfeld veel geld nodig zal zijn. Niet doen dus. Goed, we gaan dit niet doen. Is er dan geen probleem? Ja zeker! Wat gaan we dan wel doen? Vooropgesteld: wat mij betreft is er geen snelle simpele

oplossing. We moeten er goed over nadenken. Laten we beginnen met de discussie op orde te brengen. Een goede definitie van cybercrime opstellen. Kinderporno zal daar zeker onder moeten vallen maar ook phishing en het installeren van malware om betaalgegevens te achterhalen. De burger, geachte minister, heeft daar last van. We zullen de manier waarop wij omgaan met informatie moeten veranderen, onze interne processen zullen robuuster moeten worden. Dat gaat meer opleveren dan optreden voor de bühne wat nu gebeurt.

André Koot
De brief van de minister kwam eigenlijk 20 jaar te laat. Op dat moment hadden we nog niet eens nagedacht over security en al helemaal niet over security op het internet. Logisch natuurlijk, maar dan was het gewoon een wet geweest en hadden we er nu geen moeite mee. Nou, ja, ik heb er nog steeds niet helemaal moeite mee. De eerste casussen zijn vrij logisch. Dat justitie gewoon op een systeem wil rondkijken kan ik me wel indenken. De strofe 'ongeacht de locatie' hanteren we zelf ook, wij als partijen die de cloud in willen. De cloud heeft geen grenzen, laat staan dat je die kunt aanwijzen. En als je dan als opsporingsinstantie iets vindt, dan maakt het technisch gezien toch helemaal niet uit waar die data is. Dat wetten daar moeite mee hebben, pech, ik kan daar wel vrede mee hebben. En dat vierde puntje, heling, ach, dat is toch ook niet nieuw. Het dwingt ons feitelijk tot classificatie en waardering van onze data, het wordt gewoon eens tijd dat we dat gaan doen. Maar dat puntje 3, daar waar de minister op mijn pc spyware wil plaatsen, daar gaat het kriebelen. Het euvel daar is dat de crux is dat je niet weet wat software doet. Leest die software alleen? Echt waar...? Of kan die programmatuur misschien ook schrijven? En waar dan naartoe? En kan die software dan ook 'bewijs' op mijn pc plaatsen? Die grens zou keihard moeten zijn, maar die voelt nu wel heel zacht aan. Nee, over zo'n artikel zou een minister niet eens mogen nadenken.

Lex Dunn
Het probleem met de huidige aanpak van cybercriminaliteit is dat nog veel te veel de vergelijking wordt getrokken met het bestrijden van 'gewone' criminaliteit (inbraken, tasjesrovers, benzinedieven etc).
We hebben het hier over een wezenlijk andere verschijningsvorm van 'waarde'. Diefstal van digitale gegevens leidt niet tot directe materiële schade, je hebt immers je data nog (in de meeste gevallen). Pas als de gestolen informatie wordt misbruikt (creditcardgegevens, persoonsgegevens voor identiteitsfraude) kan er materiële schade ontstaan voor de eigenaar (of het subject) van de betreffende data (en dat kan heel goed pas jaren later duidelijk worden). Om dit goed en effectief aan te pakken, is een totaal andere zienswijze van criminaliteitsbestrijding nodig. De door Opstelten geformuleerde wetsvoorstellen doen een poging in die richting, maar leunen nog te veel op de traditionele aanpak. Waar dit uiteindelijk toe kan leiden wordt treffend beschreven door Cory Doctorow in zijn science fiction roman Little Brother (http://craphound.com/littlebrother/download/). Wat kunnen we daarvan leren? Het is verstandig om in gesprek te gaan met de 'cybercriminelen' om inzicht te krijgen in motieven en modus operandi (ik vind het altijd verfrissend om op een Black Hat conferentie rond te lopen, en te horen wat die jongens zoal bekokstoven). En dan zullen 'opsporing en vervolging' zich moeten instellen op die andere verschijningsvormen van criminaliteit. De voorstellen van de minister lijken een stap in de goede richting, maar (met Cory in het achterhoofd) heb ik persoonlijk nog wat bedenkingen rondom de controle op en waarborgen tegen misbruik van die nieuwe bevoegdheden. Dat is ook de uitdaging: wij moeten ons aan de wet- en regelgeving houden, maar de 'bad guys' niet.

