meij 2009 nummer 3

INFORMATIEBEVEILIGING

Business Continuity Management steeds hoger op agenda

Hoe gaan we om met ambient intelligence en convergerende technologie?

‘Artikel van het jaar 2008’ - En de winnaar is...

The impact of Cloud Computing on Identity

Op weg naar convergentie van IT- en fysieke beveiliging

ib

PvIB
Platform voor InformatieBeveiliging

Voorwoord/colofon

Beste lezer,

Dit is een belangrijk nummer. We maken bekend wat het beste artikel uit de jaargang 2008 is geweest. We hebben een deskundige jury gevraagd om uit een door de redactie opgestelde shortlist het beste artikel te kiezen. Dat is gelukt en ik denk dat we tevreden mogen zijn met het resultaat. Het winnende artikel publiceren we nogmaals in dit nummer vanaf pagina 23.

Dit nummer is ook belangrijk omdat het het laatste nummer is dat wordt samengesteld en vormgegeven door een tweetal belangrijke mensen: Sandra Kagie, onze eindredacteur, en Ron Toonen die de grafische vormgeving voor zijn rekening heeft genomen. Zij zijn al heel wat jaren betrokken geweest bij deze uitgave en volgens mij hebben zij een heel belangrijke bijdrage geleverd aan het blad zoals dat ook nu weer voor u ligt. Wij als redactie vinden het heel jammer dat de samenwerking wordt beëindigd, maar we zijn blij dat we zo lang hebben kunnen samenwerken. We zullen als redactie de periode wel afsluiten met een gezamenlijk etentje.

Sandra en Ron: Hartelijk dank!

In dit nummer hebben we verder een grote diversiteit aan onderwerpen. We zijn blij dat we een hoogst actueel artikel kunnen plaatsen over de gevolgen van de financiële crisis voor Informatiebeveiliging. Said el Aoufi promoveert binnenkort met een verhandeling over de economische aspecten van informatiebeveiliging en de financiële crisis is bij hem in goede handen.

We hebben twee artikelen die bovendien actueel zijn omdat ze een vervolg zijn op het Claims Based Access Control-verhaal uit het vorige nummer: een artikel over ontwikkelingen rond Identity Provisioning en 'the cloud' van Stuart Boardman en Michael Boley en twee pagina's van mijn hand over het ontbreken van Identity Providers.

De afgelopen jaren hebben we diverse specials gepubliceerd. We hebben daarbij al aangegeven dat zo'n special het bewuste onderwerp niet uitputtend kan behandelen. Dat bewijs wordt in dit nummer opnieuw geleverd door een vervolg op de privacy special van vorig jaar, met een artikel van Anton Vedder over ambient technology en een vervolg op de BCM special met een artikel van Sjoerd Vredenberg en Tim Willems over BCM tooling.

Een laatste uitgebreider artikel gaat over de integratie tussen logische en fysieke beveiliging. Altijd een nuttig onderwerp waarover David Ting ons bijpraat.

Hendrikus Beck schrijft over ontwikkelingen binnen het CIO platform, hierbinnen is een aantal werkgroepen bezig met het uitwerken van een aantal interessante onderwerpen, namelijk Benchmarking en Enduser Empowerment.

De laatste bijdragen komen van 'eigen' redacteuren, namelijk een bespreking van Lex Borger van het boek Zen and the art of Information Security (ik ben net bezig met motoronderhoud) en een introductie van een serie interviews met IB-functionarissen door Tom Bakker.

We hadden helaas geen ruimte meer voor de Questafette, die houdt u van ons tegoed.

Groetjes,
André Koot,
Hoofdredacteur

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
Sandra Kagie (eindredacteur,
TOPpers Media bv, Berlicum),
e-mail: sk@toppers.nl

Redactieraad
Tom Bakker (Delta Lloyd)
Mario de Boer (Logica)
Lex Borger (Domus technica)
Lex Dunn (Capgemini)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Henk Meeuwisse (Sogeti)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Ontwerp/Vormgeving
Ron Toonen, TOPpers Media bv, Berlicum

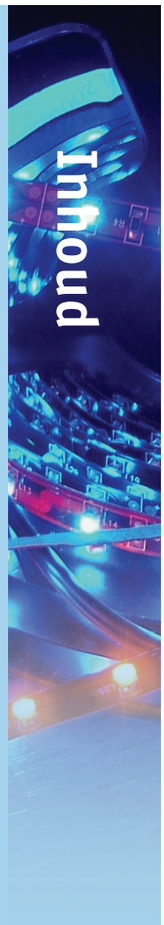
Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

Druk
Roto Smeets GrafiServices Eindhoven

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



Mijn fascinatie

'Optimale beveiliging van informatie via netwerken'

Informatie altijd en overal. Van bedrijf, overheid of particulier, voor iedereen beschikbaar. Via elk netwerk en op elk denkbaar apparaat. Prachtig, maar dat alles stelt zeer hoge eisen aan de beveiliging. Want veel informatie is lang niet voor iedereen bedoeld. Dat fascineert mij. Bij TNO werk ik aan innovatieve oplossingen om informatie die via netwerken wordt uitgewisseld, optimaal te beveiligen voor onze klanten. TNO Informatie- en Communicatietechnologie is op zoek naar een:

Senior Consultant Security

Onze afdeling bestaat uit 25 experts, gevestigd in Delft. Wij ontwikkelen innovatieve oplossingen om informatie via alle mogelijke vaste en mobiele netwerken te beveiligen, voor nationale en internationale klanten. Denk daarbij aan privacy, integriteit, authenticiteit, encryptie.

Jouw fascinatie?
Je adviseert bedrijven en organisaties over informatiebeveiliging. Je bent verantwoordelijk voor het aquireren en realiseren van security-projecten. Je hebt diepgaande kennis van de materie, langdurige ervaring en je maakt gebruik van innovatieve methodieken. Daarmee weet je potentiële klanten te overtuigen. Je signaleert trends en vertaalt deze naar concrete visies. Als brug tussen opdrachtgever en afdeling zet je behoeften van de klant om in concrete oplossingen.

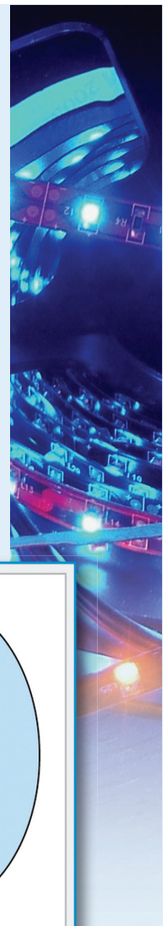
Meer weten?
Kijk op www.werkenbijTNO.NL of neem contact op met Paul de Jager (afdelingsmanager), 050-5857721 of Marleen Vrolijk (Recruitment), 015-2857326.

TNO

werkenbijTNO.NL

Identity In The Fog - New Radar Needed

Auteurs: Stuart Boardman en Michael Boley > Stuart is Director of Consulting bij CGI. Hij is per e-mail bereikbaar via stuart.boardman@cgi.com. Michael is Director Business Development for Identity and Access Management. Hij is bereikbaar via michael.boley@cgi.com.



There is little real agreement in the IT world about what exactly 'the cloud' contains and there are enough bloggers who consider it to be pure vapour. Our approach in this article is to treat the cloud as an aggregation of all recent developments, business *and* technical, which affect how we use the internet today. We focus on three loosely related phenomena: the Extended Enterprise, the Web 2.0 paradigm and Internet based IT services (the narrower definition of Cloud computing). Together these phenomena are creating a need for radical changes in the way technology supports business. Just moving the old solution into the new environment does not address this need. Worse still it can lead to a hopeless increase in complexity. Nowhere is this more true than in Identity and Access Management (IAM). We show how these changes apply to IAM and how the approach to IAM can be a critical factor in the success or failure of the brave new world in the clouds.

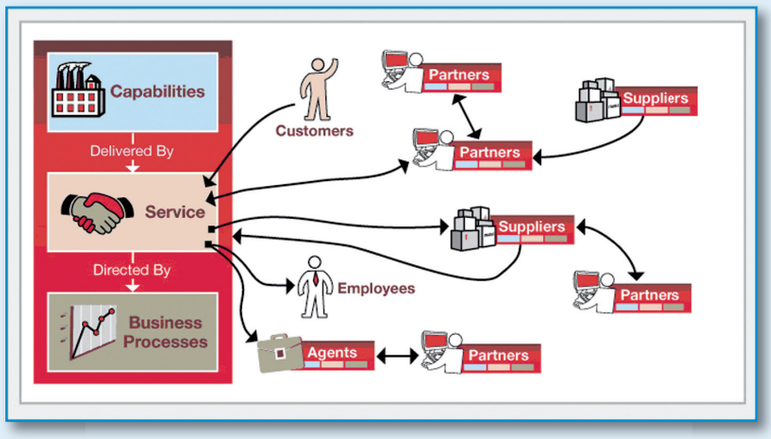
One thing is true about a cloud. There is less to it than meets the eye. Unless you're in it - and then it's fog.[1]

The Extended Enterprise is a term originated by Forrester[2], which captures a business model in which an enterprise's business processes increasingly involve activities carried out by partners and suppliers. The classic example used to illustrate this is Dell, a 'computer manufacturer' that really does little more than capture an order and supervise its fulfillment by a network of partners and suppliers (independent legal entities). All of these entities can and do perform similar work for other partners (the mother board in your Dell computer is probably identical to one in a Brand X computer).

Moreover the partnership process can be bi-directional in the sense that business processes can originate with any of these entities (not just the big one on the left). The result is not just a value chain but a value *network*.

Now this phenomenon is not particularly new. What is new is the extent to which the processes are becoming automated. It is this aspect that creates challenges for IAM. Once upon a time the world of enterprise IT was more or less exclusively concerned with what happened *inside* an enterprise. There was a clear border between 'inside' and 'outside'.

Figure 1 The Extended Enterprise



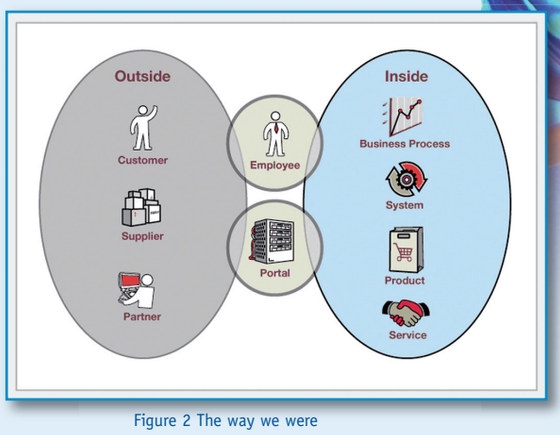


Figure 2 The way we were

The influence of the Extended Enterprise and of also Web 2.0, which we will discuss later, is causing these boundaries to erode. The outside is inside.

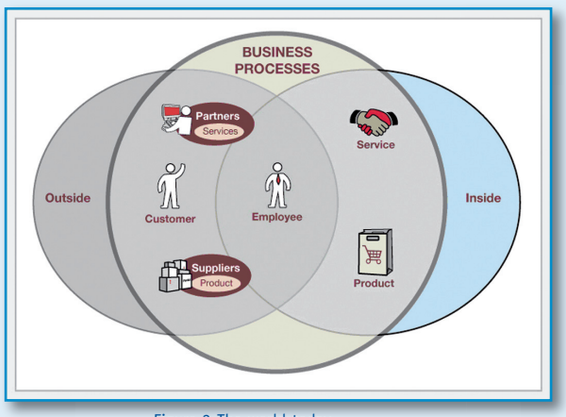


Figure 3 The world today

Effect on IAM

From the IAM point of view the most obvious consequence is the need for federation. Enterprises simply cannot maintain user repositories for all the individuals (employees of partner enterprises, customers) that may make legitimate use of the enterprise's services. And why would they want to manage all these individuals, when they are able to delegate or outsource these activities to their partners just as they do with other services they provide?

[1] Credit where credit is due. The term "fog computing" was coined (as far as we know) by André Koot, editor of this magazine.

[2] Other analysts use their own terms with the same meaning. Forrester's is the best known and most descriptive.

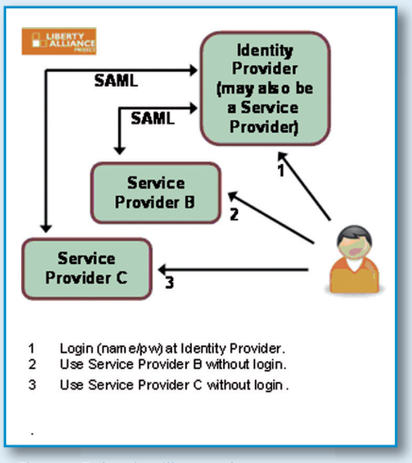


Figure 4 Federation illustrated

Another, less obvious consequence is that already strained role based access (RBAC) systems cannot reasonably manage roles for large numbers of unknown service consumers, some of which may themselves be automated systems. This makes the possibilities of claims based access control (CBAC) very interesting to consider.

Web 2.0

When we talk about Web 2.0 we are not so much concerned with specific technologies as with the use paradigm. What is really significant is the increasingly pervasive presence of the internet in all kinds of commercial (eCommerce), governmental (eGovernment) and purely personal activities (social networking, user generated content etc). In parallel we see that connection to the internet takes place from multiple devices in multiple contexts. We call this ubiquitous connectivity.

Personalization and Profiles

One of the main features of so called Web 2.0 is the drive to offer personalized services to each consumer. In the first place this raised the issue of knowing the consumer. Registration to web pages with underlying profile generation became common. Community services like Facebook or Linkedin understand these profiles as the main value for the provider but also for the consumer.

Users build up profiles and like to be guided within these services based on their interests or more generally the (personal) information they are sharing. Especially in business related communities the value of the profile is directly related to the upcoming opportunities and connections one receives. Having connections and using this profile for business purposes is the value for the consumer and to generate this value one is willing to share personal data.

Advertising companies want to know as much as possible about their target groups in order to make advertisements personalized and target specific. Having community providers who are able to provide this kind of information accurately and up to date opens new possibilities in this space. Facebook tried to change their terms and conditions recently to open the possibility to share all the data they stored of their users for purposes like advertisement. Due to heavy criticism they had to withdraw this attempt but nevertheless especially Facebook has a well established market for profile data. By offering an application framework for 3rd party providers they can share the profile and user data with all of these providers when someone uses the application. There are several – more or less official – groups within the platform to sell and exchange user data (e.g. selling 10.000 up to date profiles of students in Oxford).

This is another example of changing environments in the Internet. Mashed-up services are becoming more and more common. Services provided by external partners are integrated into other sites and have to share user data or profile information, at least information to enable the functionality in a personalized way. The best example might be Google Maps which is more and more integrated into several other services providing map information, route planning etc.

Ubiquitous connectivity (Anywhere[3])

Another feature is the seemingly unstoppable trend to use Web 2.0 services device independently. In other words people want to use the same services in more or less the same way on whatever device happens to be available or convenient at any one time. Not only Desktop computers but also Laptops, Netbooks, games consoles and mobile phones are used to access the internet. There is even the possibility to access via car specific devices. This emerging trend of mobile internet access with all devices raises the issue how to identify the user who is accessing the service. A purely mobile identity solution (i.e. a solution for mobile devices) is not enough. Access and authentication services must not limit access but have to provide a user experience which is similar and easy on every device. A *mobilized* identity, accessible without limitations but capable of being combined with a device specific security behavior is essential.

Figure 5 Ubiquitous connectivity

Effect on IAM

If Web 2.0 has been largely about the changed use of the Internet by individuals, it's hardly surprising that User-centric Identity (also sometimes known as Identity 2.0) has emerged from the same set of relationships.

User centric identity addresses complex registration, authentication and to some extent also authorization. Central to this approach is that there are three different parties involved: the user, the service provider and a new figure, the identity provider.

What's new in User-centric Identity are the control given to the user and the role of identity provider. The user forwards the request of the relying party to an identity provider who is able to provide the requested information (claims), provides his identification data to this provider and

[3] The Yankee group has developed a concept called Anywhere, which explores these tendencies in some depth.

receives a validated set of information to be handed over to the relying party who is able to verify and accept the data by trusting or communicating with the identity provider.

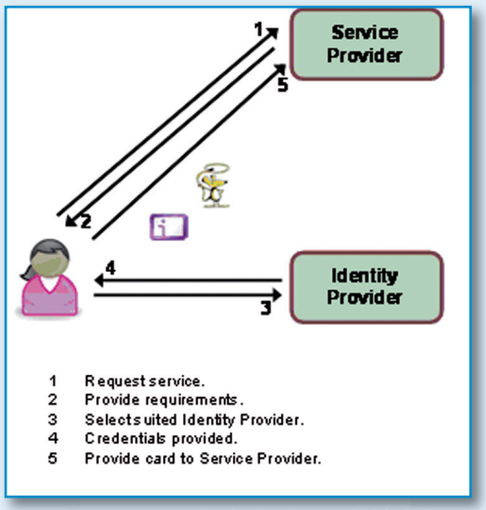


Figure 6 User-centric identity illustrated (InfoCard model)

These concepts not only abstract the existing process and introduce a new way of authentication but they are bringing the user back in control of the data he is sharing with the relying parties. In addition to this the value of the exchanged data might increase as the concept introduces a trusted partner who validates the data and shares it afterwards at the request of the user.

Cloud

'The network is the computer'[4]. Perhaps this, now visionary, phrase best captures Cloud computing.

From an IT perspective Cloud Computing means the provision of IT services (i.e. technology services or business services delivered by IT) over the internet. Gartner refers to it as a 'style' of computing and offers a classification of Cloud services into: Business Process Services, Application Services, Application Infrastructure Services and System Infrastructure Services.

The impact of Cloud Computing on Identity and of Identity on Cloud Computing depends on how many of the above classes one considers. As we move upwards from System Infrastructure Services to Business Process Services more parts of an enterprise's services are distributed across a potentially wider number of platforms and service providers. Just as with the Extended Enterprise the actual party with whom one contracts to perform a service may do little more than manage a value chain of other providers at various levels. But Cloud Computing makes this even more complex (or perhaps the Extended Enterprise makes the Cloud more complex), because not only are the business processes distributed across providers but the IT implementation of those processes may well be delivered by (a network of) entirely separate providers.

For some the last scenario may be a utopia, for others a nightmare. Will it ever become reality? Can enterprises afford the risk of including multiple intermediaries in their business processes? Can regulatory compliance be guaranteed when the service owner is in The Netherlands, the applications are managed from Canada on hardware running in Bulgaria and the data is in China? Well the Extended Enterprise is a reality, managed services run across continents and Google is already storing enterprise data… somewhere.

