mei 2010 nummer 3

# INFORMATIEBEVEILIGING

## In Marketing's shoes

## Het aspect consistentie

## Identiteiten in de Nederlandse Cloud

## Een iPhone van de zaak

## CRAMM en beveiligen in Afghanistan



PvIB
Platform voor InformatieBeveiliging

ib

# Voorwoord/colofon

**Beste lezer,**

Zoals ik vorige keer al aankondigde wordt dit nummer van IB door een andere partij begeleid. Dat is voor iedereen wel spannend, hoe werkt dat nu samen, hoe gaat het blad eruit zien, hoe zit het met de planning? Bovendien zijn er nog meer veranderingen waar we dit jaar mee te maken krijgen. Zo wijzigt ook de samenstelling van de redactie. We zijn blij met de toezegging van Ronald van Erven en Said el Aoufi om toe te treden tot de redactie. Ronald heeft al heel veel voor de vereniging gedaan, met name in de activiteitencommissie. Blij dat hij ook hier energie in wil steken.
Said is ook al een goede bekende. Hij heeft al diverse malen een bijdrage aan dit blad geleverd. Vorig jaar is hij gepromoveerd en wij blij dat hij zijn kennis ook ten dienste wil stellen van het blad. We verwachten nog wel wat wijzigingen, maar we vertrouwen erop dat we de kwaliteit van deze publicatie op niveau kunnen houden. Zoals gezegd, het wordt een spannende tijd. Wat we in ieder geval binnenkort wel kunnen aanbieden is een digitale versie van het blad. Op dit moment zijn de digitale artikelen via de website in pdf-vorm beschikbaar, maar we gaan ook een bladerversie van het blad publiceren. Lijkt ons wel leuk.

Gelukkig waren met de krappe deadline net in staat om de uitslag van de verkiezing van het Artikel van het Jaar 2009 in dit nummer mee te nemen. Het juryrapport met een paar foto's staan in dit nummer. De uitreiking vond plaats bij de BCM-thema-avond van 20 april na de ALV. De onthulling konden we ook via het PvIB-Twitteraccount (@pvib) doen. Laat ik in ieder geval zeggen dat ik zeer vereerd ben met de uitslag.

Wat verder? We hebben weer een aardig gevuld blad. We hadden het idee om er een dossier over mobiele telefonie in te plaatsen, maar dat is het niet helemaal geworden. Wel een leuk artikel over de security van de gadget van vorig jaar, de iPhone. Ik wil het maar niet het gadget van dit jaar noemen, dat zullen de i- en wePads wel worden (en voor wie de wepad-aankondiging gemist heeft: surf even naar wepad.mobi). We zijn wel volop aan het werk met een nieuwe privacy-special. Het volgende nummer belooft een aantal interessante artikelen te bevatten. We hebben, als het lukt, een paar heel aardige interviews. Nummer 6 van dit jaar wordt een special over cloud security. En, maar daar zijn we over aan het nadenken, er lijkt behoefte te bestaan aan een special over IB in het onderwijs. En dan bedoel ik niet zozeer het lesgeven, maar de organisatie en inrichting van IB. Vorig jaar hadden we een interessant artikel van Alf Moens en Fred van Noord, maar er moet meer zijn. Als u een idee hebt, aarzel niet om het aan te dragen via ons nieuwe e-mailadres: ibmagazine@pvib.nl

Voor dit nummer wens ik u in ieder geval veel leesplezier!

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
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

**Redactieraad**
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Borger (Domus Technica)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (Verdonk, Klooster & Associates)
Gerrit Post (G & I Beheer BV)

**Advertentieacquisitie**
e-mail: adverteren@pvib.nl

**Vormgeving en druk**
De Drie Poorten, Nijkerk

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

**Abonnementen**
De abonnementsprijs bedraagt 115 euro per jaar (exclusief BTW), prijswijzigingen voorbehouden.

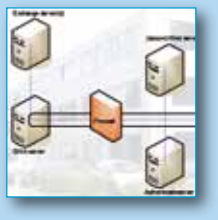
**PvIB abonnementenadministratie**
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl



ISSN 1569-1063

# Inhoud






# In Marketing's shoes

*Auteur: Wendy Goucher* > Wendy is a rare information security professional in that her background is social, rather than computer, science. She was drawn to the human interface with security and is now researching for a Doctorate in Computer Science with Psychology. She speaks widely at international conferences where she uses her perspective to give unusual insight. Wendy is MBCS and AIISP. She can be contacted at wendy@idrach.com

**In Marketing's shoes - In which the author seeks to understand why she seems at constant cross purposes with her sales-focused colleague. Delving into such questions as whether information security services can actually be successfully packaged and sold off the shelf and what is meant by the phrase "information security consultancy is built on trust, not flyers".**


Wendy Goucher.

I work for a small consultancy and a couple of years ago we worked alongside another consultancy, a specialist in management with a more marketing focus. After a while we hit a bit of a problem. He wanted to package information security in a nice pre-priced way that generated a price list and I maintained that information security is about tailor-made services and the need to cultivate trust. This seemed an insoluble problem and we both retired to our corners to think. My solution was to try and look at the situation from his perspective. How did he see security and how would he be explaining it to potential clients? In delving into this problem I have since realized that I hit upon an area of misunderstanding, that between sales and marketing on one hand and information security on the other, that is not as uncommon as I thought. In this article I will explain the process I went through in trying to gain insight into this problem.

I am not a computing person. My degree is in social science and my first career was as a management lecturer so you might have thought that I would have some sympathy and understanding, and possibly even ability in sales and marketing. No, not at all as it turns out. No idea why but it is not an aspect of the business that has been easy for me. As a security empowerment consultant I use my studies in psychology a lot, but not in the way that a good salesman does. The best sales staff know their customers, and their businesses, very well. They know when to sell and when to just build the relationship. It is all about communication and interpersonal skills.
Maybe that is why many IT and information security people are not drawn to it; it requires a very different approach.


People can be part of the solution - as well as the problem (cartoonist JimBarker.net).

This situation comes from an incident around Christmas time 2008. The associate, let's call him John, sent me an e-mail ask for a quote for preparing a client for an ISO27001 audit. I asked a series of questions about the company including size, sector and their compliance history, i.e. had they had an audit in another part of the business.
John's reply was a little shorter than I had hoped, he wanted a 'Ballpark figure' that he could offer to potential clients. I resisted as I did not want to guess and either loose a contract as the figure was too high or have to do the work at a loss so as not to be seen to go back on a quote. John was, by this time, clearly loosing his sense of humour. He then rang me and muttered about the customer's need to budget and the need to be up-front and clear with clients.
We live in a culture where you take a product off the shelves, scan it at the checkout and pay the amount asked. Many people, myself included, are happy not to have to engage in bargaining or haggling to reach a price for weekly shopping. I once had an afternoon on my own with some money to spend in the gold market in Jeddah, Saudi Arabia. I did not spend any of it because I did not know how much it was worth so I did not know how much I would be paying. Therefore, I got on the plane to London that evening without a single souvenir to show for my visit. Why then don't I feel more comfortable having all our consultancy services assigned a fixed price? This would, after all, make it easier for non-information security trained sales staff to respond to customer queries.

The old Chinese proverb says that if you want to understand your enemy you need to walk a mile in his shoes. So I will start by leading you on a short walk in John's shoes.

**In the Salesman's Shiny Shoes**
When I attend open networking events I find people react to my job either by instantly diving for the bar as it is of no interest, or are intensely interested as, it seems, it seems like a 'cool' job. John also believed that, as every business clearly needs to be operating safely, it would be an easy sale. Indeed this incident happened at the end of 2008 which was the year that information security incidents, from CDs lost at HMRC in the UK, to countless incidents of papers lost or disposed of badly, computers containing sensitive data turning up on eBay and laptops abandoned all over the world. As the year rolled on it had become clear, even to non-security based businesses, that they needed to make their operations more secure. No longer was the threat from some faceless hacker that could be met by IT defense put in place by some faceless IT admin person. The threat was from the normal business practice of each and every member or staff from the top down. Add to that the pressure for accreditation to ISO27001, the firm direction given by the Financial Services Authority towards increasing security awareness and the requirements for vendors to conform to the appropriate level of the PCIDS standards and it might seem that

selling information security was like fishing at a salmon farm. It is not so much how much you are going to catch, but how you are going to deal with it all appropriately. Certainly when we discussed work potential John had to sit on his hands to resist the urge not to rub them together in that time-honored sign of an impending pay-out. He practically needed hosing down when we were talking about forensics. Apparently folks, information security is SEXY!
Never did one phrase more encapsulate the diversity of perspective between myself and marketing, than that gem. I am the wrong age and the wrong shape (more possum than Halle Berry) for black leather or any other sexy outfit. As I cast my mind around the regulars at my local meeting of The Institute of Information Security Professionals or at the ISACA conferences I regularly speak it, I would say that I am not exactly letting the side down in that regard. So what is all this about sexy? I decided to look into this idea further so I chatted to a group of ladies at my local Scottish Women in Business event, none of whom are information security types. It seems that the concept of information security especially as related to the protecting of 'secret', sensitive or embarrassing information can come within the Halo effect[1] from James Bond and Spies. So more cocktail dress than black leather maybe, but still a little removed from operational reality.
The final positive point about information security from a sales perspective is that it is rarely a 'one-off' sale. There is often a need for maintenance, support and updating of security awareness. This in turn allows the development of a good business relationship which can help to get fellow associates, with other consultancy skills, into a position of doing business with the customer too. There are, of course problems with selling information security and the greatest of these is the lack of a single 'Shiny Box' that the company accountant can count and evaluate in a cost-benefit analysis table.

**High heels of an information security professional**

I am not speaking for all information security professionals here. I appreciate that some aspects of the business can be packaged and sold- penetration testing for example. However, much of it is based on guidance, advice and involvement in the design of policy and procedure and that is much harder to price unseen. It puts me in the mind of the story of the local man in some rural area (which I have heard variously as Ireland, Yorkshire and the Highlands of Scotland dependant on the perspective of the story-teller) who was stopped by a visitor and asked the way to a town some 15 miles away. When asked how to get there he replied "well I wouldn't start from here". The problem with this type of consultancy is that you don't know where you are starting from, for example what policies and procedures are already in place. I have also found that there can be an interesting difference between the extent to which my client tells me that information security good practice is interwoven into their culture, and the reality of walking through the office, looking at desks and sitting listening to confidential business discussions going on over lunch in the café next door.
There is often a mismatch between both the perception and the reality of the client as to their current operational state, and also between what they feel is going to be required to achieve their aim- especially if this is externally audited accreditation- and the reality of the gaps in the system. In the majority of cases businesses underestimate their gaps and then the budget for time and money is pressured right from the beginning. For this reason one way forward can be to over-estimate the cost up front- and watch their reaction carefully. Did they flinch? Was it to high? Or are they smiling and maybe it is too low. Of course this should mean that if the reality of the system is better than expected then the final cost should be lower, I am not at all sure how common that pleasant surprise is however.
What this all means is that we feel that, short of installing a fully operational crystal ball it is undesirable to reduce our consultancy services to a fixed price list.

**A matter of perspective**

As you will already have realized, what I am talking about is perspective. How we view people, or groups of people, affects the way we are going to react to them. In an extreme case a strong reaction can lead to prejudice against someone without ever meeting them. We may be sure that marketing people will not understand the security message because they are focused on presentation and sales, not on security. Indeed security can even get in the way of their ideas. The marketing team for one national bank, a few years ago thought it would be a good idea to put the company logo on the back of the laptops so they were small advertising boards. Of course the security teams saw these as invitations for thieves to steal the machine. It is a matter of how you see, things.

We learn these perspectives either from others, our new colleagues when we join a company, for example. Or we learn from personal experience. If the information security team are distant and only seen by

This marketing man could help your security (cartoonist JimBarker.net).

the rest of the organization when they are dealing with a serious incident, which might mean you are in trouble, or when they are delivering a long, dull training session then it is no surprise they don't have a popular image. This means that they are not going to be a first point of contact when there are questions or concerns and that could mean minor issues become larger ones before the security team hears about them.

So what did I do, in the situation with John? Actually I wrote the outline of what later became a presentation for ISACA, sent it to him and we sat and drank coffee and discussed it. I appreciated that he needed packages to sell and he saw that some things are two variable to bring out of a single 'Shiny Box'. What we decided was that we could make packages, but instead of specific tasks the customer bought my time. Over two years later I have found that John was right and customers do like packages. My best customer will sometimes have me design material, sometimes create training, sometimes hold discussions with staff and many other things. The great thing is that all the budget holder needs to do is allow for a certain number of 'Idrach Days' and we can react to need at the time. So he gets package and flexibility and I get to tailor the work to the customer needs.

So my walk in John's shiny shoes taught me some useful things. I have no evidence to suggest that he ever tried to step out in my size 4 heels!

[1] *Nisbett, R. E., & Wilson, T. D. (1977). The halo effect: Evidence for unconscious alteration of judgments. Journal of Personality and Social Psychology, 35(4), 250-6*

*Herstel van de zwakste schakel*

# Het aspect consistentie

*Auteur: Jan de Boer MSIT >* Jan de Boer MSIT is als managing consultant werkzaam bij Capgemini. Zijn Master Thesis betrof de psychologie in de informatiebeveiliging. Zijn vakgebied is de integrale (informatie)beveiliging. Social Engineering is zijn hobby. Hij is bereikbaar op jan.de.boer@capgemini.com.

**Dit is het derde artikel in een serie van acht waarin wordt ingegaan op de psychologische trucs die door Social Engineers worden gebruikt om slachtoffers te manipuleren. Waarom en hoe werken ze? Hoe zijn ze te herkennen en wat is de beste verdediging? In dit artikel komt het aspect 'consistentie' (het consequent handelen) aan de orde.**

Jan de Boer.

**Social Engineering; een korte terugblik**

In de informatiebeveiliging wordt de mens steeds omschreven als de zwakste schakel. Mede door extreme resultaten van security audits in de vorm van Social Engineering (SE), zoals het in ontvangst mogen nemen van vijf handvuurwapens, ben ik er steeds meer van overtuigd geraakt dat de beveiliging niet zit in firewalls, hoge hekken, SafeWord tokens en andere technische beveiligingsmaatregelen, maar in de mens zelf.

