INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 1 - 2011

BEVEILIGD MAAR WERKBAAR

ISF 2010: 21ST ANNUAL WORLD CONGRESS 2010

CLOUD SECURITY IN VOGELVLUCHT

DE MELDPLICHT DATALEKKEN: ZORG OF ZEGEN?

TRENDS IN IT-BEVEILIGING 2011

FOX-IT

... for a more secure society

Fighting cybercrime

Protecting secrets

Finding digital traces

Innovating internet interception

FOX-IT

Fox-IT is een IT Security bedrijf met het hoofdkantoor in Nederland en nevenvestigingen in Engeland en op de Caribbean. Het levert wereldwijd bijzondere security- en intelligence-oplossingen voor overheden, financiële instellingen, vitale infrastructuur en maatschappelijk belangrijke organisaties. De kernactiviteiten zijn het ontwikkelen van oplossingen voor het beschermen van geheimen, het uitvoeren van digitale rechercheonderzoeken, het bestrijden van cybercrime en het maken van analyseproducten voor opsporingsdiensten.

Cybercrime Symposium 8 februari 2011

Criminaliteit en het Internet zijn met elkaar verweven. Criminelen verleggen steeds meer hun werkterrein naar de digitale snelweg. Tijdens dit symposium werpen we een blik in de toekomst en laten we zien op welke manier cybercrime zich ontwikkelt. Aan de hand van technische tracks, demo opstellingen en algemene tracks leert u op een effectieve manier de gevaren kennen en hoe u zich er tegen kunt wapenen. Het cybercrime symposium is een echte eyeopener!

Wilt u meer informatie of deelnemen aan dit symposium? stuur dan een e-mail naar marketing@fox-it.com of kijk op www.fox-it.com

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

INHOUDSOPGAVE

VOORWOORD

Dat is vast even schrikken, deze uitgave van Informatiebeveiliging! We hebben vorig jaar natuurlijk al wel gewaarschuwd, maar als zo'n blad dan ook echt in de brievenbus ligt, dan is het ook echt weer een ander blad en een andere ervaring. Als redactie zijn we al heel tevreden over dit resultaat en we hopen dat u dat met ons eens bent. Andere uitstraling, andere lettertypes, andere vormgeving.

Zoals u in het vorige nummer al hebt kunnen lezen, willen we graag rekening houden met de wensen van onze lezersgroep. Maar ja, u bent best tevreden. We zullen dan ook de kwaliteit van de artikelen handhaven. Gelukkig zijn er wel een paar tips en die nemen we ter harte. Omdat we dit nummer helemaal nieuw moesten vormgeven, is de aanloop wat langer dan gebruikelijk. Hoewel we in de regel actueel proberen te zijn, kunnen we nu helaas geen aandacht schenken aan de reacties op het interview met Neelie Kroes dat in het afgelopen kerstnummer verscheen. Wat velen van u ook al hebben kunnen merken is dat we Twitter als communicatiemiddel meer en meer gaan inzetten. Inmiddels volgen meer dan 120 PvIB-leden het Twitter account @pvib en zien we ook af en toe een retweet van een bericht. Op die manier kunnen we heel actueel informatie verstrekken over activiteiten. Als u een volger bent, doe dan gerust actief mee en reageer.

Dit jaar hebben we wel weer heel wat plannen. Zo gaan we aandacht schenken aan Informatiebeveiliging in het onderwijsveld. Dat zal een serie artikelen van universiteiten en hogescholen opleveren over onderzoek en ontwikkeling en we willen een special uitbrengen over deze branche. Ook plannen we weer een privacyspecial. De reacties op de vorige specials waren positief en we merken dat er (ook buiten het PvIB) heel veel behoefte is aan kennis en informatie omtrent dit onderwerp. Ook schenken we aandacht aan Cloud Security. Daarbij gaan we een samenwerkingsverband aan met de Cloud Security Association. We hopen dat we een hele serie kunnen maken.
In dit nummer maken we ook een begin met een serie artikelen gerelateerd aan OWASP. Als u daar nog niets van af weet, geen probleem. Als we een jaar verder zijn bent u aardig op de hoogte.

Hoe dan ook, plannen genoeg. Nu alleen nog de artikelen...

Dit nummer tekent ook een soort einde. Met ingang van het volgende nummer zullen Lex Borger en ik van rol wisselen. Lex zal de rol als hoofdredacteur gaan vervullen en ik blijf redacteur. De redactie heeft eenstemmig besloten om Lex het vertrouwen te schenken. Ik ben zelf ook blij met deze verandering en ik wens Lex heel veel succes en plezier toe!

Namens de redactieleden wens ik jullie allemaal een veilig 2011 en heel veel leesplezier,

André Koot
hoofdredacteur

Foto omslag: Lasse Kristensen

BEVEILIGD MAAR WERKBAAR

VALKUILEN BIJ HET REALISEREN VAN VEILIGE APPLICATIES

Drs. ing. Roland Roos is oprichter en eigenaar van RICTA.
Hij is te bereiken via: roos.ict.architectures@gmail.com
Drs. Michiel Perdeck CISSP is enterprise architect en security expert bij Logica.
Hij is te bereiken via michiel.perdeck@logica.com

Voor ons contact met bedrijven, organisaties, collega's en zelfs vrienden zijn we tegenwoordig sterk afhankelijk van webapplicaties op het internet. Vluchten kan niet meer... De infrastructuur die wordt gevormd door wereldwijd met elkaar verbonden computers levert ons veel mogelijkheden op. Maar tegelijk is het juist daardoor een ideaal platform voor allerhande ongewenste en schadelijke activiteiten, van het plunderen van bankrekeningen tot het onbereikbaar maken van diensten. Webapplicaties zijn de poorten tot deze infrastructuur en vormen daardoor de frontlinie bij de aanval door indringers. Het is dus belangrijk om deze poorten sterk te beschermen door veilige applicaties te maken en deze veilig te leren gebruiken. Helaas worden applicaties nog lang niet altijd veilig ontwikkeld. Dat moet snel veranderen omdat de risico's in deze globale economie steeds groter worden.

Een veilige applicatie is een applicatie die zo is gebouwd en in productie genomen dat hij de risico's bij het gebruik, binnen de gestelde eisen aan kosten en bruikbaarheid, zo klein mogelijk maakt. We richten ons in dit artikel op webapplicaties, dus applicaties die via een browser aan gebruikers beschikbaar worden gesteld. Dat kunnen zowel applicaties op het publieke internet zijn als op een lokaal intranet. Om applicaties zo te realiseren dat ze zo min mogelijk risico's opleveren bij het gebruik, moet rekening worden gehouden met de hele levenscyclus in een organisatie, van ontwerp en bouw tot en met gebruik en zelfs uitfasering. Daarbij is sprake van een aantal valkuilen waar men voor moet oppassen. We zullen dat illustreren aan de hand van een herkenbaar voorbeeld namelijk, het maken van een 'veilige' auto. Mutatis mutandis gelden dezelfde overwegingen en maatregelen ook voor software. We zullen dat na het voorbeeld van de auto laten zien met behulp van een model voor de Secure Development Lifecycle (SDL), het Software Assurance Maturity Model (SAMM), ontwikkeld door het Open Web Application Security Project (OWASP).

Veiligheid in alle fasen van de lifecycle

Je kan met een veilige auto nog steeds ongelukken maken maar de kans daarop is wel kleiner. En als het gebeurt ligt dat aan de chauffeur en niet aan de fabrikant. Je wilt als producent van een auto niet aansprakelijk worden gesteld voor schade veroorzaakt door jouw product. De uitdaging voor alle betrokkenen bij de ontwikkeling is om de maatregelen te treffen die het product en de fabricage zo veilig mogelijk maken, binnen bepaalde grenzen van kosten en bruikbaarheid. Dit geldt voor de hele keten van ontwerp tot het einde van het gebruik. Risico's en bedreigingen dienen hierbij voortdurend te worden afgewogen tegen alle andere eisen en wensen maar een onveilige auto wordt op de hedendaagse markt niet meer geaccepteerd.

> Wie heeft niet een veiligheidsmaatregel meegemaakt die zo onhandig was dat je die weer snel uitzet?

Gebruik en opleidingen

Men moet een rijbewijs hebben en niet te hard rijden. Dat is het veilig gebruiken van de auto. Het gaat dan om bewustwording en instructie. Kortom, gedrag van de gebruikers. Hiervoor is opleiding nodig: rijlessen.
Niet alleen de eindgebruiker moet worden geschoold in veiligheid. Op elk niveau dient men voortdurend opgeleid en bijgeschoold te worden. Ook managers, verkopers, lopende bandmedewerkers, testers, documentalisten, gebruikers en garages moeten weten hoe ze met veiligheidsaspecten en risico's moeten omgaan. Een mailcampagne onder de medewerkers of e-learning is een goede start, maar zeker niet

genoeg om onder aansprakelijkheidsclaims uit te komen.

Eisen en wensen

De markt wenst of eist misschien bepaalde maatregelen, zoals brake-assist, omdat dat de nieuwe trend is. En die kunnen best botsen met andere eisen en wensen, zoals bruikbaarheid, levensduur of gewichtsklasse van de auto. Eisen moeten dus worden geprioriteerd. Kortom, alle belanghebbenden moeten nadenken over de veiligheidseisen.

De maatregelen moeten niet alleen effectief maar ook functioneel en bruikbaar zijn. Wie heeft niet een veiligheidsmaatregel meegemaakt die zo onhandig was dat je die weer snel uitzet? Als dat al kan. Vaak zijn dergelijke maatregelen helemaal niet uit te zetten of aan te passen.

Een voorbeeld. Dat mooie geïntegreerde navigatiesysteem op mijn nieuwe auto is zo gemaakt, dat ik het alleen mag bedienen als de auto stilstaat. Dat lijkt op het eerste gezicht een prima maatregel, totdat je met het gezin op vakantie bent en je bijrijder netjes de route wil invullen terwijl jij rijdt… Niet goed doordachte veiligheidsmaatregelen, die de gebruiker belemmeren, zullen averechts werken doordat de gebruiker omwegen gaat bedenken. Hij gaat in dit voorbeeld misschien zijn iPhone gebruiken als navigatiesysteem en gaat onder het rijden zijn passagier uitleggen hoe dat werkt...

We kennen allemaal wel situaties in de informatietechnologie waar veiligheidsmaatregelen zo belemmerend zijn geïmplementeerd dat gebruikers heel onveilige omwegen gaan bewandelen. Om dit te voorkomen hanteren we het bij dit autovoorbeeld goed passende acroniem BMW dat staat voor 'Beveiligd Maar Werkbaar'.

Hoe meer veiligheidsopties, hoe meer er ook iets mis kan gaan

Ontwerp

Het is een open deur dat de auto veilige remmen moet hebben, een veilige stuurinrichting en ophanging, kortom een veilig ontwerp. Het is mooi als je heel veilige sloten hebt, maar als je het ruitje zo naar beneden kan drukken, is de inbreker toch snel binnen. Het gaat niet om geïsoleerde maatregelen maar om hun effect in samenhang. Je moet in je ontwerp gebruikmaken van veilige constructiepatronen. Het over het hoofd zien van samenhang is een gemakkelijk gemaakte fout.

Alleen veilig ontwerpen is niet genoeg. De auto moet ook veilig in elkaar worden gezet. Een goed ontwerp is een ding. Alle boutjes en moertjes goed aandraaien is ook nodig, zodat je niet plotseling het stuur aan de bijrijder kan geven…

We verzekeren ons ervan dat de bouw naar behoren plaatsvindt door een goede opleiding van de constructeurs en door te testen en te inspecteren. Natuurlijk wordt er niet bezuinigd op opleiding en testen…

Veiligheidsextra's

Een auto kan ook veiliger worden met een aantal extra's (tegenwoordig trouwens vaak standaard) als ABS, airbags, alarmsystemen, enz.

Ook deze moeten veilig worden ontworpen, geïmplementeerd en getest. Een ontploffende airbag als je eens hard remt is niet leuk maar als je crasht, wil je wel graag dat hij werkt. Kortom, hoe meer (complexe) veiligheidsopties, hoe meer er daarmee mis kan gaan.

We spreken in dit verband van false positives (het veiligheidssysteem denkt onterecht dat er een noodsituatie is) en van false negatives (het veiligheidsysteem denkt onterecht dat er niets aan de hand is). Het is de kunst van een goede ontwerper om de kans op false positives en vooral die op false negatives zo klein mogelijk te maken. Complexiteit is een gevaarlijke valkuil.

Betaalbaar

De maatregelen moeten ook betaalbaar zijn. Een gezinsauto van 20.000 euro met 150.000 euro aan veiligheidsopties is wel heel veilig maar niet verkoopbaar. Opties die bedoeld zijn voor ruimteschepen kunnen technisch fantastisch zijn, maar of ze echt bijdragen aan de veiligheid van een auto is maar de vraag. Kosten en baten dienen te worden afgewogen voor alle te implementeren maatregelen. Té is nooit goed, zelfs té veilig niet…

Foto: Rainer Plendl

Niet alleen het gebruik moet veilig zijn, de auto moet ook veilig in elkaar worden gezet.

Risico- en bedreigingsanalyses
Welke risico's en bedreigingen zijn er eigenlijk? En hoe groot zijn die voor alle belanghebbenden in de levenscyclus van de auto? Voor de autoproducent, voor de bouwer, voor de gebruiker en voor de garage?
Als je niet in kaart hebt welke bedreigingen er zijn met hun gevolgen voor alle belanghebbenden, hoe kan je dan inschatten of je er wat aan zou moeten doen? En wat dan? Hoe vaak komt het eigenlijk voor dat een auto over de kop slaat? Wat zijn daar dan de voornaamste oorzaken van? Een lekke band, gladheid, te hard remmen, te hard rijden? En welke ongelukken treden op tijdens de bouw? Auto's die van de lopende band vallen, of in brand vliegen? Zware onderdelen waardoor mensen fysieke klachten oplopen tijdens de montage? Een ongeluk zit in een klein hoekje en je zult de hele cyclus goed moeten doordenken. Een veilige auto kopen en gebruiken is belangrijk, maar de garage moet hem ook veilig kunnen onderhouden.

Verificatie, testen en procedures
Verificatie speelt een cruciale rol bij het maken van veilige auto's. Deskundigen inspecteren het ontwerp van de auto, er worden NASH CAP-crashtesten uitgevoerd op productie- en prototype modellen. Steekproefsgewijs worden auto's die van de band rollen getest en wellicht moeten sommige eigenschappen zelfs op alle auto's worden getest. Tot slot doen de eindgebruikers een 'roadtest' op circuits en in de echte praktijk. Is alles in het echt ook bruikbaar, veilig en robuust?

Het testen vindt plaats in alle fasen van het productieproces
Wat gebeurt er als er ergens tijdens alle verificatieprocessen bij het maken van een auto veiligheidsmankementen worden geconstateerd? Hoe gaat het bedrijf daarmee om? Worden deze wel goed gedocumenteerd, zodat later is aan te tonen dat er echt naar is gekeken? Worden alle medewerkers in het bedrijf op de hoogte gesteld en eventueel bijgeschoold om herhaling te voorkomen? Niet voor niets bestaan er normen als ISO9000 en methoden als Lean SixSigma die erop zijn gericht het hele productie- en onderhoudsproces aantoonbaar efficiënt en herhaalbaar te kunnen uitvoeren.