Consider this: 'The best examples for us are the cyber criminals – they're the ones who are the most effective users of the cloud today, with botnets and tens of thousands of zombie computers. That kind of power. That's what we're dealing with.'[5] Interestingly it's also been suggested that the Cloud will make it easier to combat some kinds of cyber crime, because it will be harder for the criminals to trace the real location of data and the data can be moved around more easily.

Effect on IAM

Even if the Cloud were to be nothing more than System Infrastructure Services and an enterprise divested itself of all its own hardware, the reality of the Extended Enterprise and Web 2.0 would make managing all identities (and their entitlements) internally infeasible. We are dealing increasingly with entities ('users') about whom the enterprise can not possibly maintain its own authorized information. So we need solutions, which leverage trusted identity providers be they business partners or pure identity specialists. And we need solutions, which don't involve assigning all those entities to roles. And lastly we need solutions, which attract rather than repel users – solutions which are simple, secure, auditable and guarantee an acceptable degree of privacy.

Other relevant issues

Other, contemporary developments in IT and business also influence and, fortunately, help us to understand how to design the solutions that are needed today. These of course are significant topics in their own right and we only touch on them here in order to illustrate their relevance.

Service Oriented Architecture and Business Process Management are two, more or less compatible approaches that help to unify business and IT. Understood properly, with the keywords being Business and Architecture, we can see that our new solutions need to address business processes and the services that implement them rather than applications and user interfaces.
The good news is that this actually simplifies things. We really don't need to give all those new, unknown (or at least unmanageable) entities access to our vital IT applications. We just need to give them access to the services they need to use, which exist essentially at the boundaries of the enterprise. What happens in the processes that orchestrate chains of supporting services and often legacy applications too, is totally irrelevant to those users. Perhaps even more significantly, those services are (re)used in multiple processes (why otherwise do they exist as services?) and the factors controlling their use (access) are dependent on the context of the

[4] John Gage. Sun
[5] Anthony Arrott, Trend Micro

business process being implemented and simply cannot be unconditionally granted to any one user.
Mash-ups can be regarded as a variation on the same theme. Once again what is involved is the re-use of services across multiple contexts and, in this case, multiple providers too.

Another interesting but less well known phenomenon is the extent to which identity information, for a long time primarily consigned to the domain of security, overlaps with business information about customers, partners and even employees. This should really be obvious from all the above discussions but what we actually see is redundancy of information across the 'business' and 'security' domains. This cries out for the elimination of these increasingly artificial divisions. There's no reason at all that one piece of information about an entity cannot be both a business attribute used to improve service to that entity and a claim about that entity used to determine access rights. Take a look at the diagram below, which illustrates part of a telecommunications operator's business information model.

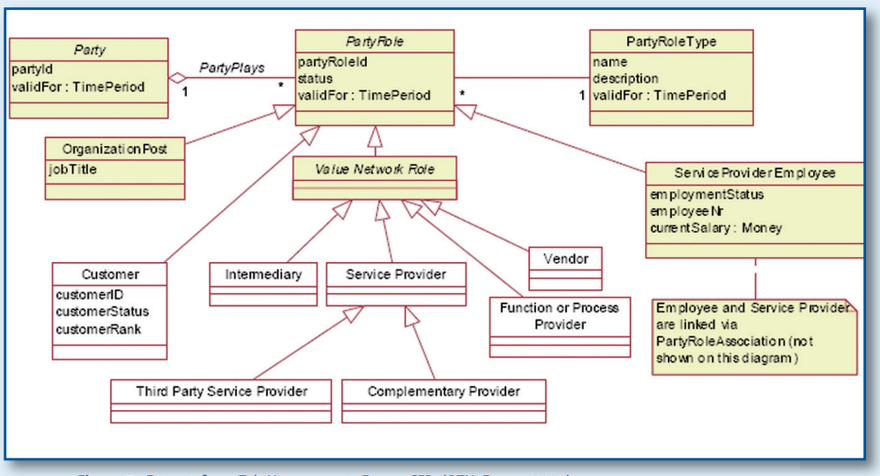


Figure 7: Extract from TeleManagement Forum SID (©TM Forum 2008)

This is also consistent with the above mentioned driver to distribute data and keep the attributes, the data, connected to the control instance of this data but available for other purposes as well

Solution options
From the above discussion we can draw the following conclusions:

- It will be increasingly difficult to maintain user identities and assign rights to identities within a single organization. Moreover there is little business logic in doing so.
- Identity as a concept, even if we restrict it to IT, is now far removed from the userid/password simplification.
- Identity is business information. How we use it and ensure privacy and regulatory compliance are business issues. How we address this with our IT solutions can make or break our business objectives
- Now more than ever, we must move away from isolating 'security' concerns into a 'non-functional', infrastructure domain. At the same time we must decouple the solutions from our applications and locate them in their own business domain. Even if we didn't want to, the Cloud will force us.

The demand for validated information will increase. This is not just relevant for authentication and authorization but is now important to the question of reputation. It affects all involved parties, whether they are providers of validation processes (IdPs) or of services. There is as yet no common measurement of reputation, so there will be a demand to find a way to provide and maintain this information for the future. With the increasing priority of privacy the value of a party with a high reputation may also introduce a new way to support user privacy in the Internet.

For all these reasons, trust relationships between providers of identities and services will become even more significant. But explicit trust agreements between all parties potentially collaboration in the cloud are unthinkable. Therefore we need a combination of standards supporting dynamic trust relationships and a network of recognized, trusted providers of identities. Government is an example of such a provider active today. Who has an explicit trust relationship with the Government? We simply assume that, if the government says it's true and the credential (e.g. password) looks authentic, then it must be OK. It's not unreasonable to see how this can be extended but it certainly argues for a limited number of identity providers and a limited set of well accepted standards to underpin that.

Solutions that support the above will essentially follow an Identity Provider paradigm. They will do this, because it is the only paradigm that can allow enterprises to adapt to the increasing pace of change in both business and technology models. That does not exclude the scenario where an enterprise itself functions as an IdP. We look to InfoCard (driven by Microsoft but with other vendors supporting either directly or via the Higgins project) as the model. What actually succeeds will depend on consolidation and acceptance of these standards. That may lead to an extended period of federation based solutions. And of course we will not eliminate legacy models overnight. As we have said there are still radical improvements to be made there using SOA compliant approaches and claims based authentication. We cannot suddenly change everything but we can and must evolve the architecture of our IAM solutions, because these will become the key enablers of the promise of the Cloud.

CIO Platform Nederland, een kennismaking

Auteur: Hendrikus Beck > Hendrikus Beck is Security Officer bij Unive-VGZ-IZA-TRIAS groep. Hij is per e-mail bereikbaar via hendrikus.beck@vgziza.nl.

Het CIO Platform Nederland is een onafhankelijke vereniging van CIO's en IT directeuren van private en publieke organisaties in Nederland. Deze bedrijven zijn allemaal als 'eindgebruikerorganisatie' te kenschetsen. Leveranciers en consultants zijn geen lid. Doelstelling van het platform is naast netwerken ook kennis op diverse aandachtsgebieden te delen. Dat laatste gebeurt onder meer in CIGs (CIO Interest Groups). Deze groepen komen regelmatig bij elkaar en ontwikkelen publicaties voor gebruik door de ledenorganisaties.

CIGs adviseren CIO's onder meer over trends en ontwikkelingen. CIO's nemen in de regel niet zelf deel aan de CIGs, daarvoor vaardigen zij medewerkers af. Vaak de verantwoordelijken uit hun eigen lijn, uit hun eigen organisaties. Er bestaan Interest Groups voor HRM, Inkoop, Architectuur en natuurlijk Informatiebeveiliging (zie de link onderaan deze bijdrage voor het volledige overzicht van CIG's)

Binnen de CIG Informatiebeveiliging zijn ruim dertig bedrijven vertegenwoordigd die medewerkers hebben afgevaardigd die werkzaam zijn op het vakgebied Informatiebeveiliging. Leuk is dat een groot aantal deelnemers (natuurlijk) ook lid is van het PvIB. We houden van platforms... Naast de reguliere kennissessies (ongeveer vier keer per jaar) zijn er ook twee projectgroepen in deze CIG bezig met twee specifieke onderwerpen waarover de CIO's hebben aangegeven meer kennis te willen vergaren. Over beide projectgroepen, **de empowered medewerker en benchmarking** zou ik graag iets meer willen vertellen.

1. De empowered medewerker

Deze projectgroep houdt zich bezig met de medewerker nieuwe stijl en zijn uitrusting. De nieuwe medewerker en de nieuwe instromers bij bedrijven willen niet meer conform de conservatieve manier werken. De 9-tot-5-mentaliteit zal steeds verder van ons af komen te staan. De nieuwe generatie medewerkers (de zogenoemde generatie Einstein) heeft een andere manier van werken ontwikkeld waaraan de huidige bedrijven zich (min of meer) moeten gaan conformeren als zij nog als aantrekkelijke werkgever willen worden gezien.
Denk hierbij aan het gebruik van MSN, Hyves, Twitter en alle nieuwe modernere manieren van netwerken. De verbinding met het netwerk van de werkgever moet ook in de avond gelegd kunnen worden om ervoor te zorgen dat je kunt werken wanneer je wilt, de plaats van werken wordt ook minder belangrijk en zelfs de manier waarop wordt meer en meer ter discussie gesteld. De zogenoemde anywhere, anytime en anyplace-behoefte wordt ook uitgebreid met de anyhow-behoefte. Als de generatie Einstein met een Ubuntu machine of een MacBook wil werken dan zal dat uiteindelijk ook toegestaan gaan worden. De Nokia die vroeger de standaard was, wordt meer en meer vervangen door iPhones, de HTC machines en allerlei andere smartphones. De netbooks worden mee naar het werk genomen omdat deze kleiner en handzamer zijn en plezieriger werken. Kortom; een enorme uitdaging om dit ook allemaal behapbaar en bovendien veilig te houden. Risico's en wellicht ook maatregelen zullen veranderen. Ik ben zeer benieuwd met welke aanbevelingen deze projectgroep uiteindelijk zal komen.

2. Benchmarking

Een tweede projectgroep houdt zich bezig met benchmarking. Hoe verhoudt het beveiligingsniveau van mijn bedrijf zich tot dat van andere bedrijven? En dan bij voorkeur in vergelijking met bedrijven in de branche waarin mijn bedrijf werkzaam is. Hoe kom ik er achter welke aanpassingen ik nog moet doen in mijn beveiligingsmaatregelen om tot hetzelfde niveau van beveiliging te komen als mijn branchegenoten?
Op basis van de Code voor Informatiebeveiliging wordt door deze projectgroep een methodiek ontwikkeld die ervoor zorgt dat op een transparante en een goed meetbare wijze een vergelijking gemaakt kan worden tussen de verschillende organisaties. Deze methodiek zal tevens in staat moeten zijn om interpretatieverschillen van de vragen zo veel mogelijk te beperken waarbij de Norm in al zijn uitgebreidheid als basis dient. De uitkomst zal uiteindelijk moeten zijn dat er een meting gedaan wordt over de verschillende aspecten van Informatiebeveiliging waarmee vervolgens de mogelijkheid geboden wordt om op basis van de metingen contact te zoeken met branchegenoten of vakbroeders. Om zodoende te leren van de ervaringen van collega's. Een zeer boeiend project waarvan we binnenkort de eerste resultaten zullen zien. Uiteraard is deelname aan deze benchmarking voorbehouden aan de leden. Dit om de toegevoegde waarde voor leden ook echt meetbaar en bruikbaar te maken.

In april heeft onlangs een plenaire sessie plaatsgevonden met de Informatiebeveiligingsmedewerkers van het CIO platform. Tijdens deze sessie zijn de tussenresultaten gepresenteerd. Ongetwijfeld zullen we deze resultaten te zijner tijd ook hier terugzien, hoewel de inhoud, zoals gezegd, uitsluitend voor leden bestemd is.

Relevante link

- De website van het CIO Platform: ***http://www.cio-platform.nl***

Publieke Identity Providers: kip en ei?

Auteur: André Koot > André is Security Manager bij Univé-VGZ-IZA-Trias en hoofdredacteur van dit blad. Hij is per e-mail bereikbaar via a.koot@unive.nl.

Wie heeft er al een digitale identiteit? Foute vraag, iedereen heeft er al minimaal een, naast diverse accounts op internet en intranet heeft iedereen immers ook een DigiD. Ik moet de vraag dan ook iets gerichter stellen: wie heeft er een herbruikbare digitale identiteit - een identiteit die aan verschillende accounts gekoppeld kan zijn? Ook dat geldt voor iedereen: DigiD is herbruikbaar. DigiD kan worden gebruikt binnen het G-C domein (government - consumer) en binnen enkele aanpalende domeinen. Zo mag (bij wijze van uitzondering) DigiD door consumenten ook worden gebruikt om in te loggen bij zorgverzekeraars.

Nu heb ik zelf een paar andere herbruikbare identiteiten. De belangrijkste is een OpenID identiteit. Die identiteit kan ik gebruiken op alle sites die OpenID toelaten. Maar dat gemak levert mij alleen maar een vervanger van een account op de betreffende website op. Mijn OpenID levert geen enkel vertrouwen op: ik heb zelf online een OpenID account aangemaakt, zonder dat iemand mijn identiteit ook maar heeft vastgesteld. Ik heb zo ook een eigen Information Card op mijn eigen pc gemaakt. Zomaar, zelf gedaan, zonder enige validatie. Erg handig, maar het kan ook alleen maar mijn gebruikersnaam en wachtwoord vervangen.

Zoals ik in het vorige nummer schreef (in het artikel over Claims Based Access Control, Informatiebeveiliging nr. 2 2009, pagina 4-8) hebben we wel grote behoefte aan een digitale identiteit om de juiste autorisaties te kunnen toekennen. We willen geen identiteiten beheren, maar wel autorisaties kunnen toekennen, zonder dus de identiteit te kennen, laat staan die te beheren.
In dat artikel schreef ik ook dat er nu wel een fors probleem bestaat. Er bestaan (buiten DigiD) op dit moment geen betrouwbare leveranciers van betrouwbare herbruikbare digitale identiteiten. Geen enkele identity provider doet iets aan verificatie van identiteiten, waardoor het digitale paspoort niet dezelfde mate van betrouwbaarheid heeft als een fysiek paspoort. Ook DigiD blijft qua verificatie eerlijk gezegd beperkt tot een check van het BSN en reikt het digitale paspoort ongezien uit. Ik ben blij dat ik het zelf uit mijn eigen brievenbus heb gehaald...

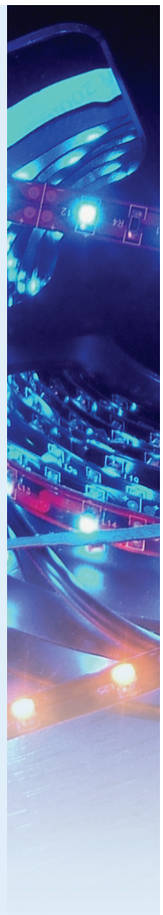
Hoe dan ook, er zijn geen betrouwbare publieke identity providers. Waarom niet? Op zich een eenvoudig antwoord: niemand heeft nog een herbruikbare digitale identiteit nodig. Want je kunt nog vrijwel nergens met een herbruikbare digitale identiteit inloggen. En dat kan niet omdat vrijwel geen enkele site nog een gebruikersgroep heeft die met een herbruikbare digitale identiteit wil inloggen. Tja, je hebt een enkele blog waar je met OpenID kunt inloggen, maar dat is toch wel iets voor 'geeks'. De LinkedIn groep van OpenID gebruikers in mijn netwerk van 4,5 miljoen personen omvat 545 leden. En de Information Card group heeft maar tien leden. Dat is niet veel. Voor die mensen ga je geen eigen inlogschermpje bouwen.

Zoals ik in het vorige nummer ook schreef is de waarde van een identiteit eigenlijk volkomen afhankelijk van de betrouwbaarheid van de identity provider. Als de Identity Provider te vertrouwen is, dan is de identiteit die door de provider wordt verstrekt ook te vertrouwen. Wat is het voordeel daarvan? Een betrouwbare identiteit maakt grote kans om hergebruikt te kunnen worden.

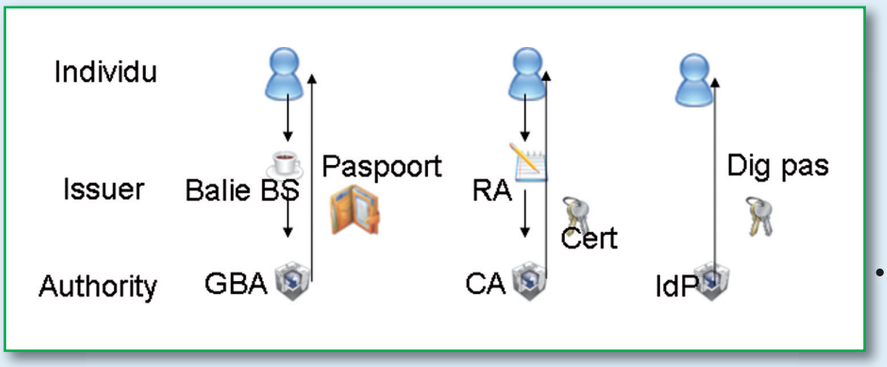
Wat maakt dan een digitale identiteit betrouwbaar?
Laat ik even een vergelijking maken tussen diverse vertrouwensmechanismen. In de eerste plaats kennen we het mechanisme waarbij we een fysiek identiteitsbewijs van een hoge autoriteit (de overheid) krijgen. Een individu meldt zich bij een ambtenaar van de Burgerlijke Stand (BS) van de gemeente, die de identiteit verifieert (op basis van een ander geldig document met een biometrisch kenmerk, de foto). De BS keurt de aanvraag goed, waarna een andere overheidsinstantie een paspoort via de BS uitreikt. Het hergebruik van het paspoort is mogelijk doordat onder meer andere overheden (in binnen- en buitenland) onze overheid vertrouwen en de echtheid van het paspoort kunnen vaststellen. Ook andere organisaties vertrouwen de overheid, zodat het paspoort ook in andere omgevingen bruikbaar is (hoewel het paspoort, als reisdocument, daar in beginsel dus niet voor is bedoeld).

Een tweede soortgelijke methode is die van de Public Key Infrastructure. Een individu meldt zich bij een Registration Authority, die na verificatie van de identiteit van het individu (aan de hand van een fysiek identiteitsbewijs) aan de Certification Authority opdracht geeft een certificaat te verstrekken. In de PKI wereld kunnen certificaten van verschillende CA's worden vertrouwd als de betreffende CA's elkaar vertrouwen (ik ben me ervan bewust dat er diverse niveaus van betrouwbaarheid van certificaten bestaan, maar laten we even de zwaarste classificatie als norm hanteren).

