02/2012

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 2 - 2012

DE IMPACT VAN BYOD

INTRODUCTIE: ACCRUAL BASED RISK MANAGEMENT

OPENING NATIONAAL CYBER SECURITY CENTRUM

ZEG MAAR DAG TEGEN PRIVACY

ACHTER HET NIEUWS: BRING YOUR OWN DEVICE

FOX-IT

... for a more secure society

Fighting cybercrime

Protecting secrets

Finding digital evidence

Ben jij de nieuwe foxer?

Fox-IT is het meest innovatieve IT security bedrijf in Nederland en dé expert op het gebied van cybercrime, crypto en digitaal rechercheonderzoek. Met een enthousiast team van zo'n 130 betrokken en gedreven medewerkers vertalen wij de ambities van onze klanten in concrete oplossingen. Innovativiteit, vertrouwelijkheid, een excellente reputatie en de drive tot ontwikkeling zijn onze kernwaarden.

Fox-IT zoekt Hackers

Werken met de nieuwste en gaafste technieken aan onderzoeken die er echt toedoen. Foxers zijn slimme, nieuwsgierige en kritische professionals. Jij ook? Kom dan bij ons werken!

Fox-IT zoekt Fraude Analisten

Ons product DetACT maakt online en mobile banking veilig en betrouwbaar. Je bent technisch zeer vaardig (JavaScripting). Je bent creatief, scherp en zeer analytisch. Tot binnenkort?!

Meer weten? Kijk op http://jobs.fox-it.com of mail naar vacature@fox-it.com

Fox-IT Olof Palmestraat 6 Delft 015 - 284 79 99 www.fox-it.com

VOORWOORD

Mijn vader was kapitein grote handelsvaart en havenloods. Hierdoor kwam hij regelmatig op de grootste passagiersschepen in de wereld. Af en toe zat er voor mij ook een bezoek bij, met rondleiding en Captain's dinner. Ik durf te zeggen dat ik alle luxe passagiersschepen die in de jaren '60 en 70' in de Caribische wateren voeren, heb bezocht. Zeker wanneer je achter de schermen kunt kijken, krijg je bewondering voor het immense bedrijf dat zich afspeelt aan boord van zo'n schip. Verder weet je dat het een risicovol bedrijf is, wat ook behoorlijk wat toevoegt aan de waardeketen waar het in deelneemt - of het nu passagiers of vracht vervoert. Of dat het een toeristische functie heeft.
Nu ik dit voorwoord schrijf, is de Costa Concordia volop in het nieuws. Mijn vader had altijd al een zwak voor Italiaanse schepen. De Carla 'C', ook een Costa-lijn schip, was een favoriet van hem. Toen het nieuws van de slagzij en het stranden mij bereikte kwamen dus naast schok ook dierbare jeugdherinneringen naar boven. Maar dan kijk je naar de feiten zoals die nu bekend zijn: de Costa Concordia is niet verongelukt door slecht weer of een aanvaring.
Het lijkt puur een bravourstunt te zijn geweest, met een kapitein die dat nog eens verergert door van boord te gaan voordat de evacuatie compleet is.
Terug naar 1956, in de buurt van Nantucket Island, voor de kust bij Boston. De Italiaanse luxe-liner Andrea Doria wordt in dichte mist aangevaren door de Stockholm, een vrachtschip. Een aanvaring in de mist. Mist waar het schip in terecht kwam na een lange oversteek over de oceaan. Duidelijk niet zo gepland, maar wel verwacht en dus een bewust genomen risico. Het was na de aanvaring direct duidelijk dat de Andrea Doria zou vergaan. Maar door het optreden van de kapitein is het schip lang genoeg drijvend gehouden om een beheerste, uitgebreide evacuatie uit te voeren. De kapitein is tot de laatste snik aan boord gebleven van het schip - minder dan een kwartier later ging het ten onder.
Waarom is dit relevant voor informatiebeveiligers? Het laat namelijk een tweetal managementprincipes zien waar wij in de dagelijkse praktijk mee te maken hebben:
1. Ten tijde van een incident is het cruciaal dat het management zichtbaar bezig is met de beheersing en afhandeling van het incident. Dat is niet het moment om je terug te trekken omdat het te heet wordt onder je voeten. Zet dit eens af tegen de grote beveiligingsincidenten in 2011...
2. Het nemen van risico moet niet nodeloos zijn. Dat aspect zie ik nog niet terugkomen in methodes van risicoanalyse. Kijk niet alleen maar of het risico volgens spreadsheet acceptabel is. Overweeg ook of het nodig is het te nemen...

INHOUDSOPGAVE

DE IMPACT VAN BYOD

John Grüter is onafhankelijk adviseur op het grensvlak van organisatie en IT en mede-eigenaar van Digital Knowledge. Digital Knowledge houdt zich bezig met het verbeteren van de effectiviteit van leren en werken. De voornaamste focus van John zijn randvoorwaardelijke aspecten van bedrijfsvoering en IT. John is bereikbaar via jgruter@digital-knowledge.com

Digitalisering van onze maatschappij heeft gevolgen voor informatiebeveiliging. Dit geldt ook voor zakelijk gebruik van consumentenelektronica, omdat die niet ontwikkeld is voor een bedrijfscontext. Dit betreft gebruik van smartphones en tablets. Voorbeelden zijn de iPhone en iPad van Apple, een apparaat op basis van Android van Google en in mindere mate de BlackBerry van Research in Motion (RIM). Microsoft lijkt op dit moment hun eerdere positie te zijn kwijtgeraakt, maar dat kan weer veranderen met de komst van Windows 8 en apparaten die daarop zijn gebaseerd.

De digitalisering leidt ook tot toename van cybercriminaliteit. Juist die combinatie vormt een serieuze bedreiging voor het informatiebeveiligingsbeleid van organisaties. Falende informatiebeveiliging kan leiden tot grote schade voor een organisatie rechtstreeks (financieel) of indirect (reputatie), bijvoorbeeld door claims van benadeelde klanten of samenwerkingspartners.

Medewerkers van (grote) organisaties gebruiken een smartphone of tablet privé en willen deze ook zakelijk kunnen gebruiken. Als antwoord daarop gaan organisaties daarom steeds vaker over tot een zogenaamd 'Bring Your Own Device' beleid.

Bij *'Bring Your Own Device'* (BYOD) staat de werkgever toe dat een werknemer een toestel (smartphone of tablet) meebrengt en aansluit op de interne bedrijfsinfrastructuur. Dit wijkt wezenlijk af van wat tot voor kort gebruikelijk was. Tot een paar jaar geleden gebruikten organisaties uitsluitend door het bedrijf zelf aangeschafte en beheerde computers binnen het eigen, interne netwerk.

> De basis van informatiebeveiliging is de scheiding tussen 'binnen' en 'buiten'

In zo'n situatie is informatiebeveiliging binnen een paar randvoorwaarden goed te realiseren. De basis van beheer is standaardisatie van de componenten. Werkstations zijn identiek met identieke software. Aanpassing van software wordt centraal geregeld. Als de automatische faciliteiten van softwareleveranciers voor updates (bijvoorbeeld Windows Update) worden gebruikt, dan gebeurt dat via de interne procedures, nadat de impact is vastgesteld. De basis van informatiebeveiliging is de scheiding tussen 'binnen' en 'buiten'. De analogie is die van de kasteelmuren met een slotgracht, met één of meer ophaalbruggen. Zo'n ophaalbrug is de gateway naar buiten. Het voordeel is dat dáár de 'verdediging' wordt geconcentreerd. De interne omgeving is homogeen; de beveiliging basaal. Eenmaal toegelaten tot het interne netwerk, wordt dat apparaat vertrouwd. Installatie van afwijkende applicaties op de werkstations is niet toegestaan. In negen van de tien gevallen verzorgt de ICT-beheerorganisatie dat. Dit om lekken in de beveiliging te voorkomen. In het Engels wordt zo'n aanpak een *'perimeter defence'* genoemd.

Fig. 1. BYOD - Geen laptop en telefoon meer, maar tablet en smartphone.

'Tethered Devices'

Daarnaast is een smartphone wezenlijk anders dan een werkstation. Het is een *'tethered device'*. Deze term wordt hier gebruikt zoals beschreven door Jonathan Zittrain in zijn boek *The Future of Internet and how to stop it* [Zittrain, 2008]. Kort gezeg: een smartphone is een apparaat dat bedoeld is om altijd aan te staan (*'always on'*). Daarmee is een smartphone ook altijd aan een netwerk verbonden (*'always connected'*). Daardoor is deze altijd geografisch te lokaliseren (*'always found'*). Daarom is de smartphone via een virtueel lijntje altijd verbonden met de maker (*'always*

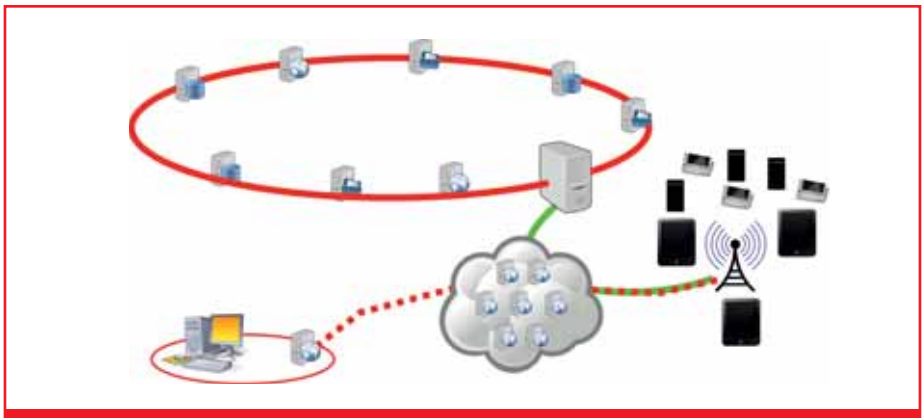


Fig. 2. Tethered device in de infrastructuur.

tethered'). Dit houdt in dat de maker van een applicatie op zo'n smartphone of de maker van het besturingssysteem contact kan leggen met de smartphone of dat de smartphone zelf communicatie kan initiëren met de maker. Dit zonder dat de gebruiker daarvan op de hoogte hoeft te zijn! In het meest extreme geval kan *via die tether zelfs de controle over het apparaat overgenomen worden*.

Zicht op de 'Cloud'

Een andere reden waarom de situatie met smartphones anders is dan PC's van een aantal jaren geleden, is de beschikbaarheid (en het veelvuldige gebruik) van internetdiensten (in de 'cloud') voor privé-mail, of synchronisatie en backup van gegevens. Ook dergelijke diensten onttrekken zich aan het zicht van de beheerorganisatie. Zo is het mogelijk dat bedrijfsgegevens via het interne netwerk op de smartphone worden geplaatst (beveiligd en binnen het zicht van de beheerorganisatie) en dan via een backup in de cloud terechtkomen, buiten het zicht van beheer. Cloud-diensten zijn daarmee een aantrekkelijk doelwit voor cybercriminelen.

Perimeter Defence?

Bij BYOD heeft de beheerorganisatie beperkte controle over de interne infrastructuur. Een *perimeter defence* is daardoor slechts gedeeltelijk toepasbaar. Namelijk tussen servers onderling, maar niet zomaar met de zelf meegebrachte apparaten. De apparatuur en de software zijn daar immers niet op gestandaardiseerd. Beheersbaarheid wordt vooral bemoeilijkt door de grote hoeveelheid verschillende versies en varianten van applicaties en besturingssystemen. Wanneer dat binnen de beheerorganisatie zou worden belegd, veroorzaakt dit een grote werkdruk. Daarnaast zijn de apparaten slechts beperkt ontwikkeld om centraal beheerd te worden; ze missen eenvoudigweg een aantal noodzakelijke functies. Het is consumentenelektronica! Om in die context informatiebeveiliging te kunnen garanderen is gegarandeerde betrouwbaarheid van *alle* apparaten cruciaal. Dit vereist een infrastructuur waarbij het gedrag van apparaten in detail bekend is en voorspeld kan worden. Omdat het onderscheid tussen 'intern' en 'extern' (via de perimeter defence) lager is, zullen apparaten binnen de infrastructuur hun eigen perimeter defence moeten inrichten, met meer nadruk op de beveiliging van de individuele apparaten. Als gevolg daarvan moet ook alle onderlinge communicatie beveiligd en versleuteld plaatsvinden. De gehele beveiligingsketen is immers zo zwak als de zwakste schakel!

> Smartphones zijn computers waar je toevallig ook mee kunt bellen

Gratis, adverteerders en inkomstenstromen

Voor makers van zowel de smartphones als de applicaties die daarop gebruikt worden, zijn advertenties een cruciale bron van inkomsten. Hierdoor

Marktplaatsen voor applicaties

Elke platformleverancier biedt de mogelijkheid om applicaties te installeren vanaf een gerichte webwinkel voor applicaties. Bij Apple is dit de AppStore, Google noemt deze de Android Market Place, RIM heeft een BlackBerry App World en Samsung heeft Samsung Apps. De in dit artikel gebruikte term is marktplaats. Let wel, in tegenstelling tot Apple en RIM is er voor Android niet één centrale ('officiële') marktplaats!

Updates en versies van besturingssystemen

De nadruk van updates van applicaties en besturingssystemen ligt uitdrukkelijk op de nieuwste versies. Dit in tegenstelling tot bijvoorbeeld Microsoft met Windows. Versies van een paar jaar oud worden minder nauwkeurig bijgewerkt. Dit geldt het meest voor smartphones op basis van Android, met name door het open karakter van het platform en de bedrijfseigen uitbreidingen. Het open karakter heeft ook gevolgen voor beveiligingsupdates. Lang niet alle leveranciers van Android-toestellen vinden het noodzakelijk om 'oudere' toestellen die op een 'oude' versie van Android werken, te voorzien van een nieuwe versie van Android. Dit is niet een activiteit die actief wordt bewaakt of gecoördineerd, laat staan wordt afgedwongen. Zo kan het dat voor v2.3 van Android vanuit Samsung wel een beveiligingsupdate wordt uitgebracht, maar bijvoorbeeld door HTC niet!