Uit een onderzoek onder 250 CIO's en CISO's van bedrijven en overheden naar (informatie) beveiliging is gebleken dat zestig procent GEEN aandacht schenkt aan het beveiligingsbewustzijn van de medewerkers. Een opmerkelijk hoog percentage aangezien zestien procent aangeeft dat er informatie is gestolen met behulp van SE en zelfs drieëntwintig procent aangeeft de dreiging van diefstal door SE als serieus te ervaren.

Deze artikelserie over het hoe en waarom van menselijk gedrag en hoe daar misbruik van kan worden gemaakt door profiteurs, is bedoeld als bijdrage aan een reeds bestaand bewustwordingsprogramma van een organisatie. Maar het is ook als zelfstandig bewustwordingsprogramma prima inzetbaar voor een risicogroep zoals secretaresses of bewakingspersoneel. De artikelen behandelen de psychologische mechanismen die door SE's worden gebruikt om tegenstanders te manipuleren. Er wordt ingegaan op de achtergrond van de werking en er vindt een verduidelijking plaats aan de hand van voorbeelden uit de praktijk. Verder worden maatregelen aangedragen om een aanval te herkennen en af te slaan.

**Commitment en consistentie: innerlijke spookbeelden**

De mens is geneigd te handelen in overeenstemming met dat wat hij daarvoor gedaan of besloten heeft. Als we een mening verkondigen of een keuze maken, zijn we geneigd om ook daarna dezelfde soort keuzes te maken of overeenkomstig de eerder gemaakte keuze te handelen. Soms zijn we achteraf niet blij met de keuzes die we hebben gemaakt. Wij onderdrukken dat slechte gevoel vervolgens door onszelf ervan te overtuigen dat het genomen besluit juist is. Daarbij leggen we de nadruk op de positieve elementen van de keuze. We voelen ons uiteindelijk beter over de genomen beslissing.

De mens heeft dus de neiging consistent te zijn en dit is een zeer effectief sociaal beïnvloedingswapen. Wie consistent is, wordt intelligent, oprecht en evenwichtig genoemd. Omdat consistentie belangrijk is, zijn we ook geneigd om er een automatisme van te maken. Het werkt dan dus als een soort kortsluitend reflex en maakt dat we niet steeds hoeven na te denken over een te nemen beslissing. Als we in het verleden al soortgelijke beslissingen hebben genomen, is die keuze ook nu een goede keuze (toch?). Dit maakt het denken voor ons een stuk gemakkelijker. Nadenken kan negatieve gevolgen hebben die we liever niet willen tegenkomen. Dit is de reden waarom we soms beslissingen in een reflex nemen. De drang om consistent gedrag te vertonen kan echter misbruikt worden door profiteurs.

Consistentie wordt bepaald door commitment. Zodra je iemand een standpunt laat innemen of een keuze laat maken, zal deze persoon in de toekomst overeenkomstig handelen. Indien dergelijke beslissingen in het openbaar worden gedaan, actief worden gedaan en veel inspanningen vergen, zal het effect veel langer blijven hangen. De innerlijke verandering wordt daardoor langdurig. We accepteren de verantwoordelijkheid van ons gedrag of het genomen besluit in toenemende mate indien we geloven dat er van buitenaf geen krachtige invloed op is uitgeoefend.

Profiteurs kunnen de behoefte aan consistent gedrag eenvoudig uitbuiten. Zij kunnen vergelijkbare situaties creëren waarin al van tevoren vast staat hoe het slachtoffer zal beslissen namelijk, door consequent gedrag te vertonen. Bovendien hoeven de slachtoffers niet steeds te worden overtuigd van de 'juistheid' van hun handelen. Het slachtoffer overtuigt zichzelf wel door de innerlijke behoefte aan consistentie.

**Verdediging**

Om de druk tot onverstandige consistentie tegen te gaan moeten we signalen leren herkennen die te maken hebben met onze intuïtie. Maar hierin ligt bij de moderne mens ook het probleem. We zijn niet meer goed in staat om naar onze intuïtie te luisteren en we proberen een minder goed 'gevoel' vaak weg te redeneren. De verdediging tegen misbruik van consistent gedrag ligt in het herkennen van signalen:

1. signalen uit je maag maken duidelijk dat we bepaalde beloftes en verplichtingen om aan verzoeken te voldoen eigenlijk toch niet willen doen;
2. signalen uit je hart maken achteraf duidelijk of we blij zijn met de inwilliging van het verzoek of niet. Je kijkt dan dus terug op het verzoek, je antwoord en de gevolgen.

In het eerste geval voorkom je dat er misbruik kan worden gemaakt van je neiging tot consistentie. In het tweede geval kom je achteraf tot de conclusie dat je een foute beslissing hebt genomen. Redeneer je gevoel niet weg en maak (ook achteraf) melding van het voorval.

## VOORBEELD

### Consistentie: eigen ervaring

Toen ik aan de medewerkster van Personeel en Organisatie vroeg om even mee te werken aan een klein onderzoek van de helpdesk was ze daartoe graag bereid. Het onderzoek was onbelangrijk en duurde maar kort, maar was uitsluitend gericht op het leggen van het eerste contact met haar. De volgende dag heb ik haar geprezen om haar hulpvaardigheid en om een iets grotere gunst gevraagd. Ook toen besloot ze mee te werken omdat ze het die dag daarvoor ook had gedaan. Na vier dagen beschikte ik over de wachtwoorden voor de cursistenadministratie en het systeem voor het aanmaken van de elektronische toegangspassen.

Door gelijksoortige en geleidelijk ingrijpendere verzoeken te doen, daarbij complimenten te geven en te refereren naar haar eerdere hulpvaardigheid, was het slachtoffer geneigd consequent en consistent gedrag te vertonen. Ze ging zonder weerstand in op al mijn verzoeken. Ze was zelf heel erg tevreden over haar eigen bereidheid om mee te werken ondanks dat ze net haar wachtwoorden had afgestaan.

**Samenvatting**

We zijn geneigd om niet al te veel na te denken over een besluit indien we een dergelijk besluit al eens hebben genomen. Daarnaast willen we graag consistent gevonden worden door onze omgeving. Profiteurs kunnen ons in een vergelijkbare situatie brengen om ons vervolgens met zachte hand te dwingen een voor hem gunstig besluit te nemen. Signalen uit je buik of je hart kunnen je vertellen of je handelen goed of slecht voelt. Redeneer dit gevoel niet weg maar sta open voor je intuïtie.

# 'Mystery man' op bezoek in Amsterdam Social Engineering bij stadsdelen en diensten

**De Stuurgroep Informatiebeveiliging van de gemeente Amsterdam heeft in 2007 een aantal onderzoeken laten uitvoeren waarbij een zogenaamde 'mystery man' een bezoek bracht aan stadsdelen en diensten. Deze 'mystery man' of Social Engineer heeft geprobeerd om zonder toestemming toegang te krijgen tot panden en vertrouwelijke gegevens in archieven en netwerken. Rienk Hoff, voorzitter van de Stuurgroep Informatiebeveiliging en directeur van de Dienst Persoonsgegevens (DPG), gaat in dit interview in op de uitgevoerde onderzoeken, de resultaten, en de toekomst.**

**Wat was de aanleiding voor het onderzoek?**

Hoff: "De beveiliging van informatie wordt een steeds belangrijker onderwerp, onder meer door de uitrol van de Basisregistratie Personen die moet voldoen aan de hoogste beveiligingsnorm. Ook bracht de gemeentelijke Rekeningencommissie een rapport uit, waarin zij aangaf dat de informatiebeveiliging binnen de gemeente Amsterdam moest worden verbeterd. De verantwoordelijke wethouder werd er op aangesproken wat prompt de landelijke pers haalde. Hierdoor kwam informatiebeveiliging op de politieke agenda. Er werd een concernbrede Stuurgroep Informatiebeveiliging opgericht. Deze had tot taak om projecten te faciliteren, 'best practices' te delen en de bewustwording te vergroten."

**Wat heb je vervolgens gedaan?**

"Begin 2006 is een directeurenconferentie gehouden", aldus Hoff. "Ik heb toen op ludieke wijze aandacht van mijn collega's gevraagd door hen voor te houden dat ze roomser waren dan de paus. Die is immers van mening dat geheelonthouding (niets doen dus) de beste bescherming biedt tegen seksueel overdraagbare aandoeningen. 'Als het over informatiebeveiliging gaat, denken jullie net zo', hield ik hen voor, waarna ik condooms uitdeelde. Daarmee had ik in elk geval de aandacht. Tijdens die bijeenkomst vernamen wij ook de resultaten van een security audit, uitgevoerd in opdracht van het stadsdeel Amsterdam Centrum.

Een 'mystery man' was er binnen en buiten kantoortijd in geslaagd om door te dringen tot het netwerk en tot grote hoeveelheden vertrouwelijke informatie in archieven.

*Als ik 's avonds afsluit denk ik nog steeds aan de 'mystery man'*

Ik heb aangeboden om twee onderzoeken op kosten van de Stuurgroep Informatievoorziening te laten uitvoeren. Uiteindelijk hebben negen stadsdelen en diensten van de gemeente Amsterdam een security audit laten uitvoeren door middel van Social Engineering."

**Je hebt ook bij DPG zelf een onderzoek laten uitvoeren. Wat was jouw reactie op de resultaten?**
"Ik had natuurlijk verwacht dat er iets gevonden zou worden, maar was wel onaangenaam verrast hoe gemakkelijk de 'mystery man' het pand was binnengekomen en tot welke vertrouwelijke informatie hij toegang had gekregen."

**Hoe heb je in de Stuurgroep terugkoppeling gekregen van de vertrouwelijke resultaten?**
"We hebben afgesproken de resultaten in geanonimiseerde vorm aan de Stuurgroep en het Platform voor Informatiebeveiligingsadviseurs (PIA) te presenteren. Uit de grote hoeveelheid foto's die tijdens de onderzoeken zijn gemaakt, is een selectie gepresenteerd van de meest aansprekende resultaten en conclusies."


Rienk Hoff, voorzitter Stuurgroep Informatiebeveiliging en directeur Dienst Persoonsgegevens (DPG).

**Kun je een paar sprekende voorbeelden geven van die resultaten?**
"Ik kan natuurlijk geen details geven, maar het blijkt dat je met enige creativiteit vaak zonder problemen een beveiligd pand kunt binnenkomen", vertelt Hoff. "Meeliften met rokers of toegang via de deur van de fietsenkelder is vaak geen probleem. Eenmaal binnen wordt een vreemde vaak niet opgemerkt of aangesproken, en kan hij zo vrij door het pand bewegen. Als dan de deuren tot archieven openstaan en werkstations niet zijn gelockt, heeft zo'n onbekende toegang tot veel vertrouwelijke informatie. Ook bleek de 'mystery man' toegang te hebben gekregen tot kluizen, gewoon door erom te vragen of omdat ze open stonden. Medewerkers zijn ook erg creatief in het omzeilen van belemmerende technische oplossingen, waardoor weer nieuwe veiligheidsrisico's worden geïntroduceerd."

*Social Engineering is een prima instrument om risico's in kaart te brengen en het bewustzijn te vergroten*

**Wat hebben de stadsdelen en diensten gedaan met de resultaten?**
"Alle onderzochte stadsdelen en diensten hebben een actieplan opgesteld en in veel gevallen is informatiebeveiliging (onder andere 'clean desk') een vast onderdeel geworden van het functioneringsgesprek. De resultaten zijn gepresenteerd in de managementteams van de onderzochte organisaties en in mijn eigen dienst ook aan alle medewerkers. Tijdens drie sessies heeft de 'mystery man' zelf verteld hoe hij te werk was gegaan en welke resultaten dat opleverde. Deze presentaties bleken een zeer goed middel om de bewustwording te bevorderen, want de kluizen, archieven, lades en kasten op de foto's werden natuurlijk herkend. Er werd ook goed meegedacht over werkbare oplossingen. Iedere deelnemende dienst en stadsdeel heeft de onderzoeksresultaten met de vele foto's op CD ontvangen. Zij hebben daarmee een goed middel in handen om zelf bewustwordingssessies te organiseren. Ik heb gemerkt dat het gedrag van mijn medewerkers, maar ook van mijzelf, is verbeterd. De resultaten blijven nog een tijdje hangen. Maar ik realiseer me dat bewustwording voortdurend aandacht nodig heeft."

**Hoe ziet de toekomst eruit?**
"Wij zijn in het verleden te reactief geweest. Er werd een audit gehouden. In de conclusies stond wat verkeerd was en daarop werd gereageerd", concludeert Hoff. "Wij zijn nu veel proactiever bezig met bewustwordingsprogramma's en het vergroten van het draagvlak. Social Engineering is daarbij een prima instrument om risico's in kaart te brengen en het bewustzijn te vergroten. Wij continueren de werkzaamheden van de Stuurgroep Informatiebeveiliging, waarbij bewustwording een blijvend aandachtsgebied is. Wij proberen de realisatie van informatiebeveiliging centraal en gemeenschappelijk aan te pakken en onderkennen daarbij vier belangrijke ontwikkelingen:

1. wij moeten van eilandautomatisering naar dienstoverschrijdende systemen en centraal beheer;
2. wij dienen er gemeenschappelijk voor te zorgen dat wij bij een calamiteit de meest wezenlijke processen van de gemeente Amsterdam kunnen continueren;
3. er is permanent gemeentebrede aandacht vereist voor bewustwording als een continu proces en het ontwikkelen van gemeenschappelijke instrumenten;
4. elk stadsdeel en elke dienst dient een goede informatiebeveiligingscoördinator te hebben."

**Heb je een aanbeveling voor andere gemeenten?**
"Ik weet niet hoe het staat met de informatiebeveiliging bij andere gemeenten, maar het zou mij niet verbazen als de resultaten van de negen onderzoeken binnen de gemeente Amsterdam representatief zijn voor de overige Nederlandse gemeenten. De mens is inderdaad de zwakste schakel en het Social Engineeringsonderzoek toont aan welke schade een gemeente daarbij zou kunnen oplopen. Door het presenteren van de resultaten creëer je betrokkenheid en motivatie en daardoor weer een betere beveiliging", sluit Hoff af.