In de 'herbruikbare digitale paspoorten'-wereld bestaat een dergelijke werkwijze nog niet. In het beste geval (DigiD) meldt een individu zich rechtstreeks bij de Identity Provider, die zelf (na een specifieke afweging en wellicht verificatie) besluit een digitaal paspoort aan het individu te verschaffen. Voor de andere IdP's (met name OpenID) gaat het ongeveer hetzelfde, maar daarbij vindt er geen verificatie van de identiteit plaats.



Schematisch kun je dit als volgt weergeven:



Er bestaan op dit moment geen vertrouwensrelaties tussen IdP's, zoals die voor overheden en CA's ('cross certification') wel al bestaan. Hergebruik van identiteiten is dus niet per definitie mogelijk. Hergebruik is echter vooral een kwestie van vertrouwen: als een service provider een identity provider vertrouwt, dan is het al goed. Er bestaat dan ook niet direct de noodzaak van onderling vertrouwen tussen IdP's, dat scheelt wel heel veel zorgen...

Om een herbruikbare digitale identiteit te verkrijgen moeten we dus het nodige organiseren:

- Er moet een identity provider zijn die identiteiten controleert op basis van een ander identiteitsbewijs. Het zou fraai zijn als die IdP gebruik zou willen maken van 'issue-ing parties', zodat een gedistribueerd systeem ontstaat. Dat betekent automatisch dat er al meerdere partijen via dezelfde IdP identiteiten zouden kunnen verstrekken, zodat er meteen een hergebruik potentieel ontstaat. Denk aan de Pass-dienst van Diginotar.

- de 'issue-ing' en 'provisioning' processen bij de betreffende instanties moeten op een transparante en toetsbare manier worden ingericht om het vertrouwen te laten ontstaan. Die processen zouden ook daadwerkelijk getoetst moeten worden. Dat mechanisme kennen we natuurlijk al vanuit de PKI wereld. Daarbij worden op basis van een accreditatieschema audits door onafhankelijke auditors uitgevoerd. Niets nieuws onder de zon.

- Er moeten Service Providers opstaan die de door de IdP verstrekte identiteiten willen vertrouwen. Dat zal natuurlijk alleen gebeuren als het vertrouwen bestaat dat de verstrekte digitale identiteiten betrouwbaar zijn. Dus eis 2 is daartoe direct voorwaardelijk.

- Het is nodig dat aangesloten wordt bij open standaarden. Wil hergebruik mogelijk zijn, dan moeten open standaarden als SAML op grote schaal worden toegepast - op dit moment waarschijnlijk het grootste obstakel.

Maar waarom bestaat het nu nog niet? Er bestaan volgens mij verschillende redenen:

- De eerste reden is misschien wel het concurrentieaspect, het in de markt onderscheidend zijn. De meeste bestaande identity providers maken gebruik van eigen oplossingen, niet van open standaarden. Denk maar aan de banken, iedere bank heeft zijn eigen oplossing voor een digitaal paspoort. Kwestie van wantrouwen in plaats van vertrouwen: ik vertrouw alleen wat ik zelf beheer. Hergebruik is nog niet mogelijk.

- Daarnaast wordt blijkbaar de noodzaak nog niet voldoende gevoeld. Consumenten zijn gewend om op elke website met een andere account in te loggen. Dat hoort erbij. Het is wel lastig, maar we zijn het gewend. Blijkbaar zijn de ideeën van Identity 2.0 nog niet voldoende doorgedrongen, de markt (de consument) vraagt er nog niet om.

- Een andere reden zou wel eens kunnen zijn dat er nog geen evidente standaard bestaat. OpenID is een standaard uit de open wereld, maar het is een authenticatieservice, net als DigiD. Maar hoe gaat OpenID zich ontwikkelen? Hoe zit het met privacy, hoe zit het met spoofing? Het alternatief Information Card is ook nog geen winnaar. Niemand kent Cardspace nog, dus hoe dat te gebruiken is?

- Vierde reden is een kostenafweging. Identity Management is een duur proces. Iedere organisatie weet daarvan. Als we nu opeens identity management als een nieuw identity provisioning product in de markt willen zetten, wie heeft daar dan baat bij? De consument, dat is duidelijk, de service provider profiteert echter ook, want die vervangt zijn eigen IdM proces door een (goedkoper) 'federatief proces. Wanneer er genoeg afnemers zijn om 'economies of scale' te laten gelden, is er voor de IdP ook een businesscase te maken, maar niet voor de early adopters... Vraag blijft: wie gaat dit initieel betalen? Zeker als er een heel accreditatieschema ten grondslag ligt aan de betrouwbaarheidstoets, dan moet de rekening ergens terechtkomen. De consument zal dat niet zonder meer willen betalen: liever een extra digitale identiteit, dan te betalen voor het gemak van herbruikbaarheid.

In het voorgaande ging ik impliciet uit van een digitale identiteit met een hoge kwaliteit, een identiteit die wordt verstrekt na verificatie tegen een fysiek paspoort. Nu is een identiteit met een dergelijke hoge kwaliteit natuurlijk niet altijd noodzakelijk. Een dergelijke identiteit is natuurlijk ook kostbaar. Verificatie is een duur proces. Als je dat als service provider niet nodig hebt, als je dus niet een hoger niveau van betrouwbaarheid van digitale identiteiten nodig hebt dan regulier gebruikersnaam en wachtwoord, wat let je dan om OpenID en Information Card inlogmogelijkheden beschikbaar te stellen?

De aanpassing aan je website die hiervoor nodig is, kost vrijwel niets, levert de gebruiker winst op door herbruikbaarheid van een bestaande digitale identiteit en doorbreekt daarmee de kip-ei cyclus. Lijkt mij een eenvoudige overweging.

Wat het convergeren van de fysieke en logische beveiliging voor uw organisatie kan betekenen

Auteur: David Ting > David Ting, oprichter en CTO van Imprivata, is actief lid van de Open Security Exchange en heeft meer dan twintig jaar ervaring met het ontwikkelen van geavanceerde imaging-software en systemen met een hoog beveiligings- en beschikbaarheidsniveau.

De toenemende mate waarin informatie digitaal beschikbaar en opvraagbaar is, vereist een nieuwe manier van beveiliging. Recentelijk bleek uit een onderzoek van het College Bescherming Persoonsgegevens en de Inspectie voor de Gezondheidszorg dat de computerbeveiliging in een aantal zaken niet op orde is met als gevolg een verder afnemend vertrouwen in de privacybescherming in het kader van het EPD. De financiële sector staat ook al een tijdje onder druk vanwege onvoldoende beveiligde systemen - denk bijvoorbeeld aan het fraudegeval bij Société Générale.

Een klein incident kan al snel een geheel eigen leven gaan leiden, of het nu gaat om een onbevoegd persoon die in een pand wordt binnengelaten of een ontevreden werknemer die zich toegang tot vertrouwelijke bedrijfsdocumenten verschaft. De resultaten kunnen variëren van omzetverlies tot schade aan de reputatie van een bedrijf of zelfs de sector.

Als gevolg van beveiligingslekken en de recente golf van bewustwording ten aanzien van privacy en gegevensbeveiliging beginnen mensen zich te realiseren dat de bedreigingen, die in het verleden louter werden beschouwd als het werk van 'outsiders', ook de kantoormuren zijn binnengeslopen. Dit kan resulteren in vrij onschuldig misbruik van vertrouwelijke data tot grootschalige fraude met alle gevolgen van dien. De beveiligingsovertredingen binnen de financiële sector hebben aangetoond dat medewerkers misbruik van de situatie maken als hun werkgever niet over een oplossing beschikt om de gehele bedrijfsvoering te beveiligen, van de voordeur tot de achterdeur en alles er tussenin. Dit heeft geresulteerd in een volledig nieuwe beveiligingsproblematiek waarop veel bedrijven momenteel nog een antwoord zoeken.

Met welke antwoorden komen ze voor de dag?

Wat doen financiële dienstverleners nu precies om hun volledige bedrijfsvoering te beveiligen tegen aanvallen van binnenuit en van buitenaf? Het antwoord: een combinatie van fysieke beveiliging en IT-beveiligingsoplossingen die hen in staat stelt om op een nieuwe manier identiteiten te beheren en de toegang te regelen. Door gebruikersgegevens uit deze twee afzonderlijke systemen te combineren, krijgen bedrijven een beter beeld van de gebruikerstoegang, hetgeen in een hechtere beveiliging zal resulteren.

Het samenbrengen van deze twee gebieden klinkt uiterst logisch en het concept bestaat al enige tijd. In het verleden stelde een dergelijke stap bedrijven echter voor een reeks van problemen.

Het eerste struikelblok vormde het feit dat de systemen voor toegangscontrole binnen de IT-beveiliging en fysieke beveiliging vanuit technisch oogpunt weinig met elkaar gemeen hadden. Hierdoor bleek de integratie van de twee gebieden een dure en complexe aangelegenheid waar veel bedrijven zich niet aan wilden wagen.

Een ander probleem was het gebrek aan samenwerking. Op basis van het oude model was de facilitaire afdeling verantwoordelijk voor fysieke beveiliging, terwijl de IT-manager zorg droeg voor IT-beveiliging. Deze 'tunnelvisie' was het gevolg van de historische scheiding van de twee disciplines en een duidelijke afbakening van het takenpakket. Zo beschikte elke afdeling over een eigen budget en moesten beide afdelingen hun unieke doelstellingen zien te behalen. Er was onvoldoende aanleiding om gezamenlijk een grootschalig project te beginnen.

Fysiek/logisch: waarom nu?

De roep om convergentie van IT-beveiliging en fysieke beveiliging wordt aangewakkerd door verschillende factoren.

Ten eerste vormen oplossingen die een holistische beveiliging bieden nog altijd een topprioriteit voor bedrijven. De IT-beveiliging wordt geconfronteerd met de richtlijnen van de wet- en regelgeving. Zo worden de richtlijnen voor de beveiliging van gemeentelijke IT-netwerken steeds verder aangescherpt. In deze markt wordt ook gezocht naar oplossingen die helpen bestanden en applicaties steeds verder af te schermen voor onbevoegden. Anderzijds willen medewerkers én IT-beheerders in de dagelijkse praktijk niet te veel geconfronteerd worden met de gevolgen van de strengere eisen.

Daarnaast is er de angst voor gegevensverlies en alle negatieve publiciteit die daarmee gepaard gaat. Geen enkel bedrijf wil de krantenkoppen halen in verband met een beveiligingslek. Bovendien hebben bedrijven ook nog eens te kampen met nieuwe bedrijfsmodellen die hen verplichten om hun digitale activa beschikbaar te stellen aan derden die zich buiten hun kantoor en bedrijfsnetwerk bevinden, zoals partners en klanten. Als

gevolg hiervan zijn de bedrijfsgrenzen verlegd, zodat de IT-organisatie onder steeds grotere druk komt te staan om ervoor te zorgen dat de juiste informatie bij de juiste persoon terechtkomt, een taak die met de dag complexer wordt.

Beveiligingsprofessionals hebben behoefte aan een logischer basis voor hun beslissingen, die hen in staat stelt om met meer zekerheid vast te stellen wie gemachtigd is een bepaalde handeling uit te voeren. Daarnaast hebben zij behoefte aan een informatiestroom die de mogelijkheid biedt om kennis over de fysieke beveiliging en IT-beveiliging uit te wisselen, zodat de gehele organisatie met meer zekerheid de identiteit van gemachtigde gebruikers kan vaststellen.

Dit is het punt waarop een derde katalysator in werking treedt. Het afgelopen decennium is Internet Protocol (IP) uitgegroeid tot de standaard voor apparaten die voor fysieke toegangssystemen worden gebruikt. Het gevolg is dat de fysieke beveiliging en IT-beveiliging dezelfde taal zijn gaan spreken. Nu beide disciplines hetzelfde protocol gebruiken, is het mogelijk ze te integreren. Dit heeft een reductie van de bedradingsvereisten, implementatietijden en uitgaven tot gevolg en geeft de mogelijkheid om met grotere zekerheid te bepalen wie toegang heeft tot het bedrijfspand en het netwerk. Deze ontwikkeling heeft geleid tot een betere communicatie tussen de medewerkers die voor de IT-beveiliging en fysieke beveiliging verantwoordelijk zijn. Dankzij deze wederzijdse dialoog bieden nu meer leveranciers van apparaten voor fysieke beveiliging ondersteuning voor het IP-protocol. De lijst van toegangsvoorzieningen die ondersteuning bieden voor IP, zoals onder meer camera's, kaartlezers en toegangscontrollers, groeit met de dag.

Wat is de volgende stap?
Bedrijven kunnen inmiddels sneller en gemakkelijker van de voordelen van convergentie profiteren dan ze denken. Ze kunnen immers hun bestaande activa gebruiken ter ondersteuning van een nieuw beveiligingsbeleid dat het vertrouwen, de controle, privacy en beveiliging vergroot en het risicoprofiel reduceert. De convergentie van fysieke en logische beveiliging vormt in wezen niet meer dan een extra dimensie, een mechanisme dat eenvoudig te ontwikkelen is binnen het bestaande toegangsbeleid.

De integratie van de beveiligingsgegevens is van essentieel belang om de identiteit van gebruikers met meer zekerheid te kunnen vaststellen. Door informatiesystemen te integreren kunnen real-time toegangsgegevens gedeeld en nieuwe beleidsregels gedefinieerd worden om zo de gebruikerstoegang te baseren op harde feiten.

Vrijwel elk bedrijf beschikt over een of ander fysiek toegangssysteem. Wanneer iemand met een pasje het kantoorpand betreedt, krijgt het beveiligingspersoneel informatie in handen op basis waarvan het gefundeerde beslissingen kan nemen met betrekking tot de rechten die aan deze persoon zijn toegekend. Wanneer dezelfde gebruiker zich op het netwerk aanmeldt, zullen diens gegevens worden afgezet tegen de gegevens van het fysieke beveiligingssysteem, zodat het IT-systeem kan achterhalen of deze persoon toestemming heeft om zich op het netwerk aan te melden. Daarnaast is het mogelijk om specifieke regels in te stellen met betrekking tot de netwerktoegang binnen bepaalde gecontroleerde gedeeltes van het gebouw.

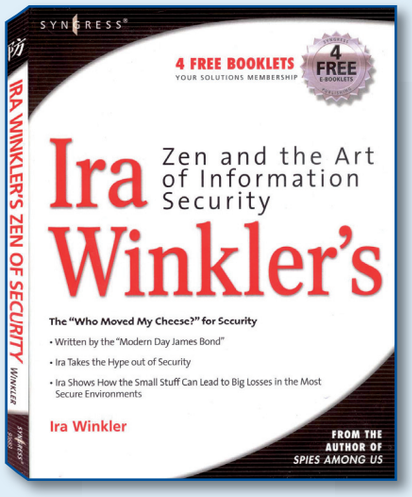
Het is niet nodig om systemen te vervangen of aan te passen om een omgeving veiliger te maken. Het ontwerpprincipe van het geconvergeerde fysieke/logische systeem kan gebruikmaken van de bestaande systemen. De sleutels tot dit integrale model zijn informatie-uitwisseling, het afdwingen van beleidsregels en de mogelijkheid om activiteiten te bewaken en in kaart te brengen. Door informatie te delen over de manier waarop de beveiliging op basisniveau is ontwikkeld, kunnen de twee disciplines tot het besef komen dat ze in werkelijkheid heel veel met elkaar gemeen hebben. Gangen in de fysieke wereld zijn net als netwerken in de IT-wereld. Kamers zijn te vergelijken met servers, terwijl je de voordeur als een soort van firewall zou kunnen zien. Zodra iemand langs de beveiliging (authenticatie) aan de poort komt (firewall), zal deze persoon vrij zijn om door de gang te lopen (netwerk) Sommige kamers binnen het kantoor (servers) zijn beveiligd (wachtwoord), terwijl andere kamers openstaan voor iedereen die in staat was om langs de beveiliging aan de voordeur (aanmelding op het netwerk) te komen of over het juiste pasje (wachtwoord) voor een zijdeur (VPN-gateway) beschikt.

IT vormt op deze manier een van de vele lagen binnen het fysieke beveiligingssysteem, en de fysieke beveiliging vormt nu simpelweg een van de vele authenticatielagen. Het afdwingen van deze beleidsregels op basis van de uiteenlopende systemen zorgt ervoor dat de afzonderlijke systemen efficiënter worden en zowel de fysieke als IT-systemen worden versterkt.

Boekbespreking:
‘Zen and the Art of Information Security’

Auteur: Lex Borger > Lex Borger is Principal Consultant Information Security bij Domus Technica. Hij is bereikbaar via lex.borger@domustechnica.com.

De titel van dit boek zet je aan het denken nog voordat je het boek zelfs openslaat. Informatiebeveiliging is niet iets dat wij professionals associëren met Zen Boeddhisme. Maar, net zoals Pirsig’s bedoeling met ‘Zen and the Art of Motorcycle Maintenance’, geeft de titel ook in dit geval de boodschap mee dat in iets zo alledaags en emotieloos ook een spirituele kant te vinden is. Dat is de aanname waarmee ik aan het boek begin. Het is geen dik boek, 144 pagina’s en gedrukt in een groot font. Het leest dan ook vrij gemakkelijk weg.



Titel: Zen and the Art of Information Security
Auteur: Ira Winkler
Gepubliceerd door: Syngress Publishing, 2007
ISBN-13: 978-1-59749-168-6

Ira Winkler heeft een indrukwekkende achtergrond. Hij is begonnen bij de NSA (National Security Agency) en heeft al verschillende boeken geschreven over spionage (*Spies Among Us, Corporate Espionage, Through the Eyes of the Enemy*). Zen and the Art of Information Security is anders van opzet. In het boek laat Winkler zien hoe je informatiebeveiliging met een dosis gezond verstand en een beetje goed gevoel inricht. Dit zou de Zen kunnen zijn waaraan Winkler in de titel refereert. Hierbij heeft hij geen techniek nodig en je zult in het boek dus ook vergeefs zoeken naar enige beschrijving van technische beveiligingsmaatregelen.
Ira maakt treffende vergelijkingen tussen de gewone wereld en de cyberwereld en gebruikt daarbij specifieke voorbeelden die we allemaal kennen. Zoals Anthrax versus Nimda, Nigeriaanse e-mailfraude, Kevin Mitnick, de ‘Evil Empire’ van Ronald Reagan en de ‘Axes of Evil’ van George W. Bush. Daaraan geen gebrek sinds 11 september. Bruce Schneier heeft daaraan ook enkele boeken gewijd.