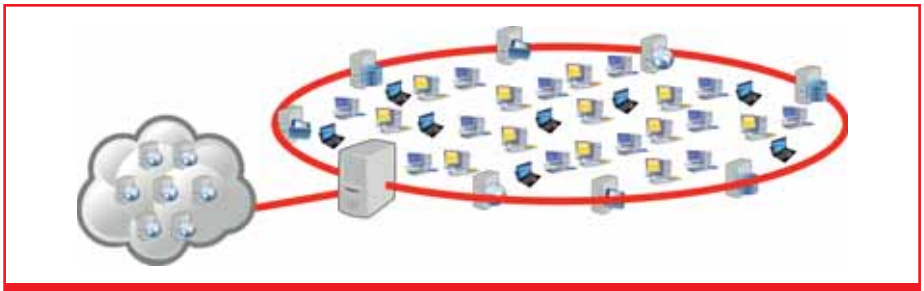


Fig. 3. Infrastructuur perimeter vóór BYOD.

is het mogelijk om applicaties 'gratis' weg te geven, of tegen zeer lage kosten. De kosten worden terugverdiend met advertenties. Om dat te kunnen doen 'onttrekken' zowel de makers van applicaties als van het platform, met name Google en Apple, zoveel mogelijk informatie over het gebruik van smartphones. De mate waarin dat gebeurt benadert spyware op PC's. Zie [WSJ, 2010] voor een aantal artikelen hierover. Google en Apple vormen hierin de spil: zij bieden het platform, gereedschappen om applicaties te ontwikkelen, bemiddelen de advertenties en bieden de marktplaats voor verkoop van applicaties.
Zij hebben hierin dus een zeer groot (financieel) belang. Gartner schat de omzet in de VS voor de mobiele advertentiemarkt op ca. 700 miljoen dollar in 2011 en ca. 5,7 miljard in 2015. Wereldwijd zou dat 3,3 miljard zijn (2011) en ruim 20 miljard in 2015. [Gartner, 2011]

Technische basis van smartphones
Smartphones zijn volwaardige en krachtige computers ('toevallig' kun je er ook mee bellen), in verwerkingscapaciteit vergelijkbaar met PC's en laptops van een paar jaar geleden. Hoewel veel verwerkingscapaciteit wordt gebruikt om de gebruiksinterface zo snel en responsief mogelijk te maken, blijft nog steeds veel capaciteit over om andere dingen te doen. Smartphones maken gebruik van (zeer) moderne besturingssystemen, vaak met een microkernel met configureerbare subsystemen, veelal op basis van een derivaat van Unix. Ze zijn ook meer vanuit beveiligingsperspectief ontwikkeld dan besturingssystemen voor werkstations. Apple gebruikt iOS, afgeleid van OS-X voor hun computers en servers, op zich weer afgeleid van DarwinOS, een Mach/BSD variant; Android is rechtstreeks afgeleid van Linux. De huidige generatie van BlackBerry OS (v6/v7) is bedrijfseigen, maar de eerstvolgende versie wordt gebaseerd op QNX, een reeds jaren bewezen kloon van Unix/Linux. Microsoft komt binnenkort met Windows 8, dat in principe dezelfde code gebruikt op alle typen platforms, van smartphone tot enterprise server. Daarnaast hebben alle smartphonebesturingssystemen een ding gemeen: het is onmogelijk applicaties te ontwikkelen die op het meest geprivilegieerde niveau uitgevoerd mogen worden. De onderliggende aanname is dat de smartphone gebruikt wordt in een publieke infrastructuur en niet in een bedrijfsmatige. Behalve bij Microsoft wordt voor applicatieontwikkeling gebruik gemaakt van Java (of derivaten daarvan) en/of HTML5. Met name het gebruik van Java zorgt voor een aantal intrinsieke beveiligingskenmerken, onder meer strenge isolatie van applicaties, waardoor zij niet met elkaar kunnen communiceren. Symantec Corporation beschrijft duidelijk de verschillen en overeenkomsten in technische (beveiligings-)architectuur van iOS en Android. [Symantec, 2011]

> Welke verborgen functies besturingssystemen hebben is niet bekend

Applicatieverificatie
Apple behandelt iOS (en de rest van het platform) als gesloten (*'proprietary'*), waarop alleen Apple bepaalt welke applicaties ter beschikking komen van de gebruikerspopulatie. Apple bepaalt ook wanneer welke updates beschikbaar komen voor iOS zelf, bijvoorbeeld wanneer er beveiligingsproblemen zijn geconstateerd. De manier waarop Apple applicaties tot de marktplaats toelaat is de meest grondige. Zie [Apple, 2011] en [Symantec 2011]. Voor bedrijven maakt Apple het mogelijk om een interne marktplaats voor bedrijfseigen applicaties op te zetten. Deze kunnen uitsluitend worden gebruikt met smartphones die via certificaten aan de bedrijfsinfrastructuur zijn gekoppeld. Gebruik zonder bedrijfscertificaat, of een certificaat dat daarvan is afgeleid, is onmogelijk.

In tegenstelling tot Apple behandelt Google Android als een open platform, via de non-profit *Open Handset Alliance* (OHA). Android ontwikkelt zich zeer snel en zijn er op moment van schrijven ten minste drie veel gebruikte versies in omloop, terwijl de meest recente net is geïntroduceerd. Door het open karakter van het platform hebben de meeste makers van Android-telefoons eigen uitbreidingen, met name voor de gebruikersinterface. Google doet slechts oppervlakkige verificatie van applicaties, noch adequate centrale registratie en verificatie van de identiteit van de makers. Daardoor is het mogelijk (wat ook in de praktijk is gebeurd) dat een geldige, correcte applicatie wordt voorzien van malware, met een namaakcertificaat 'gewaarmerkt' en vervolgens op een niet-officiële marktplaats aangeboden. Zie ook [Willemsen, 2012].

RIM zit wat betreft verificatie tussen Apple en Google in maar stelt strengere eisen, naarmate meer geprivilegieerde functies vanuit het besturingssysteem worden gebruikt. RIM heeft voor Blackberry ook één centrale marktplaats.

Platformrisico's
Geen van de smartphones staat toe dat de gebruiker de meest geprivilegieerde

delen van het besturingssysteem kan gebruiken. Dit is goed voor de beveiliging. De keerzijde is dat daardoor de interne werking van die delen van de besturingssystemen zich onttrekken aan het oog van het bedrijf dat smartphones bedrijfsmatig gebruikt. De kleinere of grotere 'schandalen' van vorig jaar maken duidelijk dat smartphones verborgen functies hebben (of hebben gehad) die de informatie laten doorgeven. Uit de situatie rondom Carrier IQ is naar voren gekomen dat geprivilegieerde functies versleutelde VPN-informatie kan tracen en loggen. Zie [xdadevelopers, 2011]. Verder is bekend geworden dat bijvoorbeeld Apple zeer gedetailleerde locatie-informatie verzamelt en via de *tether* doorgeeft. Welke verborgen functies de besturingssystemen nog meer hebben is niet bekend, maar het is waarschijnlijk (of ten minste aannemelijk) dat ze er zijn. Deze verborgen functies hangen zonder twijfel samen met de grote belangen van de platformeigenaars bij de mobiele advertentiemarkt. De gretigheid waarmee platformaanbieders profiel- en locatie-informatie verzamelen, schaadt de belangen van de organisatie waarbinnen een smartphone bedrijfsmatig wordt gebruikt potentieel. Zie ook [Oreilly, 2011].

Installatie van applicaties, zeker vanaf niet-officiële marktplaatsen, is een duidelijk risico. Los van (bij officiële marktplaatsen) de kleine kans op malware, kunnen deze een smartphone negatief beïnvloeden. Denk hierbij bijvoorbeeld aan overmatig gebruik van resources, of door slechte kwaliteit van de applicaties, of instabiliteit.

Van alle beschikbare applicaties is de webbrowser het meest gevoelig voor malware. Het bedrijfsrisico hiervan is dat wanneer de browser geïnfecteerd zou worden, malware toegang zou kunnen krijgen tot alle browserhistorie, gebruikersnamen en passwords, zowel privé als binnen het bedrijf. Het gevolg is dat de geïnfecteerde browser automatisch aan zou kunnen loggen bij internetbankieren (privé) of een afgeschermd bedrijfssysteem, bijvoorbeeld een Document Management System (DMS) of een Customer Relationship Management (CRM) systeem om misbruik te maken van de daar aanwezige informatie, bijvoorbeeld door deze door te sturen naar een extern systeem.

BYOD zal op termijn voor veel functies gemeengoed zijn

Mobile Device Management

Om bij grotere organisaties smartphones te kunnen gebruiken is een zekere vorm van beheer essentieel. RIM heeft aangetoond dat - zeker bij een homogene verzameling devices - dit zeker mogelijk is. Softwareleveranciers zien hier kansen en introduceren suites daarvoor. Dit wordt Mobile Device Management (MDM) genoemd. MDM is een verzameling functies waarmee een centrale instantie het beheer kan voeren over een verzameling smartphones. Met deze functies is het mogelijk een smartphone zichzelf op afstand uit en aan te laten zetten, door te laten geven waar deze zich bevindt, alle gegevens daarop te laten wissen, enz. Dit soort functies zijn voor (bijna) alle smartphones beschikbaar, ook voor consumententoestellen. MDM in een bedrijfsmatige context gaat verder. Bedrijfsmatige MDM zorgt dat de beheerder op afstand een smartphone volledig kan (her-)configureren. De beheerder kan instellen wat de gebruiker er mee kan en mag doen, bijvoorbeeld door toe te staan dat uitsluitend goedgekeurde applicaties geïnstalleerd mogen worden (of helemaal geen), dat passwords voldoen aan de bedrijfseigen beveiligingseisen, de gebruiker toegang krijgt tot een corporate account, dat de mail en netwerken worden geconfigureerd, enz. Daarnaast kunnen faciliteiten van de smartphone zelf worden aan- of uitgezet, zoals de camera of microfoon en logging en tracing van het gebruik.

De BlackBerry is van de grond af aan als zakelijke, beveiligde en beheersbare smartphone ontwikkeld. De MDM van BlackBerry, BlackBerry Enterprise Services (BES), is een zeer fijnmazig beheersmechanisme binnen een bedrijfscontext. Omdat Apple iOS als een gesloten systeem behandelt kan MDM door derden niet op root-niveau worden geïmplementeerd, tenzij Apple daaraan meewerkt. Apple ontwikkelt overigens sinds enige tijd zelf ook een MDM Suite. [Apple, 2011] Google, of eigenlijk OHA, beschouwt Android wel als een open systeem. Hierdoor is implementatie van beheer- en veiligheidsfuncties op root-niveau in principe mogelijk. Echter door de versnippering van ontwikkeling van en aan Android levert dit problemen op

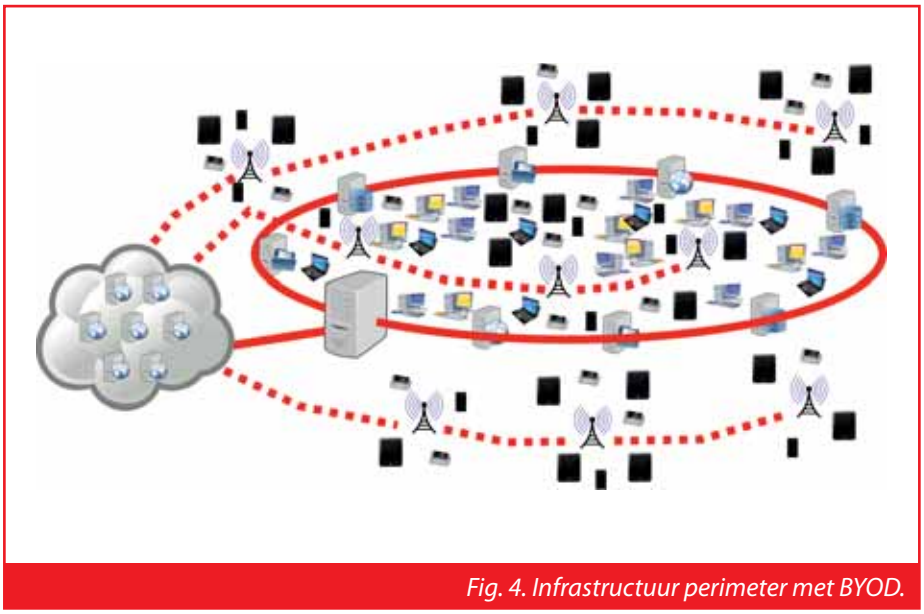


Fig. 4. Infrastructuur perimeter met BYOD.

met de verschillende versies en varianten. Microsoft migreert alle huidige 'smaken' van hun besturingssystemen naar één 'smaak', namelijk Windows 8. Deze versie komt beschikbaar voor smartphones, tablets, laptops én desktops en servers. Dit levert potentieel een groot concurrentievoordeel op. Windows 8 smartphones kunnen door Microsoft ook echt beheersbaar worden gemaakt, inclusief de mogelijkheid om periodiek beveiligingsupdates te ontvangen.

Andere smartphones dan BlackBerry zijn en blijven ontwikkeld als consumentenapparaat. Het gebrek aan MDM-functies voor smartphones heeft ertoe geleid dat derde partijen hier oplossingen voor ontwikkelen. Er is daardoor een aantal leveranciers die MDM Suites leveren die in principe alle smartphones kunnen beheren, bijvoorbeeld AirWatch, SyncShield, NotfyCorp en CommonTime. Het gevolg hiervan is dat eventuele functies van derden voor dit soort beheer achteraf is toegevoegd aan het besturingssysteem en geen deel uitmaakt van het oorspronkelijke ontwerp. Gezien de duidelijke verschillen in de opbouw van de besturingssystemen lijkt volledige integratie lastig. Expliciete medewerking van de platformeigenaars lijkt noodzakelijk. Overigens werkt RIM, de maker van BlackBerry, ook aan een cross-platform MDM, BlackBerry Mobile Fusion.

Wel of niet BYOD?

Organisaties staan onder toenemende druk om BYOD toe te staan. Die druk is begrijpelijk, BYOD sluit namelijk uitstekend aan op *Het Nieuwe Werken*. Zonder enige twijfel zal BYOD op termijn van enige jaren voor veel rollen of functies gemeengoed zijn.

Om te beantwoorden of een organisatie BYOD moet introduceren is allereerst een grondige risico-analyse vereist. Verschillen in risico zijn groot: per bedrijfstak, per organisatie of zelfs per afdeling of divisie. Bij de risico-analyse moeten het bestaande beveiligingsbeleid en de implementatie daarvan worden meegewogen. Zo zal het risico van een organisatie met beperkte risicobeheersingsmaatregelen slechts weinig toenemen wanneer BYOD wordt toegestaan. De verhoogde werkdruk op de beheerafdeling kan in zo'n geval wel een struikelblok zijn. Daarnaast moet duidelijk zijn welke faciliteiten of bedrijfsfuncties benaderd kunnen worden met een meegebracht device! Vervangt zo'n device een werkstation of alleen een (vaste) telefoon? Moeten alle interne resources via zo'n device bereikbaar zijn of alleen een subset? Vervangt het device niet het volledige gebruik van een werkstation, dan bestaat het risico - naast die van de werkdruk voor de beheerorganisatie - dat vooral de kosten toenemen! Verder is het essentieel de verantwoordelijkheden goed af te bakenen. Welke mate van ondersteuning krijgt een medewerker wanneer storingen zich voordoen? Wie is verantwoordelijk voor backup en synchronisatie van zo'n device?

Wie is verantwoordelijk voor backup en synchronisatie?

De risico-analyse dient om het totale risico van BYOD in het licht van de bedrijfsvoering te onderzoeken. Anderzijds kan de risico-analyse gebruikt worden om de risico's te differentiëren naar functie/rol, afdeling/divisie en/of soort informatiegebruik. Daaruit kan bijvoorbeeld naar voren komen dat voor telefonie en voor snelle toegang tot informatie op afstand smartphones een effectieve oplossing zijn. Voor andere taken wordt dan teruggevallen op conventionele werkstations (of laptops).

Verder lijkt het praktisch niet mogelijk om zonder enige vorm van standaardisatie elk mogelijk device toe te staan. Bij de eventuele uitrol zou daarom in eerste instantie een subset van mogelijke smartphones en/of tablets worden genomen. De beheerafdeling kan dan feitelijk ervaring opdoen met het beheer van dit soort apparaten. Invoering aan de hand van een geselecteerde Multi-platform MDM Suite is ook een optie.

Om het pad naar breed gedragen BYOD verder vrij te maken, lijkt het zinvol wanneer zakelijke gebruikers van smartphones en tablets zich organiseren in gebruikersgroepen, zodat zij als volwaardige partners van de platformleveranciers optreden. Op die manier creëren zij een kanaal om hun eisen en wensen aan de makers van dit soort technologie te communiceren en door hun massa kracht bij te zetten.

Referenties

Apple, Moble Devices Management in iOS, 2011, ingezien op 20 januari 2012, zie www.apple.com/iphone/business/integration/mdm/

Gartner, Gartner Says Worldwide Mobile Advertising Revenue Forecast to Reach $3.3 Billion in 2011, 2011, ingezien op 20 januari 2012, zie http:// www.gartner.com/it/page.jsp?id=1726614

O'Reilly Radar, Got an iPhone or 3G iPad? Apple is recording your moves., ingezien op 20 january 2012, zie http://radar.oreilly.com/2011/04/apple-location-tracking.html

Symantec, A Windows Into Mobile Device Security. 2011, ingezien op 20 januari 2012, zie http:// www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Wall Street Journal, Your Apps are Watching You, 2010, ingezien op 20 januari 2012, zie http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

Willemsen, J., Explosieve groei van Android Malware, Informatiebeveiliging, PvIB, 2012 no. 1, p. 14-17

xdadevelopers, The Sorm Is Not Over Yet – Let's Talk About #CIQ, 2011 ingezien op 20 januari 2012, zie http://www.xda-developers.com/android/ the-storm-is-not-over-yet-lets-talk-about-ciq

Zittrain, J., The Future of Internet and how to stop it. Penguin Books, 2008, zie http://futureoftheinternet.org/


KLAAR VOOR BYOD?