Rachel Marbus
De enige opportune vraag die volgens mij gesteld moet worden is een ethische: is dit de wereld waarin wij willen leven? Het gaat er daarbij niet langer om of iets mag (of het rechtens correct is of feitelijk relevant), maar veeleer om de vraag of dit in overeenstemming is met de maatschappij en democratie waarin wij wensen te leven. In hoeverre achten wij onze grondrechten sterker van aard dan de behoefte om een uitzondering daaraan toe te voegen. Het is de overheid verboden onze grondrechten binnen te treden tenzij daarbij in wet is voorzien. Willen wij onze vrijheden opgeven? Hoever willen wij daarin gaan? Hoever zouden we daarin mogen gaan? En is hier sprake van een ultimum remedium of vinden wij het normaal als dit gewoongoed zou worden? Hebben wij nagedacht over wat het betekent als politie en justitie het recht verkrijgen terug te hacken? Met andere woorden: is dit de geest van de wetten die wij wensen? Ik kan een ieder aanraden eens 'De l'esprit des lois' te lezen van Montesquieu. Al was het alleen maar opdat wij ons weer eens herinneren waarom wij onze huidige staatsvorm hebben ingericht zoals we dat gedaan hebben. Want volgens mij zijn we dat met zijn alleen een beetje vergeten. "Mijn stelling is dat in de wetgever dient een geest van gematigdheid te huizen; het politiek goede ligt evenals het moreel goede altijd tussen twee grenzen." - Montesquieu

Dit artikel is mogelijk gemaakt door:

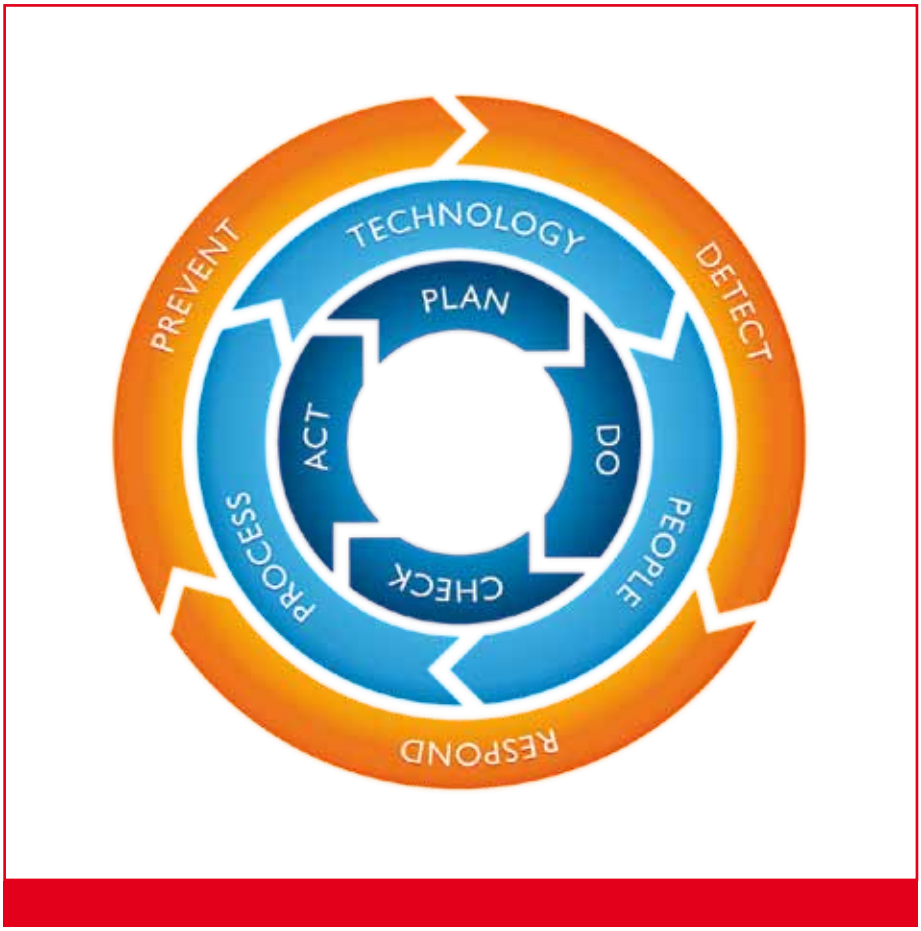
Onsight

http://www.onsight.nl/

BEN JE KLAAR VOOR CYBERCRIMINALITEIT?

Jan Jaap van der Neut werkt als business consultant bij Onsight. Hij richt zich op de organisatie van security management, zodat IT security optimaal tot zijn recht kan komen. Van der Neut heeft diverse functies bekleed voor IT service providers als Getronics en Capgemini. Op het snijvlak van business en IT weet hij steeds de brug te slaan tussen IT security en bedrijfsdoelstellingen. Vaak komt Van der Neut situaties tegen waarin security niet optimaal is georganiseerd. Zijn focus is het vinden van de balans tussen mensen, processen en technologie. Security is een kwaliteitsaspect van iedere bedrijfsactiviteit. Dit maakt het onderdeel van het dagelijkse handelen van iedere medewerker, van administratief medewerker tot directeur. Hij is bereikbaar via info@onsight.nl.

Het aantal cyberaanvallen groeit gestaag en vormt voor organisaties een steeds groter probleem. Volgens het World Economic Forum bedraagt de economische schade als gevolg van 'Major Critical Infrastructure Incidents' wereldwijd $250 miljard! [1] Door ontwikkelingen zoals de 'Meldplicht Datalekken' voelen organisaties de noodzaak om zichzelf intensief te beveiligen tegen cybercriminaliteit. Daarbij hoort dat ze meer kennis vergaren over zaken als nieuwe wetgeving, cyber threats, risicomanagement, forensisch onderzoek en bewijslast. Het is ontoereikend om te leunen op de nationale initiatieven zoals die van het National Cyber Security Center.



Enkele eeuwen geleden was bij de belegering van een kasteel duidelijk waar de vijand vandaan kwam. Hun wapens waren zichtbaar en er werd een eerlijk, soms dodelijk, gevecht geleverd.
Die duidelijkheid is in deze tijd zeer welkom. Het zou mooi zijn als we weten langs welke weg, en op welk moment, cybercriminelen hun aanvallen plaatsen. De realiteit is echter anders. Cybercriminelen hebben de tijd en het is zeer aannemelijk dat een deel hiervan door staten worden gesponsord. Het plaatsen van de aanval bestaat uit het infiltreren van de organisatie met malware, waarna de cybercrimineel geavanceerd allerlei informatie verzamelt. De malware blijft onopgemerkt en opereert onder de radar, voor zover die al aanwezig is.

1500 cyber security-specialisten nodig

Om goed voorbereid te zijn op cybercriminaliteit zullen organisaties een stevige aanpak moeten kiezen.

Die aanpak verlangt het aantrekken van specialistische kennis. De vraag is echter of die kennis op de arbeidsmarkt voorhanden is. In de Verenigde Staten is in 2011 een breed programma opgezet voor het opleiden van cyber security-specialisten: National Initiative for Cybersecurity Education (NICE). Het benodigde aantal specialisten voor de Verenigde Staten wordt geschat op 30.000. Naar verhouding heeft Nederland dan 1500 cyber security-specialisten nodig. Ik verwacht niet dat er zoveel specialisten van security-opleidingen aan hogescholen en universiteiten zullen afstuderen.