Van veilige auto's naar veilige applicaties
Alles wat voor een auto geldt, is in grote lijnen ook van toepassing op het ontwerpen, maken, in productie

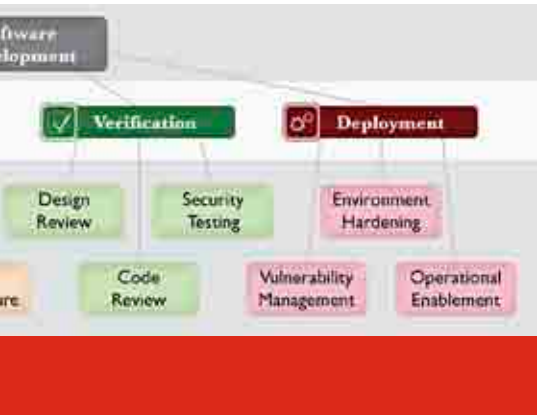
Fig. 1. Overzicht van het Software Assurance Maturity Model (SAMM).

nemen, beheren en gebruiken van applicaties. Het software analogon van een geproduceerde en door de garage gebruiksklaar gemaakte auto is een in z'n productieomgeving geïnstalleerde applicatie. In het geval van softwareontwikkeling is het veilig maken in principe niet anders maar er zijn natuurlijk wel verschillen tussen auto's en softwareapplicaties. Ook is de status quo bij applicatieontwikkeling nog niet zo ver als in de autoindustrie. Een risicoanalyse van de hele gebruiks- en onderhoudscyclus wordt bijvoorbeeld te vaak niet uitgevoerd.
Zoals hierboven bleek, zijn de verschillende fasen in de levenscyclus van een applicatie te herkennen in die van een auto. Dit geldt ook voor de verschillende activiteiten gedefinieerd in het Software Assurance Maturity Model (SAMM).

Software Assurance Maturity Model (SAMM)
Het veilig uitgevoerde traject van Requirements tot Deployment noemt men een Secure Development Lifecycle (SDL of SDLC). In een SDL wordt een aantal activiteiten uitgevoerd die allemaal veilig moeten gebeuren. Een model dat kan helpen bij het inrichten van zo'n veilige cyclus is het door de Open Web Application Security Project (OWASP) gepubliceerde Software Assurance Maturity Model (SAMM of OpenSAMM). Het helpt organisaties op alle vlakken bij het veilig maken en houden van applicaties door het beschrijven van twaalf 'practices' (activiteiten) die de bouwstenen vormen van een SDL. In fig. 1 zijn deze twaalf 'practices'


Foto: Dmitry Vereshchagin

De airbag is nu een standaard veiligheidsmaatregel.



weergegeven. Voor elk van de twaalf activiteiten zijn drie volwassenheidsniveaus beschreven. Op die manier krijgt een organisatie handvatten voor een geleidelijke verbetering van het proces van veilige systeemontwikkeling. Als voorbeeld nemen we de activiteit 'Security Requirements'. De drie in SAMM gedefinieerde volwassenheidsniveaus zijn hier:

1. houd expliciet rekening met veiligheidsaspecten tijdens het opstellen van de eisen;
2. bepaal de beveiligingseisen op basis van applicatiespecifieke risico's en misbruikscenario's;
3. verplicht tot het opstellen van beveiligingseisen voor alle software projecten en afhankelijkheden.

Net als bij andere volwassenheidsmodellen zal het volwassenheidsniveau niet hetzelfde behoeven te zijn voor elk van de twaalf activiteiten. Het SAMM helpt bij het identificeren van de te nemen stappen op dezelfde manier als het CMMi dat doet voor softwareontwikkeling in het algemeen.

De toepassing van SAMM in de Software Development Lifecycle

Fig. 2 laat zien hoe de SAMM security practices passen in de ontwikkelfasen van een softwaresysteem. De ontwikkelstadia zijn weergegeven als taartpunten in een cirkel om tot uitdrukking te brengen dat er veelal sprake is van een incrementeel verloop waarin telkens nieuwe elementen aan het systeem worden toegevoegd die elk weer door de verschillende ontwikkelfasen gaan. Dit idee is afkomstig van een van de grote theoretici van de Software Engineering, Barry Boehm. De SAMM practices zijn in de praktijk minder statisch aan een bepaalde fase gebonden dan de figuur suggereert.

Intranet en internet

In principe hoort er geen enkel verschil te zijn in de beveiliging van de applicatie of hij nu wordt gebruikt op internet of intranet. Een internetapplicatie is per definitie en bij ontwerp ontsloten aan een breder publiek. Dat betekent dat er mogelijk andere bedreigingen zijn en er in de infrastructuur extra maatregelen zijn getroffen om een beperkte toegang te regelen. De intranetapplicatie dient verder net zo veilig te zijn als de internetapplicatie. Waarom? Dat is eenvoudig. Vertrouw niet volledig op de beveiliging in het netwerk maar neem aan dat een vijand door de linies heen kan breken, of erger nog, al binnen is bij het bedrijf. Bovendien weet je nooit van tevoren of intranetapplicaties ooit internetapplicaties worden.

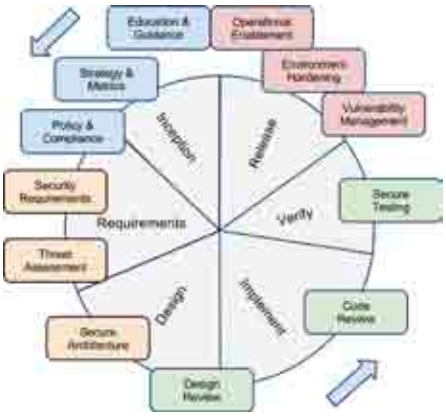


Fig. 2. De SAMM practices in de Software Development Life Cycle.

Conclusie

Net als onveilige auto's hebben onveilige applicaties in de nabije toekomst geen levensvatbaarheid meer. Onveilige bedrijven ook niet. Alleen als alle betrokkenen in de totale levenscyclus van een applicatie expliciet met alle veiligheidsaspecten bezig zijn, krijg je veilige applicaties door iedereen en voor iedereen. Je moet mensen altijd veilig laten werken, het moet een tweede natuur worden. Een garage is wat dat betreft een goede vergelijking, daar zijn het ARBO-regels en het directe risico op lichamelijk letsel die er voor hebben gezorgd dat veilig werken in alle garages de norm is.

Bij software is de afstand tussen oorzaak en gevolg iets groter. Dat een applicatie onveilig is merk je misschien pas na een hele tijd, of erger, helemaal niet! Dat maakt het onderwerp applicatieveiligheid lastiger te implementeren in de bedrijfscultuur. Een volwassenheidsmodel als het SAMM kan echter goed helpen om dit te bereiken. Je zou het SAMM kunnen zien als een aanvulling op het CMMi maar is ook heel goed los daarvan te implementeren. Vergeleken met het CMMi is het SAMM veel eenvoudiger en daardoor laagdrempeliger. Ondanks dit, vereist het invoeren van een dergelijke verandering van werkwijze wel een aantal ervaren mensen in alle disciplines om het proces te begeleiden en de organisatie te behoeden voor de genoemde valkuilen. Eerst moet het waarom in de organisatie van onder tot boven zijn doorgedrongen, voordat het zin heeft de SDL met SAMM te gaan implementeren.

Met een knipoog naar Anthoine de Saint Exupéry zouden we kunnen zeggen: *"Als je boten gaat bouwen, moet je niet alleen starten met het aanslepen van hout. Leer vooral mensen te verlangen naar veilig varen op de eindeloze zee."*

Links

OWASP: www.owasp.org

OWASP SAMM pagina: www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

SAMM: www.opensamm.org

CMMi: http://www.sei.cmu.edu/cmmi/

Barry Boehm: A spiral model of software development and enhancement - ACM SIGSOFT Software Engineering Notes, Volume 11 Issue 4, August 1986

INFORMATIEBEVEILIGING – PEOPLEWARE (1)

Hans Labruyere is directeur en mede-eigenaar van LBVD informatiebeveiligers.
Hij is te bereiken via hans.labruyere@lbvd.nl

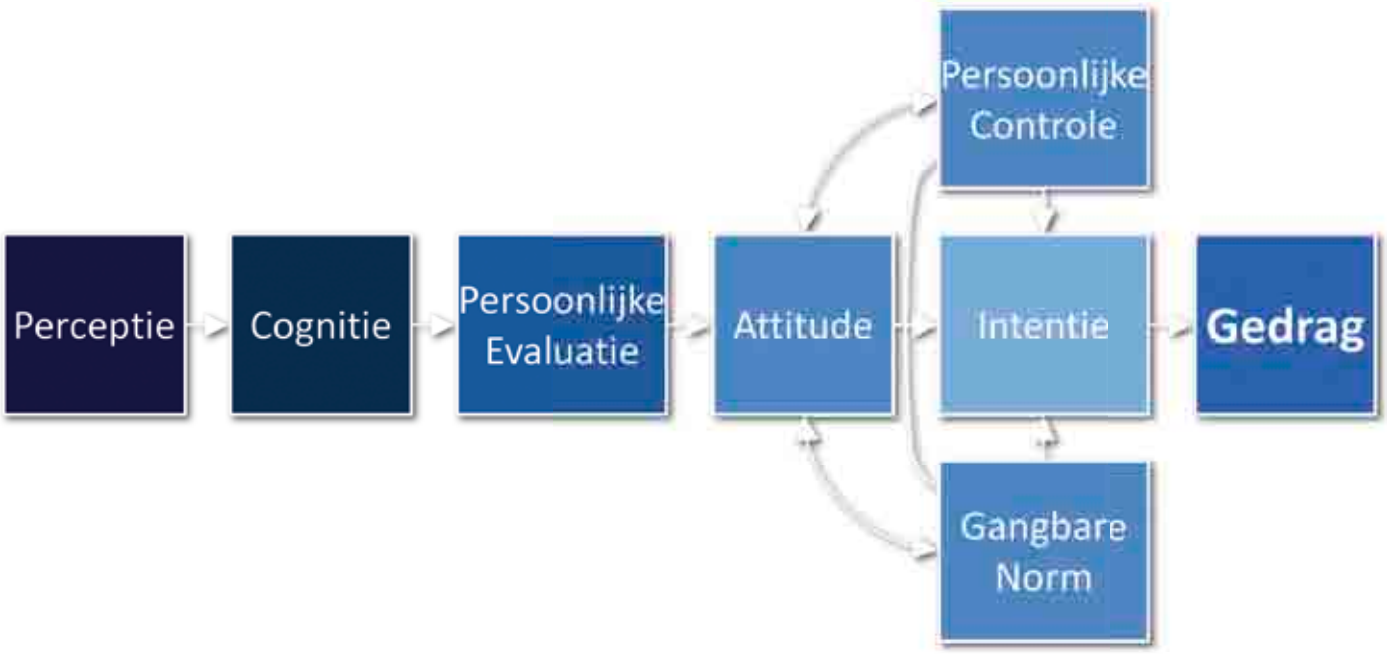
In een serie van drie artikelen over informatiebeveiliging en het bewustzijn en onbewustheid van de mens in deze, zet de schrijver een keten methoden uiteen die elkaar in de praktijk kunnen versterken. De keten bestaat globaal gezien uit analyseren, informeren, kanaliseren en toetsen. In dit eerste deel wordt ingegaan op de analyse van de (on)bewustheid.

Informatiebeveiliging. Een breed en lastig onderwerp. Veel organisaties 'hebben al wat', er is technisch een boel gedaan en er zijn allerhande protocollen, regels en convenanten. Toch lukt het maar niet de medewerkers het gewenste gedrag te laten vertonen.

Enerzijds heeft dat met cultuur te maken, of dat nu bedrijfscultuur of cultuur op regionaal of nationaal niveau is. Anderzijds is voornoemde onmacht veelal voornamelijk het gevolg van het feit dat mensen zich gewoon niet bewust zijn. Voorbeeld? Op welke verdieping bevindt u zich nu? Hoeveel verdiepingen zijn er nog boven u? Wel eens nagedacht over de kans dat het plafond waaronder u nu zit straks gelijk zou kunnen zijn aan de vloer waarop u staat? En wat dat voor uw welzijn betekent? Nee? Dat dacht ik al. Toch is het niet ondenkbaar. In Keulen gebeurde vorig jaar maart iets dergelijks. "Maar daar waren ze een tunnel aan het boren", hoor ik u denken. Tjah. Maar dat wisten ze daar ook niet... Het risico werd niet kleiner (of groter) doordat men het risico niet zag.
Een medewerker die onbewust onbekwaam is, is derhalve een lastige gesprekspartner. Hij hoort je wel, maar luistert niet. Omdat hij denkt al de juiste kant op te gaan. Een deel van de oplossing om te komen tot een meer volwassen organisatie inzake informatiebeveiliging is het migreren van (de medewerkers van) die organisatie van onbewust onbekwaam naar bewust onbekwaam.

> Het lukt maar niet de medewerkers het gewenste gedrag te laten vertonen

Onderstaand model is afkomstig uit de sociaal psychologie. Je 'leest' het van rechts naar links:



Model: beïnvloeding van gedrag volgens de sociaal psychologie.

1. Gedrag

Wat je wilt is uitvoering van het juiste gedrag. Als je op een sportveld staat en het begint te bliksemen, dan blijf je daar niet staan. Ongeacht het feit dat je 's morgens opstond en niet direct dacht: "Goh, als het vanmiddag gaat bliksemen ga ik niet op een sportveld staan".

Hoe werkt dat nou eigenlijk? Als het gaat bliksemen trek je in je onderbewustzijn een 'laatje open'. In dat laatje zitten allerhande zaken die je in je leven hebt verzameld. Goede raad van je oma, artikelen uit de krant, ervaringen etc. In een split second neem je je beslissing bijna zonder het te weten, en je gaat van het veld af. En by the way, je gaat ook niet onder een boom staan.

In dit voorbeeld is uitgegaan van het feit dat er inhoud in dat laatje zit. Informatiebeveiligings-incidenten gebeuren wel, maar wie kan ze herkennen? Wie heeft dit soort info in haar of zijn laatje? Hoe kunnen we als professionals dan het juiste gedrag verwachten bij de medewerkers...?

Het gedrag wordt echter sterk beïnvloed door:

2. Intentie

Ofwel, wil ik, of wil ik niet. Vijftig procent van het antwoord is 'ik wil niet'. Maar tegen die tijd is het dan ook een bewust genomen beslissing, al kan niet iedereen alle implicaties altijd overzien. Dit onderdeel wordt beïnvloed door:

3. Attitude

Die mede wordt bepaald door externe factoren als persoonlijke controle en de gangbare norm. Persoonlijke controle is te omschrijven als 'waar heeft je wieg gestaan?' Welke ervaringen heb je van thuis meegekregen? De gangbare norm kan per afdeling, per regio, per bedrijfsproces heel anders zijn. Voor iemand van de receptiebalie heeft een willekeurige bezoeker een heel ander veiligheidsprofiel dan voor iemand van de tweede verdieping. Voor die medewerker is dit 'gewoon een bezoeker'. Hij is immers voorbij de receptie? Dan zal hij hier wel horen...

Voor iemand van de afdeling ICT is de procedure rondom wachtwoorden logisch en vanzelfsprekend. Personeelsdossiers kun je bij deze afdeling echter nog wel eens op het bureel van de IT-manager vinden. Die periodieke beoordeling moet per slot toch gedaan worden? Voor medewerkers van HR zijn personeelsdossiers op een bureau (waar je niet direct mee bezig bent) ondenkbaar. Wachtwoordprocedures echter zijn in de praktijk soms zo onwerkbaar, dat de afdelingsecretaresse in de vakantieperiode de username-passwords van de collegae verzameld. 'Het is zo lastig als er iemand niet is...'