We vragen auteurs in de LinkedIn-groep voor IB-auteurs om een korte reactie. Twee auteurs reageren op de volgende vragen:

Is het Nederlandse bedrijfsleven klaar voor BYOD? Is de medewerker klaar voor BYOD? Aan welke regels moet BYOD gebonden worden? Moet je BYOD überhaupt wel willen?

De besloten LinkedIn groep voor IB Auteurs is te vinden via http://www.linkedin.com/groups?gid=4188826. Wij heten aspirant auteurs graag welkom.

Sjaak Laan

Wat losse (wellicht onsamenhangende) gedachten...

Ik denk dat BYOD vergelijkbaar is met Jericho. Iedereen weet dat het de toekomst is, en iedereen wil het ook, maar er zijn weinig of geen uitgekristalliseerde producten beschikbaar. Elke oplossing heeft intrinsieke nadelen en er is nog geen consensus over de beste aanpak.
Ik denk dat op dit moment de beste aanpak is om BYOD gefaseerd in te voeren. Dat betekent dat bepaalde diensten (denk aan mail of intranet) nu al relatief eenvoudig via het Internet ontsloten kunnen worden. Maar op dit moment is het volledig ontsluiten van alle functionaliteit via BYOD nog een stap te ver. Het is bijvoorbeeld volgens mij niet wenselijk om alle documenten te kunnen raadplegen, opslaan of te kunnen printen op elk willekeurig device. BYOD omvat per definitie unmanaged apparaten - systemen waar de systeembeheerders geen invloed op kunnen uitoefenen en waarop niet per definitie informatie encrypted is opgeslagen. En hoewel er technische oplossingen zijn voor het onmogelijk maken van opslaan of printen van gevoelige documenten, worden deze oplossingen gezien als omslachtig of onhandig. Ook wordt de gebruiker geconfronteerd met wijzigingen op zijn persoonlijk aangeschafte device. Dit kan weerstand oproepen en het concept van BYOD ondermijnen.
Wel moeten we de risico's van BYOD in het licht van andere risico's zien. Zolang het nog mogelijk is om ongecontroleerd met een pak uitgeprinte documenten het pand uit te lopen en deze documenten na lezing gewoon bij het oud papier te deponeren, kun je je afvragen of BYOD een veel groter risico introduceert.

Jeroen Willemsen

Wanneer ben je klaar voor BYOD? Deze vraag kunnen we vanuit verschillende perspectieven bekijken.
Ben je als bedrijf klaar voor BYOD zodra je een mobiel apparaat integreert met de Exchange omgeving? Of ben je er klaar voor als je de maximale potentie van een mobiel apparaat gebruikt?
In sommige gevallen kan een bedrijf al klaar zijn voor BYOD door mobiele apparaten op te nemen in de Exchange omgeving. Denk dan ook aan eventuele vertrouwelijke email die door de gebruiker wordt verstuurd. Hiervoor kan er al snel meer nodig zijn, omdat men de integriteit van het mobiele apparaat tot op zekere hoogte moet kunnen garanderen. Denk aan platformen zoals Zenprise of Good Technologies of het uitgeven van een eigen BlackBerry, maar het kan ook zijn dat men juist meer moet doen met policies en governance binnen een bedrijf.

Sommige verkopers vinden een bedrijf pas 'BYOD-klaar' als bijna iedere applicatie wel informatie kan ontsluiten naar een mobiel apparaat. Het blijft natuurlijk de vraag of dit in alle gevallen ook echt nodig is. Daarnaast is het een pré om afspraken te maken over verantwoordelijkheden. Ook is het belangrijk voordat men allerlei mobiele informatiestromen gaat ontsluiten, dat er een helder beleid is dat gestoeld is op bestaande standaarden.

Voordat een bedrijf er klaar voor is, is het goed om te kijken of de cultuur er klaar voor is en of men de risico's die bij de informatiestromen horen onderkent en goed behandelt.

Met de cultuur komen we automatisch bij de medewerker terecht. Sommigen zijn er klaar voor, sommigen niet. 'BYOD-klaar' zijn betekent meer dan alleen weten hoe je een smartphone of tablet gebruikt. Het betekent ook dat je voorgelicht moet zijn over hoe je een apparaat goed en veilig gebruikt en dat je als gebruiker je verantwoordelijkheid neemt om goed met je apparaat en de informatie die er op staat om te gaan.

Natuurlijk moet je je altijd afvragen of je wel 'BYOD-klaar' zou moeten of willen zijn. Dat is vaak al snel beantwoord: werknemers nemen hun smartphone of tablet toch wel mee en zullen die tijdens het werk echt wel gebruiken. Dus je moet er sowieso wat mee - als niet nu, dan ergens in de toekomst. Je kunt nu nog gewoon "nee" zeggen, maar kijk dan eerst welke voordelen het op kan leveren. BYOD kan meerwaarde zoals flexibiliteit, mobiliteit, kostenbesparingen, verhogen van werknemerstevredenheid, aantrekken van nieuw potentieel en nog wel meer geven, al is dat wel afhankelijk van de sector waarin je als organisatie opereert.

COLUMN

JURIDISCHE ASSURANCE VOOR CLOUD- EN PRIVACY-ISSUES DOOR NIEUWE EU PRIVACYWET?

Ja, ik heb me er ook schuldig aan gemaakt. Ik heb heel hard "BOE!" geroepen toen vorig jaar naar buiten kwam dat Amerikaanse cloudaanbieders contractuele waarborgen negeren ten faveure van een aankloppende Amerikaanse overheid (ik kan het ze niet al te hard kwalijk nemen, maar dat terzijde). Datavorderingen op grond van de Patriot Act kunnen dan ook worden gedaan indien in het contract met die Amerikaanse cloudaanbieder is afgesproken dat de data op Europees grondgebied blijft. De Amerikaanse overheid vordert op grond van het feit dat het bedrijf dat de dienst verleent een hoofdvestiging heeft op het Amerikaanse grondgebied. Waar de data zich bevindt, doet niet ter zake. Omdat afnemers van clouddiensten niet op hun achterhoofd zijn gevallen, hadden verschillende van hen contractueel vastgelegd dat de data niet buiten het Europese grondgebied mag komen. Die juridische zekerheid bleek dus niet zo veel waard. Vandaar mijn heel harde "BOE!"

Na het uitkomen van dat bericht over die datagraaiende Amerikaanse overheid, is er op Europees niveau veel gekrakeel losgebarsten. Vooral D'66 (in persoon van Sophie in 't Veld) heeft zich ingespannen om zaken aan het licht te brengen en te zoeken naar garanties voor Europese afnemers van clouddiensten. Een ieder binnen de EU dient zich immers aan de EU-wetgeving op het gebied van data privacy te houden, maar als externe partijen die compliance vervolgens teniet doen, dan stelt onze dataprotectie ook niet zo heel veel meer voor natuurlijk. Verheugd nam ik dan ook een tijdje geleden kennis van het uitgelekte wetsvoorstel voor een nieuwe Europese privacywet. De scopebepaling van deze verordening is breder dan onze huidige dataprotectiewetgeving, waardoor het datagraaien in ieder geval juridisch gezien aan banden lijkt te worden gelegd.

De scope-uitbreiding:
"This Regulation applies to the processing of personal data by a controller not established in the Union where the national law of a Member State applies by virtue of international public law."

Wat staat daar nu? Kort gezegd het volgende: de Europese privacywet is van toepassing als gegevens worden verwerkt van EU-onderdanen door een verantwoordelijke die niet in de EU is gevestigd. Dan nu de mitsen en de maren… Ten eerste de term 'verantwoordelijke' (controller), dit is de instantie die het doel van de verwerking van de gegevens bepaalt. Als ik de scopebepaling goed lees betekent dit dat het alleen gaat over die gevallen waar bijvoorbeeld een cloudaanbieder zelf de doelen bepaalt. In een scenario waarbij clouddiensten worden afgenomen door een bedrijf (of overheid) zal dit doorgaans niet het geval zijn, de afnemer zal de partij zijn die als verantwoordelijke kan worden aangeduid. In business-to-bussiness situaties zul je hieraan dus niet veel hebben. Een tweede mits kan worden gevonden in de scopebepaling zelf: "…where the national law… applies by virtue of international public law." Het gaat om die situaties waarin de locale privacywetgeving (denk bijvoorbeeld aan onze Wet bescherming persoonsgegevens) van toepassing is vanwege internationaal publiekrechtelijke wetgeving. Dan zou er dus bijvoorbeeld een verdrag tussen staten moeten zijn waarin zij zoiets regelen of op grond waarvan die nationale dataprotectiewetgeving toepasselijk wordt verklaard. Ik ben geen expert op het gebied van Internationaal Publieksrecht, maar ik vrees dat dit nog weleens tot interpretatie-issues kan leiden. Waarbij de Amerikaanse kant van de discussie zich al snel zal richten op de eigen souvereiniteit en de noodzaak tot het bestrijden van terrorisme waarmee zij datagraaien zal gaan legitimeren.

Zo komen we alweer snel op het probleem van jurisdictie. Want: wie heeft jurisdictie op het internet en waar worden de grenzen getrokken? Onze jurisdictieregels stammen uit de pré-internetperiode en zijn dan ook sterk territoirgebonden in hun uitwerking. Hoe dit per land uitwerkt is daarin ook nog eens verschillend. Daar waar de Nederlandse overheid haar jurisdictie (tot waar hebben zij een rechtsgrond om in te grijpen?) ent op de landsgrenzen, oordeelt de Amerikaanse overheid daar heel anders over. Zij is van mening dat er jurisdictie is op het moment dat er sprake is van een effect voor Amerika. Of de daad zelf al dan niet plaatsvindt op Amerikaans grondgebied is daarbij niet belangrijk. Alleen al daarom vermoed ik dat de Amerikaanse overheid nog wel even zal doorgaan met dat datagraaien. Want in 'the war on terror' (die immers in effect gericht is op Amerika) mag alles worden aangegrepen om te voorkomen dat er slachtoffers vallen.

mr Rachel Marbus
@RachelMarbus op Twitter

INTRODUCTIE: ACCRUAL BASED RISK MANAGEMENT

Dubbel boekhouden voor de Risk Manager

Maurice werkt 20 jaar als zelfstandige consultant met informatiemodelleren, -verwerking, -architecturen en -beveiliging. Zijn passie is de structuur en beheersing van taal, informatie en betekenis.

Maurice Gittens, CISA (maurice@gittens.nl)

Dit artikel introduceert 'accrual based risk management' als een controle-instrument dat in het domein van de corporate governance een rol kan spelen bij het verbeteren van de maturiteit van de interne controle. Hierbij worden de assets in de assetportefeuille van een concern over hun gehele levenscyclus aan een coherent controle regime onderworpen. Dubbel boekhouden speelt hierbij een centrale rol. Dit artikel introduceert - in opzet - een aanpak om de mate van controle, compliance en risico te kwantificeren. Een eenvoudig voorbeeld zal de materie verduidelijken.

Voor ieder bedrijf zijn er verschillende stakeholders (= belanghebbenden) aan te wijzen. Aandeelhouders, crediteuren, toezichthouders en personeel zijn hier voorbeelden van. Om de afgesproken behartiging van de belangen van de verschillende stakeholders te waarborgen wordt doorgaans een functie voor de interne controle ingericht.

Het doel van deze functie is om aan de stakeholders een redelijke mate van zekerheid te geven, dat hun belangen door het management van een concern worden behartigd, volgens COSO in relatie tot:

- Efficiëntie en effectiviteit van de operatie;
- De betrouwbaarheid van gerapporteerde informatie;
- Compliance met wet- regelgeving en requirements van toezichthouders.

Het instrument dat in dit artikel wordt geïntroduceerd, is voor de interne controle als geheel inzetbaar.

Instrument voor risicobeheersing

Voor de doelstellingen van dit artikel wordt een concern gezien als een verzameling assets, een assetportefeuille als u wilt. Assets zijn bijvoorbeeld:

- Processen, mensen en technologie;
- Informatie;
- Het financiële vermogen.

De opzet is om preventieve, detectieve, repressieve en correctieve maatregelen te treffen om te waarborgen dat de assets van een concern slechts conform hun bestemde doel worden ingezet. De informatiebeveiliging is op operationeel niveau een onderdeel van dit maatregelenpakket dat zich primair richt op informatie en informatieverwerkende assets. Deze assets mogen namelijk uitsluitend voor bestemde doeleinden worden gebruikt door bevoegden.

Accrual based risk management is een instrument om risicobeheersingsmaatregelen effectief over het gehele domein van de interne controle te managen. Het woord accrual duidt in deze op het 'doorlopend berekenen' van de mate van blootstelling aan risico. We steken met de introductie van dit instrument van wal door een aantal axioma's introduceren:

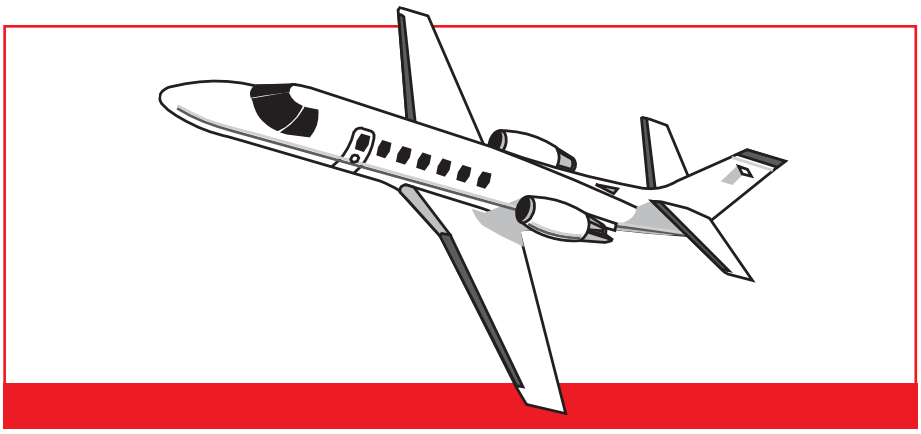
1. een asset heeft waarde dat in een valuta uit te drukken is;
2. iedere asset heeft een levenscyclus;
3. de waarde van een asset is over zijn levenscyclus in het algemeen niet constant;
4. een assetportefeuille zelf is ook een asset;
5. iets is in materiële zin blootgesteld aan risico dan en slechts dan als het een asset is;
6. zonder verandering kan voor een asset geen waardeverandering plaatsvinden;
7. als we 100% in control zijn is waardeverandering waarvoor geen voorziening getroffen is, onmogelijk.

Ik neem voor het gemak aan dat de eerste vijf axioma's aannemelijk zijn. De uitweiding over axioma zes en zeven volgt.

Verandering heeft altijd momentum

Een asset portefeuille is blootgesteld aan verandering. Deze verandering is te classificeren in veranderingen:

- die onder aansturing van de assetbeheerder in gang gezet worden
- die zonder de medewerking van de assetbeheerder plaatsvinden



Verandering van de hierboven genoemde soorten kunnen allebei de waarde van een asset compromitteren. Nu willen we appreciëren dat als in relatie tot een asset niets verandert, er ook geen sprake kan zijn van waardeverandering in relatie tot de asset in kwestie.
Als voorbeeld nemen we een vliegtuig tijdens de vlucht. Als het vliegtuig vervolgens neerstort, ligt er per definitie een logisch antecedent aan de crash ten grondslag. Bijvoorbeeld:

- de brandstof is opgeraakt;
- de piloot vergist zich in kritische zin.