# Identiteiten in de Nederlandse Cloud

*Auteur: André Koot* > André Koot is Corporate Informatie Manager bij Univé-VGZ-IZA-Trias en hoofdredacteur van dit blad. Hij is bereikbaar via a.koot@unive.nl

**In Nederland is ECP-EPN een initiatief gestart om door inzet van OpenID de drempel voor elektronisch zakendoen op Internet te verlagen. In dit artikel wordt het initiatief OpenID+.nl beschreven. Dat initiatief is voor ons vakgebied relevant omdat misbruik van de identiteit van een gebruiker voor het vertrouwen in elektronische transacties misschien wel de grootste risicofactor is.**

Naarmate we meer en meer gebruik gaan maken van cloudservices, ervaren we ook meer en meer de last bij het gebruik van digitale identiteiten. Elke website kent z'n eigen accountbeheer en iedere gebruiker moet voor elke website een nieuwe account aanmaken. Dat kost wat. Inspanning aan de kant van de gebruiker en aan de kant van de websites. Elke gebruiker moet een veelheid aan accounts onthouden, met alle risico's van dien (wachtwoord vergeten, of voor heel veel sites hetzelfde, hackbare, wachtwoord). Elke website moet gebruikersbeheerfuncties in de lucht brengen en houden. Denk alleen al aan de inlogschermen met de functie 'Wachtwoord vergeten?'. Dat lijkt triviaal, maar het beheer van de functionaliteit achter die schermen kost toch de nodige middelen.

*Per saldo is niemand gelukkig met een apart account voor elke site. En dat verhindert weer effectief en efficiënt zaken doen op het internet*

Per saldo is niemand gelukkig met een apart account voor elke site. En dat verhindert weer effectief en efficiënt zaken doen op het internet. Wat zou het gebruiksvriendelijk zijn om met een digitale identiteit veilig op meerdere sites te kunnen inloggen en wat zou single sign-on handig zijn. Gelukkig bestaan de technieken om dat mogelijk te maken (zie onder meer mijn eerdere artikelen over digitale identiteiten in de cloud)[1], maar helaas worden deze technieken onvoldoende gebruikt en is men met het gebruik daarvan dus onvoldoende bekend. Het is dan ook niet duidelijk genoeg wat de voordelen zijn van hergebruik. Maar er is mede daardoor ook niet genoeg nagedacht over hergebruik en de voorwaarden daarvan.

Een digitale identiteit is maximaal zo betrouwbaar als men de verstrekker van die digitale identiteit vertrouwd. Als ik mijn eigen digitale identiteit maak, dan zal die alleen vertrouwd worden door partijen die mij vertrouwen en dan alleen nog voor zover ze mij vertrouwen. Ik mag nog zoveel certificaten in een digitaal paspoort opnemen als maar mogelijk is, de betrouwbaarheid kan niet hoger zijn dan de betrouwbaarheid van de autoriteit die de certificaten in het paspoort plakt. De analogie naar het papieren paspoort is snel gemaakt. De burgemeester van mijn woonplaats is de autoriteit die mij een paspoort verstrekt, ik mag dat niet zelf (ook al heb ik de faciliteiten om dat te kunnen). Derden zullen het door de burgemeester verstrekte paspoort doorgaans vertrouwen. De hele vertrouwensstructuur is gericht op het verschaffen van te vertrouwen identiteiten (zie artikel)[2].

Voor digitale paspoorten is een dergelijke structuur niet ingericht. PKI voldoet alleen in gestructureerde relaties, niet in de vrije markt. Dat wil zeggen dat er geen standaardoplossing bestaat waarbij paspoorten van (onbekende) derden/identity providers kunnen worden geaccepteerd. Daarmee bestaat er dus een aanzienlijke drempel voor het realiseren van e-businessactiviteiten.

In Nederland is ECP-EPN een initiatief gestart om door inzet van OpenID de drempel voor elektronisch zakendoen op internet te verlagen. ECP-EPN is een organisatie die ijvert voor het effectief en efficiënt gebruik van elektronische middelen om het zakendoen in Nederland te vereenvoudigen. Daartoe worden diverse initiatieven ondernomen, variërend van mobiele datacom tot het digibewust programma.

Een werkgroep (de OpenID+.nl kopgroep) is onder auspiciën van ECP-EPN gestart. Deze werkgroep heeft vastgesteld dat er wel degelijk voldoende mogelijkheden bestaan om digitale identiteiten te kunnen hergebruiken. Er bestaan genoeg identity providers (IdP) en er zijn ook al verschillende relying parties (RP, de naam voor een website die 'vertrouwt op' identiteiten verstrekt door derden) die eigenlijk wel digitale identiteiten van derden willen accepteren. Maar tot op dit moment is dat nog niet echt van de grond gekomen. Partijen als Google, Yahoo en Hyves treden op dit moment al op als identity provider voor OpenID-identiteiten. Je kunt dus met je Hyves-account inloggen op OpenID-compatible sites (relying parties), zonder een account op die sites te hebben.


André Koot.

**Belemmeringen**

Maar voor al die relying parties geldt nu wel dat je met zo'n digitale identiteit vrijwel geen autorisaties hebt, je mag daar dus bijna niets. En daar is het nu wel om te doen. E-business draait om dingen mogen doen, dus autorisaties hebben. Wat is de reden van die belemmering, waarom geven relying parties die identiteiten van derden niet de nodige autorisaties? Het is een kwestie van vertrouwen. Vertrouwen in de identity provider en in het proces van registratie van identiteiten.
Iedereen wil best een mailtje naar een Gmail-account sturen, ervan uitgaande dat de geadresseerde recht heeft op dat mailtje, maar we hebben natuurlijk geen enkele zekerheid dat de geadresseerde (wiens e-mailadres tevens een OpenID is) ook daadwerkelijk hoort bij het individu aan wie we denken een mailtje gestuurd te hebben. We hebben geen enkele zekerheid omtrent

[1] *2007-1, 2008-6, 2010-2, 2010-3* [2] *Publieke Indentity providers, 2009-3*

de identiteit van de geadresseerde. Datzelfde geldt ook voor bijvoorbeeld Hyves. Er bestaan miljoenen accounts op Hyves, maar we hebben geen idee of dat echte individuen zijn, of anderen die zich voordoen alsof.

**Verificatie**

Alhoewel... Hyves kent het fenomeen van de gekwalificeerde identiteit. Het is mogelijk om een Hyves-identiteit te laten valideren door een hogere autoriteit, in casu een notaris. Na visuele vaststelling van de echtheid van de identiteit van een individu, wordt de Hyves identiteit als geverifieerd aangemerkt. En daarmee is zo'n Hyves-account waardevoller dan een willekeurige andere, niet geverifieerde account. Het is ook echt een waardevoller account, want die verificatie kost wel geld.

Dit principe is wel heel interessant. Dat betekent namelijk dat als (bijvoorbeeld) Hyves in de claims van een OpenID-account aangeeft dat de betreffende account visueel is geverifieerd door een notaris en als we Hyves op dit punt vertrouwen, dan zouden we natuurlijk dit OpenID-account ook mogen vertrouwen.

Vanuit de relying party bekeken: we kunnen dit OpenID-account dan zelfs koppelen aan een interne klant in ons CRM-systeem. Sterker, deze identiteit is zelfs betrouwbaarder dan een door een klant zelf op onze site aangemaakte account. Die is immers door niemand geverifieerd, laat staan door een vertrouwde identity provider. Daarom is het dat zo'n identiteit dan ook alleen maar op onze site te gebruiken is. Hergebruik staan we niet toe en wij autoriseren die virtuele identiteit alleen maar voor een zeer beperkt aantal bedrijfsfuncties waarbij we de risico's kunnen overzien.
Het bestaan en gebruik van geverifieerde accounts van betrouwbare identity providers is dus wat bevorderd moet worden.

**OpenID+.nl**

Deze identiteitsprincipes zijn uitgewerkt in het OpenID+.nl initiatief: wat zijn betrouwbare identity providers en hoe kunnen we vaststellen of en zo ja, welke verificatie heeft plaatsgevonden?
Om dit te realiseren heeft OpenID+.nl een trust framework ontwikkeld. Dit is niets anders dan een model waarin de vertrouwensrelaties staan vermeld. Het model reikt in opzet ook verder dan de initiële ambitie, namelijk het propageren van het gebruik van OpenID in Nederland. Bovendien blijft het in beginsel ook niet beperkt tot OpenID. Ook Information Card en OAuth en dergelijke worden ondersteund.

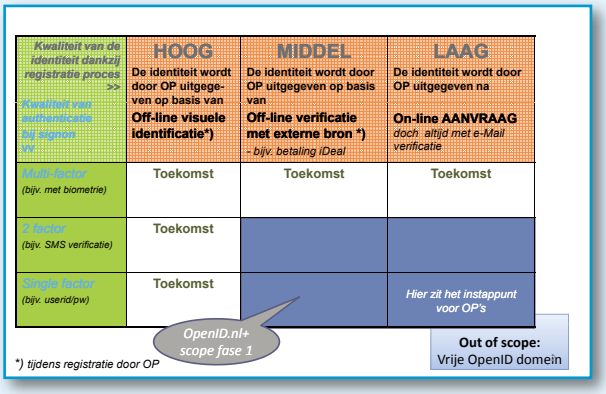


Fig. 1.

Binnen OpenID+.nl is vastgesteld dat het theoretische model, zoals weergegeven in figuur 1, niet afdoende is en dat er een grotere mate van granulatie wenselijk is. Voor OpenID+.nl is er gekozen om voor elk geverifieerd attribuut het verificatielevel in de door de IdP aan de RP geleverde SAML claim te vermelden. Daarmee kan een Identity Provider bijvoorbeeld aan de Relying Party melden dat het bankrekeningnummer is geverifieerd. Op basis van die informatie kan de Relying Party gericht autorisaties toekennen.
OpenID+.nl zal echter niet alle alternatieven invullen. Enerzijds is de techniek nog niet zo ver ontwikkeld dat alle oplossingen haalbaar zijn, anderzijds is het nog niet duidelijk welke behoefte in de markt aan fijnmazigheid bestaat die het model biedt.
OpenID is een open standaard, dat betekent dat Identity Providers en Relying Parties hoe dan ook gehouden zijn aan de inhoud van de protocollen. Als je OpenID+.nl ondersteunt, dan ondersteun je automatisch ook OpenID. Wat brengt dan de '+' in dit verhaal?

Binnen OpenID+.nl sluiten Identity Providers en Relying parties een convenant waarin regels rond het gebruik van de + staan gegeven. Zo is bepaald dat aangesloten relying parties de OpenID's van aangesloten identity providers, alsmede de door middel van visuele waarneming door een onafhankelijke derde is geverifieerd, dan is dat een gegeven waar de relying party op kan rekenen.

Evenzo verklaart de aangesloten identity provider zich te houden aan de regels binnen het convenant. Dat betekent onder meer het hanteren van het OpenID+.nl protocol, het inrichten van adequate functiescheiding en toezichtfuncties en het toestaan van een ombudsman.
Bovendien is sprake van diverse soorten van certificering op basis van een accreditatieschema (dat nu nog niet is uitgewerkt).
De aangesloten identity providers worden op de OpenID+.nl white list geplaatst, zodat Relying Parties weten dat een Identity Provider zich conformeert aan het convenant, zonder dat ze met de IdP zelf afspraken hoeven te maken.

**Trust Framework**

Het trustframework omvat de volgende uitgangspunten. Er wordt onderscheid gemaakt tussen de zekerheid omtrent het eigendom van een digitale identiteit en de zekerheid bij het gebruik van de digitale identiteit. Deze beide aspecten zijn in de assen van de matrix opgenomen.

De zekerheid omtrent de eigendom is afhankelijk van het vertrouwen in de identity provider en het vertrouwen in het registratie- en uitgifteproces van digitale identiteiten. Welke verificatie heeft plaatsgevonden? Binnen OpenID+.nl is besloten dat het minimale vertrouwensniveau verificatie via de e-mail is. Dat wil zeggen dat er in ieder geval een bestaand e-mailadres is gekoppeld aan een OpenID. Verder wordt geen enkele garantie verstrekt. Daarnaast kan de Identity provider diverse andere verificaties uitvoeren. Denk aan

*Partijen als Google, Yahoo en Hyves treden op dit moment al op als identity provider voor OpenID-identiteiten*

die identity providers bij die OpenID verstrekte claims accepteren. Als dus een Identity Provider verklaart dat een identiteit adresverificatie (door het versturen van een brief), verificatie van een bankrekeningnummer (bijvoorbeeld na betaling aan de iden-

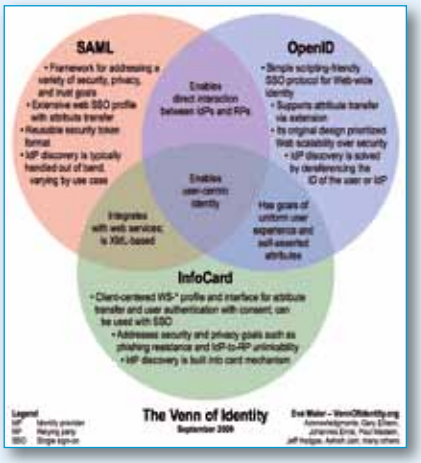
tity provider) en natuurlijk visuele verificatie (in welke vorm dan ook). Al deze verificaties worden in SAML-claims aan relying parties ingeleverd. Het is de taak van de relying party om te besluiten welke autorisaties op grond van de verificaties worden toegekend. Het ligt voor de hand dat naarmate meer zekerheid omtrent de identiteit bestaat, er ook meer autorisaties kunnen worden verstrekt.

Het zekerheid verkrijgen omtrent het rechtmatig gebruik van een digitale identiteit is een ander onderdeel van het convenant. Dit betreft feitelijk het 'traditionele' authenticatieproces. Oftewel, hoe zeker zijn we van de identiteit na de login op een site. Wordt er gebruikgemaakt van single-factor authenticatie (iets wat je weet, bijvoorbeeld gebruikersnaam en wachtwoord), of multi-factor (bijvoorbeeld iets wat je weet in combinatie met iets wat je hebt, bijvoorbeeld een token zoals een gsm).

Inherent aan het protocol van OpenID is dat een individu niet inlogt bij de relying party, maar bij de identity provider. Dat wil zeggen dat de identity provider ook weet hoe iemand inlogt. De authenticatiewijze moet dan ook aan de relying party in een claim worden meegedeeld. Het achterliggende idee is dat een relying party niet hetzelfde hoeft te doen als de identity provider. Als je bij een identity provider bijvoorbeeld een one-time password in de vorm van een sms-authenticatiebericht hebt gebruikt, dan zou je dat niet ook nog eens hoeven doen bij de relying party. Dit is extra interessant omdat OpenID in principe werd ontwikkeld om single sign-on op websites mogelijk te maken. Als je dus bijvoorbeeld al bent ingelogd bij Hyves, dan kun je zonder verdere inlogactie meteen aan de slag bij een relying party. En mocht die relying party op grond van classificatie eisen ten aanzien van een bedrijfsproces bijvoorbeeld een One Time Password vereisen, dan zou de Identity Provider dat misschien wel kunnen uitvoeren. Dat scheelt de relying party aanzienlijk in de beheerinspanningen.