Een verschillende kijk dus, op veiligheid, dreiging, realiteit. Niet per se onjuist, maar niet compleet. En die attitude wordt op haar beurt beïnvloed door:

> Als je op een sportveld staat en het begint te bliksemen, dan blijf je daar niet staan

4. Persoonlijke ervaring

Heb je in het verleden iets geleerd? Iets meegemaakt, in de krant gelezen, gehoord of bediscussieerd misschien? Kortom, een eigen interpretatie gemaakt van het dreigingprofiel voor jou persoonlijk? Want dat is mede een oplossing voor het sturen van (groepen) mensen. Elk individu laten inzien wat hij er zelf beter van wordt. Of minder slecht van wordt. What's in it for me? Maar die ervaring moet je dan ook wel hebben gehad, en ze wordt onder andere opgedaan door:

5. Cognitie

Je leert iets. Door een ervaring, een situatie, een opleiding, breder inzicht. Die cognitie echter wordt beïnvloed door:

6. Perceptie

Zie je het überhaupt? Een moedernijlpaard gaat door voor het meest dodelijke dier op aarde (ze heeft geen natuurlijke vijanden, weegt een paar ton en kan heel hard lopen). Toch heeft zo'n dier een hoge knuffelfactor, en niet iedereen die niet in Afrika is geweest kent deze dreiging. Maar hij is er wel. Een rotje is potentieel gevaarlijk. Toch onderkent niet iedere jongere rond oud en nieuw die dreiging. Maar hij is er wel.

Uit het model kan onder andere worden opgemaakt dat een individu (of een afdeling, of een proces) niet van het blok Perceptie direct naar het blok Gedrag kan worden gebracht. Men moet als individuele medewerker eerst weten (en beseffen) wat de dreiging omvat, waarom dat voor de individu persoonlijk een dreiging kan zijn, hoe te reageren en welke middelen daarvoor nodig zijn. Pas dan wordt besloten óf de gewenste actie (zoals die in de regels staat) wordt aangegaan. En het antwoord kan ook zijn: "Nou neen, nu even niet".

Dat geldt voor de werkvloer, maar natuurlijk ook en onverminderd voor de directiekamer. Ook daar kan men Onbewust Onbekwaam zijn - met verstrekkende gevolgen... Het feit dat men risico's op dat niveau niet 'ziet' kan tot gevolg hebben dat maatregelen niet worden genomen, prioriteiten niet juist (lees: reëel) worden gesteld, en er derhalve risico's worden gelopen. In plaats van genomen. Met onlangs in Keulen catastrofale gevolgen.

VERSLAG

ISF 2010: 21ST ANNUAL WORLD CONGRESS 2010

Monte Carlo, 6-9 november 2010

Aart Jochem is lid van de redactie van Informatiebeveiliging en werkt bij GOVCERT.NL, het incident response team van de overheid. Hij is bereikbaar via aart.jochem@govcert.nl.

ISF-Congres 2010 in Monte Carlo.

Het Information Security Forum (ISF) is een organisatie die kennis van de leden gebruikt om kennisproducten voor de leden te maken. De focus ligt vooral op security management en security governance en de leden zijn vaak grote organisaties. Jaarlijks is er een conferentie, in 2010 al voor de 21e keer. Deze keer in Monte Carlo.

De stad was deze keer niet het decor van voorbij flitsende raceauto's, hoewel snelle bolides wel het straatbeeld bepaalde. Informatiebeveiligers van over de hele wereld streken neer in het Gribaldi Forum, de plaats waar het zich allemaal afspeelde.

Met de salami-aanpak regelgeving verbeteren

Na de opening met het brandweerkorps van Monaco opende Vint Cerf de conferentie. Vint is een van de pioniers van internet. Hij heeft begin jaren 70 met Bob Kahn de TCP/IP protocol suite bedacht, momenteel de basis van internet. Hij gaat in op wat hij duidt als de trend om alles belangrijker te laten lijken door er cyber voor te zetten. In zijn lezing fileert hij cyber warfare, cyber health, cyber fire department en maakt duidelijk welke aspecten redelijke analogieën zijn tussen cyber space en de fysieke wereld en welke niet. Hij stelt voor om nu echt de internationale regelgeving aan te pakken en daarbij te focussen op de dingen die we met elkaar gemeen hebben. Met een salami-aanpak kunnen we dan uiteindelijk de grote drempels slechten.

De lezing wordt echt interessant als dagvoorzitter Nick Witchell vraagt of Vint in 1973 had voorzien welke maatschappelijke impact internet zou hebben. Vint blijkt een gedreven visionair en hij beschrijft de spirit waarin packet switching, GUIs, hyperlinks en TCP/IP tot stand kwamen.

Advanced persistent threats: hoe goed kun je ze weren?

Eric Montcalm van SecureOps ontrafelt het fenomeen Advanced Persistent Threat (APT). Een term die met de Aurora-aanval bij Google in de media verscheen en staat voor gerichte aanvallen die langzaam opbouwen en lang binnen de organisatie blijven bestaan. Eric geeft hierbij aan dat het gaat om een evolutie en geen revolutie: gerichte aanvallen zien we al langer. Jammer dat hij hierna vooral een sales pitch geeft, iets wat normaliter niet gebeurt op deze converentie.

Vinton Cerf pleit voor afstemmen nationale regelgeving cyber security.

Betere detectie en respons

Ik presenteerde zelf op deze eerste dag over het verminderende effect van preventieve maatregelen als firewall en antivirus en de noodzaak om detectie te verbeteren en te koppelen aan goede incident response. Binnen dit framework heb ik verteld over de ontwikkelingen op dit gebied bij GOVCERT.NL.

Bruce Schneier over online socialmedia en privacy.

Government sector special interest session

ISF wil meer met overheden doen en is benieuwd naar waar deze sector verschilt van de bedrijven die lid zijn. De aanwezigen gaven aan vooral moeite te hebben met bescherming van persoonsgegevens en het delen daarvan met andere overheidsorganisaties. Daarnaast is (federated) identity management voor publiek en de eigen medewerkers nog een belangrijke drempel. ISF gaat hier verder mee, maar hoe moet nog duidelijk worden.

Privacy en social media

De tweede dag van het congres wordt geopend door Bruce Schneier. Bruce, met altijd scherpe analyses en conclusies, leidt ons in een spreekbeurt zonder slides door de consequenties van het explosief gegroeide gebruik van social media en het leven zonder privacy. Er is geen medium meer waarmee we kunnen communiceren zonder dat er sporen achterblijven. In toenemende mate worden die door bedrijfsleven en overheid gebruikt voor doelen als marketing en opsporing. Een presentatie van Schneier is moeilijk samen te vatten. Hij was wederom goed, zette je aan het denken en eindigde zoals Al Gore zou doen met een waarschuwing: *"People are a social race, we need to socialize. And whatever way we do it, it will be a computer mediated system. This social networking is not temporary. We are gonna be asked by future generations how we handled privacy in the early ages of the information society. It better be good." Ik zeg: Schneier for president.*

Laat de business units zelf logs monitoren

Linda Cooper Angles (Guardian Life Insurance Company of America) geeft aan hoe zij als CISO met business managers aan de slag is gegaan om te bepalen welke aspecten in IT gemonitord moeten worden om de business processen betrouwbaar te houden. Een logmonitor en rapportagesysteem implementeert dit en Linda maakt vervolgens de business owners verantwoordelijk voor log monitoring en follow up. Slim! Zij ziet haar rol als CISO vooral als risk advisor en niet die van beslisser.

De positieve kanten van cloud security

Nick Coleman (IBM), in de UK een gevierd adviseur voor de overheid, laat zien dat de baten van cloud services opwegen tegen de extra kosten voor beveiliging. De besparingen worden bereikt door virtualisatie, efficiënt omgaan met energie, standaardisatie en automatisering. De vrijgekomen budgetten kunnen worden geïnvesteerd om bezwaren van clouds op het gebied van security en application integration aan te pakken. Coleman vindt dat bedrijven in ieder geval niet meer moeten investeren in een eigen ontwikkel- en testomgeving. Het opzetten van een dergelijke voorziening is veel sneller en goedkoper in de cloud. Natuurlijk levert IBM deze diensten.

De toekomst van ISF

Information Security Forum

De presentatie van het management en bestuur van ISF over de plannen voor de komende tijd was aanzienlijk minder druk bezocht dan vorig jaar en de sfeer was veel minder grimmig. ISF heeft de commentaren van vorig jaar ter harte genomen en een aantal veranderingen in de organisatie doorgevoerd. Ook is de focus veel meer op 'member value' komen te liggen en dat werd dit jaar beloond met vele positieve geluiden. ISF richt zich de komende jaren nog steeds op groei. Enerzijds om de kwaliteit van haar deliverables hoog te houden binnen de huidige fee structuur en anderzijds om met meer leden te putten uit meer experts. Daarbij richten ze zich op de Forbes 2000 en grote overheden. Ook kunnen toeleveranciers van leden lid worden tegen een gereduceerd tarief, zodat de supply chain van een lid toegang krijgt tot de best practices en tools.

Het Grimaldi Forum decor voor 21e editie ISF-Congres

De motivatie van internetcriminelen

Mischa Glenny (BBC) heeft onderzoek gedaan naar veroordeelde cyber criminals. Hij heeft ze geïnterviewd en naar hun achtergrond gekeken. Hij moest constateren dat het er nog niet zoveel zijn en dat maar de helft vanuit criminele intenties hebben gehandeld. De andere helft is in internetcriminaliteit beland doordat ze onder druk zijn gezet of simpelweg omdat de kans zich voordeed. Glenny geeft voorbeelden van diensten in de underground economy en heeft een kritische noot over gebrek aan transparantie bij de banken. Ze stoppen teveel zaken in de doofpot om de business te beschermen tegen grote maatschappelijke kosten, volgens Glenny.

Banken moeten transparanter worden over de impact van cybercrime

ENISA to the rescue

Udo Helmbrecht, directeur van ENISA, opent de derde dag van het congres. Enisa is het Europese agentschap voor informatiebeveiliging (of *network and information security*, zoals ze het noemen). Voorgaande jaren heeft ENISA zich gericht op het opzetten van incident respons teams in Europese landen die ze nog niet hadden. Daarbij werd gebruikgemaakt van lessons learned en de aanpak van meer volwassen teams in andere landen. ENISA gaat zich nu meer richten op het verbinden van incident responsteams in Europa. Helmbrecht was voorheen directeur van het Duitse *Bundesamt für Sicherheit in der Informationstechnik*, een grote federale overheidsorganisatie gericht op informatiebeveiliging.

De bedreiging van binnenuit

Steve Cummings (Deloitte) was voorheen werkzaam bij CPNI in de UK en nu special advisor bij Deloitte. Hij gaat in op vier aspecten van workforce security: strategie, preventie, detectie en response. De noodzaak voor maatregelen op het vlak van personele beveiliging wordt vaak onderschat, met uitzondering bij overheden. De meeste incidenten gebeuren door vaste medewerkers, die tussen een en acht jaar in dienst zijn en gemiddeld 37 jaar oud (maar meestal ouder dan 30). System administrators zijn relatief laag vertegenwoordigd in de statistieken. Steve gaat door een groot aantal elementen die van belang zijn voor een gebalanceerde en geïntegreerde aanpak van de insider threat. Employee Assistance Programs en SIEM, training, access control en vele andere zaken.

Ten slotte

ISF heeft goed geluisterd naar de leden en heeft dit 21e congres weer op de vertrouwde leest geschoeid. Dit keer geen plenaire discussies, maar jammer genoeg ook geen *table top exercise* met de hele zaal, zoals vorig jaar. Er was veel inbreng van de leden zelf, genoeg ruimte om te netwerken en kennis te maken met de producten van ISF, zoals de *The Standard of Good Practice for Information Security* en de *Information Risk Analysis Methodology*. Al met al zeker de moeite waard. Volgend jaar is het 22e ISF congress opnieuw in Europa, Berlijn is dan aan de beurt. Lekker dicht in de buurt. Dus gaan als je gelegenheid hebt.

De website van ISF:
https://www.securityforum.org/

COLUMN

KUNT U EEN GEHEIMPJE BEWAREN?

Mensen zijn niet goed in het bewaren van geheimen. Logisch ook, want geheimen zijn spannend. En juist daardoor willen we ze weten. En als we ze weten, willen we ze graag doorvertellen. We roddelen over die ene collega die het doet met die andere collega en in een mum van tijd verspreidt deze informatie zich als een lopend vuurtje over de werkvloer. De buurvrouw die een vreemd pakketje krijgt (wat zou erin zitten?) en de vriend die zich de laatste keer zo vreemd gedroeg (wat verbergt hij?). Publieke geheimen hebben wij ook, maar daar schrijven we eigenlijk niet over. Waar lees of zie je immers ooit dat onze vorstin rookt? En als WikiLeaks aankondigt vele documenten te openbaren waarin wellicht saillante, diplomatiek gevoelige, informatie te vinden is, zijn we er als de kippen bij om zo snel mogelijk en zo veel mogelijk van die geheimen tot ons te nemen. Als het om de informatie van WikiLeaks gaat, dan hoor ik regelmatig zeggen dat het toch informatie is 'waar we recht op hebben als burger'. Nog even afgezien van het beantwoorden van de vraag of dat ook echt zo is, laat ik dan de volgende vraag opwerpen: "Kunnen we eigenlijk wel geheimen bewaren in de online wereld?"

Uit wetenschappelijk onderzoek blijkt dat iedereen geheimen heeft. Soms een, maar meestal meerdere (ja, ik ook en dat betekent dat u er ook in ieder geval eentje meedraagt). Ook is het hebben van een geheim niet iets wat zich in eenzaamheid afspeelt, niettegenstaande dat iemand met een zwaar drukkend geheim zich daardoor wel erg eenzaam kan voelen. Geheimen hebben een sociale constructie in zich zitten. Bij een geheim zijn namelijk altijd anderen betrokken met wie vaak een klein gedeelte van dat geheim wordt gedeeld. We knippen geheimen in stukjes en we geven een deel van het geheim weg of we vertellen bepaalde aspecten van een geheim aan de een, en andere aspecten aan de ander. Het geheim en de sociale selectiviteit daarvan lijkt daarmee veel op wat begrepen wordt onder privacy en zelfbeschikking over de private sfeer van het leven. Ik bepaal zelf aan wie ik op welk moment welk stukje informatie over mijzelf prijsgeef. Geheimen lijken ook wel een sociaal smeermiddel; ik vertrouw jou met deze informatie. En degene waarop wordt vertrouwd, voelt zich bijzonder. Hij behoort immers tot de incrowd. Geheimen zijn doorgaans ook gewoon spannend. De clandestiene ontmoeting tussen twee relationeel gebonden personen is vele malen spannender juist doordat het in het geniep moet gebeuren. Ja, dat maakt het gras inderdaad groener aan de overkant. Geheimen kunnen ook grote destructieve waarde hebben en dan vaak vooral als deze openbaar worden gemaakt. Relaties lopen stuk, reputaties gaan naar de knoppen en de angst voor diplomatieke rellen en/of ernstige terroristische dreigingen maken dat we geheimen vaak toch liever geheim willen houden.