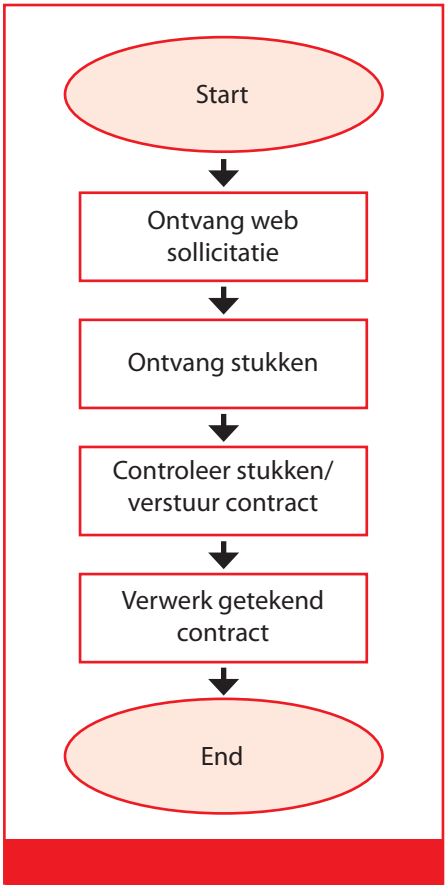
Het logische antecedent dat aan de crash ten grondslag ligt, is de verandering die in dit voorbeeld tot waardederving leidt. De stelling is dat als er in relatie tot de vlucht in materiële zin niets verandert, het vliegtuig zal blijven vliegen.
In het algemeen geldt dat er zonder materieel antecedent geen sprake kan zijn van verandering en dus ook niet van waardeverandering.
Het in materiële zin beheersen van verandering is dus essentieel om waardeverandering in relatie tot een assetportefeuille te beheersen. Op basis van deze insteek definiëren we risicomanagement als: *het treffen van voorzieningen om waardeverandering van assets in een assetportefeuille over hun gehele levenscyclus binnen vastgestelde marges te houden.*

Volledige controle

De film 'Instinct' met Anthony Hopkins en Cuba Gooding Jr geeft een treffende bevestiging van de stelling dat 100% in-control zijn een illusie is.
Toch kunnen we er niet omheen dat er controle-instrumenten zijn die in materiële zin waardeverandering tijdens de levenscyclus van een assetportefeuille beheersbaar kunnen maken.

Volledige controle is een illusie

Accrual based risk management zoals in dit artikel wordt geïntroduceerd is in essentie een controle-instrument dat wijzigingen administreert over de gehele levenscyclus van een assetportefeuille. Op deze wijze is een praktische benadering van het volledig in controle zijn te verwezenlijken.



The Balance of Control

Als eenvoudig voorbeeld van de toepassing van accrual based risk management bekijken we de happy flow van een simpel sollicitatieproces. De processtappen die we volgen zijn in de volgende schets afgebeeld.

Dit procesvoorbeeld zullen we onderwerpen aan controle door middel van het principe van accrual based risk management. We projecteren de analoge beginsituatie op een balans van een financiële administratie, de *balance of control* genoemd, met de volgende rekeningen.

Assets		**Liability**	
signed-contract	0	intention-to-employ	0
awaiting-contract	0		
submitted-exhibits	0		
receivable-good-conduct	0		
receivable-testimonial	0		
receivable-accreditation	0	**Equity**	
receivable-cv	0	employee-under-contract	0

Op deze balans zien we een aantal rekeningen die initieel het saldo van 0 heeft. We stellen dat de bedragen op deze balans in de muntsoort *currency* of *risk*, *control* and *compliance* uitgedrukt zijn.

De volgende tabel toont een aantal journaalposten met hun corresponderende effect op het grootboek. De journaalposten zijn te correleren met de stappen in het voorbeeld van het sollicitatieproces. Een operationele risicomanagementafdeling zou via dit instrument de mate van het in-control zijn kunnen meten.

#	Change Journal			Effect on Balance of Control			
1	**Job-application**			**Assets**		**Liability**	
			10	signed-contract	0	intention-to-employ	400
	Debit	receivable-good-conduct	0	awaiting-contract	0		
			10	submitted-exhibits	0		
	Debit	receivable-testimonial	0	receivable-good-conduct	100		
			10	receivable-testimonial	100		
	Debit	receivable-accreditation	0	receivable-accreditation	100	**Equity**	
			10	receivable-cv	100	employee-under-contract	0
	Debit	receivable-cv	0				
			40				
	Credit	intention-to-employ	0				
	Een ontvangen sollicitatie impliceert dat documenten zoals diploma's ingediend dienen te worden.			De waarde van verschuldigde en de te ontvangen stukken wordt bijgehouden op corresponderende rekeningen.			
2	**Submission of exhibits**			**Assets**		**Liability**	
			40	signed-contract	0	intention-to-employ	400
	Debit	Submitted exhibits	0	awaiting-contract	0		
				submitted-exhibits	400		
			10	receivable-good-conduct	0		
	Credit	receivable-good-conduct	0	receivable-testimonial	0		
			10	receivable-accreditation	0	**Equity**	
	Credit	receivable-testimonial	0	receivable-cv	0	employee-under-contract	0
			10				
	Credit	receivable-accreditation	0				
			10				
	Credit	receivable-cv	0				
	De bij de sollicitatie horende stukken zijn ontvangen.			De ontvangst van de stukken wordt in de ledger verwerkt.			
3	**Acknowledgement/send contract**			**Assets**		**Liability**	
	Debit	awaiting-contract	400	signed-contract	0	intention-to-employ	400
	Credit	submitted-exhibits	400	awaiting-contract	400		
				submitted-exhibits	0		
				receivable-good-conduct	0		
				receivable-testimonial	0		
				receivable-accreditation	0	**Equity**	
				receivable-cv	0	employee-under-contract	0
	Bevestig na controle de ontvangst van de stukken en stuur het contract ter ondertekening toe.			Verwerk de bevestiging in de administratie.			
4	**Process signed contract**			**Assets**		**Liability**	
	Debit	receivable-draft-contract	400	signed-contract	400	intention-to-employ	0
	Credit	signed-contract	400	awaiting-contract	0		
	Debit	intention-to-employ	400	submitted-exhibits	0		
	Credit	enganged-employee	400	receivable-good-conduct	0		
				receivable-testimonial	0		
				receivable-accreditation	0	**Equity**	
				receivable-cv	0	employee-under-contract	400
	Het contract is ondertekend.			Verwerk ondertekening in de administratie.			

Het bovenstaande voorbeeld maakt het aannemelijk dat processtappen uit ons voorbeeld via een journaal op een grootboek te projecteren zijn. Tijdens de uitvoering van het voorbeeldproces dienen telkens de volgende regels te gelden:

- De som van alle debitbedragen is gelijk aan de som van alle creditbedragen;
- De som van de assets is gelijk aan de som van Liabilities en Equity.

Door de rekeningen handig te kiezen zorgen we dat tijdens de uitvoering van het proces:

- Sommige onregelmatigheden worden gedetecteerd doordat er onbalans ontstaat;
- doorlopend inzicht bestaat in de status van het proces;
- in principe voor een onbeperkt aantal processen tegelijkertijd de onregelmatigheden en status worden bijgehouden.

Natuurlijk kan dit voorbeeld eenvoudig worden uitgebreid met stappen uit het *onboarding* proces. De volgende processtappen zouden dat geval op het journaal kunnen voorkomen:

- provide-corporate-policy-documentation;
- process-signed-user-policy-compliance-form;
- assign-corporate-identity-credentials;
- accept-responsibility-for-corporate-identity-credentials;
- assign-business-roles;
- accept-responsibility-for-business-roles.

Identiteit en autorisatie kunnen dan analoog aan het sollicitatieproces worden geadministreerd.
In relatie tot de *balance of control* blijven er veel aspecten in dit voorbeeld onderbelicht. Voorbeelden hiervan zijn:

- hoe voor een willekeurig proces de journaalposten en rekeningen te definiëren;
- de classificatie van grootboekrekeningen naar hun soort;
- de bedragen die per journaalpost worden gebruikt.

Omdat dit artikel zich beperkt tot een introductie van de opzet van accrual based risk management komen deze en andere gerelateerde aspecten in dit artikel niet aan bod.

Waar we het wel over willen hebben is de kwantificatie van risico door toepassing van dubbelboekhouden.

Het kwantificeren van risico door het administreren van veranderingen

Een fundamentele veronderstelling bij acrual based risk management is dat materiële verandering waarmee a-priori rekening wordt gehouden, effectief te beheersen is. Als gevolg van calamiteiten is ook afbreuk - wat opzet betreft - binnen vooraf bepaalde marges te houden (als hiermee vooraf rekening wordt gehouden). De disciplines *Disaster Recovery* en *Business Continuity Planning* bevestigen deze stelling. Met andere woorden: wat opzet betreft is alles waarmee we van te voren rekening kunnen houden op procesmatige wijze te beheersen.

Van Risk Manager naar Boekhouder

Bij het proces *patch management* bijvoorbeeld manifesteren niet uitgevoerde patches zich als een saldo op een daarvoor bestemde grootboekrekening. Hoe groter het saldo op deze rekening, des te hoger het risico voor de assetportfolio, dat afhankelijk is van patch management. Het is natuurlijk wel van belang dat de opzet van het patch management proces effectief is. Voor de volledigheid wil ik nogmaals benadrukken dat 100% controle een illusie is. De toepassing van een patch is bijvoorbeeld maar al te vaak een bron van kwetsbaarheden. IDS/IPS oplossingen zouden bij de detectie/preventie van sommige kwetsbaarheden effectief kunnen zijn.

Het is bij benadering aannemelijk te maken dat het management orde op zaken heeft gesteld door de administratieve wijzigingen over het hele domein van interne controle te beheersen.
De volgende sectie geeft een definitie van het begrip risico in de context van accrual based risk management.

Een definitie van risico

Voor een asset veronderstellen we dat:

- alle materiële veranderingen via effectieve veranderingsprocessen plaatsvindt;
- een effectief veranderingsproces gedefinieerd is als een proces dat in staat is om voor alle procesgangen waardeverandering voor de betreffende assets binnen vooraf bepaalde marges te houden. Ook geldt voor deze processen dat alle pertinente processtappen worden gejournaliseerd;
- afwijkingen op daarvoor bestemde controle grootboekrekeningen worden bijgehouden.

Onder de bovenstaande afspraken wordt *risk exposure*, het cumulatieve risico waaraan een assetportefeuille op een bepaald moment blootstaat, gedefinieerd als:

- Het saldo op het cumulatieve saldo op de grootboekrekeningen die anomalieën registreren.

Uit deze definitie blijkt:
- dat Risico toeneemt als Control en Compliance afnemen;
- dat Risico afneemt als Control en Compliance toenemen;
- dat het risico waaraan we op een bepaald moment blootstaan (*onze risk-exposure*) kunnen beheersen door de mate waarin we *in control* en *compliant* zijn.

What's in a name?

Door de relatie tussen control, compliance en risico op waarde te schatten volgt de realisatie dat de term 'accrual based risk management' synoniem is voor begrippen als:
- 'accrual based control';
- 'accrual based compliance';
- 'accrual based conformance'.

De *balance of control* is het abstractiedomein waarop deze disciplines één worden.

Hoezo 'accrual based'?

Het Engelse woord *accrual* wordt in minimaal twee contexten gebruikt. Ten eerste *accrual versus cash based bookkeeping/accounting* en ten tweede *the accrual of interest*.

De vertaling van dit woord naar het Nederlands was een uitdaging. In het Nederlands spreken we respectievelijk van het kasstelsel versus het factuurstelsel van boekhouden, of rentegroei, rentereservering of rentetoename.
In de eerste zin is accrual based versus cash based een dichotomie die bepalend is voor de administratieve periode waarin boekingen worden geadministreerd. In praktische zin impliceert dit dat de administratie preciezer weergeeft in welke periode transacties hebben plaatsgevonden.

Accrual in de zin van 'the accrual of interest' geeft aan dat de rente zich doorlopend accumuleert of wordt gereserveerd, zo u wilt. De term accrual based risk management past ook bij dit gebruik van het woord accrual om aan te geven dat de mate van blootstelling aan risico (risk exposure) doorlopend wordt bijgehouden. En om aan te geven dat er bij accrual based risk management over het niet *in-control* zijn - uitgedrukt in de currency of risk, control & compliance - rente geheven kan worden.

Een pleidooi

Het is een understatement om te stellen dat de huidige praktijk op het gebied van het operationele risico management voor verbetering vatbaar is. Er worden in dit domein verschillende administraties gevoerd. Denk hierbij aan de administratie van:
- identiteit;
- configuratie items;
- bevoegdheden, autorisaties en rechten;
- veranderingen;
- incidenten en problemen.

Hierbij ontbreekt schijnbaar de realisatie dat al deze domeinen met een grootboek over hun gehele levenscyclus te administreren zijn. De voordelen van de inzet van dubbelboekhouden zijn legio. Dubbelboekhouden is namelijk een controle-instrument dat, met wereldwijde consensus, sinds de 15e eeuw wordt ingezet. Het is in alle situaties een essentieel instrument waarbij het *in control* zijn een requirement is.
In de loop van dit jaar verwacht de auteur publicaties en uitgewerkte rekeningschema's beschikbaar te stellen die in detail ingaan op de toepassing van dubbelboekhouden voor het administreren van operationele risico's.

Samenvatting

In een tijdperk waarin onze maatschappij van de ene crisis naar de ander lijkt te strompelen, zijn capabele instrumenten voor risicomanagement geen overbodige luxe.
Dit artikel heeft accrual based risk management geïntroduceerd als een instrument dat ingezet kan worden om de maturiteit van alle domeinen van de interne controle te verbeteren. Accrual based risk management kwantificeert en administreert voor een assetportefeuille *control*, *compliance* en risico met behulp van dubbelboekhouden.
Accrual based risk management is niet nieuw maar past eenvoudigweg dubbelboekhouden toe buiten het domein van de *financial control* en *accounting*.

> Al deze domeinen zijn met een grootboek te administreren

GEORGANISEERD DOOR MADISON GURKHA

4 april 2012 | De Reehorst in Ede

Black Hat Sessions JUBILEUMEDITIE

SPREKERS ZIJN

FOTO: TONY THIJS


Brenno de Winter


Walter Belgers


Wim Verloop


Huub Roem


Job de Haas


Bert Hubert


Alex de Joode


Roel Verdult


Koen Martens


Frans Kollée


Stefan Castille

Edwin van Buuren

Dit jaar organiseert Madison Gurkha alweer de 10e editie van de Black Hat Sessions. In deze jubileumeditie op 4 april 2012 laten we de stand van beveiliging in de ICT-wereld de revue passeren, van verleden via het heden naar een blik in de toekomst.

Het dagvullend programma bestaat uit meerdere parallelle tracks, waardoor u, ongeacht uw technische achtergrondkennis, interessante lezingen kunt volgen. De onderwerpen zijn uiteenlopend, variërend van forensics tot abuse afhandeling, van hackerspaces tot NCSC, van hardware hacking tot RFID en van DNS tot social engineering. De dag begint met een keynote door journalist van het jaar 2011, Brenno de Winter, die het afgelopen jaar heel wat stof deed opwaaien in beveiligingsland. Ook de plenaire afsluiter mag er zijn: een live demonstratie van enkele courante aanvalstechnieken, belicht vanuit zowel de aanvaller alsook de verdediger. Op www.blackhatsessions.com vindt u het complete sprekersprogramma en het inschrijfformulier.

Het belooft een interessante editie te worden. We hopen dat u deze dag samen met ons wilt doorbrengen in Ede.

Registreer nu
Voor leden van het PvIB geldt een aantrekkelijke korting van 15%. Zo betaalt u i.p.v. 265 euro maar 225,25 euro excl. BTW per persoon. Vul hiervoor de kortingscode, die het PvIB onlangs in haar nieuwsbrief heeft verstrekt, in op het inschrijfformulier. Maak hiervoor gebruik van de laatste bullet en de korting wordt tijdens het afrekenproces automatisch verwerkt.