*De zekerheid omtrent de eigendom is afhankelijk van het vertrouwen in de identity provider en het vertrouwen in het registratie- en uitgifteproces van digitale identiteiten*

Binnen het framework zijn diverse verificatievormen als uitwerking en aanvulling op het OpenID-protocol voorzien.




**Stork en zo**

Waarom zou je in Nederland iets ontwikkelen op het gebied van een internationale standaard als OpenID? We zijn in ons land toch niet zo ver vooruit in de gedachtevorming dat we dit probleem als eerste willen aanpakken? Nee, inderdaad, er zijn ook internationaal gezien enkele ontwikkelingen. De bekendste is wel STORK van de Europese Unie. STORK is binnen de EU ontwikkeld om burgers toegang te geven tot overheidsdiensten. Dit initiatief introduceert een soortgelijk framework als OpenID+.nl, maar wel met een aanzienlijk verschil. Daar waar we binnen OpenID+.nl uitgaan van een combinatie van twee verschillende verificaties, hanteert STORK een combinatie trustlevel (het QAA, ofwel Quality of authentication assurance ). Dat betekent dat er trustlevels zijn gedefinieerd, waarbij de verschillende soorten van verificatie elkaar kunnen compenseren. Een matige authenticatie bij registratie en uitreiking van een digitale identiteit kan worden gecompenseerd door een hoog niveau van authenticatie bij inloggen. Dat maakt het wel een eenvoudig hanteerbaar mechanisme, maar theoretisch gezien niet helemaal zuiver. Bovendien gaat STORK uit van standaard autorisatieniveaus, passend bij de trustlevels, waarbij OpenID+.nl uitgaat van de relying party die zelf verantwoordelijk blijft voor de autorisaties.

Een ander initiatief is ICAM, een Amerikaans initiatief dat eveneens (net als OpenID+) gebruik maakt van een white list mechanisme. Ook dat mechanisme gaat wel weer uit van de gecombineerde trustlevels, net als Stork. Beide initiatieven hanteren feitelijk een model dat in 2002 door het Witte Huis is ontwikkeld. Naar de mening van de OpenID+.nl-kopgroep is dat model onvoldoende flexibel en levert het combineren van trustlevels een onjuist beeld van de zekerheid omtrent de individu achter een identiteit.

**Ontwikkeling**

ECP-EPN heeft samen met de 'kopgroep' diverse instrumenten ontwikkeld om OpenID+.nl verder te ontwikkelen. Naast de technische documentatie en het convenant is ook een voorstel ontwikkeld om het beheer van de standaarden te coördineren. En er is inmiddels een Proof of Concept uitgevoerd, waarin het de publicatie van de uitgebreide verificatieinformatie van IP naar RP is uitgetest. Die PoC is met een positief resultaat afgesloten.

Het is op dit moment nog niet helemaal duidelijk hoe de continuïteit van de standaard geborgd gaat worden. Dat is enerzijds afhankelijk van de adoptie ervan in Nederland. Maar anderzijds van de mogelijkheden om samen te werken met internationale standaarden. OpenID is immers een open standaard en het zou mooi zijn als de '+'-uitbreiding eveneens breed gedragen zou worden. Ook de uitbreiding met de opname van Information Card en andere digitale paspoorten in het raamwerk staat in de roadmap.

**Besluit**

Volgens mij is dit initiatief bij uitstek een mogelijkheid om Identity Management en Authenticatie uit te besteden. Dat is al een poosje mijn persoonlijk queeste, waarbij mijn persoonlijke ambitie zover gaat dat we ook intern af kunnen stappen van directory services waarin identiteiten worden beheerd. In de Cloud zijn die toch eigenlijk niet meer toepasbaar...

In ieder geval is het initiatief volop in beweging. En er is ruimte voor partijen om mee te doen, zowel Relying Parties als Identity Providers worden van harte uitgenodigd om mee te doen. Neem gerust per e-mail contact met mij op om er eens verder over door te praten.

# Een iPhone van de zaak

*Auteur: Erno Duinhoven* > Erno Duinhoven is managing consultant bij Capgemini. Hij houdt zich bezig met risk management- en compliance-vraagstukken op het gebied van informatiebeveiliging, met daarbij een focus op security architectuur. Hij is tevens bestuurslid van het PvIB en trekker van de professionaliseringscommissie. Erno is per e-mail bereikbaar op erno.duinhoven@capgemini.com

**De iPhone is een gigantisch verkoopsucces. In de presentatie van de kwartaalcijfers van Apple begin dit jaar bleek dat ondanks de economische crisis de winst van 2009 is verdubbeld. Dit met dank aan de iPhone waarvan er in het laatste kwartaal van 2009 ruim 8 miljoen zijn verkocht. Op 26 januari heeft Apple bovendien de iPad aangekondigd die gebruik zal maken van hetzelfde besturingssysteem. Behalve aan de goede looks, de goede interface en vele beschikbare applicaties, zal ongetwijfeld een deel van dit succes te danken zijn aan de door de fabrikant gepromote mogelijkheden om de iPhone min of meer te integreren in het bedrijfsnetwerk. De Apple website claimt zelfs: "Met ondersteuning voor Cisco IPSec VPN en WPA-2 enterprise met 802.1X-verificatie is de iPhone direct klaar voor het gebruik met Microsoft Exchange." Dit stuk zal ingaan op de mogelijkheden en risico's verbonden aan het integreren van de iPhone in het bedrijfsnetwerk.**

Eind vorige eeuw en het begin van deze eeuw is de opkomst van het internet snel gegaan, met een tijdelijke onderbreking van het uiteenspatten van de internetbubble. Snelle marketingjongens en -meisjes zetten nieuwe producten en diensten in de markt, waarbij de toch al aanwezige druk op de time-to-market nog verder opliep.
In 2000 zijn ook de eerste UMTS-frequenties geveild in Nederland. Uiterlijk in 2007 zouden bij alle aanbieders minimaal zestig procent van de Nederlanders toegang moeten hebben tot de UMTS-netwerken. We kunnen inmiddels vaststellen dat dit aantal is gehaald.
Aan het begin van deze eeuw kwamen de eerste mobiele telefoons, met wat we nu noemen, 'smartphone features'. Met de opkomst van de zogenaamde smartphones en een universele verbinding van de bedrijfsnetwerken en de beschikbaarheid van mobiele breedbandverbindingen zijn de technische voorwaarden geschapen om mobiele devices te integreren in het bedrijfsnetwerk.

### Integratie iPhone

De iPhone kan in theorie worden gebruikt voor iedere functionaliteit die op het bedrijfsnetwerk beschikbaar is, mits aan een aantal technische voorwaarden is voldaan. Uiteraard is dat binnen de beperkte form-factor van de iPhone en moet ik er persoonlijk niet aan denken dit artikel op een iPhone te schrijven.
Een van de meest gebruikte integratiemogelijkheden van de iPhone zal ongetwijfeld de e-mailfunctionaliteit zijn. Bijna overal ter wereld ben je in staat je e-mail te lezen en af te handelen op het moment dat het jou uitkomt. De vraag die natuurlijk aan de security officer gesteld kan worden is wat de regels zijn om de iPhone aan het netwerk te knopen of wat de maatregelen zijn die we moeten treffen om dit te doen. Hieronder een overzicht van de benodigde opstelling volgens de Apple-documentatie en de belangrijkste dreigingen die verbonden zijn aan het koppelen van de iPhone aan de bedrijfse-mailserver.

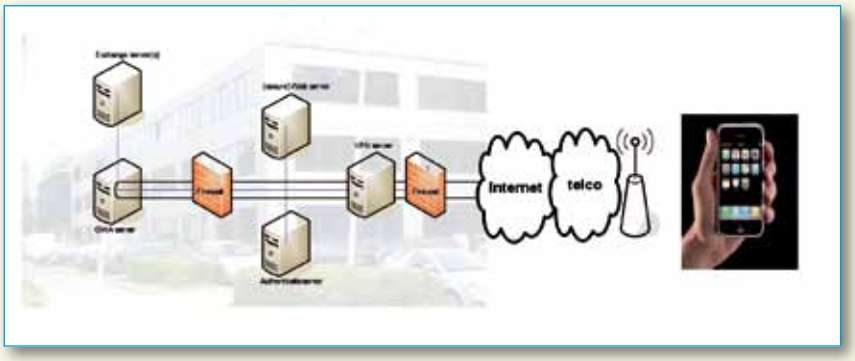



Fig.1. Typische Exchange koppeling iPhone.

### Standaard beveiligingsvoorzieningen

De iPhone is volgens Apple 'business ready' gemaakt door de iPhone standaard uit te rusten met diverse VPN-software en authenticatieprotocollen. De laatste versie, de 3GS, heeft zelfs encryptie ingebouwd waarmee volgens de fabrikant de gegevens veilig kunnen worden opgeslagen.
De bekende en onbekende zwakheden van deze protocollen en hun implementatie laat ik graag aan anderen over. Ook is de iPhone 'business ready' doordat software beschikbaar is voor het maken van corporate instellingen voor accounts en wachtwoorden.
Kortom, het lijkt erop dat de iPhone standaard al vele beveiligingsmogelijkheden heeft. Toch is het verstandig de dreigingen te inventariseren waartegen je de zakelijke gebruiker wilt beschermen, om zo een compleet beeld te hebben van de benodigde beveiliging. Uiteraard moet dit in verhouding staan met de belangen (waarde van de informatie, extra opbrengsten van mobiele functionaliteit, enz.) van het zakelijk gebruik van de iPhone.

### Dreigingen

Hieronder zijn de drie belangrijkste dreigingen opgesomd voor het zakelijk gebruik van de iPhone:

1. verlies of diefstal van de iPhone (en misbruik na diefstal, bijv. netwerkconnectie opzetten);
2. afluisteren dataverkeer;
3. malicious software en verkeerde instellingen.

*1. Verlies of diefstal iPhone*

Gegevens over gestolen en verloren gsm-toestellen zijn op internet niet gemakkelijk vindbaar. Maar een Engelse survey van enkele jaren geleden laat zien dat jaarlijks twee procent van de mobiele telefoons wordt

gestolen. Aangezien de iPhone een gewild toestel is, zal dit percentage zeker niet lager liggen dan bij andere gsm's. Een iPhone kan veel vertrouwelijke informatie van het bedrijf bevatten, maar dit verschilt uiteraard van bedrijf tot bedrijf en van toestel tot toestel. Indien een iPhone in handen komt van iemand die meer dan alleen geïnteresseerd is in het direct doorverkopen van het toestel voor gemakkelijke winst, komt de eventuele vertrouwelijke informatie op straat te liggen.

*2. Afluisteren dataverkeer*
De iPhone kan e-mails en andere gegevens op de exchange-server synchroniseren via een kabelverbinding of via 'de lucht'. Als compromittatie van de synchronisatie via de kabel een probleem is, dan heb je waarschijnlijk grotere problemen dan het voorkomen van het uitlekken van de synchronisatiegegevens. Voor synchronisatie via 'de lucht' heeft de iPhone de volgende opties:

- Bluetooth;
- WiFi;
- GPRS/Edge;
- UMTS / HSDPA.

Nu heeft elk van deze methoden zijn eigen kwetsbaarheden die al eerder in de informatiebeveiliging zijn beschreven en waar op het internet reeds veel over te vinden is. Zonder extra beveiligingsmaatregelen en -instellingen is het dataverkeer van het synchroniseren eenvoudig onopgemerkt af te luisteren. Interessante e-mails, agenda- en contactgegevens zijn daarmee eenvoudig op te vangen voor niet-gerechtigden.

*3. Malicious software en verkeerde instellingen*
Een van de grootste gevaren is de introductie van malicious software, die vervolgens allerlei zaken doet met de data op het device en de data die wordt uitgewisseld.
De iPhone is in de praktijk vooral gewild bij managers en liefhebbers van gadgets. Voor deze groepen gebruikers geldt dat zij vaak proberen om de instellingen van de iPhone zo persoonlijk mogelijk te maken en daarmee diverse beveiligingsinstellingen proberen te omzeilen.

**Maatregelen**
Hieronder wordt ingegaan op de maatregelen die tegen de belangrijkste dreigingen getroffen kunnen worden om de beveiliging op een adequaat niveau te krijgen.

**Versleuteling data op device**
De laatste generatie iPhones (3GS) is uitgerust met encryptiemogelijkheid van de data. Deze feature is enkele dagen na het uitkomen van de iPhone 3GS gekraakt door beveiligingsonderzoekers. Binnen twee minuten is de encryptie te omzeilen. Omdat encryptie van opslagmedia eigenlijk altijd op de achtergrond gebeurt, zijn er nauwelijks alternatieven beschikbaar die de data kunnen vercijferen. Het zal dan neerkomen op een complete suite van functionaliteiten die de gevoelige data vercijferd kunnen opslaan. Het product DME van de Deense firma Excitor is zo'n product. Wellicht zijn er andere fabrikanten die een dergelijk product beschikbaar hebben voor de iPhone, maar ik heb ze nog niet gevonden. Wel is een aantal fabrikanten bezig met de ontwikkeling van software voor het iPhone platform.

**Remote wipe**
De iPhone software ondersteunt het gebruik van 'remote wipe'. Zodra de beheerder het signaal binnenkrijgt dat een iPhone vermist of gestolen is, kan op afstand een signaal worden gegeven om de data op de iPhone te verwijderen. Volgens Apple moeten we daarbij rekenen op 1 uur per 8 GB data. Indien gebruik wordt gemaakt van VPN-beveiliging van de datacommunicatie, dan wordt de 'remote wipe' uitgevoerd nadat de 'eigenaar' van het toestel heeft ingelogd. De optie is eenvoudig te omzeilen door de SIM-kaart uit het toestel te halen.

**Vercijfering dataverkeer**
Een maatregel om data van het bedrijfsnetwerk naar de iPhone over te zetten, is het vercijferen van het dataverkeer. De iPhone beschikt standaard over een VPN-functionaliteit, waarmee het dataverkeer vercijferd kan worden. Diverse bekende VPN-oplossingen van marktleider Cisco worden ondersteund. Er kan gebruik worden gemaakt van dual-sided certificates, zodat beide apparaten zekerheid hebben over met wie ze communiceren.