Een aspect waar iedere beveiligingsprofessioneel mee te maken heeft, komt in dit boek niet voor: compliance. Het is duidelijk dat dat nou net niet de bedoelde ‘Zen’ is. Compliance is een nuttig aandachtsgebied, maar het zou niet de reden moeten zijn waarom we beveiligen. De wereld die Winkler schetst is er een waarin je aan beveiliging wilt doen, nee sterker nog: MOET doen. Dit is nog zo’n Zen-essentie. Hij wijdt daar een heel hoofdstuk aan. In de tijd waarin we nu leven, waarin de mate van beveiliging gedicteerd wordt door de mate van compliance die we moeten naleven, is dit wel een frisse gedachte.

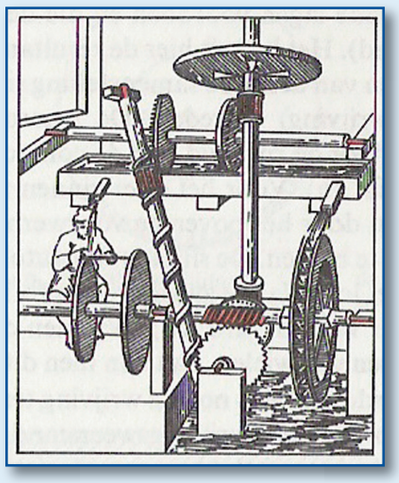
Voor wie is dit boek geschreven? Winkler beschrijft in de inleiding dat dat vooral ruimdenkende mensen moeten zijn, die kijken naar de grote lijnen, niet naar de details. Het boek is erg in de ‘I’m telling you’-stijl geschreven. Daarin verschilt Winkler van Schneier. Voldoe je aan dit profiel, dan zul je dit boek waarderen. Als informatiebeveiliger zul je er vaktechnisch gezien niet veel nieuws uithalen, wel de inspiratie om toch de verantwoording van je acties naar de business anders te verwoorden en wellicht hier en daar anders te werk te gaan.

Ik kan het boek vooral aanbevelen aan managers die verantwoordelijk zijn voor, maar ook nieuw zijn in het gebied van informatiebeveiliging. Daarnaast zal eenieder die zich openstelt voor Winkler’s gedachtegoed inspiratie kunnen putten uit het boek.

Het Business Continuity Management proces, de paradox

Auteurs: Sj. (Sjoerd) Vredenberg en T.M. (Tim) Willems > Sjoerd Vredenberg is directeur eigenaar van een BCM dienstverlener en BCM software leverancier. Tim Willems is directeur eigenaar van een Governance Risk Management & Compliance (GRC) software ontwikkelaar.

Business Continuity Management - BCM - is hot en booming. Als gevolg van wet- en regelgeving (denk aan de jongste Waterschapswet die voor waterschappen heel expliciet meer aandacht vraagt voor risico- en procesmanagement), maar bijvoorbeeld ook door toenemend besef dat bij verdergaand automatiseren van beheersmaatregelen de continuïteit van ICT van nog crucialer belang is. Maar misschien ook wel als gevolg van de huidige crisis... Sceptici prediken de spreekwoordelijke oude wijn in nieuwe zakken. De professioneel betrokkenen huldigen het belang van het onderwerp.



Zoals het met veel jonge, nieuwe ontwikkelingen gaat, kenmerkt BCM zich door de verscheidenheid aan definities, een veelheid aan verschillende functionarissen die het claimen (van de Corporate Risk Officer bij de één via de systeembeheerder ICT bij de ander tot de stafmedewerker facilitaire dienst bij een derde) en een sterk uiteenlopende mate van volwassenheid waarmee het onderwerp wordt opgepakt.
Juist in deze periode van crisis realiseren organisaties zich dat iedere failure er nu één te veel is en verschuift het onderwerp BCM zeker niet naar een lagere positie op de agenda. Integendeel.

Versnippering, historisch gegroeid
Luisterend naar functionarissen die zich bezighouden met Business Continuity Management (BCM) wordt duidelijk dat er vele beelden bestaan over BCM. Veelal blijken het verschillende subprocessen van hetzelfde hoofdproces te zijn. Waar de ene functionaris zich richt op het inventariseren en vastleggen van risico's, is de ander gericht op het ontwerpen en inrichten van maatregelen (controls). Lang niet altijd geformaliseerd, maar vaak wel met de beste intenties worden elders analyses gemaakt van de impact van risico's op de business. Tegelijkertijd zien we ook omgevingen waar BCM synoniem is voor het testen van Disaster Recovery plannen. Soms wordt BCM zelfs jaarlijks als 'issue afgevinkt' als de ICT uitwijktest positief wordt afgesloten.

In een door ons uitgevoerd onderzoek tijdens een toonaangevend Business Continuity Management congres in ons land, vroegen we in welke mate in organisaties een relatie bestaat tussen riskmanagement en BCM. Slechts 44 procent van de ondervraagden gaf aan dat er van afdoende integratie sprake is.

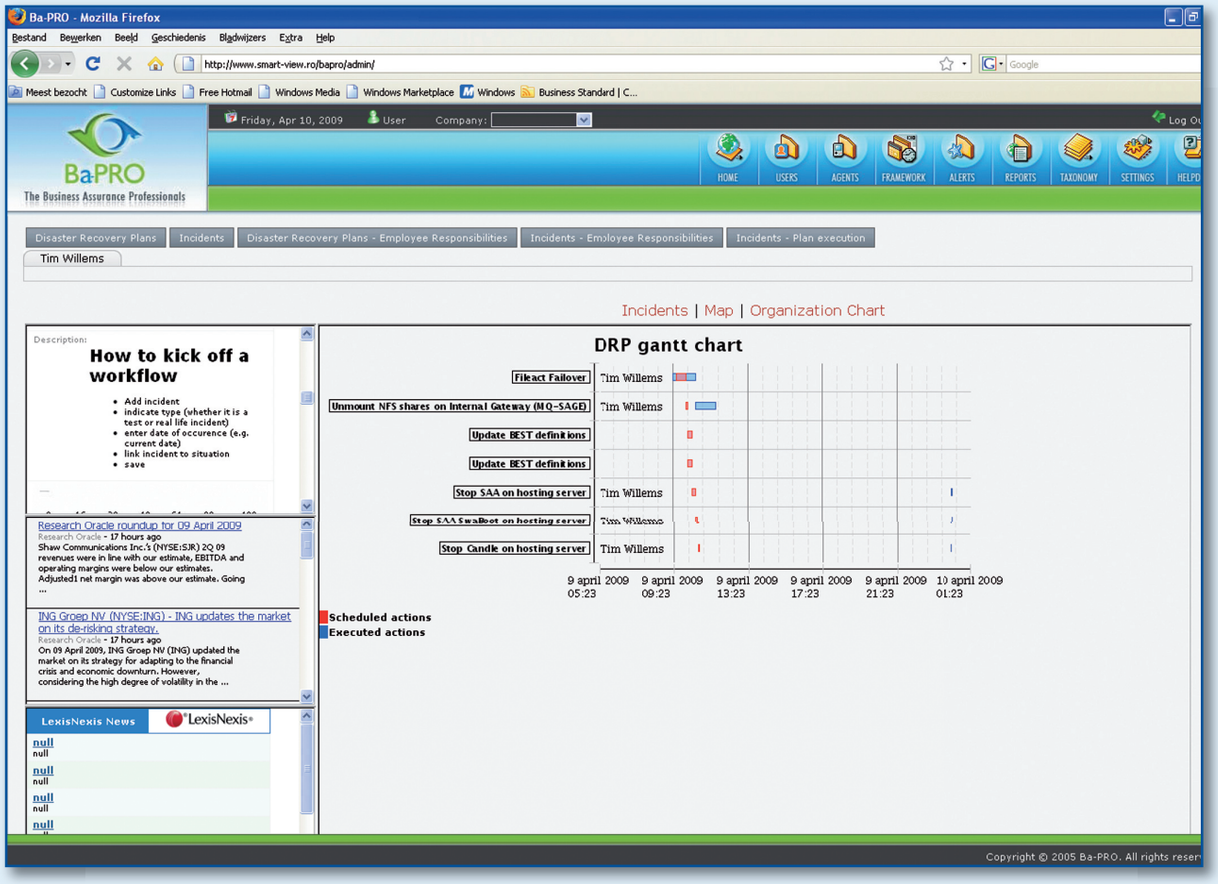
Bij een grote instelling in ons land bestaat Business Continuity Management (BCM) als afdeling naast een afdeling Operational Risk Management (ORM). Beide organisatieonderdelen kennen grote overlap in activiteiten. Onderlinge afstemming blijkt maar beperkt aanwezig.

Bij een groot productiebedrijf is Continuiteitsplanning aandachtsgebied van security, als onderdeel van facility. Hier wordt het sterk benaderd vanuit veiligheid en beveiliging. Een relatie met de aanwezige afdeling Risk Management bestaat niet.

BCM, een ICT aandachtsgebied?
BCM lijkt in de wereld van ICT uitgevonden. Nogal eens is Disaster Recovery Planning - met nadruk op herstel van hardware, software en data - de vertaling van BCM. In grote organisaties waar dataverwerking bijna de corebusiness is, kan ICT de achilleshiel zijn als het om de bedreiging van de continuïteit van de bedrijfsvoering gaat. Toch wordt meer en meer in organisaties duidelijk dat de continuïteit van de integrale bedrijfsvoering door tal van andere factoren bedreigd kan worden. Integraal Business Continuity Management vraagt dan ook om een bredere scope.
In het onderzoek gaf 80 procent van de respondenten aan dat ICT in ieder geval tot aandachtsgebied binnen BCM gerekend moet worden. Daarentegen scoorden kennisontwikkeling en -borging, marketing en HRM aanmerkelijk lager.

Van de respondenten in het onderzoek heeft 40 procent een ICT functie, 32 procent een expliciete BCM functie en de rest heeft een consultancyrol. Geen van de respondenten komt 'uit de eigenlijke business'. Terwijl tegelijkertijd 60 procent van de respondenten aangeeft te vinden dat de CEO/Directeur primair verantwoordelijk is voor BCM!

Hoewel het een veelvoorkomend beeld is dat BCM over ICT risico's gaat, kunnen organisaties tegelijkertijd heel goed benoemen dat het uit de schappen moeten halen van een product als gevolg van een productiefout, het niet meer operationeel



zijn als gevolg van het uitbreken van de vogelgriep of het (tijdelijk) niet ter beschikking hebben van het bedrijfspand evenzo denkbare BCM issues zijn.

Bij een grote voedings-, household- en bodycareproducent wordt duidelijk dat - hoewel het beheren van risico's in hun ICT omgeving een serieus aandachtpunt is - een ander minstens zo groot risico op een ander terrein ligt. Ze realiseren zich dat ze een research en development organisatie zijn. Hierdoor loopt de continuïteit van hun bedrijfsvoering ook groot gevaar als hun kennis niet geborgd is. Hier raakt BCM informatiebeveiliging, maar zeker ook de P-kolom.

Bij een grote dienstverlener realiseert men zich dat - naast de risico's die ze lopen in het domein van informatiebeveiliging (ICT) - ze ook een continuïteitsvraagstuk hebben bij het uitbreken van de vogelgriep. Het geheel of gedeeltelijk stil komen liggen van hun primaire bedrijfsprocessen levert naast de eigen schade ook een onacceptabel groot maatschappelijk risico op.

Van 'noodzakelijk kwaad' tot...

Veel van wat onder de noemer van BCM is geregeld, is voortgekomen uit wet- en regelgeving. Dat was zo, en dat gaat in de toekomst - met de huidige crisis die tot een toename van toezicht zal leiden - zeker niet minder worden. Een interessante verschuiving is echter wel waarneembaar: meer en meer gaan organisaties van hun toeleveranciers helderheid verwachten over hoe zij hun continuïteit van de bedrijfsvoering geregeld hebben. Immers, het stil komen liggen van productie en levering bij hen, kan desastreuze 'domino'gevolgen voor de eigen organisatie hebben.

Tegelijkertijd gaan zelfs (eind)consumenten transparantie verlangen van organisaties over hoe zij hun continuïteit kunnen garanderen. Recente voorbeelden in de gezondheidszorg versterken deze vraag.

Of het nu gaat om een bank waar spaargeld na langere tijd nog beschikbaar moet zijn, een leverancier waar na verloop van tijd aanspraak op een garantieregeling gedaan kan worden of een waterschap dat juíst in het geval van een calamiteit zijn werk moet kunnen blijven doen, ook eindconsumenten gaan steeds meer transparantie verlangen van organisaties.

Of dat op termijn zal leiden tot certificering als 'uithangbord' met een marketingwaarde valt te bezien. Een verschuiving van 'Continuity Management als noodzakelijk kwaad aan de achterkant richting een transparant en zichtbaar onderwerp aan de voorkant' is het op zijn minst.

Twee werelden

De wereld van controllers wordt sterk bepaald door in kaart te brengen risico's, in te richten maatregelen in combinatie met de check of die maatregelen effectief zijn en worden nageleefd. Dit leidt tot een gevoel van in-control-zijn.

Gesproken met bestuurders en ondernemers, lijkt hun wereld zich in grote lijnen te richten op de te bereiken

organisatiedoelstellingen, het uitvoeren van het managementproces gecombineerd met de check of die sturing leidt tot het behalen van de gedefinieerde doelstellingen. Hierbij is gevoel van in-business-zijn het resultaat.

Connectie
Vanuit BCM perspectief zijn enorme effectiviteit- en efficiencyvoordelen te halen door de wereld van Risicomanagement in veel nauwere relatie te brengen met 'de business'.

Dan kan in samenhang besproken worden met de mate waarin de continuïteit gewaarborgd is.

In het eerder aangehaalde onderzoek werd ook de vraag gesteld of in gebruikte methoden en technieken de link tussen risicomanagement en business te leggen was. 52 procent van de respondenten geeft aan dat dit verband er expliciet is. Volgens de overige 48 procent is deze link handmatig, impliciet of zelfs helemaal niet te leggen.

Bij veel organisaties waar we in de keuken kijken is inderdaad vanuit incident management en vanuit disaster recovery niet te zien waar in geval van een calamiteit de business wordt 'geraakt'. Daar waar asset management al deel uitmaakt van BCM, is vanuit de resource veelal niet transparant in welk kritieke bedrijfsproces de betreffende resource een rol speelt.

Business Impact Analyses (BIA's) zijn vaak separaat gedocumenteerd en niet te linken met de omgeving waarin de bedrijfsprocessen zijn vastgelegd.

Bij een calamiteit vanuit het incident via de BIA inzicht krijgen waar business in gevaar is, kan van grote waarde zijn.

Een definitie
Een poging tot een definitie van BCM: 'In samenhang met het behalen van organisatiedoelstellingen, het beheersen van risico's die de continuïteit van de bedrijfsvoering geheel of gedeeltelijk in gevaar kunnen brengen.'

Samenhang
Om tot samenhang tussen BCM en business te komen, zal binnen het BCM proces zelf veel meer samenhang moeten komen. Basis daarvan zullen de organisatiedoelstellingen en de daartoe ingerichte kritieke bedrijfsprocessen zijn. De afhankelijkheden tussen doelstellingen, bedrijfsprocessen, risico's, controls, incidenten, scenario's en herstelplannen zullen ondubbelzinnig moeten zijn vast te stellen.

Veelal vonden in het verleden - en mogelijk nog steeds wel - discussies plaats over waar het vertrekpunt lag. De ene 'school' hing het geloof aan dat het proces leidend was, de andere dat het risico de basis vormde. Een derde redeneerde primair vanuit de maatregel, de control. Altijd leidend tot een wat eendimensionaal denkmodel. De complexer wordende organisaties, externe afhankelijkheden, governance en wet- en regelgeving leiden ertoe dat risicomanagement niet meer goed past in dit 'geschakelde' model. De onderlinge afhankelijkheden lijken inmiddels veel beter te vangen in een relationeel netwerkmodel. Een ingerichte BCM omgeving volgens dat model geeft veel efficiënter sturingsmogelijkheden.

De inrichting volgens een dergelijk relationeel model zal op het eerste gezicht mogelijk afschrikken. Met de standaardsoftware is een dergelijke BCM omgeving niet meer te onderhouden, te controleren en te testen. Het kan zich niet in een gestructureerde manier ontwikkelen en herstelprocessen bij een calamiteit zijn niet of moeiziaam uit te voeren en zeker niet altijd onder controle. De nieuwe BCM applicaties zijn juist gericht op het leggen en onderhouden van relationele afhankelijkheden tussen de verschillende grootheden die alle een even belangrijke rol spelen. Daarmee de onderhoudbaar-, betrouwbaar- en uitvoerbaarheid sterk vergrotend.

Huidige softwareondersteuning
De stand van de softwareondersteuning voor BCM laat een versnipperd beeld zien. Zowel het proces als de softwareoplossingen zijn sterk plangedreven, registratief en documenterend van karakter. Organisaties gebruiken meerdere, losstaande deeloplossingen. Daarbinnen overigens vaak goede tools. Er is prima software voor het vastleggen van bedrijfsprocessen. Zo ook voor het beheer van risico's en controls. Er bestaan prachtige instrumenten voor het vastleggen en beheren van assets, zo ook voor incident management. Separate applicaties voor het uitvoeren van assessments, tests en audits zijn met goede kwaliteit voorhanden. In het onderzoek is overigens opvallend dat 44 procent van de respondenten aangeeft dat de organisatie haar BCM proces handmatig uitvoert in een 'spreadsheet omgeving'.

Daar waar het in de kritieke fase van het BCM proces aankomt op het beschikbaar hebben en kunnen uitvoeren van calamiteiten-, disaster recovery-, nood- of Business Continuity plannen, is het opvallend hoe vaak daar de traditionele tekstverwerkings- of presentatiepakketten worden ingezet. Met informatie uit verschillende bronsystemen worden handmatig plannen vastgelegd. Jaarlijks worden update rondes doorlopen om de informatie up-to-date te houden.

Gedreven door de angst dat de plannen niet voorhanden zijn op het moment dat zich werkelijk een calamiteit voordoet, hebben we meer dan eens gezien dat de plannen op papier, en dubbel uitgevoerd, in kofferbakken van auto's continu worden meegevoerd. Inclusief vertrouwelijke informatie over security en veiligheidszaken.