Extra inspanning

Wat kunnen organisaties zelf ondernemen tegen cybercriminaliteit? Dat begint bij een goed fundament. SANS Institute beschrijft met '20 Critical Security Controls for Effective Cyber Defence' [2] een goede set maatregelen. Ze zijn gelinkt aan de 'Australian Government's DSD 35 Mitigation Strategies [3]. Ook bestaat de link met 'NIST Special Publication 800-53 Revision 3' en indirect met ISO 27002. Daarmee is de set security controls van SANS goed te interpreteren en toe te passen.

Tk)Het tegengaan van cybercriminaliteit vraagt echter een extra inspanning! Organisaties zullen een zogenaamd 'cyber defense management systeem' moeten opbouwen. Een dergelijk systeem is gebaseerd op security intelligence en wordt gevoed met informatie over threats, vulnerabilities, patches, geo-location en fraude services. Ook zullen cyber security services ingericht moeten worden. Denk dan aan services als: take down, cyber incident respons, communication, monitoring, reporting, detection, forensics, correlation, dash boarding en training. De set security controls van SANS bevat al enkele van deze services. Toch zal het accent extra op cyber security moeten liggen. Beveiliging tegen cybercriminaliteit komt dus neer op een combinatie van het toepassen van best practices (bijvoorbeeld SANS) en een cyber defense management-systeem op basis van security intelligence.

De vraag is echter of organisaties in staat zijn om die combinatie te realiseren. De kennis en ervaring zijn niet beschikbaar op de arbeidsmarkt en de verwachting is dat die onvoldoende beschikbaar komt in de nabije toekomst. Organisaties zijn hierdoor afhankelijk van die partijen waar die kennis en ervaring al aanwezig is: vendoren en security experts. Ik zou zeggen voer eens een goed gesprek met uw security-partner en ontwikkel samen een gedegen ambitie voor een gedeeld probleem. Bouw aan een solide fundament met goed onderbouwde security controls en bereid de organisatie voor op cyber-incidenten. En bedenk: de malware opereert al in stealth mode in uw infrastructuur!

Over Onsight

Onsight is sinds 1999 actief op de Nederlandse markt. Het bedrijf heeft zich gespecialiseerd in advisering, levering, implementatie, onderhoud en beheer van hoogwaardige IT security-oplossingen. Het helpt bij het aanpassen van netwerk- en applicatie-infrastructuur aan de dynamiek van de business van zijn opdrachtgevers. Daarbij wordt altijd gezocht naar de oplossing die daadwerkelijk businessvoordeel oplevert, een gunstigere kostenstructuur biedt en het proces vereenvoudigt. Onsight behoort tot de top van de Nederlandse netwerkbeveiligingsbedrijven.

Bronnen

[1] *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/818&format=HTML&aged=0&language=EN&guiLanguage=en*

[2] *http://www.sans.org/critical-security-controls/*

[3] *http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm*

COLOFON

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
Lex Borger (hoofdredacteur, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (i3advies)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)
Bart van Staveren (UWV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl;
of neem contact op met MOS (Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

Vormgeving en druk
VdR druk & print, Nijkerk
www.vdr.nl

Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

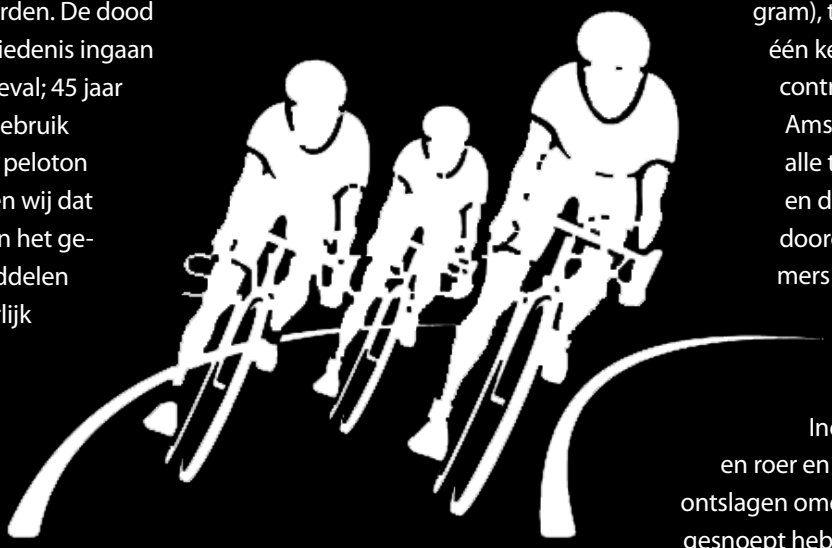
Abonnementen 2012
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