**Secure login**
Standaard ondersteunt de iPhone diverse secure identificatie/authenticatieprotocollen. Dit is noodzakelijk voor het inloggen op 'zakelijke' applicaties.

**Software ontwikkeling en distributie**
Applicaties voor de iPhone zijn verkrijgbaar via de 'App-store' of kunnen via de Software Development Kit (SDK) / iTunes worden gedistribueerd. Een derde manier die de fabrikant van de iPhone niet wil toestaan is om het toestel te kraken met de zogenaamde jailbreak. Hieronder worden deze opties kort toegelicht.

**App-store**
Het distribueren van applicaties via de App-store, waarbij de fabrikant bepaalt welke applicaties aangeboden worden, is voor het aspect beveiliging een goed idee. Voordat de applicaties op de App-store worden geplaatst 'keurt' de fabrikant de applicaties op een aantal (basis)zaken, die onder andere beschreven zijn in de voorwaarden van de SDK. Indien de applicatie achteraf toch 'evil' blijkt te zijn, kan deze zonder opgave van reden worden verwijderd. Omdat applicaties getekend zijn, kunnen verwijderde applicaties ook worden geblokkeerd op de iPhone. Een groot nadeel van distributie via de App-store is dat de fabrikant uiteindelijk bepaalt welke applicaties worden aangeboden. De strategie is niet voor iedereen even begrijpelijk en acceptabel. Zo zijn lange tijd alternatieve browsers voor de iPhone tegengehouden.

**SDK**
De SDK biedt eigenlijk geen mogelijkheid om Multi-tasking functionaliteiten in te bouwen in de applicaties. De recentelijk aangekondigde versie 4.0 brengt hier een kleine verandering in, maar ook in deze versie zal Multi-tasking gebonden zijn aan restricties. Hier klagen de traditionele ontwikkelaars van beveiligingssoftware ook over in de media en bij Apple. Toch draagt het ontbreken van Multi-tasking in belangrijke mate bij aan de beveiliging. Immers vele exploits maken gebruik van de Multi-tasking mogelijkheden. Er kleeft ook een aantal nadelen aan de App-store. Zolang Apple deze optie voor de bekende leveranciers van beveiligingsapplicaties niet openzet, zullen deze niet geneigd zijn de markt te betreden. Ze zullen te veel moeten ombouwen in plaats van een eenvoudige 'port' te hoeven maken van hun beveiligingsapplicaties. Recentelijk heeft de Amerikaanse evenknie van 'Bits of Freedom', Electronic Frontier Foundation (www.eff.org/deeplinks/2010/03/iphone-developer-program-license-agreement-all) via NASA een verzoek ingediend op basis van de Freedom of Information Act (Amerikaanse Wet Openbaarheid Bestuur) om de licentieovereenkomst van de iPhone SDK openbaar te krijgen.

Hiermee is eindelijk inzicht te verkrijgen voor gebruikers van de iPhone-applicaties waaraan deze applicaties moeten voldoen. De licentie-overeenkomst verbiedt immers verdere bekendmaking van de licentie. Uiteraard behoudt Apple zich het recht voor om de voorwaarden eenzijdig te veranderen. Niet lang na de aankondiging van de iPad heeft Apple plotseling besloten dat ze applicaties waarmee 'veel huidskleur' werd getoond, niet meer waren toegestaan. Boze tongen beweren dat dat is gebeurd omdat de iPad, die gebruikmaakt van hetzelfde besturingssysteem als de iPhone, anders niet geschikt zou zijn voor kinderen.
Met de SDK kunnen ook specifieke applicaties worden ontwikkeld die niet via de App-store worden gedistribueerd. Programma's die u wilt distribueren moeten met een eigen distributiecertificaat zijn ondertekend. Vervolgens wordt er een bedrijfsspecifiek voorzieningenprofiel aangemaakt, waarna distributie kan plaatsvinden via iTunes of via het iPhone-configuratieprogramma. Mocht dit voorzieningenprofiel ontbreken, dan kan de applicatie niet worden gestart. In versie 4 van de SDK worden de mogelijkheden voor distributie van applicaties uitgebreid.

**Jail-break**

Het model kent ook vele tegenstanders. Zo wil niet iedereen zich door Apple of het bedrijf laten vertellen welke software hij/zij wel of niet op de iPhone wil hebben. Vele gebruikers hebben onder andere daarom hun iPhone gejailbreaked. Tot voor kort betroffen alle bekende geslaagde pogingen om de iPhone te infecteren met malicious software iPhones die waren gejailbreaked. Dat het jailbreaken van iPhone redelijk populair is, mag blijken uit het feit dat de zoekterm op Google meer dan 8.000.000 hits oplevert en er zelfs speciale app-stores zijn voor jailbreaked iPhones.
Als bedrijf sta je redelijk machteloos tegen gebruikers die hun iPhone jailbreaken. Het lukt zelfs Apple niet de jailbreaks ongedaan te maken.

*Als bedrijf sta je redelijk machteloos tegen gebruikers die hun iPhone jailbreaken*

**Security suite**

Vanwege het ontbreken van Multi-tasking mogelijkheden in de door Apple beschikbaar gestelde SDK kunnen de traditionele security-softwarepakketten niet een-op-een worden overgezet op de iPhone. Er zullen dus oplossingen ontwikkeld moeten worden waarbij diverse beveiligingsoplossingen geïntegreerd worden in functionele oplossingen. Voor synchronisatie van e-mail, contacten en agenda, waarschijnlijk de meest gebruikte zakelijke toepassing van de smartphone, zal dus een complete suite ontwikkeld moeten worden waarbij diverse beveiligingsfeatures zijn ingebouwd. Op het moment van schrijven is er slechts een applicatie bekend die ook daadwerkelijk leverbaar is voor beveiliging van e-mail, contacten en agenda en synchronisatie daarvan: DME van Excitor. Vele andere bedrijven zijn daarmee bezig, maar hebben op dit moment nog geen werkende applicatie.

**Device control**

De iPhone beschikt over diverse instellingen op beveiligingsgebied. Tot de standaard hulpmiddelen behoort ook software om de (beveiligings)instellingen te kunnen installeren op de iPhone. Via profielen kunnen deze instellingen worden gemaakt.
Daarnaast is er sinds de tweede helft van 2009 ook software leverbaar (Afaria van Sybase en Good) om bedrijfsbrede en individuele (beveiligings)instellingen van de iPhone centraal te kunnen managen en beheersen, inclusief restricties op het gebruik van specifieke applicaties en mogelijkheden van het apparaat, zoals bijvoorbeeld Bluetooth.

**Recente ontwikkelingen**

November 2009 kwam een student uit Hilversum in het nieuws nadat hij diverse iPhones was binnengedrongen via het standaard user-id/wachtwoord van Open SSH van jailbreaked iPhones.
In de jaarlijkse 'pwn2own' wedstrijd, georganiseerd door TippingPoint is dit jaar de iPhone het eerste slachtoffer geworden onder de smartphones, via een hack in de browser van de iPhone. In het jaar ervoor is geen enkele smartphone gekraakt in de wedstrijd. Het geruchtencircuit dat rondom Apple de laatste jaren mytische vormen aanneemt, speculeert inmiddels over de opvolger van de iPhone 3GS (iPhone 4G of iPhone HD) en de mogelijkheden voor multi-tasking. Zoals altijd zwijgt Apple formeel over alle geruchten en is het wachten op de eerste tekenen bij het uitkomen van een nieuwe versie van de SDK of dit ook daadwerkelijk het geval is. Dit biedt dan uiteraard mogelijkheden voor de traditionele beveiligingssoftware-leveranciers, maar ook mogelijkheden voor nieuwe exploits. Deze wedloop zal gewoon doorgaan.

*De iPhone ontbeert 'security by design'*

**Algemene conclusie**

De iPhone ontbeert 'security by design'. Toch heeft Apple goed nagedacht over de ontwikkeling en distributie van applicaties voor dit platform. Of dit nu primair is vanwege de niet geringe financiële opbrengsten die Apple krijgt (de maker krijgt zeventig procent, Apple de rest) of dat beveiliging hoog in het vaandel stond, het gecontroleerd distribueren van applicaties heeft beveiligingstechnisch voordelen. De in het apparaat ingebouwde security features, die sinds de tweede generatie zijn toegevoegd, maken duidelijk dat security als add-on wordt beschouwd en maken het nog geen veilig apparaat. Of de iPhone 'veilig' genoeg is om te gebruiken voor zakelijke toepassing hangt af van het type business en de gevoeligheid van de informatie die je ermee gaat verwerken. Er is weinig keuze in beveiligingssoftware voor de iPhone en de standaard geboden opties bieden weinig bescherming van (gevoelige) bedrijfsgegevens bij verlies of diefstal van het apparaat.

**Links:**

www.apple.com/nl/iphone/enterprise/integration.html
manuals.info.apple.com/nl_NL/Implementatiehandleiding_voor_bedrijven.pdf
developer.apple.com/iphone/index.action

# Verkiezing Artikel van het jaar

**Ook voor 2009 is er weer een artikel van het jaar geselecteerd. Dit jaar werden we als jury voor een uitdaging geplaatst door niet zes maar tien artikelen te beoordelen. Nu is het lezen van de beste artikelen van een jaargang Informatiebeveiliging allerminst een uitdaging, integendeel zou ik zeggen. Bij vlagen is het zelfs genieten. Maar als het gaat om naast het lezen ook een beoordeling te geven en het beste artikel te selecteren, dan hebben we ervaren dat dat heel lastig kan zijn. Daarbij kregen we de opdracht om dit jaar niet slechts een prijs, maar drie prijzen weg te geven. Uit deze uitbreiding van het aantal prijzen leidden we af dat de redactie het belang en noodzaak van goede artikelen wil onderstrepen. Een mooie geste die we op zich wel kunnen waarderen, maar die onze opdracht er niet eenvoudiger op maakte.**

**De shortlist:**

2009 nr. 1. Vriendensites op herhaling
Marco Smitshoek

2009 nr. 2. Claims based access control
André Koot

2009 nr. 4. De rol van audits (beveiliging en architectuur raamwerken)
Saïd El Aoufi

2009 nr. 4. IB-architectuur in Jericho stijl
Aaldert Hofman

2009 nr. 4. Toegang tot patiëntgegevens
Leon van der Krogt

2009 nr. 5. Anonimiteit versus verantwoording op het internet
Ellen Wesselingh

2009 nr. 6. Interessante discussies over Elektronisch Patiënten Dossier
André Koot en Erno Duinhoven

2009 nr. 7. BCM en cloud: Continuïteit as a Service
André Koot

2009 nr. 7. De juridische aspecten van preventief monitoren en digitaal onderzoek
Erwin van der Zwan

2009 nr. 8. Een architectuuraanpak voor IB-patronen
Jaap v.d. Veen

Vorig jaar hadden we een afgetekende winnaar in de naam van Wolter Pieters die in zijn betoog 'De monsterlijke trekjes van beveiligingsproblemen' de ogenschijnlijke complexiteit van informatiebeveiliging afbeeldde op eigenaardigheden van alledag. Een bijzondere benadering waarmee hij terecht de eerste prijs mocht komen ophalen. Dit jaar helaas geen artikel vanuit een filosofische invalshoek. Wel veel actuele thema's zoals security en social sites, EPD, Cloudcomputing en meerdere architectuur en juridische onderwerpen. De kwaliteit van de artikelen was dit jaar erg hoog. Zonder uitzondering kan je zeggen dat alle tien artikelen zeer interessant en op zijn minst lezenswaardig waren. Uiteindelijk zijn we na lang wikken en wegen tot de volgende top drie gekomen:

- Claims based access control – André Koot.
- De juridische aspecten van preventief monitoren en digitaal onderzoek - Erwin van der Zwan
- De rol van audits (beveiliging en architectuur raamwerken) - Saïd El Aoufi

Het was zoals gezegd niet eenvoudig om een top drie samen te stellen, met name omdat de hoofdredacteur Andre Koot hoge ogen gooide met drie artikelen van zijn hand, waaronder een van grote klasse namelijk, Claims based access control. De jury is echter van mening dat de verkiezing van artikel van het jaar er vooral is om lezers uit te nodigen de pen ter hand te nemen en hun kennis over bijzondere en nieuwe ontwikkelingen op het vakgebied te delen. We waarderen de bijdragen van Andre in hoge mate, maar houden vast aan de doelstelling van de aanmoediging van de leden.

Daarom voor Andre een **3e plaats met claims based acces control.** Niet vanwege de kwaliteit, integendeel, maar vanwege het feit dat hij als hoofdredacteur natuurlijk een voorsprong heeft als het gaat om het hanteren van stijl, leesbaarheid, vernieuwend zijn enz. Hij kent de klappen van de zweep als geen ander. Indien we de eerste prijs aan de hoofdredacteur zouden geven dan ontnemen we wellicht andere leden de moed om dit jaar een artikel in te sturen en dat willen we hoe dan ook voorkomen. Daarom hebben we als jury besloten een extra criterium toe te voegen,

John Rudolph, spreker namens de jury.

Tijdens de Algemene Ledenvergadering van 20 april zijn de prijzen bekendgemaakt en uitgereikt aan de winnaars.

namelijk een 'handicap voor (hoofd)redacteurs' waardoor de gewone auteur een licht voordeel geniet. Claims based access control is echter wel een uitstekend artikel omdat het veel actuele zaken aansnijdt en het probleem van morgen zichtbaar maakt. Nu we allemaal volop aan de slag zijn om met veel pijn en moeite roll based access control in te voeren in onze organisaties, wijst André ons erop dat dit al weer 'zo 2009' is. Nee, in 2010 gaat het erom: 'hoe kunt u aantonen wie u bent?' binnen het wereldwijde internet. Daar heb je toch een vertrouwde instantie voor nodig? En wie is dat en hoe kan dat dan worden gedaan? Boeiend en uitdagend tegelijkertijd en daarbij zeer goed geschreven.

Op de **2e plaats de juridische aspecten van preventief monitoren en digitaal onderzoek van Erwin van der Zwan.** Eveneens een uitstekend artikel omdat Erwin er in slaagt om aan de hand van een goed gekozen voorbeeld op een zeer overzichtelijke en heldere wijze de zeker niet boeiende wetsartikelen in verband te brengen met de dagelijkse praktijk van security-incidenten. In ieder geval een 'must' voor mijn studenten, maar ook voor security officers in het veld.