Geïntegreerde functionaliteit

Significante verbetering in het BCM proces is te behalen door in procesinrichting, organisatie en softwareondersteuning functionaliteit te integreren. Een heel dankbare (voelbare) verbeterstap is het in relatie brengen van documentatie. Hoe lastig blijkt het in veel situaties om bij een incident, het juiste (bijbehorende) calamiteitenplan te vinden. Laat staan dat we snel de specificaties kunnen vinden van betrokken assets.

Bij het leggen van relaties tussen doelstellingen, bedrijfsprocessen, risico's, controls, incidenten, scenario's en calamiteitenplannen, komt inconsistentie haarfijn aan het oppervlak en wordt incompleetheid zichtbaar.
Bij het goed organiseren van het op één plek gestructureerd vastleggen van data, neemt de betrouwbaarheid en onderhoudbaarheid van plannen en rapportages enorm toe.

Bij omzetten van 'traditioneel' vastgelegde processen en risico's (in een omgeving ondersteund door point solutions) naar een geïntegreerde BCM omgeving, is het ons overkomen dat we een proces tot drie keer gedocumenteerd tegenkwamen met drie verschillende proceseigenaren. Bij navraag welke ene functionaris (in de geïntegreerde omgeving) moest worden gekoppeld, bleek bovendien geen van de drie functionarissen (meer) werkzaam te zijn.

Bij integreren van functionaliteit bestaat veelal het misverstand dat het gaat om volledig opnieuw inrichten van datastructuren. Bij bestaande systemen en data waarover tevredenheid bestaat, kan gekozen worden om die omgeving als single point of definition te laten bestaan. Het is dan de kunst om die data te integreren in de BCM omgeving. Ergo: heel belangrijk is het om het eenmalig en op één plek vastleggen van data in de BCM omgeving na te streven.

Incident managent en herstel

Van het BCM proces maakt het kunnen managen van de situatie die je probeert te voorkomen ook onderdeel uit: het incident. Daarbij hoort het uitvoeren van plannen die in een eerdere fase zijn ontworpen, vastgelegd en regelmatig getest. Een separaat geregistreerd incident is van veel minder waarde dan het incident dat vastgelegd wordt in de omgeving waar direct een relatie gelegd kan worden met waar en hoe de business wordt geraakt, welke bijbehorende risico's het betreft en welke ingerichte controls mogelijk gefaald hebben. En zelfs: welke testresultaten er zijn vastgelegd waarvan geleerd kan worden. Ook vanuit het opbouwen van intelligentie (leren) en het hebben van een audit trail, is een geïntegreerde incident managementomgeving van grote waarde.

Calamiteitenplannen zijn in veel organisaties 'hard coded' papieren documenten. Een calamiteitenplan (DRP of BCP) is te beschouwen als een proces: wie doet wat, op welk moment, aan wie rapporterend, na en vooruitlopend op welke andere activiteit. Het plan als proces vastgelegd, met relaties naar actuele data (contactinformatie in een HR systeem bijvoorbeeld), levert veel betrouwbaarder plannen.
Het als proces vastgelegde calamiteitenplan geeft de mogelijkheid om met moderne alert- en communicatiefunctionaliteit heel adequaat te informeren. Nog meer dan anders is in geval van een calamiteit de behoefte aan gerichte en heldere communicatie erg groot. Op medewerkerniveau zou geïnformeerd moeten worden over wat van hem of haar wordt verwacht. Niet meer en niet minder. Niet het hele plan, maar gerichte informatie. Met de mogelijkheid om in een feedback loop informatie terug te geven over voortgang en resultaat. Alleen deze informatie samen, geeft een complete audit trail en een heel leerzaam traject nadien.

Bij een financiële dienstverlener migreerden we de bestaande hardcoded plannen naar een gestructureerd vastgelegd proces. Daarbij legden we contactinformatie eenmalig op één plek vast.

Met een geïntegreerde, krachtige reportgenerator bleek met de data uit de database exact hetzelfde document te genereren. Zo goed lijkend, dat het aanvankelijk tot enige verwarring leidde over wat er ten opzichte van de 'oude' situatie was bereikt. Toen de inhoud in de applicatie werd getoond werd al snel duidelijk dat op gebied van beheer en gebruik enorme winst was geboekt.

Een wijziging in de data (met in ons geval het vasthouden van versies) leverde de mogelijkheid om direct aansluitend een gewijzigd plan te printen. Met gebruikmaking van een peildatum was ook de oude versie te genereren.

Intelligente systemen

Een kennisdatabase als brug tussen incident en calamiteitenplan. Vooraf vastgelegde, incidentsituaties (scenario's) en in de loop van de tijd vastgelegde werkelijke incidenten, kunnen een kennisbank vormen. Aan een vastgelegd scenario kan een calamiteitenplan

worden gekoppeld. Als bij het registreren van een incident (handmatig of vanuit automatische monitoring, zie hierna) een match in de kennisdatabase gemaakt kan worden, kan dit leiden tot het geautomatiseerd in uitvoering brengen van een calamiteitenplan.

Zo wordt BCM: van handmatig beheren, effectief reageren.

Bij veel organisaties merken we dat de behoefte toeneemt om het BCM proces in te richten als een proactief managementproces. 'Papieren tijgers' van weleer worden meer en meer vervangen door samenhangende gegevens. Met het complexer worden van bedrijfsprocessen, wet- en regelgeving en risico's neemt de behoefte aan effectiever en efficiënter geïnformeerd worden toe.

Monitoring en alerting

Met doelstellingen, bedrijfsprocessen, risico's en controls gestructureerd (als parameters) vastgelegd, en koppelingen naar (primaire) bronsystemen, is geautomatiseerde monitoring in te richten. Geautomatiseerde, continue monitoring kan een enorme efficiencyverbetering opleveren ten opzichte van traditioneel BCM.

Monitoring van doelstellingen, risico's en controls, maar ook van voortgang van in een geautomatiseerde omgeving uitgezette assessments of tests, kan leiden tot versturen van alerts. Ook de voortgang van incidentmanagement kan met monitoring alerts opleveren.

Alleen al het gestructureerd vastleggen (als proces) van recovery- of calamiteitenplannen, geeft de mogelijkheid om de juiste betrokkene op het juiste moment van de juiste informatie te voorzien. Deze toepassing van alerting functionaliteit zien we in het proces van een meer integrale inrichting van het BCM proces vaak als eerste.

Bij alert functionaliteit worden in onze optiek uiteraard hedendaagse communicatietechnieken ingezet als e-mail, sms en mobile web services.

Zo wordt BCM: van effectief reageren, proactief anticiperen.

Daar waar BCM de enge definitie van beheersing van ICT risico's betreft, bestaan al veel monitoring systemen. Het betreft hier wel point solutions. Geen relatie met de business, geen koppeling naar DRP's/BCP's.

Ook van andere risico's en controls zal het van grote waarde blijken te zijn als we ze als parameters kunnen vastleggen. De geparametriseerde grootheden kunnen we met behulp van data uit andere (bron)systemen monitoren.

Bij het risico van het uitbreken van de vogelgriep kan middels het monitoren van de indicator ziekteverzuim, mogelijk in combinatie met nieuwsalerts uit externe nieuwsbronnen, geautomatiseerd een incident gemeld worden. Na matching met een vastgelegd scenario kan dit leiden tot automatisch opstarten van een calamiteitenplan.

Nieuwe generatie BCM software

Software die ondersteunend is aan een geïntegreerd BCM proces als hier beschreven, moet schaalbaar zijn, fasegewijs ingevoerd kunnen worden, maar bovenal: de kunst verstaan om met behoud van bestaande systemen en data (geen desinvestering) samenhang aan te brengen. Het heeft functionaliteit gebundeld in zich die eerder in versnipperde omgevingen te vinden was. Naar onze inzichten heeft de nieuwe generatie BCM software een hoge mate van flexibiliteit die het mogelijk maakt het BCM proces, analyses en rapportages naar eigen wensen in te richten.

In een open vraag naar wat men verwacht van een BCM software, is (nog steeds) vaak het antwoord: een goede documentatie- en planningtool. In het onderzoek is gestuurd gevraagd naar de terreinen waar meerwaarde wordt verwacht van een 'dedicated' BCM applicatie. Hooggespannen zijn de verwachting van de applicatie als het gaat om het zijn van een dashboard reporting tool. Maar ook heel vaak wordt aangegeven dat wordt verwacht dat de applicatie het mogelijk maakt om een connectie te maken tussen Risk management en Business. Het goed inrichten en onderhouden van de crisisorganisatie - en de actuele weergave daarvan in calamiteitenplannen - scoort tot slot ook hoog.

Ergo

Het speelveld van BCM overziend, nemen we een vijftal ontwikkelingen waar: BCM

1 wordt steeds meer een integraal riskmanagement proces,
2 dat steeds meer vanuit de business gedreven wordt,
3 dat meer en meer een proactief in-control managementproces wordt,
4 dat integraler wordt, meer dan ICT alleen,
5 en verschuift van 'noodzakelijk kwaad' als gevolg van wet- en regelgeving, naar door de markt gevraagde transparantie.

De stand

De mate van volwassenheid waarmee BCM in organisaties wordt opgepakt en ingericht, varieert enorm. Natuurlijk: branche afhankelijk, omvang afhankelijk en afhankelijk van 'wet- en regelgeving gevoeligheid'. Toch lijkt er een bewustwording op gang te komen dat versnippering opheffen één van de eerste grote stappen voorwaarts is. Daarmee is het niet de oude wijn in de nieuwe zakken, maar wel met bestaande kennis, deelprocessen en organisatieonderdelen een nieuw proces inrichten. Bekende druiven, maar een andere wijn dus.

Dat juist het proces dat gericht is op het garanderen van de continuïteit van de bedrijfsvoering, zelf nog een behoorlijke ontwikkeling doormaakt, waarbij de kwaliteit van dat proces zelf sterk gaat (en moet) toenemen, is paradoxaal te noemen…

Het integrale rapport van het genoemde onderzoek is op te vragen bij de auteur: sjoerd@bcon-pro.com.

Economische crisis vraagt om het economisch borgen van informatiebeveiliging

Auteur: Saïd El Aoufi > Saïd El Aoufi is werkzaam als senior consultant bij MetaPoint B.V. en is bereikbaar via said.el.aoufi@metapoint.nl.
Met dank aan Norien Kuiper en Louis van Hemmen voor de review dit artikel.

De economische crisis zet IT-budgetten onder druk. IT-afdelingen proberen kosten te besparen en efficiënter te werken. In het licht van kostenbesparingen zullen de uitgaven ten behoeve van informatiebeveiliging nog beter moeten worden gerechtvaardigd. Beperkt budget en andere concurrerende kapitaalinvesteringen vormen uitdagingen die investeringen in informatiebeveiliging bedreigen. Organisaties moeten het budget voor informatiebeveiliging veiligstellen en juist in het huidige economische klimaat investeren in informatiebeveiliging. Risico's zijn immers toegenomen doordat criminelen zullen inspelen op de huidige economische situatie. Dit artikel gaat in op de uitdagingen rond informatiebeveiliging die zijn ontstaan door de economische crisis. Het geeft bovendien adviezen hoe informatiebeveiliging geborgd kan worden.

Organisaties zijn in grote mate afhankelijk van hun informatiesystemen die een vitale rol spelen in, en deel uitmaken van hun bedrijfsprocessen. Met de snelle groei van de afhankelijkheid van organisaties van hun informatiesystemen vereist informatiebeveiliging meer en meer de aandacht. Er zijn inbreuken op beveiliging die belangrijke bedreigingen opleveren voor en een negatieve invloed kunnen hebben op de betrouwbare uitvoering van bedrijfsprocessen. Denk hierbij aan de waarde van het bedrijf, bijvoorbeeld de winst, de aandeelhouderswaarde of de reputatie. Vertrouwelijke informatie komt steeds vaker op straat te liggen. Volgens een recent onderzoek van KPMG (KPMG, 2009) is wereldwijd het aantal gevallen waarin melding is gemaakt van verlies of openbaarmaking van gevoelige gegevens vorig jaar gestegen tot 427 incidenten. Volgens het onderzoek lijkt er een sterk verband te bestaan tussen de stijging van het aantal incidenten en het verslechterende economische klimaat. Als gevolg van de economische crisis zal het aantal incidenten, waarbij gevoelige gegevens verloren gaan of openbaar worden, nog verder stijgen. Organisaties in zowel het private als het publieke domein zullen als gevolg van investeringsbeperkende maatregelen kwetsbaar zijn en blijven voor verlies en/of diefstal van gevoelige gegevens. Een onderzoek van McAfee toonde aan dat beveiligingsproblemen tijdens een economisch crisis erger worden. McAfee ondervroeg wereldwijd meer dan duizend hooggeplaatste beslissers in de IT. De grootste dreiging die aan de economische crisis kan worden toegeschreven, bestaat volgens 42 procent van de respondenten uit ontslagen werknemers, gevolgd door gegevensdieven van buitenaf.

Investeringen in informatiebeveiliging

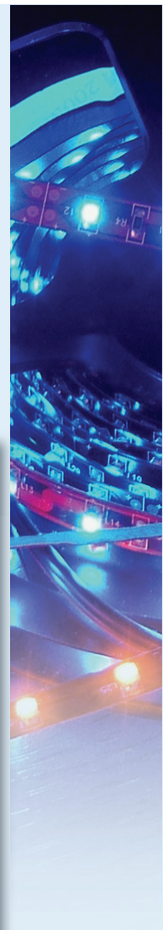
Het CSI survey (Richardson, 2008) toonde aan dat één tot vijf procent van het IT-budget aan informatiebeveiliging is toegewezen. Volgens Gartner wordt drie tot zes procent de richtlijn die organisaties zouden moeten hanteren; met een gemiddelde van tien procent voor organisaties waar de risico's groot zijn, bijvoorbeeld in geval van financiële instellingen. Hoewel volgens Gartner de uitgaven ten behoeve van informatiebeveiliging dus rond de drie tot zes procent van het totale IT-budget zouden moeten liggen, is dat percentage om een aantal redenen onderhevig aan veranderingen. Ten eerste is informatiebeveiliging voor steeds meer organisaties belangrijk. Ten tweede vergt het beheren van beveiligingsincidenten tegenwoordig steeds meer middelen dan vroeger. De kosten van de informatiebeveiliging groeien hierdoor sneller (denk hierbij aan beveiligingspersoneel).

Laag IT-budget betekent veiligstellen van investeringen in informatiebeveiliging

De economische crisis zet IT-budgetten onder druk. IT-afdelingen zullen proberen kosten te besparen en efficiënter te werken. Uit onderzoek van KPMG IT Advisory (KPMG, 2009) blijkt dat ruim zeventig procent van de onderzochte bedrijven op dit moment actief bezig is met het reduceren van IT-kosten. Nog eens tien procent van de bedrijven verwacht op korte termijn maatregelen te nemen om de kosten van IT terug te brengen. Belangrijkste argumenten voor de IT-kostenreductie zijn vooral de economische vooruitzichten.

Wat betekent de economische crisis voor organisaties?

Risicomanagement en risicoanalyse zijn niet langer theoretische oefeningen als onderdeel van de waarschijnlijkheidsberekening, maar een noodzakelijke exercitie om mogelijke bedreigingen tegen te gaan en bij te dragen aan de stabiliteit van de bedrijfsvoering. Wet- en regelgeving zullen een nog belangrijker rol spelen en er zullen nieuwe bedreigingen ontstaan die de effectiviteit van getroffen beheersmaatregelen toetsen. Tegelijkertijd zullen de uitgaven ten behoeve van informatiebeveiliging moeten worden gerechtvaardigd in het licht van kostenbesparingen als gevolg van de economische crisis. Beperkt budget en andere concurrerende kapitaalinvesteringen vormen blijvende uitdagingen die investeringen in informatiebeveiliging bedreigen. Investeringen in informatiebeveiliging moeten geprioriteerd en gerechtvaardigd worden. Veelal zal een businesscase nodig zijn om nieuwe of lopende investeringen te rechtvaardigen. Recent onderzoek (zie El Aoufi, 2009) maakt duidelijk dat informatiebeveiliging niet alleen een technisch probleem is, maar ook een onderwerp dat vanuit een economische invalshoek benaderd moet worden. De focus verschuift van wat technisch mogelijk is



naar wat economisch optimaal is. Beperkte middelen voor investeringen in informatiebeveiliging betekent keuzes maken met betrekking tot de toewijzing van deze middelen. Zelfs al hebben organisaties onderkend dat informatiebeveiliging belangrijk is, dan nog is het nemen van beslissingen over de omvang van deze investeringen een uitdaging. Organisaties moeten nadenken over hoe zij effectieve informatiebeveiliging kunnen realiseren tegen lagere kosten én hoe informatiebeveiliging kan bijdragen aan het eindresultaat van de bedrijfsvoering. De eisen vanuit de bedrijfsvoering dienen te worden vertaald in businessoplossingen en de kosten dienen gerechtvaardigd te worden.

Samengevat volgen in onderstaand kader enkele adviezen voor organisaties om informatiebeveiliging economisch aantrekkelijker te maken:

Het prioriteren van investeringen voor beveiligingsprojecten
Door de huidige economische crisis is het van belang dat binnen organisaties het toegewezen budget voor informatiebeveiliging optimaal gebruikt wordt. Verbetering hiervan kan onder meer worden bereikt door een aantal activiteiten uit te zetten om het bewustwordingsniveau, en daarmee de beslissingen ten aanzien van beleid en budget te verbeteren. Organisaties moeten bepalen met welke investeringen concrete doelstellingen tegen een zo laag mogelijke prijs gerealiseerd kunnen worden (kostenminimalisering). Daarbij moet het effect van de maatregelen maximaal bijdragen aan het realiseren van de doelstelling (effectmaximalisering). Het maken van een businesscase is hierbij essentieel.

Het ontwikkelen van een flexibele aanpak voor grote investeringsprojecten
Grote investeringsprojecten dienen anders te worden aangepakt. Het is van belang om grote projecten te splitsen in kleinere subprojecten die aan kleinere teams worden toegewezen. Dit is een noodzakelijke aanpak gezien het economische klimaat, waar geen of beperkte budgetten of middelen zijn om maanden cq. jaren aan een project te werken. Flexibiliteit speelt hierin een grote rol.

Risico-bewustwording
Managers zijn snel geneigd om risico's te accepteren in plaats van geld uit te geven om deze risico's te mitigeren. Juist in de tijd waarin het economisch niet goed gaat, zijn de risico's toegenomen en moeten managers dus kritischer kijken naar deze risico's. Adequate risicoanalyses moet niet alleen gezocht worden in technologie of strengere procedures, maar vooral in de menselijke component van besluitvorming.
Bedreigingen van binnenuit groeien wanneer het slecht gaat met de economie. Denk hierbij aan ontslag of slechte behandeling van medewerkers. Dat zal voor sommigen een reden zijn om het rechte pad te verlaten.
Het is van belang om in de toekomst, als onderdeel van risicomanagement, veel meer aandacht te schenken aan de risicobereidheid (risk appetite), deze te expliciteren en vergelijkbaar te maken. Professionals kunnen het management hierbij helpen door de risico's goed in te schatten en de juiste afwegingen te maken.