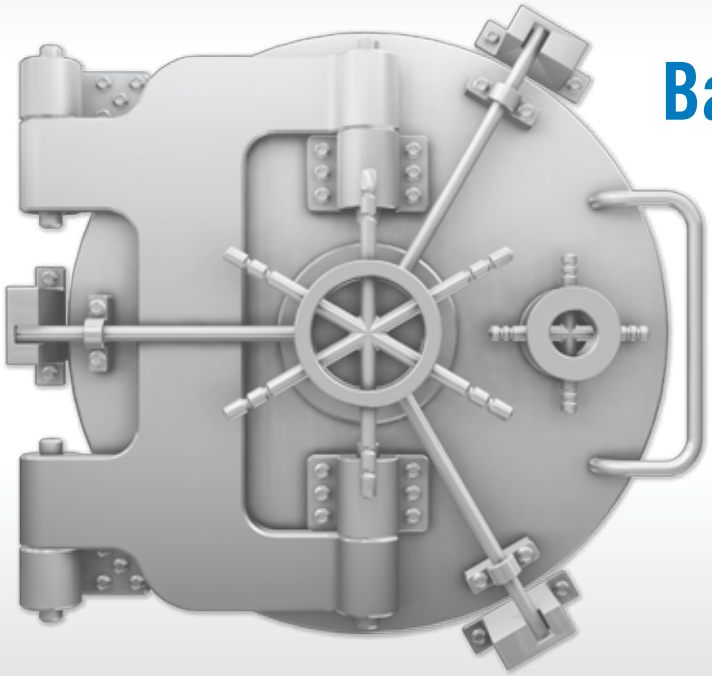
SPORT EN GELD

Ik weet voor welke doelgroep ik dit artikel moet schrijven en ik heb lang nagedacht of het door mij te bespreken onderwerp wel thuishoort in dit onvolprezen blad over informatiebeveiliging. Ik heb besloten dat toch maar te doen, alleen maar door mijn passie voor deze sport en het ongeloof over alle gebeurtenissen. In juli 1967 werd een wielrenner, die tijdens de beklimming van de Mont Ventoux bewusteloos van zijn fiets viel, afgevoerd. Later overleed hij in het ziekenhuis. Het was die dag heet en de bovenmenselijke inspanning was hem teveel geworden. De dood van Simpson zou de geschiedenis ingaan als het allereerste dopinggeval; 45 jaar geleden werd het dopinggebruik als een uitzondering in het peloton gezien. Jarenlang geloofden wij dat Simpson een eenling was in het gebruik van stimulerende middelen maar dit geloof was natuurlijk wel erg naïef.