We vinden daar al eeuwen lang allerlei manieren voor. Het meest bekende voorbeeld is het geheimschrift (cryptografie) waar, naar verluid, zelfs de Egyptenaren in oude tijden al mee aan de slag zijn gegaan. Ook de Griekse beschaving versleutelde boodschappen zodat niet iedereen deze kon lezen. Overigens raadt de aloude Kama Sutra geliefden al aan te communiceren door gebruik te maken van geheime codes. Een wijze raad waar wellicht heden ten dage nog velen van zouden kunnen profiteren. In mijn eigen onderzoek kwam ik een wat meer recent voorbeeld tegen van jongeren die op de sociale netwerksite Hyves op hun eigen manier een geheim communiceerden. Vaak bevriend met moeder en/of vader (want die willen het kroost in de gaten houden) en een open toegankelijk profiel. En omdat het toch echt niet de bedoeling is dat ouders alles kunnen lezen wat daar te lezen valt, werd in de pagina zelf tekst achtergelaten in dezelfde kleur als de achtergrond (even selecteren en je kunt het lezen). Geheimen, klein of groot, we hebben ze dus allemaal en we delen ze soms met sommigen en soms met velen. En dat delen doen we eigenlijk best wel graag, vooral ook omdat het soms zo zwaar op ons gemoed drukt om het te bewaren. Psycholoog Wismeijer, verbonden aan de Universiteit van Tilburg, onderzoekt geheimen in al zijn facetten. Hij schreef er, samen met journaliste Bots een boek over. Alle ins en outs van geheimen worden daar uit de doeken gedaan. Maar mooier nog, Wismeijer begrijpt dat geheimen gedeeld moeten worden, maar dat dit delen vaak een risicovolle aangelegenheid is. Daarom riep hij al tijden geleden de website www.geheimenvan.nl in het leven. Geheel anoniem kan een ieder die dat wenst elk geheim aan het digitale papier toevertrouwen. Kunt u een geheimpje bewaren? Het is een van de mooiste websites die ik ken omdat het de mens in zijn slechtste, mooiste, meest trieste en meest opgeluchte vorm weergeeft.

mr Rachel Marbus
@RachelMarbus op twitter

Foto: Mast3r

ACHTER HET NIEUWS

In deze rubriek geven enkele van de IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems inzake 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.

WIKILEAKS EN DE RISICO'S VAN ONZE INFORMATIEMAATSCHAPPIJ

Bij het ter perse gaan van deze editie van Informatiebeveiliging zijn Cablegate en Wikileaks onderwerp van iedere nieuwsuitzending en het verhaal ontwikkelt zich met het uur. Oprichter Julian Assange heeft inmiddels de celebrity-status gekregen, maar zit wel in de UK achter de tralies. Voor- en tegenstanders van de site bestoken elkaar met DoS-aanvallen. Het grootschalig lekken en publiceren van diplomatieke berichten van de Verenigde Staten maakt pijnlijk duidelijk welke risico's verbonden zijn aan onze informatiemaatschappij en hoe verhoudingen liggen. We vroegen vier redacteuren van dit blad welke lessen hieruit te leren vallen.

Rob Greuter: De mens wil en zal bedrogen worden. En dat gebeurt dan ook volop. Met ons onmogelijke geld- en rentesysteem, onze falende en peperdure gezondheidszorg, ons zeer matige eten, het verziekte milieu, onze zeer snel slinkende energie- en mineralenvoorraden (google eens op peakoil), de explosieve stijging van de wereldbevolking… De lijst is eindeloos. Een deel van de oorzaak bedrogen te worden is pure luiheid. Wat tot ons komt slikken wij voor zoete koek. Zelf onderzoek doen, cijfers narekenen, zelf nadenken, is te vaak en voor teveel mensen simpelweg teveel gevraagd. Totdat er iets gebeurt. Een olieramp in de Mexicaanse Golf, een instortende economie, gebrek aan zeer noodzakelijke structurele maatregelen, en falende privatisering. Er gebeurt genoeg zou je denken. Niet dus. Nog steeds niet genoeg om mensen massaal uit hun stoel te krijgen, tot serieus nadenken te stemmen, en in te grijpen. Mensen komen nu eenmaal wat lastig uit hun comfortzone. Nu WikiLeaks grootschalige Main Stream Media (MSM) aandacht krijgt, lijkt er enige beweging te komen. We worden massaal gewezen op de noodzaak tot een transparante, dienende en eerlijke overheid. Toch is deze beweging slechts een schijnbeweging, hooguit een radertje in het proces dat nodig is om naar een andere maatschappij te komen. Overheden staan in dienst van banken en industrie. Belastingbetalers en politici hebben vrijwel niets te vertellen, laat staan te veranderen. Toch zal er op korte termijn echt iets groots gaan gebeuren, iets met een veel grotere en pijnlijker impact dan Wikileaks ooit zal kunnen bereiken. Zo is het instorten van ons geldsysteem aanstaande. Veel economen weten dat. Slechts enkele durven dat nu al naar buiten te brengen. Er is niet aan te ontkomen. In ons systeem is immers schuld nodig voor geldcreatie. Snel daarna zal de fossiele energiewinning serieus gaan haperen. Sneller dan u denkt (lees: wordt voorgehouden). Slechts landen en gemeenschappen die zich daarop voorbereiden maken een kans daar redelijk uit te komen. Angst, de achterliggende hoofdoorzaak van vele problemen zal dan vanzelf verdwijnen. Tot die tijd voorspel ik gouden tijden voor de informatiebeveiliger.
Het verschijnsel WikiLeaks is absoluut nuttig en boeiend om mee te maken, maar het leidt de aandacht af van de werkelijk belangrijke uitdagingen waarvoor de mensheid staat.

Maarten Hartsuijker: Het lijkt soms net een spannende speelfilm, WikiLeaks. Als een soort 'Enemy of the state' neemt 'good guy' Julian Assange het op tegen de Verenigde Staten. De VS doen samen met grote machtige organisaties alles wat in hun macht ligt om Assange in een kwaad daglicht te stellen of het hem op een andere manier moeilijk te maken.
Als we alle emoties even laten voor wat ze zijn, is het als informatiebeveiliger interessant om te zien wat WikiLeaks teweeg brengt. Zo blijken de Verenigde Staten er geen problemen mee te hebben om de controle die zij (via ICANN) nog op generieke, internationale TLD's kunnen uitoefenen naar nationale maatstaven voor eigen gewin in te zetten. Ook zien we hoe de verschillende kampen (of sympatiserende derden) online alles uit de kast trekken om het de ander lastig te maken. Denial-of-service-aanvallen maken pijnlijk duidelijk hoe kwetsbaar we zijn, nu we ons in onze samenleving vrijwel volledig aan de techniek aan het overgeven zijn. Met relatief weinig middelen kan bijna iedereen grote organisaties digitaal ernstig hinderen. Voor veel informatiebeveiligers is dit niets nieuws, maar WikiLeaks slaagt er wel in om het in een keer op de publieke en politieke agenda te plaatsen.
Los van al dit technische geweld zal menig informatiebeveiliger vermoedelijk

de komende tijd vooral zijn hoofd breken over de menselijke invloed op informatiebeveiliging. Want als WikiLeaks boven alles een ding pijnlijk duidelijk maakt, is het hoe afhankelijk miljarden verslindende beveiligingsmaatregelen zijn van de mensen die met de informatie moeten werken.

Lex Borger: WikiLeaks is een begrip geworden door alle recente nieuwsfeiten die ermee geassocieerd kunnen worden. Ik ben op zoek gegaan naar wat WikiLeaks bezielt. WikiLeaks beroept zich in hun missiestatement op de universele rechten van de mens, met name de vrijheid van meningsuiting. Ze leveren echter alleen anoniem de grondstoffen voor onderzoekers. En hebben ook veel aandacht voor donaties, zonder verantwoording.
Vrijheid van meningsuiting heeft zijn grenzen. Het mag geen leed berokkenen en geen aanstoot geven. Hier moet dus naar een balans worden gezocht. WikiLeaks doet dat niet. Ze beoordelen materiaal alleen op echtheid, voor zover ze dat kunnen. De toegevoegde waarde is duidelijk. Door de anonimiteitgarantie maakt WikiLeaks het mogelijk informatie in het publieke domein te krijgen zonder de bron te verhullen.
Nu WikiLeaks een begrip is geworden gaat het aan zijn eigen succes ten onder. Ze zijn verworden tot een speelbal van partijen die zonder enig redelijkheidsbesef of ethiek documenten lekken waarvan je je echt moet afvragen of met de publicatie ervan het principe van geen leed en geen aanstoot niet ruim overschreden is. Laat staan de overtreding van andere mensenrechten, zoals het recht op een veilige leefomgeving.

Ronald van Erven: Laten we wel wezen, WikiLeaks doet niets. Net als Wikipedia wordt de inhoud op WikiLeaks verzorgd door 'de maatschappij'. Individuen die wat te melden hebben. Het is het publiek dat informatie op deze site neerzet.
Als we ingaan op de inhoud van de gelekte informatie blijkt het minimaal een jaar oud. Dus de waarde is betwistbaar. Een veel gehoord argument is dat er levens in gevaar worden gebracht. Dit is zeker zo, want zeker militaire informatie, bijvoorbeeld tactische methoden veranderen niet zo snel. En door deze transparantie kan de vijand bijleren.
Maar de documenten van beroepspolitici en topbestuurders, brengen geen mensen in gevaar? Hooguit brengen ze deze mensen en een paar landen in verlegenheid en laat hun ware aard zien. Deze transparantie is, naar mijn mening, waardevol omdat het aangeeft of onze leiders ons naar nieuwe oorlogen leiden terwijl daartoe geen reden is.
Zo blijkt in een gespreksverslag uit 2009, tussen de Australische minister-president en de Amerikaanse minister van Buitenlandse Zaken, dat China's economische en militaire expansiedrift als een gevaar wordt gezien die eventueel met geweld moet worden tegengehouden. Let wel, ik ben voor de stille of geheime diplomatie om tot oplossingen te komen zodat landen zonder gezichtsverlies oplossingen kunnen implementeren. Maar als nu blijkt dat de stille diplomatie ook voor wellicht persoonlijke belangen wordt gebruikt, is een website als WikiLeaks interessant.
De eigenaar van WikiLeaks is aangehouden maar niet vanwege de informatie die op zijn website staat. Deze arrestatie komt toevallig wel goed uit omdat andere landen, zoals de Verenigde Staten en Australië, nu verzoeken tot uitlevering hebben ingediend. Deze landen willen toch wel een stevig gesprek hebben met de heer Assange en toegang hebben tot informatie om de klokkenluider te achterhalen. Heel logisch. Want het zijn deze klokkenluiders die hun geheimhouding en bedrijfsrichtlijnen schenden. Maar waar ligt de grens tussen ethiek en iemands geheimhouding? Deze WikiLeaks-zaak veroorzaakt meer. Namelijk, een drang naar meer transparantie en snellere verandering van de gevestigde orde. En niet via een wet zoals in de vorm van openbaarheid van bestuur, maar echte rauwe informatiedeling, precies waar het internet voor bedoeld was. De informatieontvanger moet zelf een waarde toekennen aan de informatie en bekijken of hij de informatie wel of niet gebruikt dan wel interessant vindt om te lezen. Dit komt nu tot uiting door diverse hack-aanvallen en digitale protesten op websites van financiële en overheidsinstellingen.

Source: The Australian (6 december 2010)

Ik denk dat er met WikiLeaks-gate veel meer vragen en complexe maatschappelijke problemen naar boven komen en dat er zich nieuwe grenzen zullen ontwikkelen aan wat een maatschappij wel en niet toelaat. En maar kijken in hoeverre de gevestigde orde met wetgeving in de hand de censuur en bigbrother-principes kunnen en zullen toepassen en de klokkenluiders zullen opsporen… Wordt vervolgd. Zeker als we WikiLeaks-gate eens tegen informatiebeveiligingsprincipes kunnen houden.

Bron: http://www.transparency.org en http://213.251.145.96 (wikileaks)

CLOUD SECURITY IN VOGELVLUCHT

Wolter Pieters, Universiteit Twente

Cloud computing is dé hype in IT op het moment, en hoewel veel aspecten niet nieuw zijn, leidt het concept wel tot de noodzaak voor nieuwe vormen van beveiliging. Het idee van cloud computing biedt echter ook juist kansen om hierover na te denken. Wat is de rol van informatiebeveiliging in een wereldwijd netwerk van afhankelijkheden? Op een workshop in Brussel in januari 2010 kwamen experts uit technische, juridische en filosofische hoek bijeen om hierover van gedachten te wisselen. Binnenkort verschijnen de bijbehorende artikelen in het boek 'Computers, privacy and data protection: an element of choice' (Gutwirth et al., 2011). Ter gelegenheid daarvan een overzicht over het thema.

Wat opvalt is dat zowel begrippen als gevolgen nog niet duidelijk in kaart zijn gebracht. Dat geldt in eerste instantie voor het begrip cloud computing zelf. Volgens Paolo Balboni, advocaat en lid van de European Privacy Association, is het karakteristieke van cloud computing dat het als een 'commodity', een massaproduct, wordt aangeboden. Daardoor is, in tegenstelling tot outsourcing, onderhandeling over de voorwaarden vaak onmogelijk. Net zoals je niet kunt onderhandelen over de eigenschappen van artikelen in de supermarkt.

Deze standaardisatie van voorwaarden heeft belangrijke gevolgen. In de bestaande privacywetgeving is sprake van een 'data subject', 'data controller' en 'data processor'. Hierbij wordt ervan uit gegaan dat de data controller verantwoordelijk is voor de informatieverwerking, en dat deze kan controleren dat de uitvoering daarvan door de data processor ook daadwerkelijk aan de eisen voldoet. Juist die auditing is in een cloudscenario echter vaak onmogelijk. Je kunt niet even bij Google of Amazon binnenwandelen en kijken hoe het met de beveiliging staat. Daardoor moeten deze begrippen wellicht in een nieuwe versie van de wetgeving, die op dit moment in voorbereiding is, worden herzien. De wet zal echter pas over een jaar of vijf van kracht worden, en de vraag is natuurlijk hoe de technologie zich in de tussentijd ontwikkelt.

Een ander belangrijk juridisch struikelblok is de locatie van de data. Privacygevoelige data mag niet zomaar naar alle landen worden geëxporteerd, maar hoe kun je dit beleid afdwingen? Immers, je kunt je data wel aan een Nederlands bedrijf in beheer geven, maar het zou best kunnen dat via een aantal stappen de data toch in India terechtkomt. Dit kun je natuurlijk in je contract uitsluiten, maar interessanter is wellicht of er technische oplossingen te bedenken zijn voor dit probleem. Dit is dan vergelijkbaar met het zogenaamde 'location-aware access control' (Van Cleeff et al., 2010), alleen gaat het dan niet om de locatie van de gebruiker, maar om de locatie van de data zelf. Vergelijkbare oplossingen zijn al voorgesteld voor het ontoegankelijk maken van gegevens na een verloopdatum, dus voor tijd in plaats van locatie (zie bijvoorbeeld Tang, 2010).

Versleuteld bewerken

In het algemeen is het versturen van data in de cloud met behulp van standaard PKI-technieken goed te doen. Afgezien van het vraagstuk van locatie is ook opslag in de cloud niet zo moeilijk. Je versleutelt de data, stuurt ze naar een server, haalt ze weer op als je ze nodig hebt, en ontsleutelt ze dan weer. Ze kunnen dan door de server niet worden gelezen. Eventueel kun je ook de integriteit nog controleren met een hash of een handtekening. De grote vragen liggen op het gebied van het *bewerken* van data in de cloud.

Afgelopen jaar is er een theoretische doorbraak bereikt op het gebied van versleuteling. Het grote vraagstuk dat is opgelost is of het mogelijk is een versleutelingsmethode te maken waarmee je willekeurige bewerkingen kunt toepassen op versleutelde data, zodat je de data niet meer 'in the clear' hoeft te hebben om deze te kunnen bewerken. Met het zogenaamde fully homomorphic encryption zou dit mogelijk zijn. Hiermee kun je versleutelde gegevens optellen én vermenigvuldigen, en je kunt laten zien dat daarmee alle mogelijke bewerkingen voorhanden zijn. Er is dus nu theoretisch aangetoond dat zo'n methode bestaat (Gentry, 2009). Het slechte nieuws is dat dit voor de praktijk nog geen enkele betekenis heeft. De methode is bij lange na niet efficiënt genoeg voor praktische toepassingen.