Op de **1e plaats het artikel over de rol van audits van Saïd El Aoufi.** Hoewel de titel daar op het eerste gezicht geen melding van maakt (klein minpuntje!) geeft het artikel een bijzonder goed overzicht van architectuur en de rol die architectuur zou kunnen innemen bij audits. Een goed onderbouwd artikel met veel goede referenties en bovendien plezierig leesbaar. Toch blijft er bij het lezen voortdurend iets bij je knagen; 'goede en slimme gedachte om architectuur mee te nemen als onderdeel van een audit, maar kan dat wel?' In de laatste zin van het artikel geeft de auteur ook zelf zijn twijfels bloot en slaat hij de spijker op z'n kop. Laten we architectuur vooral inzetten om grip te houden en wellicht komen we er ooit aan toe om architectuur ook een onderdeel te laten zijn van een audit. Kortom, toekomstgericht en vernieuwend en spannend tot het slot.

Aan het slot nog eervolle vermelding voor nummers vier, **Anonimiteit versus verantwoording op het internet van Ellen Wesselingh** en vijf, **Een architectuuraanpak voor IB-patronen van Jaap v.d. Veen** voor respectievelijk de opbouw van het betoog en de omvang, plus diepgang van het onderzoek dat is uitgevoerd door de gehele werkgroep. Dank uiteraard aan alle auteurs voor de artikelen in 2009 en veel succes bij het schrijven van uw bijdrage(n) aan Informatiebeveiliging in 2010.

Namens de jury bestaande uit
Kees Hintzbergen, John Rudolph
en Leo van Koppen

# Interview
# Hans Alfons over CRAMM en beveiligen in Afghanistan

*Auteur: Lex Borger* >Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.
Hans Alfons is security officer bij Univé. Hij is te bereiken via e-mail: h.alfons@unive.nl.

**Na jaren bij de Nederlandse Defensie te hebben gewerkt, werkt Hans Alfons sinds kort als Information Security Officer bij het Univé bedrijfsonderdeel Distributie. Voor zijn aanpak van informatiebeveiliging binnen de Koninklijke Landmacht kreeg Hans in 2005 met zijn team het Risk Management Bedrijf Award en haalde hij de tweede plaats bij de Joop Bautz Award. In 2009 ontving Hans de koninklijke onderscheiding 'Lid in de Orde van Oranje Nassau met de zwaarden', voor het inrichten en onderhouden van informatiebeveiliging in de breedste zin van het woord. Hierbij inbegrepen de militaire missies naar Irak en Afghanistan.**


Lex Borger.


Hans Alfons.

Ik sprak met Hans over zijn visie op, en zijn ervaring met informatiebeveiliging. Wat mij opviel was de rust en eenvoud die Hans uitstraalt als hij over zijn passie spreekt. Ik heb in mijn optekening getracht die stijl vast te houden. Hans had zoveel te vertellen, dat we besloten hebben dit gesprek over twee nummers van Informatiebeveiliging te verdelen. In deze uitgave het tweede deel, waarin Hans spreekt over CRAMM en beveiligen in Afghanistan.
"De CRAMM methodiek is rond 1995 naar Nederland gehaald door Deloitte, In 2000 is het importeurschap overgegaan naar 3-Angle. Ik ben er meteen bij betrokken geweest en we hebben een eerste proef gedaan bij Defensie. We hebben ook gekeken wat de beheerwaarde ervan was. Een ander gemak wat CRAMM biedt, is dat je maatregelen kunt exporteren naar een ander systeem. Je kunt dus CRAMM door een externe partij laten uitvoeren, dat laat je eens in de zoveel tijd doen. Vervolgens moet je zorgen dat je zelf een managementsysteem hebt waarin je alles verwerkt. Zo komen we van CRAMM naar het Intergrale Beveiligings Informatie Systeem (IBIS). Bij Defensie hebben we een systeem ontwikkeld waarin iemand een aanvraag kan doen, bijvoorbeeld 'ik wil een geheim systeem gebruiken in die kamer van dat gebouw, mag dat?' Dat systeem bevat het beveiligingsplan, dat vanuit CRAMM is geïmporteerd. Het systeem is zó verfijnd, dat ik kan zien aan de ruimteaanduiding van het systeem hoe die ruimte beveiligd is. De mensen van fysieke beveiliging hebben heel gedetailleerd in een deel van die database een goedkeuring gegeven dat die ruimte op norm is. Dan krijg je het informatiesysteem waarbij je kunt zien in de aanvraag wie van het personeel ermee gaat werken. Daar kun je ook goedkeuring voor geven. Vervolgens kijk je naar de rubricering van het systeem en als alles goed is, dan mag je daar ermee werken. Als je nu verder kijkt hoe IBIS is opgebouwd, zit er een module in waar risicomanagement mee gedaan wordt. Het doel van die module is om de behoefte van Defensie te bevredigen. Zij moeten in staat zijn om van de eenheden die gereed moeten kunnen staan binnen een dag vast te stellen dat ze aan de beveiligingsnormen voldoen. Dat rolt daar gewoon uit. Als je weet wat de BIV-classificatie is, dan weet je ook wat de set met maatregelen is. Wij hadden in CRAMM de mogelijkheid om aan te geven welke componenten je meeneemt, en konden aangeven volgens welke rubricering je gaat werken en wat je beschikbaarheidseis is. Nadat dit is ingevoerd, rolt je set aan maatregelen eruit. En we hadden daarin ook geregeld dat de eisen omgezet werden naar normenkaders. Dan wist de commandant die te velde ging wat het normenkader is waar hij aan moest voldoen. Dan heb je het voordeel, omdat je bij Defensie werkt, dat er voorbereidend werk is gedaan. Dus je weet wat de beveiligingsniveaus zijn van bepaalde componenten die zijn aangekocht op dat niveau. Daarna is de controle heel simpel, als jij die componenten meeneemt, dan zit dat beveiligingsniveau er in. Dus eigenlijk moet je het zo zien: je weet wat je wilt, je gaat naar de kast toe, haalt de Legoblokken eruit, die prik je op elkaar en dan heb je de beveiliging op orde. De keuze van de componenten is hierin cruciaal. We moesten hiervoor de expertise in het bedrijf hebben. Wij hebben heel nauw samengewerkt met mensen van de luchtmacht en van de landmacht die wij in de beginfase bij het project hebben betrokken en die hebben de blokken die op uitzending zouden kunnen gaan gedefinieerd, met duidelijke omschrijving wat daarin zat. Die blokken die definieerden we dan in CRAMM. En als jij dan een homebase-link had, dat is een straalzenderverbinding naar waar ook ter wereld, dan moet die op een bepaalde manier beveiligd zijn. Die heb je mobiel en die heb je statisch, in het beveiligingsplan heb je dat al beschreven. Dus als ze zo'n homebase-link meenemen, dan weet je ook wat het bijbehorende pakket met maatregelen is. Dan ga je er al van uit dat er in zo'n inzetgebied sowieso tot en met geheim gewerkt gaat worden. Daar houd je dus al rekening mee. In het systeem wat we na CRAMM ontworpen, hebben we de blokken in gestopt en je

maakt daaruit de keuze: 'Wat neem je mee?' Je kon van bovenaf ook onmiddellijk vaststellen dat aan het beveiligingsniveau voldaan werd, want iemand moest aangeven dat hij dat blok mee heeft en dat hij de beveiliging van dat blok gecontroleerd heeft. Dus op hoog niveau was dat ook te zien en te controleren. Fysieke beveiliging neem je niet mee, die ga je ter plekke inrichten. Daar gaan mensen voor aan het werk. Die zeggen op een moment: 'ik heb aan de fysieke beveiliging voldaan, dus die IT-blokken kunnen nu ingevlogen worden.' Die IT-blokken vlieg je dan in, terwijl de fysieke beveiliging al geregeld is. De verantwoordelijke daarover geeft in het systeem aan dat hij dat geregeld heeft. Dus dit is weer te zien op hoog niveau. Die halen weer uit het systeem dat hun beveiliging op groen staat. Als je kijkt naar de awards die we gewonnen hebben, daarvoor hebben we twee zaken die we gedaan hebben ingezonden. Het risicomanagementproces en de toepassing daarvan door middel van een geautomatiseerd middel. Bij de risicomanagement-award lag de nadruk op het eerste gedeelte, bij de Joop Bautz-award lag de nadruk op het tweede gedeelte. Ze zijn wel als een geheel aangeboden. Bij de risicomanagement-award gaven ze aan dat ze het heel slim vonden dat je heel snel tot een beveiligingsplan kwam en vastgesteld hebt dat daar maatregelen zijn geïmplementeerd. Ook het anders denken was daar deel van. Hoe kan je simpel en eenvoudig tot hetzelfde resultaat komen? Bij de Joop Bautz-award ging het veel meer over de techniek, daar ging het voornamelijk om het programma. Dat hebben we niet gewonnen. We hebben wel gehoord dat er een tweede stemming nodig was. We hebben een certificaat gehad dat we tweede zijn geworden. We zien dat als bewijsvoering dat het systeem in orde was. Daar zijn we ook blij mee.

**Afghanistan**

In Afghanistan hebben we deze methodiek ook toegepast. Voor de inzet in Afghanistan vinden er voorbesprekingen plaats, daar bepaal je hoe de ICT zich gaat ontwikkelen. Wij zaten erbij om de beveiligingsaspecten in de gaten te houden. Daar wil ik een paar leuke voorbeelden van geven:

*Bepantsering*

Juist doordat je met risicomanagement bezig bent, heb je de maatregelset in je hoofd. Daardoor benader je dingen anders. Men bedacht dat gepantserde containers zouden worden gebruikt voor werkplekken. Ik snap dat, je kunt daar veilig werken in drieploegendienst. De werkploeg ligt dan gepantserd, de andere twee ploegen zijn op dat moment ongepantserd. De enige vraag die ik daarbij gesteld heb is 'Wat houd je over als de andere twee ploegen worden uitgeschakeld? Kun je dan verder werken?' Men heeft uiteindelijk iedereen onder pantser gebracht. En dan ging het er niet om dat ik dacht dat het handig was dat ze zouden overleven, het ging om de continuïteit van het bedrijfsproces.

*Stroomvoorziening*

Men had de simpele gedachte uit beheersmatig oogpunt dat het slim was om alle aggregaten bij elkaar te zetten. Daarbij hadden ze wel aan continuïteit gedacht, want ze hadden een serie van drie aggregaten. Een draait, de andere staat stand-by en de derde is reserve. Dat was dus goed geregeld. Het enige nadeel was dat alles op een grote hoop bij elkaar stond. Dus als je daar een explosie hebt, ben je alles kwijt. Gewoon door vragen te stellen over hoe ze dat dan zouden oplossen, zie je dat ze dan zelf ook met ideeën komen: 'Laten we de aggregaten dan spreiden.' En dat hebben ze ook toegepast. Dus de kwetsbaarheid van een beschadiging bij een

aanval is hierbij ondervangen, de andere aggregaten blijven beschikbaar om het over te nemen.

Een ander aspect van Afghanistan is dat beveiliging niet het doel is. Eerst dacht ik 'Ja jongens, beveiligen is toch ook belangrijk', maar uiteindelijk merk je dat er twee dingen zijn. En daar onderscheid Defensie zich niet van Univé. Je hebt de business, bij Defensie is dat de operatie, en je hebt beveiliging. Uiteindelijk zul je altijd zien dat de directeur, degene die verantwoordelijk is voor de business c.q. operatie, dat ook als primair doel neemt. Beveiliging is altijd ondergeschikt. Dus is het de taak van een beveiliger om dat op een juiste manier onder de aandacht te brengen.

En zo kijk ik ook naar CRAMM, je hebt de maatregelen, je kijkt ernaar en je kijkt naar de omgeving waar je zit en je kiest wat het beste bij de omgeving past. En dat kan gemakkelijk zijn dat geen van de maatregelen direct bruikbaar is. Dan ga je nadenken. Er staat in CRAMM 'er moet een omheining rond het complex staan.' Wat is nou een omheining? Als je de foto's van Afghanistan ziet, zie je allemaal grote zakken zand staan. Dat is nou een omheining. En daar ligt dan prikkeldraad op of voor. Zo los je dat op. Wat CRAMM ook voorschrijft is 'de inrichting moet zoveel mogelijk volgens rechte lijnen lopen.'

Dan denk je bij jezelf 'Ja, dat klinkt allemaal logisch,' maar je ziet ook vaak dat mensen gaan bouwen volgens de contouren van het veld. Dan krijg je dode hoeken. Dan zie je dus dat je als informatiebeveiliger ook de fysieke beveiliging mee moet nemen in je kennis en expertise om te kunnen zeggen 'hoe doe je dat nou precies?' Aan het grootste gedeelte van de fysieke beveiliging hebben wij allemaal bijgedragen. Ook het omgekeerde kwam voor. Dat komt omdat de vakgebieden eigenlijk niet losstaan van elkaar, maar in elkaar overlopen.