Verdere informatie
Black Hat Sessions Part X Jubileumeditie vindt plaats op woensdag 4 april bij Hotel en Congrescentrum De Reehorst te Ede. Het programma start om 09.25 uur en duurt tot 16.40 uur. Aansluitend wordt nog een borrel georganiseerd. Registratie is mogelijk vanaf 08.30 uur.
Meer informatie over het congres is te vinden op www.blackhatsessions.com.

SPONSORS

itsX Information Technology Security eXperts

PvIB Platform voor InformatieBeveiliging

SCOS

MEDIA PARTNERS

Ngi Platform voor ICT-professionals

Secure Link Networking Security Solutions

ORGANISATIE

Madison Gurkha
Your Security is Our Business

VERTROUWEN IS GOED… (deel 2)

We vervolgen onze discussie over vertrouwen uit de LinkedIn-groep voor IB-auteurs. Dit is het tweede deel in reactie op de vraag:

Stalin wist het al: "Vertrouwen is goed, controleren is beter." Maar hoe controleer je dat vertrouwen? En hoe vertrouw je de controleur? Ergens blijft er een stuk vertrouwen over en een stuk controle liggen. Of niet? Is het systeem waterdicht te krijgen?

Deze discussie is nu gesloten. De besloten LinkedIn groep voor IB-auteurs is te vinden via http://www.linkedin.com/groups?gid=4188826

Chris de Vries:

… is mensenwerk en m.i. cultuurbepaald.

Geert Hofstede heeft in 1991 een boek het licht laten zien dat heet: 'Cultures and organizations - software of the mind'. Daarbij omschrijft hij al op de omslag dat interculturele samenwerking van betekenis is voor overleving.

Waarom willen controleren? Waarschijnlijk omdat wij het niet vertrouwen. Maar wat vertrouwen wij dan niet? Deze vraag ligt ten grondslag aan de door Lex Borger opgeworpen vraag 'of vertrouwen gecontroleerd moet worden en/of dat systeem waterdicht te krijgen is?'

Mijn antwoord op de laatste vraag luidt: "Nee!"

Als bankier had ik veel te maken met vertrouwelijke gegevens enerzijds. Ondernemers die mij om vertrouwen vroegen anderzijds. En dat in de jaren '80, toen het fundament werd gelegd voor de huidige krediet- en Eurocrisis en waar relatief gezien een zwaardere aanslag op de samenleving werd gepleegd dan nu. Maar daarover een andere keer.

Om te begrijpen hoe ik in de vraagstelling vertrouwen/controle sta, verzoek ik om geduld om mij te volgen in de destijds gangbare beslissingsprocedure voor het toekennen van bancaire financieringen.

Als bankier hanteerde ik een eenvoudige stelregel die uit vier elementen bestaat:

1. De moraliteitsdrempel;
   De gedachtegang hierachter was dat - als een ondernemer niet te vertrouwen was - je zelfs geen ƒ 1,- moest uitlenen - al was het gedekt door een goudstaaf. Hoe slim en voorzichtig je ook bent: een oplichter is altijd net iets slimmer. Het vervelende is dat de oplichter er niet als een oplichter uitziet, maar als iemand aan wie je jouw geldbeurs zou willen meegeven. Moraliteit moet je hierbij niet te beperkt opvatten. Het is niet alleen een ethische norm, maar ook een norm met oog voor opleiding, achtergrond en (sociale) vaardigheden. Het is een totaal mensbeeld. Voor dit criterium moest de ondernemer voor de volle 100% slagen.
2. De rentabiliteitsdrempel;
   Zodra de ondernemer jouw vertrouwen heeft verdiend - laten we hopen dat je het niet ten onrechte iemand onthoudt dan wel iemand ten onrechte toekent - dan is de 2e toets die van rentabiliteit. Een ondernemer moet financieel winst kunnen draaien. Anders is vroeg of laat zijn geld op en gaat hij failliet. Dan kun je beter ten halve keren en iets overhouden dan de hele weg aflopen en failliet gaan. Winstgevendheid is niet altijd alleen een groot bedrag in euro's, maar kent ook andere (sociale) verschijningsvormen.
   Dit criterium telt voor 60% mee van het eindoordeel.
3. De solvabiliteitsdrempel;
   Soms kost het tijd om winst te behalen. Dan moet je het even kunnen uitzingen en is het goed over voldoende beginvermogen te beschikken. Dat betekent dus dat de derde afweging over de solvabiliteit oftewel het eigen vermogen gaat.
   Dit criterium telt mee voor 20% van het eindoordeel.
4. De liquiditeitsdrempel;
   Het laatste afwegingspunt was de liquiditeit. Is er een tekort aan liquiditeit - een wet van Meden en Perzen, want waarom zou je anders bij de bank aankloppen? - dan hoeft dat niet erg te zijn indien er voldoende winstgevendheid wordt verwacht. Dan komt met de tijd de liquiditeit en dus de oplossing.
   Wie kan tellen komt snel tot de conclusie dat ook dit criterium voor 20% meetelt.

Uit de voorgaande procedureomschrijving valt af te leiden dat de menselijke inschatting een heel belangrijk bestanddeel uitmaakt van het uiteindelijk

resultaat. De meer kwantificeerbare controlestappen 2 t/m 4 volgen pas nadat de eerste stap genomen was.
Zo behoort dat mijns inziens ook te gaan in de hele wereld. Of we het nu hebben over bancaire financieringen, ICT- of landenrisico's. Gaat het nu ook zo? Wederom moet ik spijtig genoeg zeggen: "Nee!"
Neem de banken. Er bestaat een aan waanzin grenzend vertrouwen dat controle bancaire risico's tot een minimum kan beperken. Dit controlemechanisme heet Basel II en III. Het is een stelsel van normen, ratio's en controles die moeten voorkomen dat banken te veel risico's nemen. Resultaat: het bankwezen verstrekt het MKB (de zo genoemde motor van de economische groei) geen kredieten meer. Als er kredieten worden verstrekt dan is de tarifering onredelijk hoog.
Neem dan de landen. Eerst Griekenland, dan Italië, België en nu zelfs alle 'Triple A' landen van Europa. Door wie? Door Amerikaanse ratingbureaus, die er mogelijk elk belang bij hebben de euro onderuit te halen ten faveure van de dollar. Doel: behoud van de Dollar als sleutelvaluta. Dit staat gelijk aan onbegrensde kredietverlening van de wereld aan dat land, hier dus de USA. Voordeel: consumptie blijft mogelijk, het zetten van de tering naar de nering kan worden uitgesteld. De euro was hard op weg de sleutelvaluta te worden. Je kunt je dus afvragen of er sprake is van ondergrondse economische oorlogsvoering door de USA tegenover de EU.
Neem vervolgens de ICT. Wij bouwen antivirusmuren, encrypteren dat het een lust is en bouwen in onze systemen de ene na de andere controle. Alles rationeel en systematisch. Het probleem? Wij hebben te maken met mensen! Mensen nemen vaak besluiten op onvolledige informatie en mede op basis van emoties/gevoelens en inschattingen. Daarbij hebben mensen een onbegrensd vertrouwen in de door hen gebouwde systemen. Zo wordt bij banken al heel vaak het kredietbesluit genomen door geautomatiseerde systemen, die de gebruikers niet kunnen doorgronden. Wat nu als er een programmeerfout in voorkomt? Of erger: een programmeur bewust fouten maakt of achterdeurtjes inbouwt? De reflex van branchemensen is dan: kan niet, gebeurt niet.
De werkelijkheid is echter vaak anders. Kijk maar naar onze politici; de een na de ander maakt fouten, liegt of bedriegt of toont overduidelijk als beste

vaardigheid over onkunde te beschikken.
Hoe was het ook al weer? Waren het niet slechts Nederland, Ierland en Denemarken welke voldeden aan de toelatingseisen van de euro? Hadden toen ook al niet Duitsland (ik herinner mij de debudgettering van de ziekenhuisuitgaven), Frankrijk en Italië met een truc de eurodrempel gehaald?! En nu spreken wij over de fraude van Griekenland? Vergeten wij even de 120% inflatie bij de inwisseling van de gulden voor de euro (koers 2,20371 voor de sterkste valuta destijds van de wereld en de koffie ging van ƒ 1,75 naar € 1,75 of meer!). Durven onze politici nu serieus te spreken over de afschaffing van de euro?
Het bovenstaande mag duidelijk maken dat ik niet geloof in het Amerikaans rationeel, instrumenteel denken dat je in voorgaande voorbeelden terugvindt. Amerikaans denken is stellen dat de wereld maakbaar is. Amerikaanse studieboeken staan vol met structuren als:

- samenvattende inleiding van de lesstof;
- de lesstof zelf;
- de samenvatting;
- de quiz over de stof en
- vragen en problemen.

In een Amerikaanse boek vind je altijd rijtjes van 'do & don't'. Dit 'aan het handje meenemen'-denken heeft Europa geïnfecteerd en daarmee Europa van haar identiteit en zelfstandig/oorspronkelijk denken beroofd. Wij moeten onze eigen weg gaan en dat betekent terug op de weg naar een meer menselijk ondernemerschap.
Een menselijk ondernemerschap houdt in dat wij er van uit moeten gaan dat de mens te vertrouwen is en dat een zekere mate van controle passend is. Waarbij controle dan vooral te zien als een handreiking tot steun aan de gecontroleerde en niet als straf. Daarbij zal controle niet altijd sluitend zijn noch dat de controle zelf foutloos zal zijn.
Samenvattend: dit is bijna al een heel artikel geworden. Ik geloof niet dat controle op de eerste plaats moet staan noch dat controle sluitend is. Vertrouwen behoort op de eerste plaats te staan en verificatie op de tweede!

Eric Luiijf:
Mee eens dat we vaak teveel kijken naar de VS. Vandaag de hele dag bij de EU proberen te bestrijden dat Smart (energy) Grids in de VS en die in de EU een totaal andere doelstelling hebben. De security-regels in de VS worden soms ingericht om schijnbaar een probleem aan te pakken. In werkelijkheid is het niet meer dan een mooie verpakking. Zoals bijvoorbeeld de NERC CIP-standaarden: deze gelden alleen voor bulkpower generation > 300 MW. Heb je drie eenheden die je stelselmatig op 280 MW laat draaien, dan hoef je geen maatregelen te treffen omdat je ineens niet vitaal bent. Volgens de NERC-standaarden is het distributienetwerk van New York ook niet vitaal. Feitelijk vallen onder de NERC standaarden alleen de al eerder sterk beveiligde NPP's waar nu extra ICT-security eisen aan gesteld worden…
In Europa kijken we verder…

OPENING NATIONAAL CYBER SECURITY CENTRUM

Onderweg naar een veilig cyber-Nederland

Lex Dunn CISA CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is tevens voorzitter van de MSP-ISAC. Hij is bereikbaar via lex.dunn@capgemini.com. Aart Jochem is werkzaam bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid en bereikbaar via a.j.jochem@nctv.minvenj.nl. Beide auteurs zijn redacteur van het blad Informatiebeveiliging.

Op 12 januari 2012 heeft de Nederlandse Nationale Cyber Security Strategie (NCSS) een flinke stap voorwaarts gemaakt. Op die dag werd in het World Forum in Den Haag de officiële opening van het Nationaal Cyber Security Centrum (NCSC) verricht door Minister van Veiligheid en Justitie, Ivo Opstelten.

Onder leiding van dagvoorzitter Ruben Maes begon rond 9.00 uur de officiële opening van het nieuwe Nationaal Cyber Security Centrum (NCSC). Zo'n 250 genodigden waren aanwezig in het World Forum in Den Haag en werden welkom geheten door de Burgemeester van Den Haag, Jozias van Aartsen. In zijn welkomstspeech ging hij in op Den Haag als cyberhoofdstad van Europa. Hij schetste de ambitie van zijn stad om in 2015 de 'City of Innovations in Peace, Justice and Security' te zijn. Er is al een groot aantal organisaties en bedrijven met een link naar cybersecurity gevestigd in Den Haag, dus het is niet meer dan normaal dat het NCSC ook hier is gehuisvest.

Vervolgens was de beurt aan de Minister van Veiligheid en Justitie, Ivo Opstelten. Hij greep terug op de lancering van de Nationale Cyber Security Strategie (NCSS) vorig jaar. Het NCSC is een eerste stap vanuit de Overheid om een goede privaat-publieke samenwerking op het gebied van cybersecurity te realiseren. Uiteraard is het primair de eigen verantwoordelijkheid van bedrijven, organisaties en sectoren om zich te wapenen tegen cyberbedreigingen, maar middels het NCSC en goede samenwerking is het mogelijk een goede, sterke en weerbare ICT infrastructuur voor Nederland te realiseren. De Minister nodigt dan ook private partijen, maar ook de wetenschap en internationale gremia van harte uit om zich bij het NCSC aan te sluiten. Er wordt nu al gewerkt aan de aansluiting van overheid (als eerste EL&I, Defensie, BZ&K, BuZa en V&J), kritische infrastructuren

Lasershow officiële opening NCSC.

(middels de al bestaande Information Sharing & Analysis Centra of ISAC's) en de financiële sector.

Het NCSC geeft invulling aan de zes lijnen uit de NCSS:

- een integrale aanpak voor publieke én private sector middels samenwerking;
- een adequaat en actueel beeld van de (cyber)bedreigingen en risicoanalyse;
- het versterken van de weerbaarheid van de ICT-infrastructuren van de BV Nederland;
- het versterken van de responsecapaciteit bij cyberincidenten;
- het intensiveren van opsporing en vervolging van cybercrime;
- het stimuleren en coördineren van onderzoek en onderwijs inzake cybersecurity.

Vorig jaar al is de Cyber Security Raad geïnstalleerd, met daarin vertegenwoordigers van overheid, bedrijfsleven én onderwijs en wetenschap. Na deze stimulerende woorden ging de minister over tot de officiële opening van het Nationale Cyber Security Centrum door een druk op een grote, rode knop. Met een grootse lasershow en veel harde muziek werd het de aanwezigen duidelijk dat de opening gelukt was.

In een korte film werd de aanwezigen verteld wat het NCSC is, wat het kan en waar het vandaan komt (GovCERT is nu geheel opgegaan in het NCSC, in de film waren dan ook veel bekende gezichten te zien).

Onder leiding van Ruben Maes werden vervolgens drie vertegenwoordigers van de verschillende groepen ondervraagd over hun beeld bij, en relatie tot het nieuwe NCSC:

- Corien Prins, hoogleraar in Tilburg, en lid van de Cyber Security Raad;
- Cees Pisuisse, directeur Legal, Regulatory & Public Affairs bij de Gasunie;
- Wil van Gemert, de kersverse directeur van het NCSC (op zijn eerste werkdag).

Uit deze forumdiscussie werd duidelijk dat alle partijen inzetten op goede samenwerking. En: dat wij in Nederland voorop lopen met het NCSC.

Vervolgens was het woord aan Erik Akerboom, de Nationale Coördinator Terrorismebestrijding en Veiligheid, en co-voorzitter van de Cyber Security Raad. De overheid wil een open, innovatief en tegelijk veilig internet. Dat brengt risico's met zich mee. Welke? In het cybersecuritybeeld van december 2011 (nog uitgebracht door GovCERT) worden de bedreigingen zichtbaar. Het komt niet als een verrassing dat het aantal incidenten weer is toegenomen, zoals met de identiteitsfraude. De bedoeling is om dit cyberbeeld twee maal per jaar te updaten, en kwetsbaarheden en nieuwe ontwikkelingen (o.a. cloud) steeds scherper in beeld te krijgen. Dat kan door een gezamenlijke aanpak met het NCSC als spin in het web.

Tot slot werd een videoboodschap van de Eurocommissaris voor de Digitale Agenda, mevrouw Neelie Kroos, vertoond. Hierin feliciteert zij Nederland met het zetten van deze belangrijke stap voor het verhogen van de cybersecurity. Zij uit naar samenwerking in Europees verband.