Voor cloud computing zou fully homomorphic encryption betekenen dat ook de aanname van een 'nieuwsgierige' server, die mogelijk je geheimen zou

kunnen misbruiken, geen belemmering meer hoeft te vormen voor cloud processing. De server krijgt de plaintext data dan immers nooit te zien, maar bewerkt slechts een versleutelde versie. Nu dit nog niet praktisch is, wat kan er dan wel? Allereerst is er de mogelijkheid van 'secure multi-party computation'. Hiermee kun je vergelijkbare dingen doen, namelijk bewerkingen uitvoeren zonder dat de deelnemers de oorspronkelijke data zien. In een bekend voorbeeld willen twee miljonairs weten wie er rijker is, zonder elkaar te vertellen hoeveel geld ze hebben. Echter, zoals de naam al zegt, moet je daarbij data heen en weer sturen. Dit wil je in de cloud nu juist niet. De cloud provider moet zelf de bewerkingen kunnen uitvoeren, want dat is waar de efficiëntiewinst te halen is.

Gelukkig blijkt dat, hoewel willekeurige berekeningen toepassen op versleutelde data nog niet haalbaar is, dit voor specifieke bewerkingen wel degelijk kan. Een beperkte versie van homomorphic encryption (alleen optellen) wordt bijvoorbeeld al toegepast voor het tellen van stemmen in de toekomstige generatie elektronische verkiezingssystemen (zie bijvoorbeeld Cramer et al., 1997). De stemmen kunnen dan in versleutelde vorm worden opgeteld, zodat het stemgeheim gewaarborgd blijft, waarna de uitslag kan worden ontsleuteld.

Ook kunnen we bijvoorbeeld zoeken in versleutelde databases (Brinkman, 2007). Dat laatste gaat als volgt. Voordat het document naar de server wordt verstuurd, voeg je aan het document de keywords toe waar je op wilt kunnen zoeken. Je versleutelt deze gegevens nu zodanig dat de server 1) het document niet kan lezen, en 2) de keywords niet kan zien, maar 3) wel kan controleren of een later aangeboden (versleuteld) keyword overeenkomt met de oorspronkelijke keywords. Je kunt nu dus zoeken in de data zonder dat de server informatie verkrijgt over je document of zoektermen.

Informatievoorzorg

Bovenstaande laat zien dat er in de cloud naast risico's ook kansen liggen voor informatiebeveiliging, in termen van nieuwe technische mogelijkheden. De vraag die overblijft is of er een algemeen principe ten grondslag ligt aan wat we met informatiebeveiliging willen bereiken in het tijdperk van cloud computing. Op dit moment lijkt beveiliging nog te veel als een uitvoeringskwestie te worden gezien, terwijl het steeds duidelijker wordt dat al in het ontwerp belangrijke keuzes moeten worden gemaakt. In dit kader hebben wij eerder voorgesteld het zogeheten voorzorgsprincipe, dat in de milieuethiek met name binnen de EU zeer succesvol is geweest, ook op IT toe te passen (Pieters en Van Cleeff, 2009). Daarbij geldt dat bij twijfel over mogelijk misbruik van een systeem, zelfs als niet zeker is hoe groot de kans daarop is, ontwerpmaatregelen moeten worden genomen om dergelijke risico's af te dekken. De vraag die gesteld zou moeten worden is hoe machtsverhoudingen verschuiven door het nieuwe systeem. We hebben hier problemen gezien met de uitbesteding van het verkiezingsproces via stemcomputers, maar het gaat ook over rechten van bijvoorbeeld administrators en veiligheidsdiensten. Een dergelijk principe zou er bijvoorbeeld toe hebben kunnen leiden de vingerafdrukken van de paspoorten niet in een centrale database op te slaan, en sociale netwerksites veel eerder te dwingen iets aan hun privacy te doen.

'You decide'

De tendens lijkt op dit moment vooral in te zetten op gebruikerseducatie ter voorkoming van misbruik van informatie. Zo heeft de overheid actief campagne gevoerd om mensen ervan bewust te maken dat ze niet alle data, zoals wanneer ze met vakantie zijn, zomaar op internet moeten zetten. In Noorwegen zijn filmpjes gemaakt om kinderen en jongeren te wijzen op de gevaren van sociale netwerksites (www.dubestemmer.no).

Ondanks de sympathieke uitstraling van deze initiatieven lijkt de nadruk op de gebruikers een onmacht te laten zien ten aanzien van de technische mogelijkheden. Het voorzorgsprincipe kan hierin verandering brengen, maar alleen als wij als informatiebeveiligers het standpunt uitdragen dat 'in the cloud' informatiebeveiliging niet alleen maar een technische kwestie is, maar iets dat al op beleidsniveau verankerd moet worden. Alleen dan kunnen we ook in de toekomst rekenen op veilige systemen.

Literatuur

Brinkman, R. (2007) *Searching in encrypted data.* PhD thesis, University of Twente. CTIT Ph.D.-thesis series No. 07-98.

Van Cleeff, A., Pieters, W. & Wieringa, R.J. (2010) Benefits of Location-Based Access Control: A Literature Study. To appear in *Proceedings of the 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom-2010).*

Cramer, R., Gennaro, R. & Schoenmakers, B. (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. *European Transactions on Telecommunications 8(5): 481-490.*

Gutwirth, S., Poullet, Y., De Hert, P. & Leenes, R. (Eds.) (2011) *Computers, Privacy and Data Protection: an Element of Choice.* Dordrecht: Springer. www.springer.com/law/international/book/978-94-007-0640-8

Gentry, C. (2009) On homomorphic encryption over circuits of arbitrary depth. In *the 41st ACM Symposium on Theory of Computing (STOC).*

Pieters, W. & Van Cleeff, A. (2009) The Precautionary Principle in a World of Digital Dependencies. *IEEE Computer,* 42 (6):50-56.

Tang, Q. (2010) Timed-Ephemerizer: Make Assured Data Appear and Disappear. In *Sixth European Workshop on Public Key Services, Applications and Infrastructures.* Volume 6391 of LNCS, Berlin: Springer.

25 JAAR RISICOMANAGEMENT, … EN NU DE MENS NOG

Cees Coumou adviseert op het gebied van risicomanagement en informatiebeveiliging vanuit Coumou Security Continued. Hij is betrokken bij opleidingen van de UvA, VU en HHS. Hij is bereikbaar via cees.coumou@planet.nl

Deze tekst is een bewerking van het verhaal, gehouden te Amsterdam op 4 juni 2010 tijdens de viering van het 25-jarig bestaan van het Genootschap voor RisicoManagement (GvRM).

Het Genootschap bestaat 25 jaar terwijl risico's er altijd al zijn geweest. Dat doet de vraag rijzen naar de reden van de oprichting. Die reden lag niet in het feit dat er geen aandacht zou zijn geweest voor risico's. Die aandacht was er wel maar volgens de oprichters destijds, werd die aandacht teveel gericht op slechts een van meerdere strategieën, namelijk het overdragen van financiële aspecten van risico's door een verzekeringspolis af te sluiten. Op die manier werd voorzien in een dekking tegen mogelijke (financiële) schade door ongewenste gebeurtenissen. Het Genootschap ging zich inzetten voor een brede en integrale benadering van risicomanagement.

Het is duidelijk dat in de achter ons liggende periode risicomanagement veelzijdig is geworden. Maar ook is duidelijk geworden dat risico's niet alleen behoren in het domein van deskundigen. Iedereen heeft ermee te maken. In alle aspecten van het leven doen zich risico's voor en zal er door individuen en in groepsverband 'iets' met risico's moeten worden gedaan. Risico's worden in de maatschappij van vandaag gemakkelijker en openlijker besproken en genoemd als verschijnsel waarmee rekening moet worden gehouden. Ook een individuele persoon doet (ook al is dat vaak onbewust) aan een vorm van risicomanagement en is zijn eigen risicomanager. Dat is een reden voor de keuze van het thema voor dit lustrum. Het betreft ons allen.

Maar er is nog een andere reden voor de keuze van dit thema. Het onderwerp risico 'staat op de agenda', de moderne uitdrukking voor het verschijnsel dat een onderwerp niet verborgen hoeft te blijven, dat er aandacht voor kan worden gevraagd. Dat is wel eens anders geweest. De huidige maatschappij weet dat er risico's zijn. Breed uitgemeten incidenten (had dat voorkomen kunnen worden?) en onderzoeken naar aanleiding, oorzaak, nalatigheden en verantwoordelijkheden worden door de media gretig gevolgd. Het gevolg daarvan is dat er meer tijd wordt genomen om vooraf na te gaan welke kwade kansen er zijn bij activiteiten van bedrijven en andere organisaties. Nieuwe projecten worden vaak wantrouwig bekeken door actiegroepen die niet zullen nalaten te wijzen op 'negatieve gevolgen' van een initiatief. Kortom, risico's als begrip zijn bekend. Ook weten de eigenaren van een probleem of de verantwoordelijken voor een project of onderneming wat hen te doen staat. Zo niet, bij enig incident zal verantwoording worden gevraagd.

Incidenten

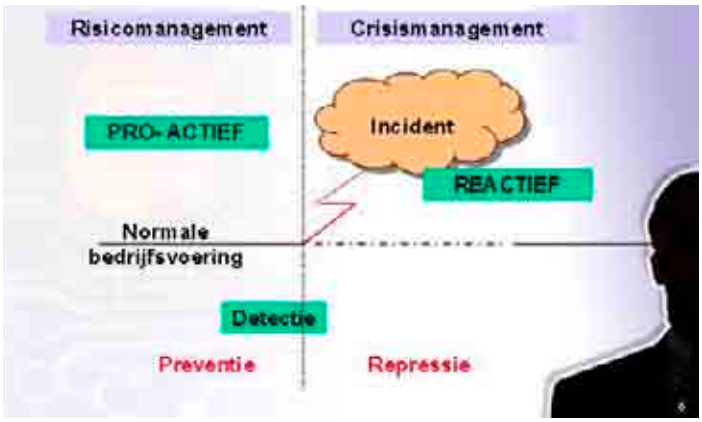
Er is inmiddels een cultus ontstaan in het onderzoeken van incidenten. Natuurlijk is dat bedoeld als leermoment en het voorkomen van toekomstige narigheid. Maar tegelijkertijd weten wij ook dat honderd procent veiligheid niet haalbaar is. Dat geldt ook als (met name vertegenwoordigers van de overheid) na een incident roepen: "Dit mag nooit meer gebeuren!"

Soms treffen wij dus maatregelen tegen risico's. Zoals wetgeving die bedoeld is om het drankmisbruik door jongeren te voorkomen. Maar is het wel de wetgever die hier als eerst verantwoordelijke aangemerkt moet worden? Zouden de ouders misschien ook een rol moeten spelen bij dit risico? Die verantwoordelijkheid voor risico's en dus voor het treffen van maatregelen is een spel dat niet altijd duidelijk en controleerbaar verloopt. Zoals in het geval van een grote aardbeving waarbij steeds de bewoners van sociale woningbouw het slachtoffer worden. Betekent dit dat de eigenaren van die bouwwerken geen oog hebben voor het risico van een aardbeving? Of zou het de bouwer zijn die het geld dat is bedoeld voor de bescherming tegen een aardbeving liever in zijn zak dan in het gebouw steekt?
Risicomanagement gaat over dat spel. Nemen wij een risico (accepteren wij het)? Of treffen wij maatregelen? En zo

ja, hoe serieus doen wij dat? Incidenten gebeuren nadat risicomanagement is gedaan, of anders gezegd, als een incident optreedt heeft risicomanagement geen zin meer. Dan is de fase van het crisismanagement aangebroken.

Bij crisismanagement gaat het om:
- redden;
- stabiliseren;
- herstellen;
- de draad weer oppakken.

Risicomanagement is proactief. Dat wil zeggen dat het erom gaat de organisatie voor te bereiden op mogelijke negatieve gebeurtenissen. Dat kan door maatregelen te treffen die kunnen voorkomen dat een incident optreedt (preventie) of die de schade kunnen beperken als het incident (onverhoopt)



toch optreedt (repressie). Reflexen en rituelen kunnen daarbij worden gemist. Studies en rapporten achteraf hebben beperkt effect. Als men daarvan wil leren dan kan dat alleen bedoeld zijn voor een volgend incident want dat is op dat moment nog een risico.

Het proces risicomanagement

Voor een doeltreffend proces voor risicomanagement is nodig:
- een verantwoordelijke (proces)-eigenaar die aanspreekbaar is zowel voor als na een incident;
- informatie en communicatie;
- kennis en inzicht in relaties tussen verschijnselen en gebeurtenissen;
- een bewuste keuze waarvoor de (proces)eigenaar staat.

Wie verantwoordelijk is, is altijd duidelijk ook al wil de (proces)eigenaar nog wel eens duiken voor een verantwoordelijkheid als dat even niet uitkomt. Informatie is per definitie nooit compleet. Wij weten nooit alles. Daarom moet een bewuste en verantwoorde beslissing worden genomen. De (proces) verantwoordelijke moet over de keuze die daarbij wordt gemaakt, duidelijk en open zijn tegenover de betrokkenen.

Een bekend voorbeeld waarbij dat mis is gegaan zijn de weerswaarschuwingen die in 2009 werden gegeven naar aanleiding van grote onweersbuien. Uit het verleden is bekend dat waarschuwen voor stormen nuttig kan zijn. En inderdaad, verschenen er aan het strand minder mensen. Maar ook op andere plaatsen bleken mensen de waarschuwing ter harte te hebben genomen en thuis te zijn gebleven in afwachting van de voorspelde stormen. Gelukkig bleek het weer zich wat anders te gedragen dan voorspeld waardoor het verwachtte noodweer uitbleef. Dat leverde veel kritiek op, de waarschuwing was 'voor niets' geweest want er kwam geen noodweer. De teleurstelling over het uitblijven van het noodweer leidde ertoe dat de bron van de waarschuwing, vervolgens het waarschuwingssysteem aanpaste. Het omgaan met onzekerheid is moeilijk. Dus is het wachten nu tot het weer eens een keer 'raak' is en de kritiek zich richt tegen de te slappe waarschuwing. Achteraf weten wij immers altijd alles precies.

Kennis en inzicht in de relaties tussen verschijnselen is een moeilijk onderwerp. Weliswaar weten wij heel veel maar op een aantal gebieden weten wij erg weinig. Zo is het niet moeilijk te voorspellen wat er gebeurt als een ijsblokje op het aanrecht wordt gelegd. Na verloop van tijd zal er een plasje water overblijven. Maar andersom is het niet zo eenvoudig een plasje water terug te herleiden op een gesmolten ijsblokje. Dit soort dingen zit de mens vaak in de weg. Twijfel en onzekerheid worden vaak gemaskeerd door grote woorden waar weinig achtergrond bij zit.