Als sponsoren zich met een sport gaan bemoeien wordt het lastiger om alles open en eerlijk te houden.
Miljoenen worden in de sport gestopt met het doel airplay te krijgen om de naamsbekendheid te vergroten. De verdiensten van de toprenners zijn inmiddels immens geworden en de druk om te presteren is bijna onmogelijk te dragen. Toch gaan we ervan uit dat de sport clean is. Natuurlijk worden er wielrenners betrapt op het gebruik van doping, maar we denken nog steeds dat het een uitzondering is. Het is en blijft een geweldig gezicht om het peloton tijdens een zomerdag een berg te zien beklimmen. Het is warm, de renners banen zich een weg door de mensenmassa en komen uiteindelijk boven tijdens deze heroïsche etappes. De finish is nabij en er springt nog een renner uit de groep om als eerste deze etappe te beëindigen. Je neemt een laatste slok van je biertje en leest de volgende dag met chocoladeletters in de krant dat jouw held gedeclasseerd is wegens opvallende bloedwaarden. Je besluit die middag niet weer te gaan kijken maar dat blijkt lastig vol te houden zijn. Even later zit je weer voor je TV en heb je een andere favoriet gekozen.
Jaren verstrijken en meer en meer helden zijn van hun troon gevallen Contador, Schleck, Ulrich en hoeveel wil je nog horen? Eddy Merckx, Joop Zoetmelk, Hinault - en zo zijn er vast nog wel een paar te noemen - zijn nooit gepakt en lijken dus helemaal clean. Lance Armstrong was ook nooit gepakt maar die blijkt dus zijn gehele carrière zwaar gebruikt te hebben. Teruggekomen van een ernstige ziekte had hij zoveel credits gekregen dat hij blijkbaar ongestoord zijn grootschalige dope-activiteiten kon ondernemen. Zeven maal een tour winnen is een enorme prestatie, maar misschien is het nog wel een grotere prestatie dat hij nooit betrapt is op doping. Honderden testen moest hij ondergaan en nooit zijn er sporen van verboden middelen aangetroffen. Vreemd dat Contador wordt gepakt met een minuscule hoeveelheid Clenbuterol (voor de kenners 50 picogram, een picogram is één miljoenste gram), terwijl Amstrong nooit één keer is gepakt bij een controle. De gevolgen voor Amstrong zijn rampzalig; alle tourzeges is hij kwijt en de zeges worden niet doorgegeven aan de nummers 2 omdat deze vaak ook betrapt zijn op het gebruik van verdovende middelen.
Ineens is iedereen in rep en roer en ploegleiders worden ontslagen omdat zij vroeger ook gesnoept hebben van de verboden middelen. Sponsoren stoppen, want ze willen toch niet in diskrediet worden gebracht met deze praktijken? Meer en meer renners en oud-renners geven aan dat zij ook jaren hebben gebruikt. Sommigen geven zelfs aan dat ze de bloedtransfusies zelf hebben aangebracht en dat zij zichzelf injecteerden met rotzooi. Doctoren die in de wielerploegen waren opgenomen hebben nooit iets gemerkt. Ploegleiders die hun renners boven zichzelf zagen uitstijgen brachten dat niet in verband met doping. Mark Cavendish (topsprinter met een inkomen van meer dan vijf miljoen per jaar) schiet helemaal door en noemt de wielersport de meest schone sport die er is. De grootverdieners hebben hun eigen sport zo ziek gemaakt dat het bijna niet meer levensvatbaar is. Sponsoren blijven hun geld in deze zieke sport steken omdat ze er beter van worden.
Ik schrijf dit op om aan te geven dat de wielerwereld, waarin alles gecontroleerd wordt, blijkbaar toch in staat is de boel te saboteren. Dagelijks de mogelijkheid om getest te worden op dopinggebruik en toch wordt het gebruikt. Wij leven in een vakgebied waarin onze tegenstanders vaak ondergronds hun werk uitvoeren. Anoniem worden hacks gepland en uitgevoerd. Medewerkers maken misbruik van zwakheden in onze controles. Wij denken alles onder controle te hebben maar is dat wel zo? Ik denk dat jullie mijn mening wel kennen.

Berry



Batten Down Your Patches

- » Find What Needs Patching
- » Remediate *ALL* the Holes
- » Repeat Easily
- » Reduced IT Risk

Get Started at

lumension.com / batten-down

Patching Solutions for Complex IT Environments.

Reduce your IT risk with the leading patch management solution, providing the industry's broadest OS and 3rd party application vulnerability coverage.

Lumension®
IT Secured. Success Optimized.™

CRYPSYS
secure computing

sales@crypsys.nl | www.crypsys.nl | 01883 - 62 44 44