De aanwezige deelnemers konden vervolgens in twee sessies een keuze maken uit een achttal verschillende workshops. Doel hiervan was nader met elkaar van gedachten te wisselen over cybersecurity. Passende oplossingen voor cybersecurity bedreigingen werden getoond. De workshops waren afwisselend, variërend van een workshop waarin de rol van Defensie in cybersecurity werd verdiept door luitenant-kolonel Volmer tot presentaties van oplossingen voor knellende cybersecurity problemen door samenwerkingsverbanden van bedrijven. Gedurende de hele dag was er in de centrale hal een markt. Hier konden 21 bedrijven zich aan de aanwezigen presenteren op het gebied van cybersecurity.

Als laatste plenaire sessie vóór de lunch was de beurt aan Melissa Hathaway (Cyber Security Expert en voormalig Director Joint Interagency Cyber Task Force onder president George W. Bush). Zij feliciteerde Nederland met de opening van het centrum. Bovendien haalde ze de snelheid aan waarin Nederland niet alleen een cybersecurity strategie formuleerde, maar ook de daad bij het woord voegt en uitvoering geeft aan deze strategie. Nederland kan een leidende positie innemen in Europa. In het bijzonder valt de aanpak op, die gebaseerd is op publiek-private samenwerking. Dit is in de Europese context uniek. Melissa Hathaway zette de ontwikkeling van de cybersecurity

Forum vlnr: Cees Pisuisse, Wil van Gemert en Corien Prins.

Vlnr: Erik Akerboom, Ivo Opstelten en Jozias van Aartsen.

strategie in het daglicht van de aanpak na de watersnoodramp in 1953. Nederland ontwikkelde een Deltaplan voor de bescherming tegen water en zou dit ook voor de aanpak van cybersecurity moeten doen. Nationaal Cybersecurity Centrum moet kennis en expertise bundelen en de problemen daadkrachtig aanpakken. Een boeiende lezing.

Na de lunch, waarbij ruimschoots gelegenheid bestond om te netwerken, nam Arie van Bellen (Directeur ECP.NL) de handschoen op om de 'lunchdip' door te komen. Hij vertelde over de ervaringen die ECP.NL al heeft opgedaan met 'privaat-publieke samenwerking' (PPS), en waar deze voor NCSC van waarde kunnen zijn.

Hierna werden er nogmaals twee sessies van de workshops gedaan, waarna de middag werd afgesloten met een speech van Martin Borrett (Directeur van IBM Institute of Advanced Security Europe). Als 'kastelenfreak' begon hij zijn verhaal dan ook met een kasteel in Italië uit 1151, dat op het moment van bouwen de laatste veiligheidstechnieken had, maar ongeveer een eeuw later werd verrast door de uitvinding van het buskruit en kanonnen. De beveiligingsmaatregelen moesten dan ook anders. Hetzelfde zien we in cyberland: het is een *'continuing journey'* waarin steeds nieuwe (en geavanceerdere) bedreigingen opduiken. Het is dan ook zaak een goed overzicht van deze bedreigingen te hebben en te houden!

Na het formele programma was er nog gelegenheid om onder het genot van een hapje en een drankje verder met elkaar te netwerken. Het viel op hoe makkelijk de verschillende partijen (overheid, bedrijfsleven en onderwijs/wetenschap) dat al deden. Dat dat hard nodig zal zijn om de gewekte verwachtingen waar te maken moge duidelijk zijn. Dat is misschien de grootste uitdaging voor het nieuwe centrum: de opening ging met een knal, maar dat betekent niet dat alle problemen voorbij zijn. Er zal in het centrum door alle partijen hard gewerkt moeten worden om met de nieuwe aanpak een open en veilig internet in Nederland te bewaren.

Alle foto's bij dit artikel zijn welwillend ter beschikking gesteld door NCSC, waarvoor onze hartelijke dank.

Links:

De tekst van de speech van Minister Opstelten:
http://www.rijksoverheid.nl/regering/het-kabinet/bewindspersonen/ivo-opstelten/toespraken/2012/01/12/opening-van-het-nationaal-cyber-security-centrum.html

De website van het Nationaal Cyber Security Centrum:
http://www.ncsc.nl/

BOEKBESPREKING

LIARS & OUTLIERS - BRUCE SCHNEIER

Lex Borger

Het komt niet vaak voor dat je als klein Nederlands tijdschrift een primeur hebt. Soms krijg je het onverwachts in je schoot geworpen. Net voor de kerst ontving ik een preview exemplaar van Bruce Schneier's nieuwe boek, dat in maart 2012 uit zal komen.

Het is 12 jaar geleden dat Bruce het boek schreef dat in mijn ogen nog steeds zijn meesterwerk is: 'Secrets & Lies'. Ik heb dat boek aan verschillende managers cadeau gedaan om ze hiermee aan de inhoud bloot te stellen. Bruce heeft hierna nog een aantal boeken geschreven, die zonder meer goed zijn, maar niet dat uitzonderlijke niveau bereikten van 'Secrets & Lies'. De titel van zijn nieuwste boek, 'Liars & Outliers', heeft eenzelfde klank - dat begint goed. In dit boek pakt hij de sociologie van de informatiebeveiliging op, bekeken vanaf een evolutionair standpunt en legt zo uit wat vertrouwen betekenis geeft.

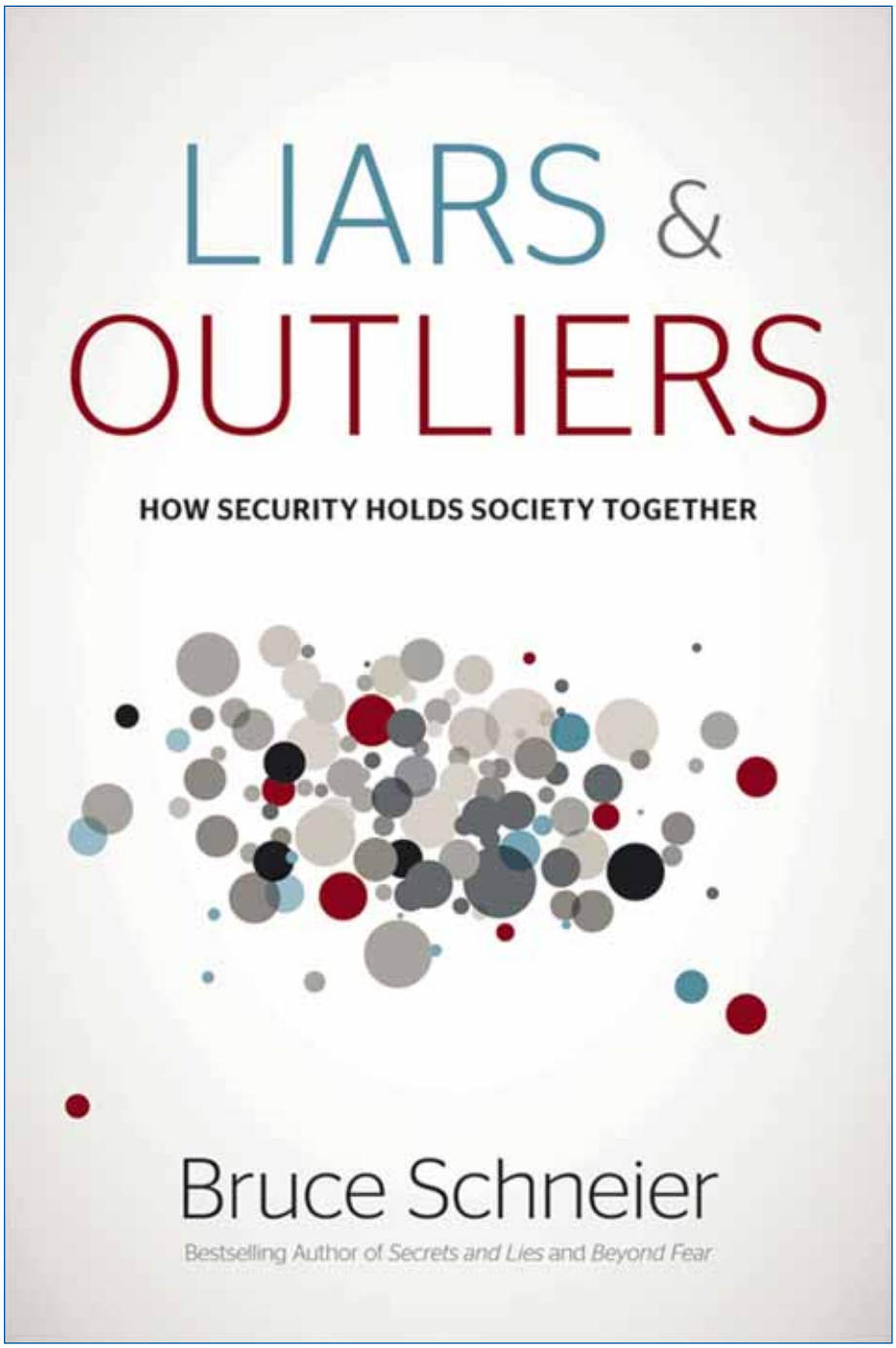
De titel getuigt direct van durf: in het boek komen de beide woorden van de titel nauwelijks voor. Dat heeft uiteraard een reden. Hij vat de twee termen samen tot één: 'defectors'. Defectors zijn de mensen die zich niet conformeren aan de groep. Bruce is zelf een defector, vandaar waarschijnlijk dat hij juist hier pakkend over kan schrijven. Uiteindelijk beschrijft 'Liars & Outliers' hoe je in een groep nog steeds vertrouwen kunt hebben, ondanks het feit dat er defectors zijn die het aantasten. Maar hij laat ook zien dat op het moment dat het vertrouwen wegvalt, de defectors de overhand hebben gekregen.

Het boek leest niet overal makkelijk weg. Bruce besteedt veel ruimte om de evolutionaire en sociologische theorieën uit te leggen voordat hij aan de kern van zijn verhaal begint. Als lezer zul je hier eerst in mee moeten gaan. Dat neemt 46 pagina's in beslag - deel 1. Vervolgens heeft hij 78 pagina's nodig om uit te leggen welk model hij daaruit gedestilleerd heeft (deel 2) en 68 pagina's om dat model op de samenleving te projecteren (deel 3). Het is nodig al die stappen te nemen om zijn betoog te kunnen volgen, maar er zijn momenten waarbij ik mezelf door stukken tekst heen moest slepen. En dan komt het feest der herkenning: deel 4. Dit leest als vanouds snel en simpel weg en is daardoor verrassend snel afgelopen. Wat er dan overblijft zijn ruim 100 pagina's aantekeningen en referenties. Iedere pagina bevat wel verschillende verwijzingen hiernaar. Dat laat aan de ene kant zien hoe fundamenteel Bruce dit boek heeft aangepakt, maar je kunt van de lezer nauwelijks verwachten dat hij iedere verwijzing naar de aantekeningen gaat natrekken. Dat zul je selectief moeten doen.

Bruce Schneier

Ben je al bekend met speltheorie? Dan kom je in deel 1 veel bekends tegen: het 'prisoner's dilemma', het 'red queen effect' en het 'hawk-dove' spel. Dat laatste was nieuw voor mij, dus de winst is al binnen. Dunbar's theoretische groepsgroottes voor verschillende soorten sociale interactie worden ook in de mix gegooid. Als je de boeken van Malcolm Gladwell interessant vindt, dan is deel 1 een feest van herkenning. Dit alles komt ook weer terug in zijn conclusie in deel 4. Laat je hier niet afschrikken door de 'kretologie'. Bruce legt alles ruimschoots uit - en als je het boek niet leest is het ook terug te vinden op Wikipedia.

In deel 2 definieert Bruce een vertrouwensmodel . De bouwstenen die hij hiervoor gebruikt, zijn verschillende vormen van sociale druk. Hij voegt daar beveiligingssystemen aan toe. Die combinatie werkt niet altijd even lekker. Hij geeft dat ook zelf toe en ik denk dat het zomaar zou kunnen dat hij het boek in de toekomst op dit punt nog wel eens gaat aanpassen. Het vertrouwensmodel heeft nog wat ruwe randjes, maar is zeker al toepasbaar. In deel 3 past Bruce het model toe op



dilemma's uit de hedendaagse praktijk. Ik realiseerde me dat hij hiermee ineens ook een fundament legt onder de analyses in zijn andere boeken, zoals 'Beyond Fear' en 'On Security'.

Dit boek geeft inzicht waarom je er van uit moet gaan dat er altijd mensen zullen zijn die zich niet aan de regels houden. Die zelfs op zoek zullen gaan naar de mogelijkheden om buiten de regels om te gaan. Tegelijkertijd laat het zien dat de samenleving die van die regels aan elkaar hangt hiermee niet omver valt, ook al lopen we met de beveiliging achter de feiten aan. Ik heb hier ook uit geleerd waarom die achterstand in tijden van snelle innovatie juist toeneemt.

Is het een nieuw meesterwerk? In mijn ogen stijgt het niet boven 'Secrets & Lies' uit, maar komt het wel dichtbij. Voor informatiebeveiligers is het een absolute aanrader: het geeft goed inzicht in het krachtenspel wat je op iedere werkvloer tegenkomt. De eerstvolgende keer dat iemand je een beetje glazig aankijkt als je moet uitleggen dat 100% beveiliging niet bereikt kan worden: raad ze dan aan dit boek te lezen.

ZEG MAAR DAG TEGEN PRIVACY

mr Rachel Marbus, KPMG IT Advisory en bestuurslid PvIB

Een kort onderzoek naar de algemene voorwaarden van sociale netwerksites Facebook, Hyves, Google+, Twitter en Linkedin

Er wordt doorgaans flink geklaagd over de stand van zaken op het gebied van privacy en sociale netwerksites. Gezien de hoeveelheid informatie die daar gedeeld, gebruikt en hergebruikt wordt, lijkt dat niet geheel vreemd. Maar waar ligt nu de juridische bron van deze privacy-erosie? Binnen de algemene voorwaarden die niemand leest. Die staan bol van de bepalingen die de privacy van gebruikers uithollen. In dit artikel ga ik op drie daarvan in: niet-exclusieve licenties tot overdracht van de intellectuele eigendomsrechten, de real name policies en het commercieel gebruik van persoonsgegevens.

Niet-exclusieve licenties tot overdracht van de intellectuele eigendomsrechten

Elke sociale netwerksite heeft in haar algemene voorwaarden een clausule opgenomen waarin de intellectuele eigendomsrechten van de gebruikers in een niet-exclusieve licentie worden overgedragen aan de aanbieder. Door deze overdracht kunnen sociale netwerksites praktisch alle content die een gebruiker plaatst, hergebruiken. Hoe een dergelijke clausule is ingericht en wat de reikwijdte van de bepaling is, verschilt echter weer per netwerksite. De gevolgen van een dergelijke clausule voor gebruikers wat betreft privacy c.q. beschikkingsmacht over persoonlijke gegevens kunnen daarmee verschillen. De clausule van Facebook lijkt vrij ver te strekken en bevat alle zogenoemde IP-content waarbij Facebook niet exact uitlegt wat dat dan precies is. Ze geeft aan dat het gaat over bijvoorbeeld foto's en filmpjes, maar er kunnen ook andere zaken onder worden geschaard. De licentie eindigt op het moment dat een gebruiker de content wist - tenzij iemand anders de informatie opnieuw heeft gedeeld. Ook Twitter maakt gebruik van een zeer brede licentie waarin ze benadrukt dat de informatie kan worden gebruikt in "any and all media or distribution methods". Zelfs mogelijk toekomstige dienstverlening wordt onder de clausule geschaard. Wat betreft de dienstverlening van Hyves: zij lijkt haar gebruikers meer houvast te bieden door specifiek te benoemen dat de licentie alleen geldt met betrekking tot commerciële doeleinden. Hiermee perkt ze het gebruik van de gegevens zeer specifiek in. Ook Google+ kent een dergelijke beperking tot de Google-services. Daarnaast kan voor bepaalde services een dergelijke licentie worden uitgesloten. Van alle onderzochte clausules lijkt die van Linkedin echter het meest omvattend. De scope wordt breed getrokken naar alle beschikbare informatie, of die nu direct of indirect wordt verkregen. Daarnaast wordt niet gesproken over een licentie (hetgeen ingetrokken zou kunnen worden) maar over een 'recht' dat aan Linkedin wordt verleend.