En dan de keuze van de (proces)eigenaar. Als hij kiest voor bungee jumpen, is dat een eigen keuze die een ander weinig aangaat. Net zoals het besluit zijn geld op een bepaalde rekening te zetten omdat iemand dat aanraadt, of omdat er zoveel rente wordt beloofd. Maar de proceseigenaar die diensten of producten aan anderen aanbiedt, heeft de plicht verantwoording af te leggen. Hij zal een open en transparant proces moeten kunnen tonen en duidelijk zijn over zijn keuzes, ook op het gebied van risico's. En dat dient te gebeuren nog voor een incident plaatsvindt zodat er een beroep mogelijk is. Ook over de maatregelen die zijn getroffen om risico's te beperken, zal duidelijkheid moeten worden gegeven. Op zich is het niet erg als maatregelen deels worden uitgesteld omdat er onvoldoende financiële ruimte is om een gewenst beveiligingsniveau te bereiken. Maar de (proces)eigenaar zal dan wel moeten laten weten hoe in de toekomst aan verdere verbetering gewerkt zal worden.

… en nu de mens nog

Wat doet de mens met risico's? De moderne mens is vrij (althans in delen van de wereld) en kan daarnaar handelen. Individuele ontplooiing heeft hoog aanzien en de ruimte die er is wordt volop benut. Grenzen vervagen op allerlei terreinen. Weliswaar zijn er nog zorgen maar er is ook veel zorgeloosheid. Er zijn instanties en buffers die tegenslagen kunnen opvangen. Er zijn ook veel spelregels maar die kunnen wij vaak ook ongestraft negeren als ons dat beter uitkomt. Kortom, wij denken onze risico's onder controle te hebben. Behalve dat risico's bewust of onbewust geaccepteerd kunnen worden, is

het ook mogelijk om maatregelen te treffen. Daarnaast kan ook nog worden geprobeerd een specifiek risico geheel uit te sluiten of over te dragen aan een andere partij.
Peter Bernstein[1] geeft in zijn definitie aan waar het om draait:
"The essence of risk management lies in maximizing the area's where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden for us".

Wij willen beheersen. En daarvoor is kennis nodig die wij in een aantal gevallen niet hebben. Risico's zijn daarvan een voorbeeld. Wij kennen de kansen niet waarmee een onzekere gebeurtenis zal optreden evenmin als de gevolgen daarvan. Maar wij kunnen ons daar wel een beeld van maken, en een poging doen de risico's in te schatten. Daarbij spelen aannames over de relatie tussen 'oorzaak en gevolg' een grote rol. Wat wij doen is een gedrag zoeken dat past bij de mate van onzekerheid en de kennis die wij denken te hebben.

Herkennen van risico's
Wij kunnen risico's tegenkomen op drie gebieden:
1. in technische systemen;
2. in organisatorische systemen;
3. bij de individuele mens die besluiten neemt, kiest en acteert.

De eerste twee zijn het resultaat van menselijk optreden en worden gekenmerkt door een doelstelling. Mensen daarentegen hebben belangen die bepalend zijn voor hun keuzes.
Risico's van technische systemen zijn eenvoudig. Er kan in een dergelijk systeem worden gemeten en er kan mee worden geëxperimenteerd. Het systeem doet wat 'erin is gestopt' en verzint zelf geen nieuwe dingen. Een technisch systeem heeft geen last van creativiteit of plotseling afwijkende gedachten. Terwijl de oorzaken van falen zijn toe te schrijven aan menselijk gedrag, wordt dat graag ontkend. De 'wet van Murphy' is daarvan een goed voorbeeld. De boterham met jam die altijd 'door het toeval' ondersteboven valt, is de uitdrukking van de neiging om falen buiten onszelf te plaatsen.

De wet van Murphy is een vereenvoudiging van wat Murphy bedoelde te zeggen. Een versimpeling die goed uitkomt want toeval is een prettiger verklaring van falen dan het eigen menselijk tekort. Murphy was chef van de constructieafdeling van Wright Air Development Center in Ohio. Zijn ervaring leerde hem het volgende[2]:
- *als er zich een probleem voordoet dan zijn er altijd meerdere oplossingen te vinden;*
- *bij deze oplossingen zijn er die 'goed' zijn maar ook oplossingen die verkeerd uitpakken;*
- *er zijn altijd mensen die erin slagen een 'niet goede' oplossing voor te stellen en door te drukken.*

Kortom, de mens speelt een belangrijker rol dan hij wil weten.

Voortdurend zijn er technische systemen die falen. De kranten worden ermee gevuld. Of het nu gaat om de HSL-veiligheidssystemen, de A73-tunnelbeveiliging, de aanleg van de metro in Amsterdam of Keulen, of een lekkende olieboorput in zee. Steeds zijn er 'verrassingen'. Maar wij blijven meten en vertrouwen hebben in de toekomst.

Organisatorische systemen werken bij de gratie van afspraken en regels. Daarmee kan star maar ook flexibel worden omgegaan. Meten is hier lastiger want het gedrag van de deelnemers staat niet altijd vast. Over het algemeen bepaalt de doelstelling van het systeem hoe het gedrag van de deelnemers zal zijn. Maar mensen doen wel eens iets anders dan is afgesproken. Er is sociale interactie dus kan nooit vooraf worden bepaald hoe zal worden omgegaan met een 'afwijking'. Falen betekent meestal dat de doelstelling niet wordt gehaald, maar daar kunnen inter-

SAP-implementatie nekt topman Sam

Business case ICT-systeem politie rammelt

Ondanks vele ict-rapporten, vele risicoanalyses en expertpublicaties in bijvoorbeeld Computable…

1 Peter Bernstein, Against the Gods, a remarkable story of risk, John Wiley & Sons 1996

2 Judith Stone, Das Grundgesetz vom scheitern, GEOwissen nr.1 1992

pretaties van worden gemaakt. Niet iedereen heeft hetzelfde oordeel over een gebeurtenis of afwijking. Zo zal de een roepen om het aftreden van de (proces)eigenaar terwijl de ander meer heil ziet in verbetering en vermeerdering van regels en afspraken. Zie wat er gebeurt rond de actuele financiële crisis. Kortom, er is onzekerheid over de vraag hoe wij omgaan met een falen van een organisatorisch systeem.

Het individu is de eigen baas (en dus proceseigenaar). Maar kent hij zijn eigen gedrag en de gevolgen daarvan? Wil hij die wel kennen? Flexibiliteit leidt tot snel aanpassen. Het individu is wendbaar en heeft vooral zijn eigenbelang als drijfveer. Rationaliteit speelt vaak een minder grote rol dan de intuïtie ook al ontkennen wij dat. Een duidelijk effect van het eigenbelang is het gemak waarmee wij een institutie of collectiviteit 'de schuld' geven van eigen falen.

De mens heeft een blinde vlek voor een aantal aspecten dat bij een risico hoort. Taleb[3] heeft daarvan mooie voorbeelden gegeven. Hij wijst er bijvoorbeeld op dat wij slecht kunnen omgaan met 'onvoorspelbare' gebeurtenissen. Door hem een zwarte zwaan genoemd naar het fenomeen dat tot in de 16e eeuw zwanen geacht werden wit te zijn. De eerste zwarte zwaan werd in de 16e eeuw in Australië gezien. Maar ook gebeurtenissen met een 'extreme impact' zijn voor mensen slecht te 'voorzien'. Bovendien wijst Taleb op onze neiging om achteraf gebeurtenissen toch nog voorstelbaar en voorspelbaar te noemen.

Onze beperkingen ten aanzien van onzekerheid wordt door Taleb onder meer geïllustreerd met een voorbeeld. Aan proefpersonen wordt de volgende vraag voorgelegd:
Wat is het meest waarschijnlijk?

- *Jan was gelukkig getrouwd, hij doodde zijn vrouw*
- *Jan was gelukkig getrouwd, hij doodde zijn vrouw om haar geld*

De meeste mensen kiezen voor optie 2. Rationeel is dat niet want optie 2 is ook van toepassing als voor 1 wordt gekozen. De verklaring zit in de neiging van de mens om een verklaring voor het doden te willen als de voorwaarde 'gelukkig getrouwd' geldt. Dat maakt het makkelijker te accepteren dat er iets gebeurt dat 'niet logisch' is.

Maatregelen treffen

Vooral na een incident worden maatregelen getroffen. Er is dan geleerd en de mens wordt creatief.
Een ander effect van een incident is vaak de reactie: 'dit mag nooit meer gebeuren'. Dat het hierbij vaak om rituele dansen gaat, moeten wij voor lief nemen. Als er een impuls vanuit gaat om risicomanagement serieuzer te nemen is dat een winstpunt. Helaas hebben veel maatregelen de vorm van regels en voorschriften. Dat zou nuttig zijn als het gedrag van mensen daar makkelijk door zou worden beïnvloed. Maar de handhaafbaarheid van veel regels is dubieus en daardoor zijn veel regels weinig effectief. Het argument dat er dankzij een regel een mogelijkheid is om achteraf te straffen, kan niet verhelpen dat de preventieve werking van regels beperkt is. Alleen in het geval dat de regels door betrokkenen 'vanzelfsprekend' in acht worden genomen gaat er een preventieve werking vanuit.

Deze mededeling hangt in een zaal in een museum in New York. Juridisch correct is de werking evenwel twijfelachtig. Wie kan overzien hoeveel mensen er in de zaal aanwezig zijn? Kan ik weten dat ik nummer 564 of hoger ben? En dan te bedenken dat de mededeling niet bij de entree hangt. Kortom, wat kan het effect zijn van deze maatregel?

Taleb geeft ook een voorbeeld van de beperkte denkkracht die de mens heeft om maatregelen als oplossing te bedenken. De ongeveer 3.000 slachtoffers van 9/11 worden ieder jaar herdacht. Aan de nabestaanden werd en wordt veel aandacht besteed. In de drie maanden na 9/11 zijn er in de Verenigde Staten echter duizend slachtoffers extra gevallen in het verkeer. Dat gebeurde omdat in die tijd velen niet durfden te vliegen en de auto namen. Meer autoritten betekent meer ongevallen. Maar aan deze slachtoffers van 9/11 wordt niet gedacht en hun nabestaanden hebben geen hulp gekregen.

Tenslotte

Tijdens de afgelopen 25 jaar is er op het gebied van risicomanagement veel gebeurd. Ook op het gebied van preventieve en repressieve maatregelen zijn er stappen gezet. Er wordt meer publieke aandacht gegeven aan risicomanagement en dat is winst. De mens blijft een onberekenbare factor. Maar de mens is ook creatief en kan innoveren. De mens gaat uitdagingen aan en kan leren. En dat betekent dat wij in de toekomst een plaats moeten inruimen voor de rol van de mens in alle onderdelen van het proces van risicomanagement.

Het Amsterdamse ICT-drama

De problemen bij de ict-trajecten van de gemeente Amsterdam beginnen 'Noord/Zuidlijn-proporties' aan te nemen.

3 Nassim Nicholas Taleb: Fooled by randomness, the hidden role of chance in life and in the markets Penguin Books, 2004 en The Black Swan, Penguin Books, 2007

DE MELDPLICHT DATALEKKEN: ZORG OF ZEGEN?

Mr Rachel Marbus is juridisch adviseur op het gebied van ICT & Recht en eigenaar van BetterID4ALL. Daarnaast is zij verbonden aan het Tilburg Institute for law, Technology, and Society (Tilt) waar ze zal promoveren op een proefschrift over identiteit en identiteitsmanagement in de online-wereld.

2011 wordt het jaar dat voor de gehele Europese Unie de meldplicht datalekken in werking zal treden. Als alles volgens planning verloopt, moet in de zomer de implementatie van de wet in Nederland gereed zijn. Vooralsnog geldt de meldplicht alleen voor telecommunicatiebedrijven (telco's) en Internet Service Providers (ISPs). Gezien de uitlatingen van mevrouw Kroes in de Digitale Agenda, is het de vraag of het daartoe beperkt blijft.[1]

Foto: Joe Gough

Uitbreiding van de plicht richting de gehele private sector staat in ieder geval op de EU-discussieagenda. En ook in Nederland is door Hirsch Ballin toegezegd dat een bredere meldplicht onderzocht gaat worden. Voorstanders zoals onder meer burgerrechtenorganisatie Bits of Freedom en de Consumentenbond staan hier uitermate positief tegenover. Mede vanuit de wens tot meer transparantie en openheid daar waar geknoeid wordt met de persoonlijke gegevens van burgers en klanten. Het bedrijfsleven wijfelt. De gevolgen van een dergelijke meldplicht kunnen groot zijn. Reputatieschade en praktische uitvoering lijken de meest voor de hand liggende factoren bij terughoudendheid. In dit artikel gaan we nader in op de meldplicht datalekken. Wat is het en hoe zal het gaan werken? Daarnaast worden enkele voor- en tegenargumenten op een rijtje gezet.

Wat is de meldplicht datalekken?

De meldplicht komt voort uit wijzigingen van de Europese privacy,- en telecommunicatiewetgeving[2]. Als een inbreuk heeft plaatsgevonden waarbij persoonsgegevens in het geding zijn, dan moet de nationale bevoegde instantie in kennis worden gesteld van dit datalek. Voor Nederland is dat het College bescherming persoonsgegevens. Dit moet zonder onnodige vertraging (lees eigenlijk 'vrijwel direct') gebeuren. Daarbovenop vereist de nieuwe regelgeving dat ook de personen om wiens gegevens het gaat een bericht ontvangen, echter, dan moet er wel sprake zijn van waarschijnlijk onnadelige gevolgen voor de persoonlijke levenssfeer van het individu. Er moeten dus mogelijk nadelige gevolgen voor de privacy van personen in het geding zijn. Zijn de gegevens bijvoorbeeld dermate versleuteld dat leesbaarheid daarvan niet erg aannemelijk is, dan mag die aanbieder ervan afzien om zijn klanten van het lek op de hoogte te brengen.

De nationaal bevoegde instantie kan de aanbieders zelfs dwingen om het datalek in de openbaarheid te brengen als ze van oordeel is dat de inbreuk ongunstige gevolgen kan hebben. Als aanbieder moet je in het geval van de melding wel een aantal zaken op orde hebben. Zo moet gemeld worden:

- de aard van de inbreuk op de persoonsgegevens;
- de contactpunten voor meer informatie;
- aanbevolen maatregelen om de gevolgen van de inbreuk te verlichten (voor degene wiens gegevens betrokken zijn in het lek);

- een omschrijving van de gevolgen, en;
- een omschrijving van de getroffen of voorgestelde maatregelen om de inbreuk daadwerkelijk aan te pakken.

De regeling kan zelfs zover strekken dat de nationaal bevoegde instantie specifieke aanwijzingen mag geven over hoe deze publieke kennisgeving gedaan moet worden. Daarbij moet worden gedacht aan de manier waarop (online, via de eigen website, in de landelijke media, enz.) en het toepasselijke formaat daarvan. Overigens, als de aanbieder verzaakt het datalek te melden aan de bevoegde nationale instantie, kunnen sancties worden opgelegd. Wat betreft het College bescherming persoonsgegevens kan dan worden gedacht aan een last onder dwangsom of een bestuurlijke boete[3]. En, daarbovenop kan dan dus nog eens die openbaarmaking van het lek komen.

Niet iedereen wacht op het verschijnen van de wetgeving. BoF heeft al enige tijd een eigen Zwartboek datalekken waarop verschillende forse lekken uitgebreid uit de doeken worden gedaan[4]. Dat het echt niet alleen maar gaat om uit burgerrechtelijke hoek gedane meldingen van datalekken, bewijst Gawker Media dat recentelijk in het openbaar te kennen gaf dat op de servers van het bedrijf een inbreuk had plaatsgevonden[5]. Bedrijven nemen dus ook zelf de verantwoordelijkheid op zich om lekken kenbaar te maken. Sterker nog, Gawker Media hield het niet alleen maar bij het melden dat er iets misgegaan was. Zo legde ze een uitgebreide FAQ aan waar gebruikers van hun websites onder meer kunnen lezen wat te doen als ze de account van Gawker-websites gelinkt hebben aan Facebook of Twitter, hoe de account van Gawker gedelete kan worden en waarin ook uitgebreid aandacht is voor datgene wat het bedrijf zelf doet om het lek te dichten en de gevolgen zoveel mogelijk te beperken.