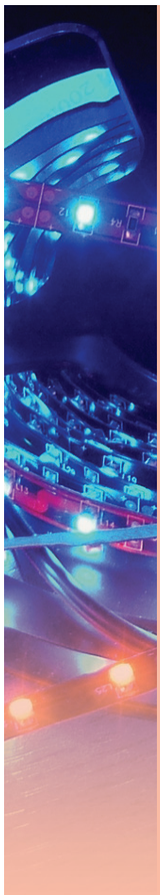
Informatiebeveliging als een investering zien
Hoewel het belang van informatiebeveiliging begrepen wordt, beschouwen organisaties informatiebeveiliging als een kostenpost. Informatiebeveiliging blijft moeilijk te verkopen aan businessmanagers. Als informatiebeveiliging wordt gezien als 'investering' in plaats van als 'kostenpost' zal de businessmanager een andere kijk op informatiebeveiliging krijgen. Nieuwe businesskansen kunnen bijvoorbeeld mogelijk worden gemaakt door effectieve informatiebeveiliging. Wanneer organisaties informatiebeveiliging als een investering gaan zien, wordt het ook waarschijnlijker dat organisaties inspanningen verrichten om de toegevoegde waarde van informatiebeveiliging zichtbaar te maken (net als bij andere investeringen). Dan zullen regelmatig betekenisvolle metingen die gebruikt worden om de effectiviteit te beoordelen, worden verzameld en gerapporteerd. Deze informatie kan vervolgens worden gebruikt om beveiligingsactiviteiten te waarderen en te prioriteren.

Bescherming dichtbij de gevoelige data zetten
Complexere en sneller veranderende business vergt meer data en meer infrastructuur. Data wordt breder verspreid, meer gedeeld en is voortdurend in beweging. Zo is er ook veel meer vraag naar grotere mobiliteit en samenwerkingsmogelijkheden. Omdat gevoelige informatie altijd in beweging is, is het ook kwetsbaarder, want met elk beweging worden risico's geïntroduceerd. Het is daarom ook een uitdaging om de snellere businessveranderingen te ondersteunen terwijl de data goed beschermd is, zoals de business dat vraagt. Het is nog uitdagender wanneer het economisch klimaat slecht is en medewerkers zich meer zorgen maken over hun toekomst. Organisaties dienen ervoor te zorgen dat waardevolle informatie goed is beveiligd en dat er snel en doeltreffend gereageerd kan worden op nieuwe bedreigingen. Organisaties zouden meer moeten nadenken over een informatiecentrische aanpak voor informatiebeveiliging en architectuur, dus het verschuiven van bescherming dichter naar de gevoelige informatie.

conclusie
Met het snijden in IT-budgetten, nu en in de toekomst, en het vaker stellen van de vraag hoe schaarse middelen zullen worden aangewend, is een businesscase in een vroeg stadium essentieel. Organisaties dienen beveiligingsinvesteringen te prioriteren en te rechtvaardigen. De CISO zal zijn of haar beveiligingsprogramma aanpassen aan de situatie zoals die is ontstaan door de economische crisis. Wanneer de businessprioriteiten veranderen, zal aansluiting moeten worden gezocht. Dit betekent dat de prioriteiten en het programma voor informatiebeveiliging mee moeten veranderen.

Referenties

- (El Aoufi, 2009) *Saïd El Aoufi, 2009, Economic Evaluation of Information Security, Ph.D. thesis, VU University Amsterdam*
- (ISBS, 2008) *Information Security Breaches Survey 2008*
- (KPMG, 2009) *Meerderheid Nederlandse bedrijven snijdt in IT-budgetten, www.kpmg.nl*
- (Richardson, 2008) *CSI Computer Crime & Security 2008*



Verkiezing 'Artikel van het jaar Informatiebeveiliging'

En de winnaar is...

Auteur: Leo van Koppen > Namens de jury van de 'Artikel van het jaar-verkiezing'

Voor het eerst een 'Artikel van het jaar-verkiezing', dus kwam ook voor het eerst in haar bestaan de jury bij elkaar om een uitspraak te doen over het artikel van het jaar 2008 uit het blad Informatiebeveiliging. De jury bestaande uit John Rudolph, Kees Hintzbergen en ondergetekende Leo van Koppen heeft zich op donderdag 9 april gebogen over het beste artikel van het afgelopen jaar. In dit verslag leest u de uitkomst en het uiteindelijke oordeel van de jury.

Bij een blad als Informatiebeveiliging en de bijbehorende cultuur van de beroepsgroep is het van belang dat er sprake is van een transparant proces van uitverkiezing. Geen 'achterkamertjes gedoe', maar een open en eerlijke beoordeling op basis van heldere criteria. Hierover was de jury het onderling al snel eens, maar helaas moesten we constateren dat we geen van drieën inzicht hebben gekregen in de wijze waarop de ons aangeboden shortlist tot stand is gekomen... Daar ga je dan met al je goede uitgangspunten, wellicht ligt de reden hiervan in het feit dat het onze taak is om slechts uit de shortlist van zeven titels een winnaar te kiezen.

We hadden een levendige discussie waarin argumenten over en weer gingen en uiteindelijk was er één winnaar. Ieder van ons heeft zich aan de hand van de door de hoofdredacteur opgestelde criteria voorbereid op deze bijeenkomst. Voor de duidelijkheid zijn de criteria in het bijgaand kader weergegeven.

Beoordelingscriteria
1. Opzet van het artikel
2. De leesbaarheid
3. De doelgroep
4. Vernieuwend element
5. 'Out of te box' denken

Ieder jurylid had een persoonlijke lijst opgesteld en had zijn keuze onderbouwd met argumenten. De top drie van deze lijstjes bleek bij alle juryleden hetzelfde, alleen de volgorde van de nummers één tot en met drie verschilde onderling. Na wat eerste bespiegelingen en een uitwisseling van argumenten over de verdeling van de podiumplaatsen, besloten we eerst de onderste helft van de ranglijst eensgezind vast te stellen, om daarna de top drie te bepalen.

Als de genomineerde artikelen een goede weergave vormen van waar we ons binnen het vakgebied informatiebeveiliging mee bezighouden, dan is het beeld dat opdoemt dat van groei naar volwassenheid waarbij we elkaar alert houden over zaken die ertoe doen en modellen waarin we meer grip willen krijgen op de samenhang in ons vakgebied. Soms is dat opiniërend, de andere keer is dat weer heel feitelijk al dan niet in een poging te komen tot een verbindende schakel in de vorm van een nieuw model. We zijn er ten slotte uitgekomen!

Op de derde plaats is geëindigd het artikel over het forensisch framework van Hans Buijtelaar, waarbij de waardering van de jury vooral uitging naar het feit dat de auteur de moed heeft getoond ongebaande paden te betreden en op een zeer heldere en gedegen manier een model heeft neergezet dat bruikbaar is en als referentie kan dienen bij ontwikkelingen op het terrein van forensics in relatie tot informatiebeveiliging. Vanwege de lengte van dit verslag zal ik niet alle argumenten uit de discussie aanhalen die uiteindelijk hebben geleid tot de eerste en tweede plaats. Beide artikelen komen naar de mening van de jury echter in aanmerking voor een prijs, juist omdat ze zo verschillend zijn en daardoor moeilijk met elkaar te vergelijken.

Hoewel het 4-aspecten model van Alf Moens zich richt op een kleinere doelgroep biedt het goede kansen om ook door andere doelgroepen te worden overgenomen. Het artikel is helder qua opbouw en geeft, onderbouwd met onderzoek, aan dat volwassenheidsmodellen in volwassenheid groeien. Uiteindelijk zijn we unaniem van mening dat het artikel 'monsterlijke trekjes van beveiligingsproblemen' van Wolter Pieters met de eerste plaats beloond moet worden. De auteur is er op meesterlijke wijze in geslaagd ons een spiegel voor te houden. Hij wijst ons erop dat we alert moeten zijn met betrekking tot het denken in modellen omdat deze modellen ook weer allerlei beperkingen met zich meebrengen. Ook geeft hij aan dat we vooral over de muren van ons eigen werkterrein heen moeten kunnen kijken, dat informatiebeveiligingsproblemen met andere woorden niet opgelost kunnen worden met een kookboek en dat andere domeinen in veel gevallen al oplossingen kennen voor soortgelijke problemen in informatiebeveiliging. Dit alles verpakt de auteur in een mooie metafoor, waardoor het artikel naast het feit dat het een vernieuwend karakter heeft ook nog eens heel plezierig leest. Kortom een terechte eerste plaats. Voor degenen die het winnende artikel nog niet kennen of voor degenen die het nogmaals willen lezen, hebben we het artikel van Wolter Pieters vanaf pagina 23 nogmaals geplaatst.

Daarmee is ons werk gedaan en kijken we alweer uit naar de lijst van 2009. Hopelijk vinden meer auteurs inspiratie om de komende maanden hun kennis en inzicht te gaan delen en te opteren voor een nominatie voor de verkiezing van het Artikel van het jaar 2009. Wij zijn, denken we, helder geweest in ons oordeel; het is nu aan de redactie om nog duidelijkheid te verschaffen over de prijsuitreiking en natuurlijk nog over de totstandkoming van de shortlist.

De monsterlijke trekjes van beveiligingsproblemen

Auteur: dr. ir. Wolter Pieters > Wolter Pieters is op 21 januari 2008 gepromoveerd aan de Radboud Universiteit Nijmegen op een proefschrift over de stemcomputercontroverse.

Geen grote rode knop meer op verkiezingsdag. De stemcomputers zijn afgeschaft; ze bleken niet betrouwbaar genoeg. Hoe komt het dat dit niet eerder is ontdekt? Het zit 'm in de monsterlijke trekjes van beveiligingsproblemen. Net als monsters in films tarten ze onze hokjes door te lijken op dingen die we kennen, maar toch ook weer niet. Monsterbezwering kan helpen om beveiligingslekken eerder te identificeren.

Pangolins en tweelingen

Bron: estherase via Flickr

Gevaarlijk, niet echt verwant aan iets wat we kennen, of toch weer wel, en bij voorkeur groen. Bij een monster denken we doorgaans aan Frankensteinachtige figuren in films. Monsters lijken daarbij vooral gekarakteriseerd te worden door hun wereldvreemdheid en verwoestende gedrag. Die wereldvreemdheid gaat echter niet zo ver dat we niets herkennen in de monsters. Hoe eng ze ook zijn, ze hebben toch vaak iets menselijks, en, zoals in het geval van Frankenstein, iets dat daar lijnrecht tegenover staat: iets machinaals. Ze passen, met andere woorden, niet in ons hokjesdenken.

Al sinds mensenheugenis worden zaken die niet in de bekende hokjes passen afgeschilderd als monsterlijk. De combinatie van eigenschappen die doorgaans niet samen voorkomen, leidt al snel tot een afschuw van of juist fascinatie voor het onbekende. Zo werd de pangolin (geschubde miereneter) door het Lele-volk als heilig beschouwd, omdat deze schubben heeft als een vis, in bomen klimt en de jongen zoogt. Andere stammen beschouwen tweelingen op hun beurt als verschrikkingen, omdat ze dierlijke aspecten – het krijgen van meerdere nakomelingen – combineren met menselijke.

Plastic en gentech

Ook in de moderne maatschappij vinden we monsters. In haar boeken *Purity and danger* en *Risk and culture* toont antropologe Mary Douglas dat de vaak als primitief beschouwde hokjesgeest in de moderne maatschappij alles behalve verdwenen is. Veelal hebben we de neiging te denken dat de moderne wetenschap volgens volstrekt andere principes werkt en dat de primitieve indeling van de wereld en de daarbij behorende ambiguïteiten verleden tijd zijn. Ook de wetenschap denkt echter in hokjes. Wanneer we gewend zijn aan categorieën als ruimte en tijd, vergt het een Einstein om een theorie te ontwikkelen die de relativiteit van beide als basis heeft. Ook wij hebben onze indelingen – en we hebben moeite met dingen die daar niet in passen.

De Nederlandse techniekfilosofe Martijntje Smits liet zien dat dit idee ook toe te passen is op controverses over nieuwe technologie. Technologie is bij uitstek een middel om dingen te creëren die niet binnen de bestaande kaders passen. Reacties van fascinatie en afschuw vonden we bij bijvoorbeeld de uitvinding van plastics. Deze materialen leken in niets op de bekende natuurlijke producten en konden bovendien rekenen op de aandacht van zowel sciencefictionfans als doemdenkers.

Meer recent was (en is) genetische manipulatie onderwerp van controverse. Ook hier staat weer het natuurlijke tegenover het kunstmatige. In hoeverre zijn die twee aspecten te verenigen? Mag je sleutelen aan iets dat natuurlijk is? En waar liggen dan de grenzen van de hokjes?

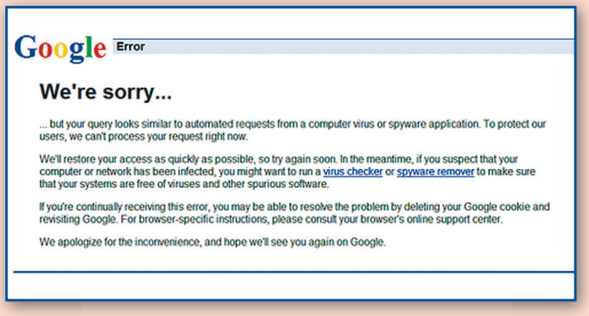
Ook in de IT kunnen monsters gefabriceerd worden. De stemcomputer heeft het niet gered, omdat de combinatie van de openheid van democratie en het black-box karakter van technologie toch wel erg problematisch leek te zijn. De vereiste transparantie van het verkiezingsproces kon schijnbaar niet waargemaakt worden door technologische ontwerpen die slechts door een enkeling te begrijpen waren. Los van de precieze argumenten voor of tegen was het dit monsterlijke karakter dat aan de basis lag (en ligt) van de discussie.

Sub-monsters

Dit soort effecten doet zich echter niet alleen voor op het niveau van een samenleving als geheel. Ook subculturen - wetenschappelijke disciplines, bedrijven, et cetera - kennen hun eigen categorieën, hun eigen hokjes en de daarbij behorende monsters. We moeten nu eenmaal ook binnen onze specialismen onderscheid maken tussen verschillende dingen - ze in een hokje kunnen plaatsen - om überhaupt iets te kunnen herkennen. Een specialist die niet geleerd heeft welke verschillende aandoeningen er zijn, zal ze op een röntgenfoto ook niet kunnen onderscheiden. Net zo goed als Chinezen het onderscheid tussen de L en de R niet horen.

Wat betekent dit voor de discipline van de informatiebeveiliging? Belangrijke beveiligingslekken doen zich vaak voor als iets over het hoofd is gezien. Denk je dat je alles dichtgetimmerd hebt, komt uit compleet onverwachte hoek toch nog een hacker binnen. Juist omdat deze manier niet in de bestaande hokjes paste. En dus niet in het handboek stond. Beveiligingslekken zijn in die zin monsters: fenomenen die onze categorieën uitdagen.

Een belangrijk monster in de informatiebeveiliging was het optreden van virussen in documenten. Oorspronkelijk had het concept 'virus' vooral betrekking op uitvoerbare bestanden (programma's). Deze werden dan ook door virusscanners onder de loep genomen. Het feit dat binnen Microsoft Word-documenten kleine stukjes programma aanwezig konden zijn (macro's) liet het toe dat de hokjes van programma en data niet langer adequaat waren. Het eerste virus in Word-bestanden werd dan ook als iets radicaal nieuws ervaren: een monster.



bron "Go away, you virus!" robleto via Flickr

Een ander voorbeeld is het verkrijgen van informatie over de gegevens op een smartcard aan de hand van het stroomgebruik of de tijdsduur van berekeningen, de zogenaamde side-channel attacks. Zo kan bijvoorbeeld de geheime sleutel worden verkregen waarmee berichten beveiligd worden. Wanneer je denkt in hokjes van hardware en software, dan zie je dit probleem helemaal niet. Het is immers noch een hardware noch een software-kwestie. De aanval zit 'm juist in dat wat de categorieën overstijgt: het afleiden van informatie over de software aan de hand van de hardware.
Wanneer we informatiebeveiliging vanuit deze antropologische hoek bekijken, zien we vooral een dynamisch spel van hokjes. Meer nog dan bijvoorbeeld social engineering vormt dit een essentieel onderdeel van de menselijke kant van informatiebeveiliging.

Perceptie en werkelijkheid

De meeste deelnemers aan discussies over informatiebeveiliging zijn echter geen antropologen. Veelal worden beveiligingsproblemen gekarakteriseerd in termen van werkelijke veiligheid en perceptie van veiligheid ('actual and perceived security'). Als er iets misgaat, wordt dat verklaard doordat in het verleden de werkelijkheid niet op de juiste wijze onder ogen is gezien, zoals bij de stemcomputers. Eerst bestond er vertrouwen in de apparaten op basis van een vertekend beeld van veiligheid, maar nu weten we hoe het werkelijk zit. Een bepaalde manier van naar de wereld kijken, wordt daarbij als de juiste gezien, namelijk degene die overeenkomt met de werkelijkheid.

Deze manier van denken bestond al bij de oude Grieken. Plato schreef een allegorie waarin mensen vastgebonden in een grot zitten en slechts de schaduwen kunnen zien van voorwerpen die door een vuur verlicht worden. Alleen de filosoof (die tegenwoordig allerlei gedaanten als wetenschapper kan aannemen) kan de grot verlaten en zien wat zich werkelijk afspeelt.
Het onderscheid tussen werkelijkheid en beelden daarvan wordt door wetenschapsonderzoekers als Bruno Latour gezien als een belangrijk kenmerk van het moderne westerse denken.

Foto: Jerzy Kociatkiewicz

De monster-theorie draait deze analyse om. Waargenomen veiligheid staat niet tegenover werkelijke veiligheid, maar tegenover niet-waargenomen veiligheid. We kunnen niet spreken van een werkelijkheid buiten onze waarneming; zelfs als deze zou hebben bestaan, hebben we er geen toegang toe. Immanuel Kant stelde dit in de achttiende eeuw al vast. Het gaat juist om wat we *wel* kunnen waarnemen. En, zoals we inmiddels ook weten, wat we kunnen waarnemen, wordt bepaald door onze hokjes. Dingen die daar niet in passen, ervaren we als monsters.
Dit betekent uiteraard niet dat we elke poging om iets zinnigs over onze omgeving te zeggen moeten opgeven, omdat toch iedereen zijn eigen waarheid heeft. Wel gaan we niet langer uit van één speciale visie op de wereld ('actual security') die anders is dan alle andere ('perceived security'). En door te erkennen dat het allemaal om waarneming gaat, kunnen we ook beter reageren op veranderingen daarin.