DE CLAUSULE VAN LINKEDIN LIJKT HET MEEST OMVATTEND

Wat is nu het risico dat hier direct aan wordt verbonden? De gebruikers geven de aanbieders met een dergelijke licentie een recht om gebruik te maken van de informatie die zij verstrekken. Niet alle aanbieders gaan daarin even ver, zoals in het voorgaande besproken. Niettemin betekent het wel dat de informatie die binnen de reikwijdte van de clausule valt, door de sociale netwerksite in kwestie gebruikt mag worden. De persoon is weliswaar vrij de informatie zelf ook te gebruiken, maar kan door het akkoord gaan met de algemene voorwaarden niet voorkomen dat de aanbieder de informatie ook daadwerkelijk gebruikt. De beschikkingsmacht over persoonlijke gegevens wordt daarmee ingeperkt. Dit staat op gespannen voet met die gevallen waar een gebruiker zijn informatie expliciet beperkt deelbaar maakt door bijvoorbeeld de instellingen van het profiel op 'meest privaat' te zetten.

Real name policies

Doorgaans eisen sociale netwerksites dat er gebruik wordt gemaakt van de 'echte' naam bij het aanmaken van een account. Elke sociale netwerksite heeft ergens in de algemene voorwaarden een clausule staan, waarin wordt bepaald dat de gebruiker ervoor instaat dat hij accurate informatie verschaft. De enige echte uitzondering is Twitter;

die kent een dergelijke verplichting niet. Twitter hanteert wel een regel dat gebruikers zich niet mogen voordoen als een ander als dat tot doel heeft 'to mislead, confuse, or deceive others'. Voor de gebruiker staan deze verplichtingen al vrij lang in de voorwaarden van sociale netwerksites, maar hebben praktisch nooit tot veel oproer geleid. Dat veranderde door het handhavingsbeleid van Google wat betreft haar sociale netwerksite Google+. Binnen de voorwaarden hanteert zij het beleid dat personen de naam moeten gebruiken waarmee zij bekend staan bij vrienden, familie en collega's. Nu geeft deze formulering nog enige ruimte aan het creatief omgaan met de naam. Google+ werkt deze eis echter uit in een set 'Guidelines'[1]. Zo mogen geen titels worden gebruikt of verschillende 'language scripts', nicknames en pseudoniemen, vreemde tekens zoals cijfers of het '@'-teken en het mag niet meer dan 1 individu vertegenwoordigen (Familie Marbus is dus verboden). Mononaamaanduiding (mononyms) mag wel, maar daarvoor moet de persoon een verzoek indienen met ondersteunende juridische documentatie. De mononaam moet daarmee dus wel een juridische erkende naam zijn en bijvoorbeeld geen artiestennaam zoals Prince of Madonna. Die juridische documentatie is dan vaak een kopie van het paspoort of een andere identiteitskaart. Met als gevolg dat veel personen die in verband met identiteitsfraude[2] of veiligheidsoverwegingen niet willen verstrekken of versturen. Voor zover bekend is Google+ de enige aanbieder die haar beleid zeer actief handhaaft. Dit heeft voor veel onbegrip gezorgd bij mensen die bekend zijn onder hun peudoniem zoals IdentityWoman[3], mensen met een mononaam zoals Stilgherrian[4]. Maar ook voor privacyvoorstanders die zich zorgen maken over de macht van Google[5]. Ook Facebook legt haar gebruikers beperkingen op als het om naamgebruik gaat. De algemene voorwaarden bevatten namelijk een clausule dat de 'echte' gegevens gebruikt moeten worden. Net als bij Google wordt dit nader uitgewerkt in een aantal richtlijnen omtrent het (toegestaan) gebruik van namen. Zo moet de naam die wordt gebruikt, terug te vinden zijn op documenten als een ID-kaart of een creditcard. Bijnamen mogen alleen worden gebruikt als deze zijn afgeleid van de echte naam (bijvoorbeeld Bob voor Robbert) en mag het slechts de naam van 1 persoon bevatten. Tekens, symbolen en anderstalige toevoegingen zijn niet toegestaan. Een andere naam (bijvoorbeeld een meisjesnaam of een professionele titel) kan als alternatief worden gebruikt naast de echte naam.

Wat is nu het risico dat hier direct aan wordt verbonden? Het eerste dat in het oog springt, is een beperking in de keuzevrijheid van individuen om zonder onredelijke beperkingen vorm te geven aan de identiteit. Niet alleen het feit dat de echte naam moet worden gebruikt, maar dat dit tevens zal worden gedeeld met iedereen. Voor een account van Google+ is er een zogenaamd publiek stuk van het profiel dat altijd publiekelijk zichtbaar is. Wat dat aangaat is elke vorm van keuze uitgesloten. Er kunnen legio redenen zijn waarom iemand niet met de naam die op het paspoort staat vermeld, bekend wil zijn in de online wereld. Denk hierbij bijvoorbeeld aan stalking, reputatie, klokkenluider, dissident, slachtoffer identiteitsfraude, bekendheid onder een andere naam, en ga zo maar door. Als je je niet houdt aan het beleid van Google, wordt je account bevroren. Dit is niet alleen te zien op de Google+ account, maar op alle diensten die van Google worden afgenomen. Inclusief bijvoorbeeld email en Google Docs, omdat Google alle diverse accounts van haar diensten aan elkaar koppelt. Het niet volgen van het beleid kan daarmee dus zeer verstrekkende gevolgen hebben. Ook het scheiden van deelidentiteiten wordt daardoor bemoeilijkt. Daarentegen wordt het koppelen van de verschillende identiteiten van een persoon en het vergaren van alle beschikbare informatie daarbij zo wel erg gemakkelijk gemaakt.

DE BESCHIKKINGSMACHT OVER PERSOONLIJKE GEGEVENS WORDT INGEPERKT

HET VERANDERDE DOOR HET BELEID VAN GOOGLE VOOR GOOGLE+

Commercieel gebruik van persoonlijke gegevens

Sociale netwerksites bieden hun diensten gratis aan. Sommige sites bieden een aantal extra zaken aan, die tegen betaling kunnen worden afgenomen. Hiermee krijg je het zogenoemde 'premium'-lidmaatschap. Daar staat tegenover dat de verschillende sociale netwerksites vormen van advertising benutten op grond van de informatie die zij over gebruikers verkrijgen. Daarom hebben praktisch alle sociale netwerksites ook clausules daarover opgenomen in de algemene voorwaarden. Het is een bekend gegeven dat sociale netwerksites adverteren. Hoe zij dat doen en welke gegevens zij daarbij gebruiken, verschilt per aanbieder. Om het bereik en de gevolgen van de diverse clausules te begrijpen, is het ook hier weer belangrijk de beperkingen in scope te doorgronden. Zo stelt Hyves bijvoorbeeld zeer expliciet dat zij gegevens gebruikt voor marketing in verband met Hyves zelf. Dit geeft dus een duidelijke beperking aan wat het doel betreft. Daar moet echter wel bij worden gezegd dat het dan niet alleen marketing op of via Hyves betreft, maar ook in andere media. De clausule uit de privacypolicy van Twitter levert nog wel een aantal mooie breinbrekers op die wellicht te maken hebben met interpretatieverschillen en eventuele definitie-issues tussen Europese en Amerikaanse opvattingen: wat is nu precies private informatie? Twitter behoudt zich het recht voor non-personal information te delen en scharen de

publiek geuite tweets daaronder. De onderliggende redenering dat alles wat publiekelijk gedeeld is daarmee niet meer *personal information* zou zijn, staat op gespannen voet met de opvattingen die op Europees niveau worden gehuldigd in de dataprotectiewetgeving. Een tweet kan namelijk wel degelijk een persoonsgegeven bevatten. Het enkele feit dat een gegeven openbaar is geplaatst, maakt niet dat er ineens geen sprake meer zou zijn van een persoonsgegeven. Zelfs als dataprotectiewetgeving niet direct in de weg lijkt te staan aan het verdere verwerken van het persoonsgegeven, dan nog moet de vraag worden gesteld: wat kan/mag daar dan mee worden gedaan? Niet elk hergebruik zal mijns inziens toegestaan moeten worden. Dat is ook in overeenstemming met de basisprincipes van de Europese dataprotectiewetgeving die het zogenaamde 'secondary use' toestaan. Maar niet onbeperkt! Een ander aspect dat hieraan is verbonden is het principe van contextualiteit. Gegevens krijgen immers betekenis binnen de context waarin zij zich bevinden. Daarbuiten kunnen zij een andere betekenis krijgen, dat weer impact kan hebben op het beeld dat van een individu bestaat (of daardoor kan ontstaan). Hierdoor kan dit implicaties hebben voor de identiteit van personen. Google lijkt een uitzondering te maken wat betreft het commerciële gebruik van persoonlijke gegevens. Zij maken weliswaar zeer veel gebruik van advertentiemogelijkheden, maar doen dit niet op grond van persoonsgegevens of het verwerken daarvan. Zij kiezen op basis van de woorden die het meest relevant lijken te passen in de situatie. Stel dat iemand de woorden 'vakantie + Egypte' intypt, dan krijgt die persoon bijvoorbeeld reclame voorgeschoteld van reisbureaus die reizen naar Egypte aanbieden. Google behoudt zich nog wel de mogelijkheid voor om toch persoonsgegevens te verwerken met betrekking tot commerciële doeleinden. Maar dan alleen nadat er toestemming is gegeven. Linkedin lijkt het gebruik van persoonsgegevens te beperken tot het verzenden van commerciële boodschappen (email). Hiermee lijkt het erop dat zij met de data verder geen handelingen

HET VERGAREN VAN INFORMATIE WORDT ZO WEL ERG GEMAKKELIJK GEMAAKT

verrichten om bijvoorbeeld persoonsprofilering te verrichten. Of dit ook een correcte interpretatie van de clausule is, kan niet geheel met zekerheid worden gezegd. Juist omdat zij wel aangeven dat van diverse categorieën datagebruik wordt gemaakt voor *targeted advertising* waaronder ook geslacht, ras, nationaliteit en 'other aspects of your personal life'. Vooral onder die laatste categorie zal erg veel geschaard kunnen worden. De vraag die dit ook oproept is: waar komen die gegevens vandaan en wat wordt hier precies onder verstaan? Facebook gebruikt in beginsel de gegevens van haar gebruikers standaard (zoals een naam en foto. Maar Facebook gebruikt ook andere gegevens voor de verschillende vormen van adverteren. Personen kunnen via de instellingen van de sociale netwerksite het gebruik van de naam en de foto voor commerciële doeleinden beperken. Facebook kent verschillende vormen van advertering voor wie ze de persoonlijke gegevens van de gebruikers aanwendt. Daarnaast gebruikt ze ook gegevens die ze van haar adverteerders of klanten krijgt over de gebruikers. De enige restrictie die daaraan is verbonden, is dat ze na 180 dagen de gegevens vermengt met die van andere gebruikers. Hierdoor wordt het niet langer met de persoon in kwestie geassocieerd.

ONDER 'OTHER ASPECTS OF YOUR PERSONAL LIFE' ZAL ERG VEEL GESCHAARD KUNNEN WORDEN

MISSCHIEN DAT DE IN WORDING ZIJNDE NIEUWE EU PRIVACYWETGEVING MOGELIJKHEDEN BIEDT

Wat is nu direct het risico hieraan verbonden? Ook hier speelt weer de kwestie van contextualiteit. De gebruikers van Facebook geven weliswaar impliciet toestemming door akkoord te gaan met de algemene voorwaarden. Maar betoogd kan worden dat zij bij het vullen van het profiel geen rekening zullen houden dat de gegevens ook voor andere – lees: commerciële - doeleinden gebruikt kunnen worden. Ook zullen zij actief iets moeten ondernemen om te voorkomen dat de naam en de profielfoto door Facebook worden gebruikt. Dit moet namelijk binnen de instellingen worden veranderd. Maar dat geldt niet alleen voor Facebook; het contextueliteitsissue speelt in principe binnen alle sociale netwerksites. Hyves lijkt daarmee nog het minst ingrijpend, omdat die onder de Nederlandse wetgeving valt. Bovendien beperkt haar scope tot commercieel gebruik ten behoeve van promotie van Hyves zelf. Die contextualiteit staat onder druk. Dit komt doordat persoonlijke informatie (persoonsgegevens) door de aanbieders wordt gebruikt voor een ander doel dan waarvoor de persoon in kwestie de gegevens plaatste. Google geeft aan dat ze geen gebruik maakt van personally identifyable information (PII) rondom hun adverteringsbeleid en ook Linkedin verwijst naar PII. Echter PII is een Amerikaans begrip en het is enger dan het Europese 'persoonsgegeven'. Ook hier is de kans groot dat meer informatie over personen gebruikt wordt dan (Europese) gebruikers zouden verwachten.

En wat nu?

Het lijkt er dus echt op dat het magertjes is gesteld met de rechten van de gebruikers van sociale netwerksites. Iedereen vinkt netjes af dat hij de algemene voorwaarden heeft gelezen en gaat vrolijk sociaal interactief verder. Het roept de vraag op of algemene voorwaarden niet eigenlijk een lege huls zijn en ik besef terdege dat ik niet de eerste jurist ben die een dergelijk statement plaatst. Onder het Nederlands recht kennen we zogenaamde onredelijk bezwarende bedingen. Daarnaast een grijze en zwarte lijst in het consumentenrecht op grond waarvan bepaalde voorwaarden vernietigbaar zijn. De meeste sociale netwerksites zijn echter van Amerikaanse makelij en elk van hen verklaart dan ook het Amerikaanse recht van toepassing in geval van geschillen. Of je op dit moment dus als gebruiker daar mee geholpen bent, is maar zeer de vraag. Misschien dat de in wording zijnde nieuwe EU-privacywetgeving mogelijkheden biedt. Het wetsontwerp bevat namelijk een bepaling waarin het de Europese wet van toepassing verklaart op de gegevensverwerkingen van Europese onderdanen, ook als de aanbieder van buiten de EU komt. De enige voorwaarde daarbij is dat de dienst zich ook daadwerkelijk op dat EU-land richt. Dus als de tekst op de website bijvoorbeeld in het Nederlands is, wat voor alle hier besproken sociale netwerksites het geval is. Dus wie weet… kan nieuwe wetgeving gebruikers de helpende hand toesteken om uit te komen onder deze privacyschendende algemene voorwaarden.

Referenties

[1] *<http://www.google.com/support/plus/bin/answer.py?answer=1228271>.*

[2] *Zie bijvoorbeeld het relaas van Stilgherrian: 'Stilgherrian versus Google Round 2', verkrijgbaar via: < http://stilgherrian.com/only-one-name/stilgherrian-versus-google-round-2/>.*

[3] *Zie hierover Identitywoman in haar blog, 'Nymwars: IRL on Google's lawns', te lezen via: <http://www.identitywoman.net/nymwars-irl-on-googles-lawns>. Zie hierover ook danah boyd in haar blog, 'Desiging for social norms (or how not to create angry mobs)', te lezen via: <http://www.zephoria.org/thoughts/archives/2011/08/05/design-social-norms.html>.*

[4] *< http://stilgherrian.com/>.*

[5] *Zie bijvoorbeeld de blog van danah boyd, '"Real names" Policies are an Abuse of Power', verkrijgbaar via: < http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html>.*

ACHTER HET NIEUWS: BRING YOUR OWN DEVICE

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

Als we de voorspellingen voor 2012 mogen geloven zal Bring Your Own Device, of 'BYOD', de informatiebeveiligingsvloek van het jaar zijn. 'BYOD als engste acroniem voor beveiligers' of als 'mijnenveld voor informatiebeveiliging' zijn zomaar een paar beloftes die ons worden gedaan. Hoe denken onze redacteuren hierover? Welke spanningsvelden worden er onderkend en op welke wijze kunnen wij deze steeds verder oprukkende *consumerization* in goede banen leiden?