Wat is er nu voor en wat is er nu tegen?

Overduidelijk pluspunt: meer privacybescherming voor individuen. Althans, meer wetenschap over het feit dat er een inbreuk heeft plaatsgevonden. Het kwaad is al wel geschied, maar dat is praktisch inherent aan een inbreuk op de privacy en wordt daarom door privacyspecialisten al geruime tijd een van de 'privacyparadoxen' genoemd[6]. Zijn de gegevens eenmaal overgegaan in andere handen, dan kan weliswaar actie ondernomen worden, maar de zaak kan nooit meer volledig ongedaan worden gemaakt. Wat een dergelijke meldplicht echter wel kan bewerkstelligen is dat bedrijven alerter zullen reageren indien er een inbreuk heeft plaatsgevonden en wellicht zullen zij ook meer toezien (voor zover mogelijk) op het voorkomen van dergelijke lekken. In zoverre zou de meldplicht dus ook een preventieve werking kunnen hebben. Daar staat echter wel tegenover dat een inbreuk dan ook daadwerkelijk moet kunnen worden opgemerkt. In het huidige voorstel van wet is een verplichting opgelegd om iedere inbreuk te melden. De onmogelijkheid van detectie van elke inbreuk en het feit dat ook geringe inbreuken gemeld zouden moeten worden, zijn dan ook van meet af aan kritiekpunten op de meldplicht geweest[7]. KPN geeft aan dat het 'lastig, zo niet onmogelijk' is om altijd te achterhalen of er een veiligheidsinbreuk heeft plaatsgevonden die mogelijke gevolgen heeft voor de privacy van een individu. Caiway, Tele2 en Vodafone lopen te hoop tegen de onmogelijkheid om elk lek te ontdekken. In hun reactie schrijven zij dan ook dat *"Indien een aanbieder veiligheidsmaatregelen heeft genomen die redelijkerwijs van hem kunnen worden verwacht, en hem een inbreuk op persoonsgegevens niet bekend is geworden, duidelijk zal moeten zijn dat hem niet kan worden verweten dat hij geen melding heeft gemaakt van de inbreuk[8]."*
In haar samenvatting van de consultatie stelt het Ministerie van EZ de betrokken partijen in zoverre gerust dat zij aangeeft dat er gevallen denkbaar zijn waarin het niet melden van een datalek de aanbieder niet verweten kan worden. "Wat betreft mogelijke uitvoeringsproblemen wordt het volgende opgemerkt. Op grond van artikel 11.3 [red: Telecommunicatiewet] dient de aanbieder van openbare elektronische communicatiediensten passende maatregelen te nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. Indien die beveiliging op orde is en er vindt een veiligheidsinbreuk plaats die waarschijnlijk zal leiden tot een aantasting van persoonsgegevens, en die inbreuk wordt niet opgemerkt, dan kan de aanbieder niet verweten worden dat hij de melding ervan heeft nagelaten. Een aanbieder behoeft en kan ook niet altijd op de hoogte zijn van het feit of als gevolg van een veiligheidsinbreuk er waarschijnlijk persoonsgegevens worden aangetast. Maar in veel gevallen zal de aanbieder voldoende aanwijzingen hebben dat bij het transport persoonsgegevens betrokken zijn[9]." De laatste zin laat raden dat de wetgever niet zo heel snel zal aannemen dat een aanbieder niets verweten kan worden.

Is het nu een zorg of een zegen?

Waarschijnlijk een beetje van beiden. De angst voor de publieke schandpaal doet menig bedrijf beven. Reputatieschade wordt over het geheel genomen toch vaak zwaarder gewogen dan de (geringe) boete van het College bescherming persoonsgegevens. Ook de praktische uitvoerbaarheid – het moeten melden van elk lek – zal vermoedelijk enige kopzorgen opleveren (om nog maar te zwijgen van de kosten, een aspect waar ook verschillende aanbieders op wezen binnen de consultatieronde op het wetsvoorstel). Maar toch ook een zegen. In ieder geval voor het individu wiens gegevens met enige regelmaat op straat lijken te liggen. Openbaarheid noopt wellicht tot meer voorzichtigheid. Hoe een en

ander in de praktijk daadwerkelijk zal uitpakken is vooralsnog gissen. Maar dat erover gepraat zal worden in 2011 staat in ieder geval vast. En, hopelijk zal ook serieus nagedacht worden over uitbreiding van de meldplicht. Datalekken komen namelijk echt niet alleen maar voor bij telco's en ISPs. Zo was zeer recent ook de klant van McDonalds de klos[10], lekte het KLPD een fax met tapgegevens[11], zagen miljoenen Amerikanen hun medische gegevens op straat liggen[12], lagen de medische gegevens van enkele Nederlanders bij de Kringloop[13], en werd een Amerikaanse bank aangeklaagd omdat zij een datalek had geprobeerd te verdoezelen[14].

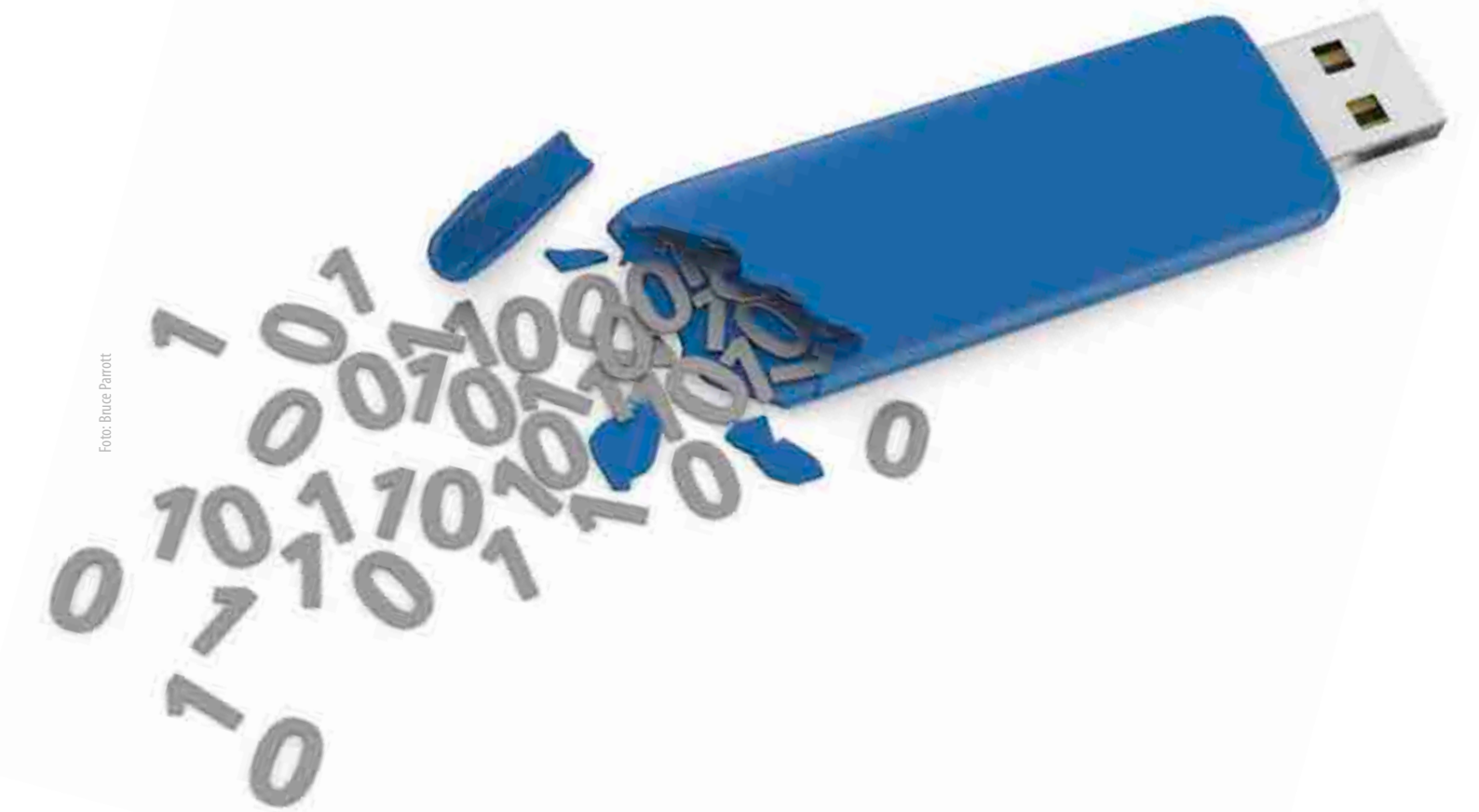


Foto: Bruce Parrott

1 Zie in de Digitale Agenda onder meer onder 'Versterking van vertrouwen en de beveiliging' waarin aangegeven wordt dat "Voorts kan worden nagedacht over acties om een website-exploitant ertoe te verplichten zijn gebruikers te informeren over beveiligingsinbreuken waarbij de gegevens van die gebruikers zijn betrokken."

2 richtlijn 2009/136/EG van het Europees Parlement en de raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

3 Artt. 65-75 Wbp.

4 Zie: www.bof.nl/category/zwartboek-datalekken/

5 Zie: http://lifehacker.com/5712785/faq-compromised-commenting-accounts-on-gawker-media

6 Een ander vaak gehoord paradox is dat personen vaak zeggen veel waarde te hechten aan privacy en dus niet willen dat bijvoorbeeld de overheid veel gegevens verwerkt, maar tegelijkertijd wel zelf gemakkelijk (door middel van social media) allerlei persoonlijke informatie delen. Zie bijvoorbeeld: S. Barnes, A privacy paradox: social networking in the United States, Firstmonday, vol. 11, no. 9, 4 September 2006.

7 Zie hierover bijvoorbeeld de reactie van KPN in de consultatieronde van het Ministerie van Economische Zaken over het voorontwerp van wet tot implementatie van Richtlijnen 2009/136/EG en 2009/140/EG (versie 15 april 2010), verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/

8 De reactie van Caiway, Tele2 en Vodafone in de consultatieronde van het Ministerie van Economische Zaken over het voorontwerp van wet tot implementatie van Richtlijnen 2009/136/EG en 2009/140/EG (versie 15 april 2010), verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/

9 Consultatieverslag wetsvoorstel implementatie gewijzigd Europees regelgevend kader (NRF) in de Telecommunicatiewet, verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/

10 Zie: T. Van Ringelestijn, Hackers stelen data McDonalds-klanten, Webwereld, 13 december 2010.

11 Zie: R. Zenger, Datalek: KLPD lekt fax met tapgegevens, 25 november, Zwartboek Datalekken BoF.

12 Zie: T. Van Ringelestijn, Miljoenen medische gegevens Amerikanen gelekt, Webwereld, 26 november 2010.

13 Zie: R. Zenger, Datalek: Medische gegevens in Kringloopwinkel, 13 december, Zwartboek Datalekken BoF.

14 Zie: D. Browning, U.S. bank allegedly concealed data breach, Star Tribune, 7 december 2010.

VERSLAG

EUROCLOUD NEDERLAND SYMPOSIUM

Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via lex.borger@domustechnica.com

Foto: Ron from York

Op 22 november 2010 was Microsoft Nederland gastheer voor het derde EuroCloud Nederland Symposium. Een van de speerpunten op deze middag was Cloud Security en twee redacteuren van dit blad waren uitgenodigd om hierover te debatteren.

Het was meteen na de opening een stoer gebaar dat Maurice van der Woude zijn presentatie helemaal via de cloud deed. Hij lichtte de digitale agenda van de Eurocommissie toe in een flitsende presentatie die zelfs Powerpoint powerusers even over hun hoofd zou doen krabben. Meteen hierna was het eerste debat van de middag, wat de visie van de overheid en de samenleving op Cloud Computing zou behandelen. Als je dan een lid van de Tweede Kamer in het debat plaatst, dan heb je ook gelijk een stuk diepgang bereikt. Brigitte van der Burg was veelvuldig aan het woord omdat ieder debatpunt wel op een of andere manier bij haar uitkwam. Opvallend genoeg ging het in dit debat ook snel over de veiligheid van de cloud. Ook het gebrek aan adoptie in de Nederlandse overheid was een terugkerend thema. We moeten de nieuwe regering nog even wat meer tijd geven... Ramon Chaloi presenteerde de eerste voorzichtige conclusies van zijn wetenschappelijk onderzoek in deze richting.

Na de pauze was het thema direct beveiliging, met eerst een presentatie van de ervaringen van Marcel Jak (DigiNotar), met daaropvolgend het debat hierover. De, door de organisatie bedachte, stelling was: 'De cloud is niet veilig te krijgen'. Remco Bakker modereerde het debat tussen tegenstander Lex Borger en voorstander Gerrit Post, en liet zijn onpartijdigheid bij vlagen rustig liggen. Het debat werd een vervolg op discussies die voor de pauze al gestart waren. Met name Mike Chung (KPMG) wist deze brug effectief te slaan. Uitkomst? De cloud is (nog) niet veilig. Maar… de cloud afserveren vanwege onveiligheid kan niet. Er kan nog veel meer worden gedaan. Veel maatregelen zullen in overeenkomsten afgesproken moeten worden. De vraag is dan wel op welke manier dat allemaal moet worden gecontroleerd en gehandhaafd.

Links

www.eurocloudnl.eu

www.eurocloud.org

http://prezi.com/9me2eey5dqqb/de-digitale-agenda/

TRENDS IN IT-BEVEILIGING 2011

Remco Bakker is sinds 1996 actief in de informatiebeveiliging en momenteel werkzaam als resource manager voor Cqure, detacheringsbedrijf voor IT Security professionals. Hij is bereikbaar via remco.bakker@cqure.nl.
Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is een van de redacteuren van het blad Informatiebeveiliging en editor van een schriftelijke CISSP-cursus. Hij is bereikbaar via lex.dunn@capgemini.com.

Op 16 december vond in een luxe hotel in Soestduinen de presentatie van alweer de zevende editie van het boekje Trends in IT-Beveiliging plaats. Ondanks de slechte weersverwachting (die aan het einde van de middag inderdaad bewaarheid werd) was er een grote opkomst van PvIB-leden. Dit was de eerste keer dat de presentatie van het jaarlijkse boekje voor alle PviB-leden openstond. Voorheen was dit alleen voorbehouden aan de leden met het managementpakket.

PvIB-voorzitter Fred van Noord opende de bijeenkomst. Hij vertelde dat het boekje (een gezamenlijke inspanning van Cees Coumou, Loek Sleper en Kees van der Zwan) na de sessie voor alle aanwezigen beschikbaar was.
De eerste presentatie werd verzorgd door Han van der Zee van Atos Consulting, en tevens hoogleraar Business Transformation and IT aan de Universiteit van Tilburg. Hij begon zijn betoog met een citaat van Douglas Engelbart (de uitvinder van de computermuis) uit 1956, die voorzag dat IT op den duur zou worden ingezet om complexe en urgente wereldproblemen op te lossen. Om dit mogelijk te maken zou het open uitwisselen van informatie en ideeën mogelijk moeten zijn. Vandaar dat Van der Zee stelde dat het einde van informatiebeveiliging nabij is. Een tamelijk prikkelende stelling in een zaal vol met IB'ers!
Van der Zee liet drie verschillende tijdperken zien, het begon allemaal met de 'DP-era', de tijd van het mainframe (DP = Data Processing) met zijn centrale beheer en de klassieke beheerder. Na zo'n twintig jaar begon de volgende periode, de 'IT-era' met in netwerken gekoppelde kleinere computers en de opkomst van de pc's. Tussen deze beide perioden zat een technische discontinuïteit (denk aan het verschil in belevingswereld tussen de 'mainframe manager' en zijn klanten, die liever hun eigen computers wilden hebben).