Monsterbezwering

Volgens Smits zijn er verschillende manieren om monsters het hoofd te bieden. Deze zien we ook allemaal terug in casussen uit de informatiebeveiliging.
Zo kunnen we monsters als iets buitengewoons beschouwen en daardoor een plaats geven als iets heiligs. In de informatiebeveiliging ontaardt deze strategie van *omarming* echter al snel in 'it's not a bug, it's a feature'. Stemcomputerfabrikant Nedap schreef in relatie tot de manipulatie van het apparaat door de actiegroep dat dit bewees dat de stemcomputer precies deed wat hem was opgedragen.
Ook kunnen we het monster *uitdrijven*. Het probleem wordt dan de kop ingedrukt door het weg te stoppen: een nieuwe technologie naar de prullenbak verwijzen of een beveiligingsprobleem ontkennen. Zolang de media niet al te hard op het lek duiken, heb je misschien een kans om er mee weg te komen zonder dat je systeem ook in de praktijk wordt gekraakt.

Ook bij de virussen in Word-bestanden werd aan monsterbezwering gedaan. De strategie die hier gevolgd werd, was het hercategoriseren van Word-bestanden als programma-

bestanden. Ze pasten niet langer in de categorie data, dus stopten we ze in een ander hokje. Daardoor werden ze nu ook door virusscanners gecontroleerd. Deze strategie heet *monsteraanpassing*: het herdefiniëren van het monster ten opzichte van de hokjes.

Assimilatie

Al deze strategieën hebben echter iets gemeen: de hokjes, de categorieën, blijven ongewijzigd. Sommige monsters vereisen een meer radicale aanpak. Zoals we al zagen werd het onderscheid hardware-software op de proef gesteld door zogenaamde side-channel attacks op smartcards. Een speciaal onderzoeksgebied was nodig om deze monsters het hoofd te bieden. Er ontstonden nieuwe hokjes, waarmee het probleem *wel* goed te definiëren was. We hebben de side-channel attacks nu netjes in categorieën ingedeeld en weten nu ook wat we aan maatregelen kunnen nemen om deze aanvallen tegen te gaan. Dit aanpassen van de hokjes noemt Smits *monsterassimilatie*. Deze laatste strategie biedt de meeste kansen binnen een filosofie die uitgaat van waargenomen veiligheid tegenover niet-waargenomen veiligheid in plaats van waargenomen veiligheid tegenover werkelijke veiligheid. Om veiligheid beter waar te kunnen nemen, moeten we steeds op zoek naar de beste hokjes. Om de monsters vóór te zijn, zouden we ons bij al onze hokjes af moeten vragen of er geen dingen buitengesloten worden die uiteindelijk als monsters de beveiliging van onze systemen zouden kunnen bedreigen.

De monsters van de stemcomputer

In het geval van de stemcomputer zijn er in ieder geval twee hokjes die eerder tot problemen hebben geleid. Ten eerste werd controleerbaarheid van de stemcomputer vooral gedefinieerd als het laten testen van het apparaat door TNO. Controleerbaarheid werd gezien als *controleerbaarheid van de stemcomputer zelf*. Door dit "hokjesdenken" werd over het hoofd gezien dat ook het resultaat van een verkiezing zelf wellicht controleerbaar zou moeten zijn. Juist deze laatste betekenis heeft in de recente discussie veel nadruk gekregen.

Een tweede 'hokje' werd gevormd door de bescherming van het stemgeheim. In de 'Regeling voorwaarden en goedkeuring stemmachines' werd gesteld dat de stemcomputer de stemmen op zodanig wijze moest opslaan dat een stem niet aan een kiezer gekoppeld zou kunnen worden. In de praktijk kwam dit neer op opslaan op een willekeurige plaats in het geheugen. Bescherming van het stemgeheim werd hierdoor echter impliciet gedefinieerd in termen van *software*. De problemen met compromitterende straling en het afluisteren van de stem waren daardoor niet gedekt door de eisen. Dat is immers vooral een *hardware*-probleem.
Als we deze verschuivingen van de hokjes beschrijven in termen van perceptie van veiligheid versus werkelijke veiligheid, zien we over het hoofd dat ook onze huidige categorieën per definitie dingen uitsluiten. We spreken, zeker als het gaat om risico's, over een werkelijkheid die we zelf met onze hokjes gemaakt hebben.

Monsters voorkomen?

Wat kan ons vakgebied hiervan leren? Als we als informatiebeveiligers blijven denken in termen van werkelijke veiligheid en waargenomen veiligheid, lopen we altijd het risico dat wat we werkelijke veiligheid noemen toch uiteindelijk niet de meest effectieve oplossing blijkt te zijn. Het gaat daarbij niet alleen om wat we zelf wel en niet zien, maar vooral ook om wat onze 'tegenstanders' wel en niet zien. Zodra de mogelijkheden om een stemcomputer af te luisteren eenmaal gedemonstreerd zijn, hebben we te maken met een veel hoger risico. Hetzelfde geldt voor het kopiëren van Mifare toegangspassen.
Met de Duitse filosoof Martin Heidegger kunnen we beter spreken van aspecten van veiligheid die verborgen zijn en aspecten van veiligheid die 'ontborgen' worden: uit de verborgenheid tevoorschijn worden gehaald. Zodra buffer overflows als een belangrijke bron van security-problemen worden ontborgen, duiken zowel hackers als beveiligingsexperts massaal op de mogelijkheden hiervan. Zo worden vergelijkbare risico's veel sneller zichtbaar gemaakt. Aan de andere kant blijven wellicht heel andere kwetsbaarheden daardoor juist verborgen.

Dit actieve karakter van het definiëren van wat werkelijk is, is essentieel in een proactieve houding ten opzichte van beveiliging. Bij elk aspect van risico dat we vaststellen zouden we dan ook moeten vragen: wat sluiten we uit? Wat past niet in de hokjes? Als we eisen dat software een bepaalde eigenschap heeft, dan stellen we dus meteen de vraag: is dit ook relevant voor de hardware? Systematisch op deze manier denken - denken als een antropoloog die een vreemde cultuur bezoekt - is uiteindelijk de enige manier om de bedreigingen voor te blijven. De dynamiek van de hokjes bepaalt immers wie er uiteindelijk wint: de beveiliger of de hacker.
Uiteraard is de monster-theorie zelf ook weer een indeling in hokjes en sluit deze daarmee zelf ook dingen uit. Maar dat is nu eenmaal de prijs die we betalen om de problemen van de informatiebeveiliging beter *waar te nemen*.

Samenvatting/conclusie

Het gaat bij informatiebeveiliging niet om perceptie van veiligheid versus werkelijke veiligheid, maar om verschillende groepen mensen die de wereld op verschillende manieren in hokjes indelen. Dit lijkt triviaal, maar in de manier waarop er over stemcomputers gesproken wordt, lijkt Plato's grot nog zeer dominant aanwezig. Het is dus tijd om onze hokjes wat serieuzer te gaan nemen. Ofwel: laten we zorgen dat onze indeling van het informatierijk zo weinig mogelijk pangolins kent.

URLs

http://www.cs.ru.nl/~wolterp
http://www.wijvertrouwenstemcomputersniet.nl
http://www.election-systems.eu

Literatuur

M. Douglas. Purity and Danger: *an Analysis of the Concepts of Pollution and Taboo*. Routledge, London, 1994 [1966].

B. Latour. Politics of nature: *how to bring the sciences into democracy. Harvard* University Press, Cambridge, MA, 2004.

W. Pieters and L. Consoli. Vulnerabilities as monsters: the cultural foundations of computer security (extended abstract). In: *Proceedings of the European Computing and Philosophy Conference (E-CAP 2006)*, Trondheim, Norway, June 22-24, 2006.

M. Smits. Monsterbezwering: *de culturele domesticatie van nieuwe technologie*. Boom, Amsterdam, 2002.

De normatieve impact van ambient technology en converging technologies:

Privacy en (veel) meer

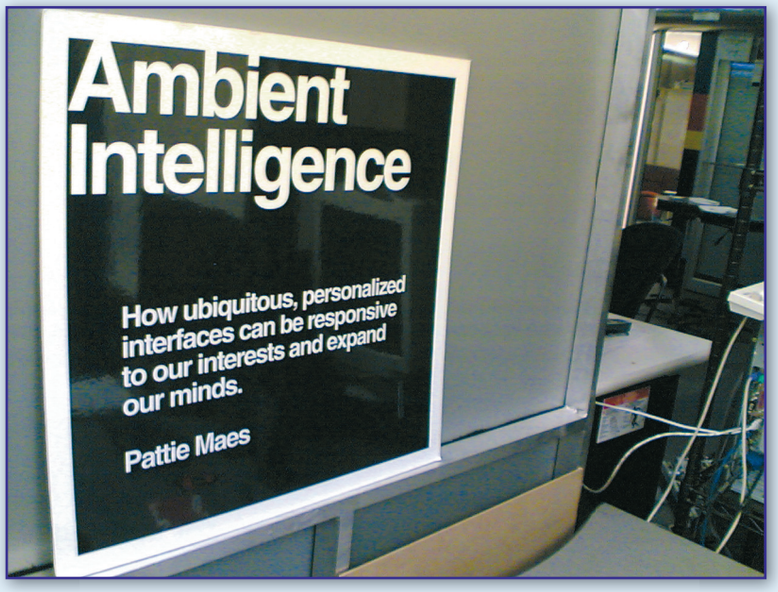
Auteur: Anton Vedder > Dr Anton Vedder is Univeritair Hoofddocent Ethiek en Recht bij TILT, het Centrum voor Recht, Technologie en Samenleving van de Universiteit van Tilburg.

We staan aan de vooravond van grote veranderingen in onze leefwereld. Hippe benamingen als 'ambient intelligence' en 'convergerende technologieën' kondigen voor de komende tien tot vijftien jaar belangrijke ontwikkelingen aan. Welke gevolgen zullen deze veranderingen hebben voor onze manier van samenleven? Hoe moeten we er tegenover staan? Soms lijken er in de discussies over techniek maar twee kampen te bestaan. Enerzijds is er het kamp van degenen die dol zijn op vernieuwing en alleen oog hebben voor de voordelen. Anderzijds is er het kamp van de bezorgde toeschouwers die naast alle goeds vooral veel nadelen zien. Hiertoe behoort in elk geval een groot deel van de mensen die zich professioneel met ethiek en recht rond nieuwe technologie bezighouden.

Dat de zorgen vooral onder deze groep breed gezaaid zijn, hoeft geen verbazing te wekken. Hun professionele 'grondstof', het normatieve perspectief, is organisch verbonden met de bestaande leefwereld. Wanneer met behulp van bestaande normen en waarden toekomstige ontwikkelingen worden beoordeeld, zal er achter dat oordeel altijd een zeker conservatisme schuilgaan. Men oordeelt immers vanuit een leefwereld waarin de aangekondigde ontwikkelingen nog niet bestaan.
Het is echter de vraag of deze traditioneel zorgelijke kijk verstandig is. Aan de hand van enkele voorbeelden van de mogelijke maatschappelijke impact van ambient intelligence en convergerende technologie zou ik willen pleiten voor wat minder somberheid en wat meer bezinning op de bestaande normatieve kaders.

Waar hebben we het over?
Ambient intelligence staat voor het geleidelijke opgaan van techniek en technologie in de omgeving en voor het steeds meer en beter communiceren van apparaten met elkaar en met hun gebruikers. Dit wordt mogelijk door:

- voortgaande miniaturisering van computers, sensoren en actuatoren (instrumentjes om processen in gang te zetten of bij te sturen),
- vergroting van opslag-, transmissie- en bewerkingscapaciteit van gegevens, en
- alomtegenwoordigheid van netwerken en draadloze communicatiemogelijkheden.



Ambient Intelligence
(bron: akaalias, www.flickr.com)

Apparaten zullen steeds minder om bediening vragen door middel van knoppen, menu's of toetsenborden en beeldschermen. Ze zullen zelf achterhalen wat we van ze verwachten en daarop reageren of anticiperen.

Convergerende technologieën staan voor toepassingen die voortkomen uit de kruisbestuiving tussen nanotechnologie, biotechnologie, informatie- en communicatietechnologie en cognitieve wetenschappen. Naast vele andere mogelijkheden zullen in elk geval extra mogelijkheden worden geschapen om van buitenaf in te grijpen in het gedrag van mensen. Deze toepassingen kunnen voor een deel als vervanging gaan dienen voor de nu bekende manieren om mensen te beïnvloeden, zoals opvoeding, onderwijs, pillen, hekken, muren en geschreven en ongeschreven wetten.
Welke impact kunnen deze technologieën hebben op onze manier van (samen)leven? Ik noem slechts enkele voorbeelden.[1]

Privacy achterhaald
Voor het realiseren van toepassingen van ambient technology en convergerende technologieën zal veel meer informatie worden gegenereerd, bewerkt en gecombineerd dan we ons nu kunnen voorstellen. Om de technologieën te laten

[1] De volgende analyse is grotendeels gebaseerd op: Teeuw, W.B., A.H. Vedder (eds.) (2008), Security Applications for Converging Technologies. Impact on the constitutional state and the legal order, Den Haag: Boom Juridische uitgevers; Vedder, A. Convergerende technologieën, verschuivende verantwoordelijkheden. Justitiële Verkenningen 2008; 34; 1: 54-66; Vedder, A.H., De oudere en de paradoxale gevolgen van nieuwe technologieën. In: Berg, M. van den, J.E.J. Prins en M. Ham (red.), In de greep van de technologie - Nieuwe toepassingen en het gedrag van de burger. Amsterdam: Van Gennep, 2008, p. 135-150; Vedder, A.H. e.a., Van privacy-paradijs tot controle-staat? Opsporing, terreurbestrijding en privacy aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut, 2007.

werken en de toepassingen te kunnen laten functioneren zal er over individuen vrijwel continu allerlei informatie over hun fysieke toestand, locatie, context (bijvoorbeeld familiale en sociale achtergrond) moeten worden verzameld en geanalyseerd. Deze ontwikkeling vereist een grondige herziening van het gangbare privacydenken. De huidige privacy wet- en regelgeving zal haar zin grotendeels verliezen. Allereerst is die grotendeels gebaseerd op de vooronderstelling dat individuele personen in staat moeten zijn om controle uit te oefenen over wat er met gegevens en informatie over hen gebeurt. In de toekomst zal van het individu echter steeds minder verwacht kunnen worden dat hij die controle uitoefent. De informatiehuishouding over en rond hem wordt simpelweg te complex en onbevattelijk.

In de tweede plaats beperken bestaande gegevensbeschermingsregelingen zich tot persoonsgegevens die nogal rigide worden gedefinieerd als gegevens die tot individuele personen te herleiden zijn. Bij veel van de gegevens en informatie die in de toekomst moet worden gegenereerd zal het echter niet gaan om persoonsgegevens, maar om gegevens of profielen van groepen.

Tenslotte zullen we onder invloed van *converging technologies* te maken krijgen met een fenomeen dat belangrijke consequenties kan hebben, maar waarvoor het huidige privacydenken geen enkel handvat biedt om onze houding richting te geven. De toepassingen van converging technologies zullen leiden tot een grote toename van gegevens over de fysieke en klinische toestand van mensen. Dit brengt in feite een enorme domeinexpansie van medische gegevens met zich mee. Medische gegevens zullen niet meer alleen relevant zijn in de traditionele domeinen van de zorg, met hier en daar wat uitbreidingen naar het domein van verzekeringen. Ze zullen eveneens een grote rol gaan spelen op terreinen als veiligheid en onderwijs en zo tot een ongekende medicalisering leiden.

Dit alles nodigt niet zozeer uit tot een verdere aanscherping of haarkloverij over privacy. Veeleer zou het moeten aanzetten tot een radicale bezinning over een nieuw type medicalisering en, meer in het algemeen, de informatiehuishouding in onze maatschappij. Daarbij zou met name ook kunnen worden gekeken of de techniek zelf een rol kan spelen bij een heilzame vormgeving van die informatiehuishouding. De techniek zal zonder meer al een grote rol kunnen spelen bij alle beveiligingsproblemen veroorzaakt door de extra informatiseringsgolf die *ambient intelligence* en *converging technologies* met zich mee zullen brengen.

Respecting Privacy (bron: joe shlabotnik, www.flickr.com)

Groeiende invloed private partijen

Over tien tot vijftien jaar zullen overheden om redenen van efficiëntie en effectiviteit hun traditionele regulerings- en handhavingstaken meer dan nu het geval is, laten uitvoeren door de techniek. Nu gebeurt dat al op kleine schaal met redelijk eenvoudige technologie in bijvoorbeeld het verkeer. Denk aan rotondes en verkeersdrempels. In de toekomst zal het gedrag van mensen op veel gesofisticeerdere manieren worden beïnvloed met instrumenten die ofwel rechtstreeks op hun gedrag aangrijpen ofwel hun omgeving aanpassen waardoor ze hun gedrag wijzigen.

Voor het produceren, beheren en onderhouden van die technieken zal vaak een beroep worden gedaan op private partijen. Daarnaast zullen private partijen, los van de oveheid, ook meer mogelijkheden krijgen en gebruiken om het gedrag van medeburgers, klanten of mogelijke belangstellenden te gaan regelen. Nu kennen we al enkele soorten van technologieën die met dit doel in de private sector zijn ontwikkeld: *digital rights management* (DRM) systemen, waarmee bijvoorbeeld de afspeelbaarheid van muziek of film wordt beperkt, en *genetic use restricting technologies* (GURTs). Bij GURTs worden plantenzaden zodanig gemodificeerd dat tweedegeneratie zaden steriel zijn of behandeling met een aanvullende stof nodig hebben om te kunnen ontkiemen. Beide methoden doorkruisen traditionele akkerbouwmethoden waarbij de boer zelf kan voorzien in zijn zaaigoed.