Hetzelfde geldt voor de brandweer. Er was ook een brandweercommandant mee. Hij had bepaalde ideeën over hoe het kamp er uit mag zien. We kwamen tot de conclusie dat het in Afghanistan anders was dan in Nederland. Je wilt de wetgeving wel volgen, maar dat botst met andere dingen. Toen wij daar vanuit de drie expertises aanwezig waren, zag je de expertises ook in elkaar schuiven. Als ik vanuit informatiebeveiligingsoogpunt zei 'dat wil ik eigenlijk zo beveiligen', dan zei de brandweer 'houd er rekening mee, dat zit zo' en de fysieke organisatie had ook zijn eigen idee. Uiteindelijk kies je dan de beste oplossing om het daar te doen. En dat wil

niet zeggen dat dan 100% de informatiebeveiligingsoplossing gekozen wordt. Nee, je probeert de meest werkbare oplossing te kiezen. Bijvoorbeeld, als wij praten over een militaire operatiekamer, dan snapt iedereen wel dat dat zwaar beveiligd moet worden als we in Nederland zouden zijn. In Irak was het gewoon een tent. Dat komt voort uit een belangrijk aspect van hoe we objecten beveiligen, door met ringen van beveiliging te werken. Als je een locatie hebt waar alleen maar eigen personeel zit, met de juiste machtiging, dan maakt het niet uit of de operatie in een tent zit of dat het zwaar beveiligd is. Als je de serverruimte als voorbeeld neemt, dat kan een gewone kamer zijn. Mits je maar weet wie naar binnen gaat, dat je weet wie er langs komt zodat ze niet moedwillig beschadiging kunnen aanbrengen. En vervolgens moet je een ring van beveiliging om de buitenzijde van het gebouw leggen, dus goede toegangsbeveiliging tot het gebouw. Dat zie je bijvoorbeeld hier bij Univé. Je komt hier niet gemakkelijk binnen en mensen laten hun laptop staan als ze weglopen. Dan ga je het risico bekijken en dan constateer je dat de ring van beveiliging hier op de rand ligt. Het enige wat hier nog een nadeel lijkt is dat mensen niet overal geclusterd zijn per afdeling. Hierdoor weet je niet eenvoudig of er een vreemd iemand tussen zit. Je hebt hier op kantoor ook geen documenten, dus die kunnen niet gestolen worden. Laptops zijn beveiligd met encryptie. Dus wat wil je hier eigenlijk stelen? Ringen van beveiliging leggen is een betere aanpak dan overal maximaal beveiligen. Want dat zie je ook toegepast worden. Maximaal beveiligen is domweg alle maatregelen uitvoeren die moeten, zonder er verder over na te denken. Die ringen van beveiliging kun je op verschillende plaatsen leggen. Het hangt ervan af wat je hebt hoe je dat doet. Er zijn twee aspecten:

1. *Het financiële aspect*
   Als je een groot bedrijf bent en je gaat je belangen beveiligen, dan kan dat in een kleinere ruimte. Je zegt dan 'daar stop ik mijn hoogste belangen, dan kan de rest een stukje minder.' Je ziet dat nu een heleboel mensen afhankelijk zijn van hun laptops, en daar veel informatie doorheen laten gaan waarvan het toch niet handig is als iemand anders daar vanaf weet. In die situatie mag je de serverruimte wat minder beveiligen, maar dan moet je de buitenkant beter beveiligen. Dat zijn allemaal financiële afwegingen van wat de risico's zijn die je loopt en waar je dan die ring van beveiliging legt.

2. *Logische toegangsbeveiliging*
   Bij computersystemen heb je altijd nog de logische toegangsbeveiliging, dus je bent niet zomaar bij de data. Dat is al een maatregel wat maakt dat wij het niet erg zouden moeten vinden dat er een vreemde in je serverruimte loopt, ervan uitgaande dat jij je servers goed beveiligd hebt. Dan doet een persoon al zoveel moeite om bij de data op een server te komen - we gaan er niet vanuit dat hij steelt, dat is een ander verhaal - voor de fysieke beveiliging. Het gaat even om de denkwijze. Je zag dat de fysieke beveiligers bij de landmacht op een bepaald moment ook begonnen in te zien dat een computer geen wapen is. Je wilt dat het niet gestolen wordt, maar je neemt bij de computer extra beveiligingsmaatregelen om te voorkomen dat men over de data kan beschikken. Dat is van cruciaal belang. Dus als je de computer stuk maakt is de data niet beschadigd, omdat die data altijd nog ergens anders staat.

De fysieke beveiliging richt zich op het voorkomen van fysieke schade. Bij ICT mag dat best voorkomen, want als alles goed beveiligd is, hebben we altijd nog een back-up. Belangrijke systemen draaien altijd nog ergens anders, dus dan zorg je voor je continuïteit.

Bij de landmacht zie je dat fysieke beveiliging en ICT-beveiliging in elkaar geschoven zijn. Bij Univé-VGZ-IZA-Trias zie je dat wat minder. De beveiliging wordt daar op verschillende plaatsen gerealiseerd en dat zou ook moeten worden samengebracht. Ik hoop dit samen met mijn collega's in de komende tijd te realiseren. En zo komen we op het volgende onderwerp.

**Univé-VGZ-IZA-Trias**

Ik zocht iets zodat ik met mijn passie, informatiebeveiliging, door kon gaan. Eigenlijk

zocht ik iets waarbij ik datgene wat ik uitgedacht had bij Defensie in de praktijk kon brengen. Ik vond een vacature die daar honderd procent aan voldeed. Op vijf minuten voor het sluiten van de markt heb ik een e-mailtje verstuurd, ik ben op gesprek geweest en mijn conclusie was dat de bij Defensie gebruikte methode ook hier toepasbaar is.
Als ik ga kijken naar mogelijkheden voor geautomatiseerde systemen om de informatiebeveiliging bij Univé-VGZ-IZA-Trias (UVIT) te ondersteunen dan moet ik op de markt kijken wat er is. UVIT beschikt over een aantal CRAMM-licenties. Het enige wat ik dus moest doen is zoeken naar een soort IBIS.
Bij UVIT heb ik met de diverse functionarissen informatiebeveiliging de methodiek van de Koninklijke Landmacht besproken en aangegeven dat dit de controleerbaarheid van het informatiebeveiligingsproces voor onder andere de interne accountantsdienst en de Nederlandsche Bank zal vergroten.
Aan de hand van de risico's uit FIRM (van de Nederlandsche Bank) is een UVIT risicomodel gemaakt en met gebruik van de ondersteunende tool CRAMM kan je aantonen welke informatiebeveiligingsrisico's gekoppeld zijn aan de het UVIT-risicomodel en met welke maatregelen de informatiebeveiligingsrisico's worden gemitigeerd.
Als vervanger van het tool IBIS zijn we nu met een pakket bezig, STREAM van Acuity Risk Management. Wat ik daarvan belangrijk vind is dat wat we ook in IBIS hadden … Ik zal een voorbeeld geven: functioneel beheerders dienen iedere drie maanden voor hun systemen aan te geven dat de beveiligingsmaatregelen waar zij verantwoordelijk voor zijn nog aanwezig zijn en werken.
Dit wordt nu schriftelijk gedaan. De beveiligingsfunctionaris consolideert de gegevens en rapporteert dit aan zijn directeur en de afdeling Risk & Compliance. Als iedere functionaris die verantwoordelijk is voor beveiligingsmaatregelen dat doet op zijn gebied zoals fysieke beveiliging, personele beveiliging, netwerkbeveiliging enzovoort, dan weten diverse functionarissen op verschillende managementlagen elke drie maanden door middel van allerlei rapportages, managementsamenvattingen, enz. hoe de beveiliging van de hele of een gedeelte van de organisatie er voor staat.
Door de input van Stream, iedere drie maanden of bij wijzigingen te laten uitvoeren/controleren door de functionarissen die verantwoordelijk zijn voor informatiebeveiligingsmaatregelen genereer je door middel van dwarsdoorsneden, managementsamenvattingen, dashboardsinformatie voor het management.
Wat de output betreft kan je het zo gek maken als je zelf wilt. Op elke laag kun je de directe chef, bijvoorbeeld de IT-directeur, tonen dat al zijn systemen en processen op orde zijn. De controlerende instanties kunnen hun relevante gegevens, in een op hun gewenste format eruit halen. De functionaris informatiebeveiliging overziet zijn speelveld tot op het laagste niveau. En ook de Raad van Bestuur overziet real time op een dashboard de beveiliging van UVIT.
En als je nu ziet hoeveel werk er mee gemoeid is om gegevens te verzamelen en om te zetten naar diverse managementinformatie en dat dit op reguliere basis gebeurt, dan is er grote tijdwinst te behalen met een geautomatiseerd systeem.
Dit is mijn beeld, we zullen zien of het werkelijkheid wordt. Je moet toch een toekomstvisie hebben…"

# Podium

**Afgelopen november tijdens de ALV zijn Tom Bakker en Kees van der Maarel toegetreden tot het bestuur van het PvIB. Tom volgt André Koot op in het bestuur. Tom heeft zich in nummer 2 van 2009 al eerder voorgesteld toen hij toetrad tot de redactie van dit blad. Hieronder stelt Kees van de Maarel zich aan u voor.**

"Mijn naam is Kees van der Maarel. Tijdens de ALV van vorig jaar ben ik als bestuurslid van het PvIB gekozen. In het bestuur neem ik de taak over van Piet Goeyenbier namelijk, het helpen ontwikkelen van de Young Professionals.
Net als Piet werk ik bij de Rijksauditdienst als IT en Operational auditor. In 1992 ben ik in het vakgebied van de informatiebeveiliging gestapt. In eerste instantie voor de theoretische onderbouwing van mijn werk heb ik de IT-auditopleiding gevolgd (kan ik aanbevelen!). Na diverse functies als informatiebeveiliger heb ik in 2001 de overstap gemaakt naar het auditing vakgebied. Daarbij blijft informatiebeveiliging / IT-security een belangrijk aandachtsgebied. Naast het beoordelen van de betrouwbaarheid van informatiesystemen en

het onderzoek naar bedrijfsvoeringsprocessen ben ik betrokken bij de ontwikkelingen op informatiebeveiligingsgebied binnen de Rijksoverheid. Daarnaast heb ik als hobby er lol in bewustwordingssessies op het gebied van informatiebeveiliging te geven en (natuurlijk in opdracht) aan social engineering te doen. Kortom, ik ben en voel mij volop betrokken bij de ontwikkelingen rond informatiebeveiliging. Omdat ik daarnaast veel plezier heb in het in beweging brengen van mensen ben ik blij met het aandachtgebied Young Professionals dat ik bij PvIB heb gekregen.
Informatiebeveiliging is een lastig onderwerp. Mijn ervaring is dat als je voor jezelf de lat niet hoog legt, en met kleine beetjes tegelijk aan de slag gaat het een bijzonder leuk en uitdagend vakgebied is!"

# Achter het nieuws

*Over deze rubriek >* Met ingang van dit nummer start Informatiebeveiliging met de nieuwe rubriek Achter het nieuws. In deze rubriek geven enkele van de IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems inzake informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en geeft niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Vragen en opmerkingen kunt u sturen naar ibmagazine@pvib.nl

## Elektronisch Patiënten Dossier (EPD)

**Deze eerste Achter het nieuws gaat over het Elektronisch Patiënten Dossier (EPD). Recentelijk was er heel veel aandacht voor de blijkbaar onvoldoende beveiliging van het Elektronisch Patiënten Dossier (zie onder andere www.security.nl/artikel/32880/1/Beveiliging_EPD_schiet _ernstig _tekort). Wat moeten we daar nu mee en hoe kijken de redacteuren van Informatiebeveiliging nu zelf naar het EPD?**

**André Koot**: "Soms vraag je je af waarom we beginnen aan dat waar we aan beginnen. Het EPD is zoiets. Een oplossing voor een klein probleem (namelijk medicatie-informatie, ook voor waarnemende artsen) en we krijgen er een fiks privacy- en securityprobleem bij. Zoiets is van opzet oké, maar qua werking niet zo heel lekker. Tot nog toe merk je dat eigenlijk alleen de bedenkers ervan enthousiast zijn. Verder is vrijwel iedereen kritisch. Maar dat is typisch politiek.
Ik zou niet verbaasd zijn als we over minder dan tien jaar een parlementaire enquête krijgen over ófwel een paar heftige privacyproblemen óf over een enorme kostenoverschrijding. En dan weten we het wel: fout gestart, we zullen leren van de fouten. Maar ja, dat doen we nooit. Typisch politiek.
Dat EPD is schieten met een kanon op een mug omdat we denken dat het een olifant is. Symptoombestrijding is riskant en duur, dat is zeker. Typisch."

**Rob Greuter**: "Het EPD, wat moet je ermee? Probeer maar eens bezwaar aan te teken tegen opname. Krijg je doodleuk te horen dat je een kopie van je identiteitsbewijs erbij moet doen. Jawel, gewoon met de post. De papieren post. Tekenend voor deze wanstaltig slecht beveiligde infrastructuur die bovendien nog in aanbouw is. Als men er werk van maakt zal er nog zeker een jaar nodig zijn om de procedurele en technische beveiliging naar een enigszins aanvaardbaar niveau te tillen. Aanvaardbaar inderdaad, wat zo lazen wij onlangs, het moet wel vooral functioneel blijven. En dan, zo'n 400.000 mensen hebben straks toegang tot het EPD. Geef mij een dag en ik vind 5 mensen die chantabel zijn... Ik blijf het een grote schande vinden dat onze overheid alweer kwistig smijt met belastingcenten omdat er onder grote politieke druk ooit een EPD toegezegd is. De uitkomst van deze 'investering' is allang bekend. Waste of time and money."

**Tom Bakker**: "Ik heb bezwaar aangetekend tegen opname in het EPD. Waarom? Op zich is er niets tegen het idee. Een presentatie die ik onlangs heb bijgewoond vergeleek het EPD-project met het bouwen van een huis zonder bouwvergunning, architectuur, regelgeving, planning enz. Gewoon een hoop stenen en cement. We beginnen en we weten niet waar we eindigen. Met zulke gevoelige informatie als medische gegevens moet je voorzichtig omgaan. Het is mij niet duidelijk welke personen straks toegang krijgen tot mijn gegevens. Zorgverzekeraars bijvoorbeeld? De praktijk wijst uit dat personeel het niet zo nauw neemt met het geheimhouden van accounts en wachtwoorden. Denk bijvoorbeeld aan uitzendkrachten die op zich geen toegang zouden moeten krijgen maar wegens tijdgebrek 'even' het account van een wel geautoriseerde collega lenen. Daarvan zijn genoeg voorbeelden te vinden. Dat gebeurt in het bedrijfsleven en ongetwijfeld ook in de zorg. Kortom, de bedoeling is goed, maar de uitvoering rammelt."

**Lex Dunn**: "Vanuit mijn persoonlijke situatie herken ik de voordelen van een EPD. Mijn vrouw heeft een langdurige medische geschiedenis en het zou fijn zijn als die informatie voor geautoriseerde medici beschikbaar is mocht er onverhoopt iets gebeuren. Toch hebben ook wij bezwaar aangetekend tegen opname in het EPD. De reden daarvoor is tweeledig. Enerzijds is de aanpak om tot het EPD te komen een schoolvoorbeeld van hoe het niet moet zoals mijn collega's hierboven al betogen. Anderzijds was recentelijk in het nieuws dat er wordt gesproken over uitwisseling van medische gegevens tussen Europa en de US. Ik moet er niet aan denken dat onze medische gegevens terechtkomen bij Uncle Sam. Denk alleen al aan de langdurige weigering van toegang tot de US voor HIV besmette personen. Bovendien staat 'privacy' niet hoog in het vaandel in het land van de onbegrensde mogelijkheden. Het zou dus zomaar kunnen zijn dat die (zeer gevoelige) medische gegevens ineens opduiken bij Amerikaanse verzekeraars..."