Groot vertrouwen in leveranciers

Social discontinuity
Vandaag de dag zitten we in de 'Network-era', waarin vele koppelingen tussen systemen bestaan, en de data belangrijker is dan waar het staat, of wie het beheert. We zien nu dus een organisatorische discontinuïteit en Van der Zee voorspelt het einde van bedrijven die niet meegaan met deze nieuwe ontwikkeling. Informatiestromen zijn overal, straks zelfs op (en misschien in) het menselijk lichaam. Gebruikers bepalen zelf waar, wanneer en hoe ze informatie willen consumeren (any place, any time, any where, any device) en laten zich weinig gelegen liggen aan de inherente risico's. We stevenen volgens Van der Zee dan ook af op de volgende discontinuïteit: een 'social discontinuity'. Er ontstaat een verschil tussen de mensen die de nieuwe gadgets, technologie en mogelijkheden omarmen, en zij die dat niet doen. Op basis van deze ontwikkelingen vraagt Van der Zee zich af of er nog plaats is voor informatiebeveiliging. Argumenten waarom IB zou uitsterven kwamen echter weinig naar voren in zijn betoog.

Omslag van het boek

Zevende editie
Hierna was de beurt aan Coumou om de zevende editie van het Trends boekje toe te lichten. De bedoeling van deze boekjes is altijd geweest om:
- IB onder de aandacht te brengen;
- in een voor niet-IB'ers leesbaar verhaal;
- met interessante gesprekken aan de hand van een thema.

Het thema voor de 2011-versie is de (on)mogelijkheid om een acceptabel niveau van IT-beveiliging te bereiken. Over dit thema zijn zeven personen door de samensteller geïnterviewd. Coumou gaf aan dat de conclusies uit de editie van 2010 nog steeds actueel bleken te zijn:

- IT-beveiliging is niet vrijblijvend meer;
- de leertijd is voorbij, het is nu tijd om dingen te doen;
- maar dat lukt alleen met anderen.

Coumou gaf aan dat de samenstellers aan de hand van het thema zoeken naar begeleidend beeldmateriaal. Dit jaar zijn de illustraties van de hand van Anne-Marie Abcouwer. Voorbeelden van haar werk hingen in de vergaderruimte.

Hierna overhandigde Van Noord namens SDU de eerste exemplaren van het boekje aan de drie samenstellers, die daarna door Bart van Staveren en Hans van Linschooten met bloemen en een goed gekozen beeldje in het zonnetje werden gezet als dank voor de zeven edities. Vanaf volgend jaar zal een andere redactie het boekje gaan verzorgen, maar voor de 2012-editie zullen ze nog ondersteuning krijgen van deze drie 'eminences grises' van de Nederlandse IT-beveiliging. Voor de details verwijzen we graag naar het boekje zelf aan alle PvIB-leden wordt verstrekt.

Groot vertrouwen in leveranciers
In de volgende presentatie ging Herbert van Zijl (Unit4) in op 'verantwoordelijkheid'. Hij gaf inzicht in verantwoordelijkheid van leveranciers van software (zoals ERP), en de verantwoordelijkheid van afnemers / gebruikers van die software. De praktijk wijst uit dat bij het midden- en kleinbedrijf een (soms te) groot vertrouwen bestaat in leveranciers. Grotere bedrijven geven meestal blijk van meer inzicht in IT-beveiliging. Daarbij zijn er grote verschillen in de mate van openheid. Zo blijkt de Noorse belastingdienst de aangiften van alle Noren gewoon voor iedereen toegankelijk op internet te publiceren.

Verschillende verschijningsvormen van Cyber-bedreigingen

Cybersecurity
Na de pauze, waarin ruimschoots door de aanwezigen genetwerkt werd, was het woord aan Ronald Prins, CEO van Fox-IT, met een presentatie over de trends in Cybersecurity. Hij nam de gelegenheid te baat om een oproep te doen aan de Nederlandse overheid om een actieve rol te spelen in de bestrijding van de verschillende vormen van criminaliteit in Cyberspace.

Voor het gemak wordt vaak gesproken over Cybercrime. Maar in zijn presentatie maakt Prins duidelijk, dat onderscheid moet worden gemaakt naar oorlogsvoering, spionage en 'gewone' cybercriminaliteit, die ook door verschillende overheidsdiensten worden bestreken.
Zo kennen we Cyberwar, electronische oorlogsvoering, met als typerend voorbeeld Stuxnet, met als corresponderende overheidsdienst (het ministerie van) Defensie.

Oorlogen worden niet langer alleen om grondgebied gevoerd, maar staten voeren oorlog om economisch voordeel te behalen. Ook worden cyberdivisies ingezet naast conventionele legers, een recent voorbeeld zijn de aanvallen op vitale infrastructuur van Georgië door Rusland. Een vertrouwelijk FBI-rapport geeft aan dat China in het diepste geheim een leger van 180.000 cyberspionnen heeft, dat in potentie in staat geacht moet worden om vitale infrastructuur te vernietigen, bancaire systemen te verstoren en zelfs gevoelige militaire informatie te compromitteren. Effectiever dan bommen? Hier zien we in ieder geval, dat Cyberspionage, het werkterrein van de AIVD en MIVD, op veel terreinen dicht tegen de oorlogsvoering aan ligt. Spionage is dan ook van alle tijden en wordt ook bij tariefsonderhandelingen op tal van terreinen tussen overheden ingezet. Helaas is de awareness op dit gebied nog steeds een ondergeschoven kindje in ons land. In bijvoorbeeld het Verenigd Koninkrijk wordt actief beleid gevoerd om langs deze weg (economisch) voordeel te behalen.
Cybercrime kennen we, volgens Prins, in onder meer de verschillende vormen van fraude, inbraak, maar ook de bestrijding van zaken als kinderpornografie, waar de bestrijding op het terrein van politie en openbaar ministerie ligt. Financiele fraude is inmiddels een miljarden business geworden, waarbij criminelen een bijzonder effectieve eigen marktplaats hebben gebouwd, waar vraag en aanbod van warez, gebouwd door goed opgeleide mensen gekoppeld worden aan professionele lever- en betaalsystemen. Ook 'traditionele' vormen van hacking, waarbij criminelen anderen, bij voorkeur jonge kinderen, misbruiken door in chats hun webcams op afstand open te zetten, wordt hieronder gerekend. Kinderpornografie is strikt genomen geen vorm van cybercriminaliteit, maar gebruikt veel techniek om te verhullen en te verbergen wat het licht niet kan zien. Zolang sommige politici menen, dat 'deep packet inspection' de oplossing voor de bestrijding van dit gruwelijke fenomeen is, zijn we nog ver verwijderd van het aanpakken van de vervaardigers.

Too little, too late?

Bij het beantwoorden van de vraag 'wat hier aan te doen' haalt Prins allereerst het voorbeeld aan van minister De Jager, die op Twitter trots meldde met zijn Android buiten de reguliere beveiligingsmaatregelen om zijn mail te lezen. Of bewindslieden zich realiseren wat de implicaties van hun voorbeeld zijn, valt te betwijfelen, maar volgens hem hebben informatiebeveiligers hier geen antwoord op. Dit geeft aan, dat de aanpak van informatiebeveiliging tot een maand geleden nog altijd niet op het juiste, hoogste niveau geadresseerd werd. Wat dat betreft zijn WikiLeaks en het in vervolg daarop platleggen van sites als om.nl een godsgeschenk. Terecht wordt vastgesteld, dat de rol van de overheid over vele departementen en diensten verspreid is, hetgeen een gecoördineerde en effectieve aanpak niet direct ten goede lijkt te komen. Ook spelen hier tegenstrijdige belangen en blijft Nederland jammer genoeg achter bij het ontwikkelen van een nationale Cybersecurity-strategie, waar landen als de VS, de UK en Frankrijk al veel verder zijn. Momenteel vindt een consultatie van private partijen plaats en verwacht de Tweede Kamer in maart volgend jaar een actieplan. Volgens Prins niet direct een toonbeeld van doelgericht, gecoördineerd en effectief overheidsoptreden.
Prins hoopt op een toonbeeld van doelgericht, gecoördineerd en effectief overheidsoptreden. Ze dient zich bewust te zijn van haar beveiligingstaak voor het publiek, die verder gaat dan de spam-bestrijding door de OPTA, of de tandenloze bestrijding van de overtredingen van de wet op de privacy. Ook moeten preventieve maatregelen worden afgedwongen op vitale infrastructuren en diensten. Het is toch op zijn minst vreemd te noemen, dat de kwaliteit van ons drinkwater op tal van manieren wordt beschermd, op basis van wettelijke voorschriften, maar dat de bescherming van de bijbehorende IT-infrastructuur volledig vrijgelaten wordt?
Ook ziet hij graag een samenvoeging van de verschillende overheidsdiensten op dit terrein, op operationeel gebied voegden bijvoorbeeld de Engelsen hun afluister- en e-spionage-afdelingen met groot succes samen.
Prins' laatste wens is voor een wettelijk kader om opsporing te kunnen doen. Zoals de VS nu servers buiten hun landsgrenzen uitzetten, moet dat ook door de bevoegde Nederlandse instanties gedaan kunnen worden.
Maar hij stelt vast, dat de overheid nu in ieder geval (nog) niet de baas is op het internet. Sterker nog, door de aard van het internet zal zij dit wellicht ook nooit echt worden en zijn de mensen die het internet maakten tot wat het is medehandhavers van de orde. Voorwaar, er ligt een schone taak voor een actieve rol van de informatiebeveiligers!
Tot slot werd door een panel onder leiding van Wijnand Westerveld (hoofdredacteur Automatiserings Gids) aan de hand van een aantal stellingen gediscussieerd over IT-Beveiliging. Daarbij werd vanuit de aanwezigen in de zaal ook gereageerd op de uitspraken van het panel.

Wie is de baas op het internet?

Wensenlijst van Ronald Prins

REGISTER INFORMATIEBEVEILIGING 2010

ARTIKELEN

ACHTER HET NIEUWS

BOEKBESPREKING

COLUMN

INTERVIEW

OVERIG

VERSLAGEN

KENNISMAKING MET…

COLOFON

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Borger (Domus Technica)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
Rachel Marbus (BetterID4all)
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

ISSN 1569-1063

WIKILEAKS

Op de verjaardagen die ik regelmatig (moet) bezoeken is momenteel een onderwerp erg geliefd. Namelijk, de lotgevallen van Julian Assange. Tot voor kort had nog niemand van deze man gehoord maar inmiddels kent de hele wereld hem. En niet alleen vanwege zijn ontboezemingen op internet maar ook door het krachtenspel wat hij op gang zette. Nadat hij honderdduizenden documenten op internet zette werd een groot aantal 'belangrijke' mensen in de wereld angstig. Bijzonder angstig zelfs, omdat allerlei zaken boven tafel komen die eigenlijk niet onthuld mochten worden.

Shell maakt zich bijzonder druk omdat de wijze van handelen in Afrika niet direct een schoonheidsprijs verdient. En daarmee druk ik mij voorzichtig uit. Regeringen rollen over elkaar heen omdat alle achterkamerpolitiek ineens op de voorpagina staat. Verborgen agenda's zijn ineens niet meer verborgen en daar worden veel mensen heel zenuwachtig van.
Die zenuwachtige mensen doen rare dingen. Ze dreigen bedrijven dat ze hen zullen boycotten als ze langer zaken doen met deze verklikker. Sommige bedrijven sluiten meneer Assange af en verzorgen zijn betalingsverkeer niet meer. Andere bedrijven zorgen ervoor dat meneer Assange niet in de top 10 topics komt te staan terwijl deze daar wel degelijk had thuisgehoord.
Dat geeft wederom reacties vanuit de hackerswereld. Zij vallen instellingen aan die meebuigen met de tegenstanders van Assange. Beginnende hackers worden gepakt door de politie omdat ze een hackaanval op hun privé machientjes uitvoeren. In mijn jeugd gingen we naar Den Haag om daar op het Binnenhof te demonstreren. Of we bezetten een ambassade. Tegenwoordig hoef je de deur niet eens meer uit om je stem te laten horen. Lekker makkelijk. Politici geven aan dat ze een verbod zullen uitvaardigen om de pagina's langer aan te bieden. Anderen (die blijkbaar de afgelopen jaren onder een steen hebben geleefd) roepen dat ze alle pagina's van internet zullen laten verwijderen. Kortom, paniek in de wereld. Alleen maar omdat allerlei geheimpjes naar buiten dreigen te komen.

Assange geeft zich zelf aan in Engeland, en een tijdelijke vrijlating op borgtocht zit er niet in. Zweden wil de man eigenlijk uitgeleverd hebben op basis van zeer sterk doorgeschoten wetgeving waarop Assange zich moet verdedigen. Amerika wil Assange eigenlijk ook hebben om ervoor te zorgen dat er niet verder wordt gepubliceerd. Ook in Amerika leven ze blijkbaar al jaren onder de eerder genoemde steen want Assange arresteren betekent echt niet dat de publicaties stoppen. Het grappige is dat er altijd over ethiek wordt gesproken op het moment dat de discussie in huiselijke kring wordt gevoerd. Assange zou geen documenten mogen publiceren die hij via onrechtmatige weg heeft verkregen. Assange mag niet publiceren over de onrechtmatige zaken die in de documenten worden beschreven. Assange is van huis uit een hacker en met hackers heb ik een haat-liefde verhouding. Ik ben tegen het destructief hacken, maar verdien er wel mijn brood mee. Ik ben tegen het stelen van wat dan ook maar heb bewondering voor het feit dat deze documenten blijkbaar overal voor het grijpen liggen. Ik kan anonieme protestacties niet waarderen maar ben verrast dat een van oorsprong individualistisch werkende hacker ineens georganiseerd gaat aanvallen. We zijn in een nieuwe fase beland van het internet. Het internet bevat veel informatie waarvan een groot deel geheim zou moeten blijven maar dat gaat niet meer lukken. We gaan een tijdperk in waarin informatie beschikbaar komt waarmee eindelijk de verborgen agenda's opengeslagen worden. Openheid is goed, achterkamertjespolitiek is uit.

Uit mijn reactie mag blijken dat ik sympathie voel voor Assange en zijn vele metgezellen. Niet dat ik zover ga om mee te werken aan een dDos aanval op een van de vele doelen die zich nog zullen aandienen, maar het wordt pijnlijk duidelijk dat niet iedereen op deze aardbol die openheid en transparantie betracht die mij voorstaat. Ik ben benieuwd of er ooit nog een Assange binnen ons bedrijf opstaat, of een Assange binnen de DSB. Of misschien zou het ook wel leuk zijn als er binnen ABN-AMRO een opstond. Ik kan mij heel veel bedrijven en instanties bedenken waarvan we bijna zeker weten dat er veel meer gebeurt dan ons wordt verteld maar wat we nooit te weten komen. Misschien is dat ook wel goed.

Groetjes,
Berry

Hét alternatief voor FTP!

Gratis evaluatie
via www.crypsys.nl!

· Uitwisselen van grote bestanden tot 2GB
· Leverbaar als server, virtual server of appliance
· Ontvang een bevestiging van download
· Veilige opslag en verzending

cryptshare®

CRYPSYS Data Security B.V. - Benelux Distributeur van Cryptshare
www.crypsys.nl - sales@crypsys.nl - (0183) 62 44 44

CRYPSYS