Maarten Hartsuijker

Mooie, snelle, handzame IT-apparatuur is in de privésfeer normaler geworden dan op het werk. Waar we e-mail privé al hebben ingeruild voor IM en de telefoon voor Skype, geeft onze baas ons nog steeds een telefoon waarop we smsjes in elkaar moeten puzzelen. Werken tussen 9 en 5 is voor veel medewerkers een uitje naar het openluchtmuseum geworden, waar de IT-afdeling nog eens rustig uitlegt hoe het vroeger was.
Dit houdt natuurlijk geen stand. Maar zomaar privéapparatuur aan het netwerk koppelen is om problemen vragen. Met de smartphones en tablets als *intelligence hub* voor de medewerker heeft het bedrijf veel te verliezen als de apparatuur (virtueel of fysiek) in verkeerde handen valt. We weten dat veel Android-apparatuur al geen beveiligingsupdates meer ontvangt zodra het de winkel verlaat. En dat *device encryption* niet altijd conform gangbare standaarden is. Tel daarbij op dat de meeste gebruikers genetisch niet in staat lijken een goed wachtwoord te kiezen, dan kunnen we stellen dat de waarschuwingen uit de introductie niet ver van de werkelijkheid zijn.
Tegelijkertijd is BYOD gewoon een gegeven. Het is óf gecontroleerd faciliteren, óf door je gebruikers worden gefaciliteerd. Goede oplossingen zijn er inmiddels genoeg, maar alleen goede bescherming van je netwerkgrenzen is met deze ontwikkeling natuurlijk niet meer voldoende. BYOD is wederom een goede herinnering dat we ons in onze beveiligingsoplossingen nog meer op de gegevens dienen te richten.

Lex Dunn

Ik heb net een eerste ervaring met BYOD achter de rug. Wat is het geval? Mijn werkgever heeft al jaren geleden besloten dat het weinig zinvol meer was om iedereen dezelfde (en qua mogelijkheden zeer beperkte) mobiele telefoon te geven. We hebben toen allemaal een SIMkaart gekregen, en een klein budget om zelf een mobiele telefoon te kopen. In de praktijk werkt dat prima, en is iedereen gelukkig. Geen onderhoud of support meer voor het bedrijf, en iedereen koopt het toestel wat hij of zij leuk vindt. Maar toen kregen we *'pushmail'*, de mogelijkheid om op die telefoon (of een tablet, of ander mobiel device) toegang te krijgen tot de email van het bedrijf. In eerste instantie leidde dat tot wat excessen in data-verbruik (navigeren met Google Maps vanuit Nederland naar Zuid-Frankrijk lijkt ideaal, maar consumeert wel gigantische hoeveelheden data). Een campagne om dit onder de aandacht van de medewerkers te brengen, en een maandelijks overzicht van hoeveel data je hebt verbruikt (inclusief alle andere kosten voor het mobiele gebruik), zorgde ervoor dat dit onder controle kwam. Eind vorig jaar besloot het bedrijf om een policy uit te rollen naar alle pushmailgebruikers om het gebruik van een pincode af te dwingen. Vanuit bedrijfsoogpunt een zinvolle maatregel om met name de vertrouwelijkheid van bedrijfsinformatie af te dwingen. Maar: drie keer foute pincode intikken zou leiden tot het 'wipen' van het device. En daar zit nou precies het pijnpunt: hoe ver mag je als bedrijf ingrijpen op privé-eigendom van een medewerker? Gezien de hoeveelheid tijd die het mij heeft gekost om mijn huidige smartphone zijn kunstjes te leren, vind ik het geen goed idee als mijn baas dat toestel gaat wissen als ik even niet goed oplet. Daarom heb ik besloten om geen pushmail meer te gebruiken. Ik ben benieuwd hoe deze discussie verder gaat. Binnen onze security gemeenschap heeft iedereen daar wel een mening over, en het wordt ook voorgelegd aan de OR. BYOD klinkt leuk, maar je moet er wel heel zorgvuldig over nadenken.

Lex Borger

BYOD wordt vaak gepositioneerd als een losstaand verschijnsel. Dat is niet het geval. Het is een element in de keten van ontwikkelingen die uiteindelijk de IT-infrastructuur van bedrijven heb-

ben veranderd en nog aan het veranderen zijn. Dertig jaar geleden was er infrastructureel geen bedrijfsnetwerk, hooguit een paar vaste verbindingen voor heel beperkte doeleinden. Als een medewerker een PC op zijn bureau had staan, was het niet opgenomen in een netwerk. Twintig jaar geleden was alles via een netwerk verbonden, maar dat waren eigen netwerken. Het internet bestond wel, maar bedrijven deden daar niets mee. Tien jaar geleden keken we terug op een 'dot-com bubble'. De wereld was veranderd, iedereen zit nu aan hetzelfde netwerk vast en gaat het geleidelijk aan voor alles gebruiken. Het gebruik van eigen apparatuur - eerst thuis en later mobiel - past gewoon in deze ontwikkeling. Net zoals laptops voor medewerkers, outsourcing, virtualisatie, software-as-a-service, het nieuwe werken.
Als beveiligers lopen we nog steeds achter deze feiten aan. We proberen het netwerk te beveiligen, maar het is uitgegroeid tot de Hydra van Lerna. Sla er een kop af en er groeien twee terug… We moeten echt onze strategie aanpassen en de data weer gaan beveiligen. En dan doel ik op die ongeveer 5% data die het speciaal beveiligen waard is. Deze willen we niet zo maar op het netwerk plaatsen, outsourcen, op afstand toegankelijk hebben of als een dienst aanbieden.
En laat de rest van de data meedraaien in de netwerkbeveiliging zoals we die nu kennen, inclusief BYOD. Zoals the Borg al zeiden: "Resistance is futile." BYOD zet wel door.

Andre Koot

In zijn werkzame leven was mijn schoonvader timmerman. En als timmerman wist hij het beste welk gereedschap hij voor zijn werk moest gebruiken. Bring Your Own Hammer was heel gewoon. Waar maken wij ons dus druk om? Ik weet zelf het beste wat ik kan gebruiken, toch? Sinds het eerste PC-privéproject heb ik zelfs betere hardware dan mijn werkgever. Ik heb thuis een sneller netwerk dan mijn werkgever en ik wil meer dingen tegelijk dan mijn werkgever nodig vindt. Wij zijn gewoon veel sneller dan al die organisaties.
Dat mag dan zo zijn, toch is de situatie met de timmerman natuurlijk niet helemaal vergelijkbaar. Dat zou wel zo zijn als wij onze devices uitsluitend voor onszelf zouden gebruiken, net als de hamer van mijn schoonvader. Maar een belangrijk verschil is dat de processen en gegevens van mijn baas worden beveiligd door onder meer te vertrouwen op de traditionele hulpmiddelen. Verschillende lagen van het beveiligingsmodel werden gerealiseerd door de devices. En met BYOD valt dat deels weg. Voor een aannemer maakt het niet uit welke hamer een timmerman gebruikt, als de timmerman zijn werk maar uitvoert. Met de nieuwe devices is dat anders. We moeten nieuwe beveiligingslagen bedenken.

Artikel van het Jaar 2011

Dit jaar is de vierde keer dat het PvIB een prijs uitlooft voor het artikel van het jaar. We hebben een vernieuwde jury die een flinke lijst van artikelen gaat beoordelen.

Er worden opnieuw drie prijzen uitgereikt. Dit geeft de jury de ruime gelegenheid om gepaste waardering uit te spreken. De eerste prijs heeft een waarde van vijfhonderd euro. Maar toch is de meest belangrijke reden om een prijs uit te reiken eigenlijk bedoeld voor onze auteurs. We waarderen al hun inzet en willen onze auteurs dan ook van harte bedanken voor de goede artikelen die ze ons bezorgen.
De jury is samengesteld uit een vertegenwoordiging van de onderwijswereld, de lezers en de auteurs. De redactie heeft dit jaar geen voorselectie gedaan. Alle artikelen die niet door een redactielid of een jurylid zijn geschreven, kunnen dus in aanmerking komen. De criteria die we de jury meegeven zijn ongewijzigd en van oplopend belang. De redactionele begeleiding die iedere auteur kan krijgen, helpt om de eerste drie criteria goed in te vullen. De laatste twee criteria doen echt een beroep op de creatieve inbreng van de auteur. We vragen de jury met name die creativiteit zwaar mee te laten wegen in hun beoordeling.
De uitreiking van de prijzen wordt opgenomen in het programma van de ledenvergadering en workshop op donderdag 26 april.

Beoordelingscriteria:

1. **Opzet artikel**
2. **Leesbaarheid**
3. **Benadering van de doelgroep**
4. **Vernieuwend gehalte**
   Heeft het artikel aspecten die getuigen van visie bij de auteur en/of nieuwe gezichtspunten op een onderwerp? In het Engels noemen we dit ' thinking out-of-the-box'.
5. **Zet het de doelgroep aan het denken?**
   Ook als de auteur verslag legt van een gezamenlijk denkgoed of misschien zelf rapporteert over unieke gedachten van anderen: in hoeverre slaagt hij of zij er in om de lezer aan het denken te zetten?

IMF
INTERNATIONAL MANAGEMENT FORUM

Certified Ethical Hacker

5-daagse training inclusief het internationale EC-Council examen

C|EH™ Certified Ethical Hacker

De Certified Ethical Hacker (CEH) training is de meest actuele en diepgaande security training in zijn soort en is platform- en productonafhankelijk.

Na deze training weet u hoe kwaadwillende hackers, sniffers en phishers proberen in te breken in uw organisatie. Door hun wapens te leren gebruiken, wordt uw verdedigingsstrategie intelligenter.

EC-Council

De opleiding wordt afgesloten met het officiële CEH examen van EC-Council. Het CEH certificaat staat internationaal bekend als een waardevolle aanvulling op Microsoft, Cisco of Linux certificaten.

SABSA® Foundation

SABSA

Deze 5-daagse training leidt op voor het SABSA Foundation certificaat

SABSA heeft zich ontwikkeld tot een 'best practice' methode voor het verkrijgen van informatiebeveiligingsoplossingen binnen een organisatie en wordt wereldwijd gebruikt door zowel bedrijven als overheden.

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

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 (hoofdredactie, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.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
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

Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie (CC BY-SA 3.0).

creative commons

ISSN 1569-1063

LEVER DE BOEL MAAR IN

Trouwe lezers van mijn columns weten dat mijn columns vaak geschreven worden op basis van mijn opwinding over iets wat voorvalt. Deze opwinding kan zowel een positieve invloed hebben op mijn humeur maar helaas is het ook weleens zo dat deze opwinding nogal negatief uitwerkt op mijn humeur. Deze maand ga ik iets schrijven in de categorie 2.
Voordat ik met het daadwerkelijke onderwerp begin zal ik u even meenemen naar de tijd dat ADSL of kabel niet bestond en dat als je met je computer naar 'buiten' wilde, je dan een rochelend en piepend apparaat nodig had die connecties kon maken naar buiten. Van de bulletinboards kon je een plaatje, foto, ombouwschema voor je homecomputer of een klein leuk programmaatje voor je Atari of andere spelcomputer downloaden. Behalve de bulletinboards schuimde je ook het openbare telefoonnet af om met behulp van war-dialing eens te kijken of je een modem kon bereiken die toevallig openstond. Op de bulletinboards stond vaak wel een lijstje met allerlei bedrijven en modems. Leuk en onschuldig zat je dan een paar uur te neuzen op het bedrijfsnetwerk van je slachtoffer totdat je vrouw je tot de orde riep omdat ze met haar vriendin wilde bellen. De combinatie van bellen en internetten was toen een onmogelijke en zo werd je dan door je huisgenoten gecorrigeerd.
Inmiddels zijn de tijden veranderd, compressietechnieken hebben een enorme groei doorgemaakt en het aanbod van muziek is grenzeloos. Muziek was de eerste content die illegaal te downloaden was - sorry, ik vergeet de porno die als eerste in de elektronische schappen lag. De muziekindustrie heeft daardoor een immense verandering doorgemaakt en het einde is nog niet in zicht. Daarna volgde de filmindustrie en inmiddels is iedere dvd of tv-serie ook wel te vinden op internet. Met mijn huidige modem die aan een snelle ADSL-verbinding is gekoppeld zou ik (met nadruk op zou) een dvd binnen een uur binnentrekken. De boekenindustrie is nu volop het middelpunt en de sombere berichten over Selexyz zou daarmee te maken kunnen hebben. Daar wind ik mij in mindere mate over op, al realiseer ik me wel dat artiesten of auteurs met deze ontwikkeling ernstig tekort worden gedaan.
Nee, mijn ergernis zit hem in de maatregelen die Justitie en de overheid wil gaan nemen om dit fenomeen tegen te gaan. De rechter heeft bepaald dat Ziggo en XS4all Pirate Bay moeten gaan blokkeren. Deze maatregel lijkt in landen als China wel te werken, maar in Nederland is deze maatregel waanzinnig.
Zonder al te technisch te willen worden, noem ik een aantal wijzen waarop dit verbod zonder enig probleem te omzeilen is. Het is kinderspel om jouw machine een IP-adres uit het buitenland te geven en daardoor onder dit verbod uit te komen. Een schaduw-database is in een aantal uurtjes opgezet en die noemen we geen Pirate Bay maar gewoon kopie 1167. Nog eenvoudiger is het om een zogenaamde API te ontwikkelen die voor jou de nodige relevante informatie weghaalt (met dank aan publicaties van Webwereld.nl).
Het probleem zit hem niet in Pirate Bay; de content staat immers overal. Pirate Bay is slechts één van de vele aanbieders. Gestolen content is overal te vinden en overal te downloaden. Het verbod op Pirate Bay is niet eens een druppel op de gloeiende plaat. Elektronische bestanden zijn niet meer weg te krijgen, ze zullen overal en nergens weer opduiken. Hetzij door een gebruiker die het weer ergens neerzet, dan wel een back-up die wordt teruggezet. Gelukkig denkt de 2e kamer nu ook in actie en Fred Teeven had in eerste instantie ook de meest wilde gedachten over hoe we het te verfoeien downloaden zouden kunnen stoppen. Inmiddels is de heer Teeven iets rustiger en krabt zich nu ook op het achterhoofd. De BUMA/Stemra maakt zich ook enorm druk over de downloadpraktijken, maar ondertussen wordt vanuit het gebouw van deze organisatie ook vrolijk gedownload.
Gelukkig ben ik een nuchtere en weldenkende Noorderling die natuurlijk altijd zijn oplossingen klaar heeft: ik stel voor de tijd een tijdje terug te draaien. We gaan ADSL en de kabel verbieden! Om volledig te zijn zullen de telecombedrijven ook mee moeten doen om hun dataverbindingen af te sluiten (scheelt direct weer een discussie dat het dataverkeer helemaal uit de hand loopt). En de satellietmodems zullen helaas ook ingeleverd moeten worden. Dat is de eenvoudige kant van mijn oplossing. Een iets lastiger probleem is dat iedereen die zijn verbinding inlevert, wel koper moet krijgen om zijn lage snelheidsmodem weer aan te kunnen koppelen en om via het vaste net te kunnen telefoneren (ik heb overigens nog drie bijna niet gebruikte exemplaren in de aanbieding).
Lijkt mij allemaal meer haalbaar dan de oplossingen van de Nederlandse rechter en de vermoedelijke oplossingen van de heer Teeven.

Groetjes, Berry

Discover the best thing since the introduction of FTP!

BEFINE cryptshare®

BEFINE cryptshare® For Microsoft Outlook 2010

BEFINE cryptshare® For Lotus Notes

- Easily send large files up to 2GB
- Confirmation of file download
- Simple and secure file transfer

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Cryptshare. Neem contact op via sales@crypsys.nl of via 0183 62 44 44 voor een gratis evaluatie.

CRYPSYS data security