DRM en GURTs kunnen worden beschouwd als private initiatieven om als private partij de eigen intellectuele eigendomsrechten (auteursrechten op muziek en rechten inzake de ontwikkeling en veredeling van zaden) veilig te stellen. Uiteraard zijn hierbij de nodige kanttekeningen te plaatsen vanuit het perspectief van het algemeen belang. Hoe het echter ook zij; het gebruik van technologie voor doelen van 'privé-regulering' zal de komende decennia alleen maar toenemen. Zowel de uitbesteding van de overheidsregulering aan techniek en private partijen als de toename van particuliere reguleringsarrangementen nodigen uit om verder na te denken over de afbakening van het publieke en het private en over de controleerbaarheid en legitimiteit van regulering.

De rol van de overheid bij regulering en handhaving zal veranderen. Welke rol zij zal spelen zal onder meer afhangen van de uitkomsten van de debatten over de controleerbaarheid en legitimiteit van regulering en handhaving door private partijen. In de tussentijd ligt het wel voor de hand dat de overheid een rol zal spelen bij het op gang brengen en houden van die debatten.

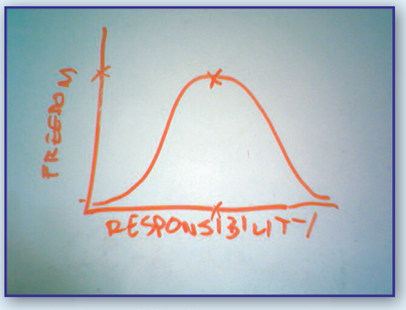
Steeds vaker versmelting van normering en handhaving

Juist omdat het om redenen van efficiëntie en effectiviteit zo aantrekkelijk is om regulering te incorporeren in techniek, zal de verleiding steeds groter worden om in die techniek de regels en de handhaving te versmelten. In traditionele vormen van regulering, zoals recht en sociale moraal, is het van belang om een norm te kennen en om zelf te beslissen dienovereenkomstig te handelen. Bij die beslissing bestaat een zekere vrijheid doordat men kan kiezen om de regel niet te volgen ondanks eventuele sanctierisico's.

Bij een versmelting van norm en handhaving in techniek kan de techniek er steeds vaker voor zorgen dat mensen automatisch doen wat de regel zegt: ze blijven niet langer voor een rood licht staan omdat ze dat willen, maar omdat ze niet anders kunnen. Dit is interessant om twee redenen. Allereerst is het zaak goed in de gaten te houden dat de juiste regels in de techniek worden geïncorporeerd en dat ze rechtvaardig en billijk worden toegepast. Gerechtvaardigde burgerlijke ongehoorzaamheid is immers onmogelijk. Ten tweede maakt de versmelting van normen en handhaving in technologie kennis van normen en morele motivatie om normen te volgen (bijvoorbeeld omdat je de normen goed vindt of omdat je een goed mens wilt zijn) overbodig. In veel levensbeschouwingen en filosofisch-ethische stromingen wordt deze morele motivatie van groot belang geacht. Dat is op zich al een mooi idee, maar het is ook een nuttig idee. Versmelting van regels en handhaving in techniek zou mensen moreel lui kunnen maken doordat ze uiteindelijk kennis van normen en de sensitiviteit en de principiële bereidheid om volgens die normen te handelen overbodig maken. Dit zou ons flink kunnen opbreken zodra die techniek een keer uitvalt.

Meer vertrouwen

Ontwikkelingen in de techniek - en daardoor in onze leefwereld - beoordelen we vaak op basis van de normatieve kaders van het huidige moment. Die zijn echter geënt op aannames over een leefwereld waarin die ontwikkelingen zich nog niet hebben voltrokken. Daardoor lopen we het risico om die ontwikkelingen, inclusief hun positieve kansen en voordelen, voortijdig te stoppen. Bovendien kan het gaan om transformaties die niet zozeer vragen om veroordeling van de technische ontwikkeling, maar om herbezinning op de vooronderstellingen van onze normatieve kaders. Bij de hier beschreven ontwikkelingen lijken elementaire opvattingen in het geding over wat vrijheid, verantwoordelijkheid, individualiteit en privacy en de taakafbakening voor overheden en private partijen in de realiteit van alledag kunnen betekenen. Koste wat kost vasthouden aan de huidige opvattingen kan ons op een grote achterstand plaatsen.



Freedom/responsibility (bron: mamamusings, www.flickr.com)

Dit betekent niet dat we maar bereid moeten zijn om deze waarden op te offeren aan de voortgang van de techniek. Vrijheid, het vermogen om verantwoordelijkheid te kunnen dragen, individualiteit en transparante afbakeningen tussen het private en het publieke zijn fundamentele uitgangspunten en idealen die - naast andere beginselen - de grondslag vormen van onze rechtsstaat. Het betekent wel dat we bereid zouden moeten zijn om een nieuwe, aan de veranderende omstandigheden aangepaste, inkleuring te geven aan deze elementaire uitgangspunten.

Denk hierbij bijvoorbeeld aan de mogelijkheid dat we in een zeer verre toekomst een technologie ontwikkelen waarmee we ongewenst gedrag van zedendelinquenten kunnen voorspellen en desgevallend voorkomen, zonder verdere negatieve consequenties voor de betrokken persoon. Het volgen en het aansturen van die persoon zou vanuit het perspectief van het *huidige* vrijheidsbegrip waarschijnlijk neerkomen op een sterke inperking van diens persoonlijke vrijheid. Het beschikbaar komen van technologieën als deze zou ons echter ook juist kunnen laten ontdekken dat we met een overzichtelijke vrijheidsbeperking niet alleen leed voor anderen kunnen voorkomen, maar ook een leven in vrijheid op grotere schaal voor de betrokken persoon zelf mogelijk kunnen maken.

Uiteraard zal het erop aankomen om op dit gebied een fijngevoeligheid te ontwikkelen. Zoals we nu echter in staat zijn om - zij het zonder al te grote nauwkeurigheid - te onderkennen waar onderwijs (in het algemeen niet gezien als een beperking van individuele vrijheid) overgaat in indoctrinatie of manipulatie, zo zullen we wellicht over enkele decennia in staat zijn een onderscheid te maken tussen toepassingen van technologie die de individuele vrijheid wel inperken en toepassingen die dat niet doen of deze vrijheid zelfs vergroten.

Ambient technology en convergerende technologieën zullen over tien tot vijftien jaar onszelf en onze omgeving grondig veranderen. De weg erheen zal echter geleidelijk gaan. Dat geeft ons de gelegenheid om ons stapje voor stapje voor te bereiden op wat komen gaat en ons niet te verliezen in de morele waan van de dag. Technologieprofessionals kunnen er zelf in hoge mate toe bijdragen dat mensen de ontwikkelingen met meer vertrouwen tegemoetzien. Ze kunnen dat doen door in het ontwerp van de technologie en de toepassingen rekening te houden met mogelijk ongewenst gebruik. Allerbelangrijkst zijn echter openheid en informatie waardoor samen met andere burgers kan worden nagedacht over verantwoorde toepassingen voor de toekomst.

Functionarissen in de Informatiebeveiliging

Tom Bakker > Tom is lid van de redactieraad van Informatiebeveiliging en te bereiken via e-mail: tom_bakker@deltalloyd.nl.

Het is weer enige tijd geleden dat onze eigen studie *Functies in de informatiebeveiliging* is gepubliceerd (december 2006 - https://www.pvib.nl/?page=6398212). In dit visiedocument wordt een handreiking gegeven om ordening en profilering aan te brengen in de onduidelijkheid over functies in de informatiebeveiliging. Er wordt namelijk een grote verscheidenheid aan functiebenamingen en titels aangetroffen in de internationale literatuur, in regelgeving en in de praktijk bij organisaties. Daarbij kan vaak de vraag worden gesteld in hoeverre het om dezelfde soort functies gaat.

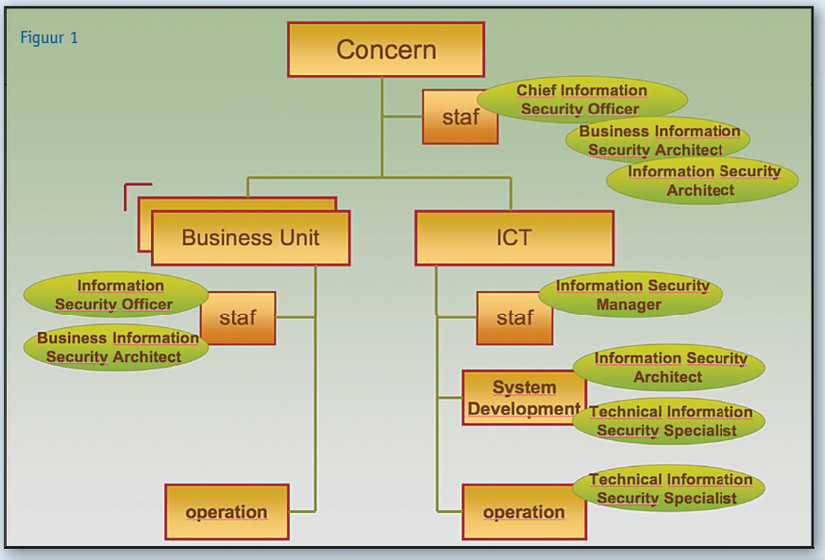
Wanneer betreft het een technische functie en wanneer een functie waar meer nadruk wordt gelegd op organisatorische en managementaspecten? En als functies dan naar aard en niveau verschillen, hoe hangen ze dan samen? Hoe verhouden ze zich bijvoorbeeld ten opzichte van verwante functies op het gebied van beveiliging-, risico- of continuïteitsbeheer? Welke eisen moeten er eigenlijk aan functies worden gesteld en hoe kan een carrièrepad in de informatiebeveiliging eruit zien? Tot zover de problematiek, maar hoe gaat het nu in de praktijk na het uitkomen van *Functies in de informatiebeveiliging?*

In de komende nummers zullen we mensen aan het woord laten die werkzaam zijn in de (informatie)beveiliging met functies zoals die genoemd zijn in tabel 1. Er zal worden ingegaan op vragen over hoe het functiemodel in formele zin wordt gehanteerd en hoe hun positionering is in de organisatie in relatie tot de taken en verantwoordelijkheden zoals die genoemd worden in de studie (figuur 1). Daarnaast komt ook aan bod of de functieprofielen worden toegepast en of de competenties in de praktijk ook zo worden herkend.

Interviewkandidaten

We weten nu dus welke functies er bestaan, maar we weten niet wie een dergelijke functie vervult. Misschien ben jij wel werkzaam in een van de genoemde functies? Wanneer dat het geval is en wanneer je tijd voor ons wilt maken, meld je dan als interviewkandidaat bij de auteur van dit artikel via: tom_bakker@deltalloyd.nl.

Figuur 1



IB-functies	Afk.	Nederlandse namen
Chief Information Security Officer	CISO	Concernmanager Informatiebeveiliging
Information Security Officer	ISO	Functionaris Informatiebeveiliging
Business Information Security Architect	BISA	Procesarchitect Informatiebeveiliging
Information Security Manager	ISM	Manager Informatiebeveiliging
Information Security Architect	ISA	Informatiebeveiligingsarchitect
Technical Information Security Specialist	TISS	Technisch Informatiebeveiligingsspecialist

Tabel 1

Agenda

18/05/2009
IB-opleidingen markt 2009
Organisatie: PvIB
Tijdstip: van 15.00 uur tot en met 19.30 uur
Locatie: 2B-Home in Zoetermeer
Thema: van Kennis naar Kunde
Voor meer informatie: www.pvib.nl / www.ibopleidingen.nl

10/06/2009
IBO-10: Esmeralda lezing
Organisatie: IBO evenement
Tijdstip: van 15.00 uur tot en met 22.00 uur
Locatie: Kloostersalons Mariënhof in Amersfoort

18/06/2009
Bedrijfsbezoek: Vitale netwerken
Organisatie: PvIB
Tijdstip: 14.30 uur tot en met 18.00 uur
Nadere informatie: www.pvib.nl/agenda

29/06/2009
Een kijkje in de keuken van Getronics
Organisatie: Young Professionals evenement
Tijdstip: 15.00 uur tot en met 19.00 uur
Locatie: Lelystad
Onderwerpen: BCM, Green IT, Security Architectuur

"Black Hat events are the premiere cyber security events you can attend... (with) the hottest, most relevant speakers and leaders in the field."
–Jim Christy, Director of Futures Exploration, DOD Cyber Crime Center

THE BAD GUYS KNOW YOUR TRICKS. DO YOU KNOW THEIRS?

Are you the kind of security professional that craves the freshest information?
Are you the kind of hands-on network defender that needs to be the first to know?
If you stand out from the crowd because you're seriously committed to security,
then youre our type – the Black Hat type.

The Black Hat Briefings are the most important technical security events on the planet, and we create them for people just like you – people who know security and want to be part of the solution. Join us in Las Vegas for 10 full tracks and over 60 intense hands-on training sessions of timely, actionable security information.

Black Hat
BRIEFINGS AND TRAINING

Black Hat USA 2009
July 25-30 Las Vegas, NV

SPONSORS

DIAMOND
Microsoft

PLATINUM
CISCO
QUALYS
RSA

GOLD
CORE
IBM
IOActive
mcafee security
NORMAN

SILVER
Aladdin
ArcSight
BIGFIX
BlueCoat
Booz | Allen | Hamilton
BREACH
CENZIC
hp
intel
Looking Glass
McAfee
nCircle
NETWITNESS
PROLEXIC
redseal
SAINT
SecureWorks
SOLERA
splunk>
StillSecure
Sunbelt Software
TippingPoint
TRUSTED
WHITEHAT

Automatisering of IT?

Sinds een aantal jaar ben ik werkzaam in de informatiebeveiliging, niet alleen één van de jongste vakgebieden binnen de IT (vroeger noemde je dat automatisering), maar zeker één van de vakgebieden waarin de veranderingen elkaar snel opvolgen.

Mijmerend denk ik terug aan het moment dat de meeste automatisering nog op papier gebeurde, per kamer hadden we de beschikking over één 'domme' terminal. Naast deze terminal stond steevast een microfiche lezer met microfiches vol met historische bestanden. Deze microfiches waren niet alleen vreselijk duur, voor zover mijn geheugen me niet in de steek laat: fl. 2,50 per stuk. Sorry voor de jongere lezers onder ons, dat is iets meer dan één euro, maar bovendien vreselijk lastig te lezen. Fysieke beveiliging was op dat punt volstrekt overbodig want voordat je doorhad hoe je gegevens kon aflezen en interpreteren was je inmiddels bevorderd tot chef (sorry, ik bedoel manager) van de afdeling. De terminal was eveneens geen enkel probleem qua security want het ding moest fysiek aangesloten zijn op de bekabeling van het gebouw en het mainframe. Security officers waren toen domweg niet nodig omdat er niets te beveiligen was. Natuurlijk waren we wel eens stiekem in de systemen aan het kijken of onze buurman erin stond, maar daar deed niemand moeilijk over. En dat je een stapel dossiers op je bureau had liggen daarvan werd evenmin iemand warm of koud.

Langzaam gingen de jaren voorbij en halverwege de jaren negentig van de vorige eeuw werden pc's iets beter betaalbaar en dus werden de apparaten ook toegankelijk voor de gewone man. Onze bulletinboards werden vervangen door internet en het installeren van internet werd voorgedaan in een handleiding die mijn werkgever verstrekte. Maar liefst 35 pagina's waren nodig om mijn Windows 3.1 machine op internet te krijgen en mijn 14k4 modem deed het perfect. Wel even ervoor zorgen dat je altijd met een bosje bloemen naar huis kwam wanneer de telefoonrekening door de brievenbus was gevallen, zo ging dat toen. Niemand maakte zich zorgen over beveiliging.

De terminals van vroeger zijn niet meer te vergelijken met de pc's van vandaag. Op de hedendaagse pc's hebben we antivirussystemen draaien (virussen komen alleen niet meer voor), firewalls staan aan, de harddisk is geëncrypt, Intrusion detection systemen, anti-spamsystemen, anti-weet-ikveelsystemen. Ontzettend grote investeringen om de onzichtbare vijand van ons af te houden.
Het netwerk is helemaal complex geworden, behalve de hierboven genoemde systemen willen we controle hebben over de websites die onze medewerkers bezoeken, we beschikken over software die de gigantisch grote bestanden uit de logs van al onze servers kan lezen en interpreteren, we hebben specialisten in huis die (veilige) verbindingen kunnen opzetten, security consultants, toezichthouders, wetgevers en legal hackers worden ingehuurd, regelmatig worden al onze externe verbindingen getest op zwakheden en we proberen onze medewerkers uit te leggen dat het niet handig is je password op te schrijven en het papiertje onder je toetsenbord te plakken. Om het gebouw in te komen moet ik door draaideuren en metaaldetectoren en langs boos kijkende beveiligingsmensen om vervolgens mij laptop aan het bureau vast te leggen met een ketting.

Tussen de terminal en microfiche van toen en de kettingen en legal hackers van nu zit ongeveer 25 jaar en ik durf er niet aan te denken hoe mijn kinderen later aan het werk gaan. In het jaar 2035 zou het misschien zo kunnen zijn dat het helemaal niet meer mogelijk is op een normale manier je werk te doen. Misschien lopen de beveiligingsmedewerkers wel met je mee en kijken ze de hele dag over je schouder mee of je niet iets fout doet of misschien zijn de logging systemen zo geperfectioneerd dat je in je oortje hoort dat je nu dreigt te verdwalen in de transacties die je ter beschikking staan met daarbij het vriendelijke verzoek weer terug te gaan naar waar je mee bezig moet zijn. Misschien dat we nog veel meer (potentiële bedreigingen) hebben ontdekt waar we nog meer maatregelen tegen moeten nemen. Misschien lopen er dan weer medewerkers rond die wél begrijpen hoe alle systemen aan elkaar gelinkt zijn. Misschien...

Misschien moeten we helemaal geen pogingen doen om er achter te willen komen hoe de IT er in 2035 uitziet. Wie in 1985 had durven voorspellen hoe het IT-landschap er nu uitziet, zou ongetwijfeld langdurig opgesloten zijn geweest op basis van het vermoeden van krankzinnigheid.

Ik weet in ieder geval wel waarom IT geen automatisering meer heet, het is al te lang geleden dat we taken echt konden automatiseren!

Groeten,

Berry

NIEUW!

SOPHOS
secured.

Sophos Endpoint Security

Nu ook volledige disk encryptie, removable storage encryptie en Windows-based pre-boot authenticatie!

Kijk voor meer informatie op www.crypsys.nl of bel (0183) 62 44 44.

CRYPSYS Data Security B.V. - Benelux Distributeur van Sophos
Edisonweg 4 - 4207 HG Gorinchem - Postbus 542 4200 AM Gorinchem
T (0183) 62 44 44 - F (0183) 62 28 48 - E sales@crypsys.nl

CRYPSYS data security