# Boekbesprekingen

*Reviewer: Ingeborg Kortekaas* > Ingeborg Kortekaas is Information Security Manager bij Syntrus Achmea Vastgoed en student aan de postdoctorale opleiding Master of Security Science & Management van Delft TopTech, School of Executive Education van de TU Delft. Zij is bereikbaar via i.kortekaas@student.tudelft.nl.

**Identiteitsmanagement – Beheersen van identiteiten**
**Auteur**: R. van der Staaij
**Uitgeverij**: Tutein Nolthenius, 's-Hertogenbosch
**ISBN**: 9072194918, 9789072194916
**Druk**: 1e druk, oktober 2008
**Vorm**: paperback, 240 pagina's

De auteur, Rob van der Staaij, is werkzaam voor Atos Origin. Hij heeft jarenlange ervaring in onderzoek, training en consultancy op het gebied van wet- en regelgeving, risicomanagement, informatiebeveiliging en vooral identiteitsmanagement. Hij heeft diverse grote organisaties begeleid bij de invoering van een identiteitsmanagementomgeving en heeft talloze publicaties over dit onderwerp op zijn naam staan. Als ervaringsdeskundige kent hij de complexiteit van identiteitsbeheer en -beleid en de waarde van de onderbouwing, uitleg en argumentatie die hieraan ten grondslag ligt.

Mede door steeds stringentere wet- en regelgeving zijn organisaties voortdurend bezig met het transparant en controleerbaar inrichten van hun interne processen ofwel het 'in control' zijn. Autorisatiebeheer is een concreet voorbeeld van een proces dat nauw samenhangt met 'in control' zijn en onderdeel uitmaakt van de discipline identiteitsmanagement. Autorisaties moeten immers dusdanig worden ingericht dat te allen tijde duidelijk is wie, wat, wanneer mag doen in de informatiesystemen, en de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie is gewaarborgd. Identiteitsmanagement is een van de belangrijkste instrumenten om dit te realiseren. Hoewel het onderwerp identiteitsmanagement zeer actueel is, is er waarschijnlijk vanwege de snelle ontwikkelingen op dit terrein weinig literatuur voorhanden.
Rob van der Staaij heeft met zijn boek Identiteitsmanagement waarin hij de basisprincipes, voornaamste ontwikkelingen, technieken en services op het gebied van identiteitsmanagement bundelt, geprobeerd om hier verandering in aan te brengen.

Het doel van het boek is een overzicht te geven van identiteitsmanagement en de middelen die daarvoor ter beschikking staan. Het doel omvat in feite twee onderzoeksvragen:

1. Wat is identiteitsmanagement en welke vraagstukken liggen hieraan ten grondslag?
2. Met welke technieken en hulpmiddelen kunnen identiteitgegevens worden beheerd en beschermd?

Om deze vragen te beantwoorden, staat de auteur in de eerste hoofdstukken stil bij wat er wordt verstaan onder identiteit en identiteitsmanagement. Al snel blijkt dat het erg lastig is om deze veelomvattende begrippen te definiëren. Om deze reden kiest de schrijver voor een andere benadering. Hij leidt de betekenis van de begrippen identiteit en identiteitsmanagement af van de context die wordt gevormd door de problemen en vraagstukken die met behulp van identiteitsmanagement moeten worden opgelost. Deze kwesties worden ruwweg gegroepeerd in drie aandachtsgebieden, waarvan de belangrijkste in de onderstaande tabel worden weergegeven:

| Categorie | Problemen en vraagstukken |
|---|---|
| Kostenbesparing en efficiency | Productiviteitsverlies, personalisatie, wachtwoordproblemen, fusies en overnames, delen van diensten |
| Risicomanagement | Ongebruikte accounts, autorisaties niet op orde, wachtwoordproblemen, fraude waaronder identiteitsfraude, internetfraude, computerfraude en andere illegale activiteiten |
| Wet- en regelgeving | Nieuwe wetten en regels, toezicht, gevolgen van niet compliant zijn, inspanningen die samenhangen met in control zijn |

Uiteindelijk komt de auteur, met inachtneming van het nodige voorbehoud, uit op de volgende definitie van identiteitsmanagement:

*Identiteitsmanagement is het op efficiënte, veilige en transparante wijze overzien, beheren en beschermen van identiteits- en toegangsgegevens van personen en andere entiteiten.*

Nadat is vastgesteld wat onder identiteitsmanagement wordt verstaan, komen in het boek de belangrijkste identiteitsmanagementservices en –technieken aan bod, te weten: directory services, provisioning, role-based access control, sterke authenticatie, password-management, single sign-on, web access-management en federated identity. Vanuit het oogpunt van beheer, toegangscontrole en audit wordt er enige ordening in de verschillende services en technieken aangebracht en welke daarmee in verband staande issues kunnen worden aangepakt, hoewel veel services en technieken meerdere gebieden bestrijken.

In navolging op het toelichten van de verschillende identiteitsmanagementservices en –technieken passeert vervolgens een aantal richtlijnen de revue voor het invoeren van identiteitsmanagementoplossingen. Grofweg wordt in het boek een identiteitsmanagementproject opgedeeld in vier fasen: initiële fase; architectuurfase; productselectie; en de realisatiefase. Wanneer je deze projectaanpak vergelijkt met de stappen die worden onderscheiden in het procesmodel van de projectmanagementmethode Prince2 [1], wordt het direct duidelijk dat het om een sterk vereenvoudigde benadering gaat. Identiteitsmanagementtrajecten zijn in de praktijk vaak complex, omdat er meestal meerdere services moeten worden geïmplementeerd. Vooral binnen grote organisaties

nemen zulke projecten enkele jaren in beslag waarbij er bovendien een professioneel en ervaren projectmanagementteam is vereist om het project tot een goed einde te brengen. De informatie moet dan ook worden beschouwd als nuttige achtergrondinformatie bij het implementeren van een identiteitsmanagementoplossing en niet als een model om een identiteitsmanagementoplossing daadwerkelijk te implementeren.
Mijns inziens is de auteur er goed in geslaagd om een overzicht te bieden van de belangrijkste ontwikkelingen en technieken op het terrein van identiteitsmanagement. Hij verwoordt deze complexe materie in begrijpelijke taal en haalt in de grijze kaders die je verspreid in het boek tegenkomt, praktijkvoorbeelden aan die je helpen om de informatie te visualiseren. Verder heeft het boek een prettige lay-out en wordt er een redelijk groot lettertype gebruikt. Hierdoor leest het boek gemakkelijk weg en is het geschikt voor een brede doelgroep. Iedereen die beroepsmatig te maken heeft met identiteitsgegevens en identiteitsmanagement, maar hier niet dagelijks mee bezig is en er niet in is gespecialiseerd, heeft met dit boek een waardevol en handzaam naslagwerk in handen. Het biedt een inleiding in het vakgebied van identiteitsmanagement en schetst een overzicht van de diverse technieken en hulpmiddelen waarmee identiteitsgegevens kunnen worden beheerd en beschermd.

Tot slot een kritische noot ten aanzien van het laatste hoofdstuk van het boek waarin aandacht wordt besteed aan maatregelen die particulieren zelf kunnen toepassen om hun privacy en identiteitsgegevens te beschermen. De informatie in dit hoofdstuk bevat een aantal praktische tips die volgens mij kunnen bijdragen aan het vergroten van het (informatie)beveiligingsbewustzijn van particulieren. Echter, ik ben bang dat deze doelgroep nauwelijks via het verkoopkanaal van het boek zal worden bereikt. Het boek is namelijk grotendeels gericht op het beheersen van identiteiten in organisatie- en bedrijfsomgevingen. Ik vind het dan ook verrassend dat er aan het einde van het boek een hoofdstuk wordt gewijd aan identiteitsmanagement voor particulieren. Het hoofdstuk lijkt een beetje uit de lucht te komen vallen. Daarnaast zullen particulieren het boek naar mijn mening ook niet zo snel bestellen, omdat de meesten zich simpelweg niet realiseren dat het onderwerp identiteitsmanagement ook voor hen relevant is, hoewel dit natuurlijk wel het geval is!

Ingeborg Kortekaas.

*Reviewer: Gerhard Mars CISA* > Gerhard Mars CISA is werkzaam als IT auditor bij Capgemini Outsourcing B.V. waar hij onder andere security en compliancy audits uitvoert. Hij is bereikbaar via gerhard.mars@capgemini.com


**Information Security Management with ITIL V3**
**Auteurs**: Jacques A. Cazemier, Paul Overbeek en Louk Peters
**Uitgeverij**: Van Haren Publishing, Zaltbommel
**ISBN**: 978-90-8753-552-0
**Druk**: 1e druk, januari 2010
**Vorm**: paperback, 132 pagina's

Dit boek is uitgebracht in de serie IT best practices als bijgewerkte versie van de titel in relatie met de voorgaande versie van ITIL.

De auteurs geven aan dat de business- en IT-managers de doelgroep vormen voor dit boek. De doelstelling van het boek is om vanuit een best practice naar informatiebeveiliging en ITIL V3 te kijken en de lezer bruikbare adviezen te geven over de toepassing in de praktijk.

Het boek gaat in op de wijzigingen in ITIL V3 ten opzichte van V2 en de ontwikkelingen op het vakgebied en de veranderingen en trends in de wereld van informatiebeveiliging en het beheer daarvan. Het boek kent vijf hoofdstukken en drie bijlagen.

De auteurs beginnen het boek met een inleiding over informatiebeveiliging als eis voor het beveiligen van gevoelige informatie. Het onderwerp informatiebeveiliging wordt besproken aan de hand van diverse korte statements en waar nodig iets verder uitgewerkt. Voorbeelden hiervan zijn:
De waakhondhouding van de IT-afdeling door regels op te leggen om een veilige IT-infrastructuur te kunnen beheren. Het afdwingen van meer en langere wachtwoorden, beperkingen op toegang tot netwerk en de toepassing van meer firewalls. Hierdoor krijgt de IT-afdeling een slechte reputatie en wordt soms 'business prevention department' genoemd.

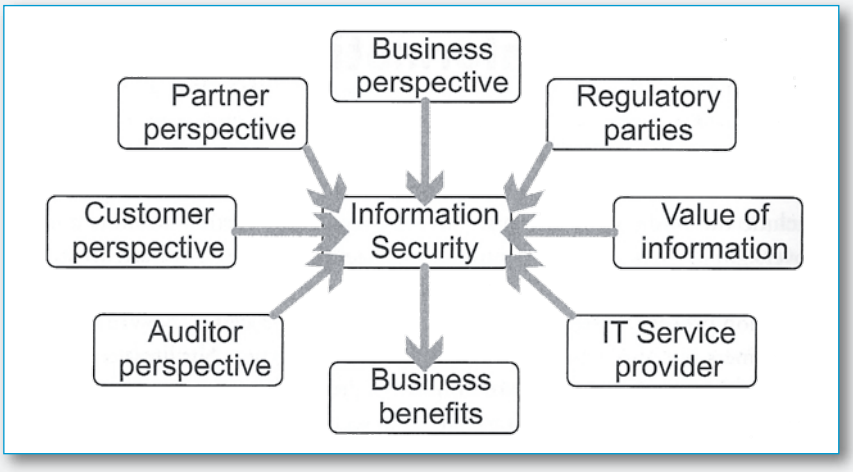
*Informatiebeveiliging is geen proces op zichzelf*

Informatiebeveiliging is geen proces op zichzelf maar heeft relaties met alle andere managementprocessen en is onderdeel van veel activiteiten binnen de organisatie.

Hoofdstuk 2 gaat in op de basisbeginselen van informatiebeveiliging.

Informatiebeveiliging wordt besproken vanuit de verschillende invalshoeken die in onderstaande figuur zijn weergegeven. De besproken invalshoeken zijn:

- de waarde van informatie;
- de business;
- de klant(en);
- de partner;
- auditing en toezicht;
- de IT dienstverlener.




Ten opzichte van de figuur wordt er niet verder ingegaan op de invalshoeken vanuit wetgeving en richtlijnen, en de opbrengsten voor de business. De waarde van informatie wordt zeer beknopt behandeld en de auteurs gaan met grote stappen door de kwaliteitsaspecten heen. Een diepgaande uitleg van vertrouwelijkheid, integriteit en beschikbaarheid en de afleiding hiervan naar privacy, anonimiteit, betrouwbaarheid en controleerbaarheid in de vorm van voorbeelden wordt niet gemaakt.
Dat de waarde van informatie door de business dient te worden aangegeven is niet benoemd. Dit is een gemiste kans om met name de verantwoordelijkheid van de business aan te geven. Zij zijn in principe eigenaar van de informatie en bepalend voor welke (soorten) informatie beveiligd dient te worden. In hoofdstuk 4.3.2. Service asset en configuratiemanagement wordt verder ingegaan op de kwaliteitskenmerken waarmee de informatie geclassificeerd wordt.

De auteurs gaan verder met de beheersmaatregelen voor informatiebeveiliging. Daarmee wordt de verdere uitleg van de invalshoeken verlaten om daarna weer te worden opgepakt. Waarom dit zo gebeurd is mij niet duidelijk omdat de beheersmaatregelen niet verderop in de uitleg worden gebruikt. In de beheersing van informatiebeveiliging wordt uitgegaan van de beschikbaarheid van een security-organisatie. Door budget en mensen beschikbaar te stellen voor de security-organisatie wordt de betrokkenheid van het management zichtbaar. Een mix van processen en technische maatregelen worden benoemd waarbij de balans tussen beide soorten maatregelen met het business-proces belangrijk zijn voor de effectiviteit. Tevens wordt ingegaan op een security-incident; de verschillende fasen van bedreiging tot het oplossen zijn benoemd. De begrippen van preventieve, detecterende repressieve en correctieve maatregelen komen beknopt aan de orde.

Het business-perspectief wordt behandeld op basis van het model van informatiebeveiliging. Hierbij wordt uitgegaan van het informatiebeveiligingsbeleid als input voor risicomanagement. Over het ontstaan van dit beleid wordt niet verder geschreven, terwijl dit de kapstok vormt voor de risicoanalyse en de te nemen beheersmaatregelen. Op het gebruik van risicoanalysetechnieken en -systemen wordt niet verder ingegaan daar dit afhankelijk is van het volwassenheidsniveau van de organisatie op dit gebied. Aansluitend wordt gesteld dat management 'in control' dient te zijn zodat hij of zij kan garanderen dat de continuïteit van de business en het behalen van de business-doelstellingen geborgd is.

Het klantperspectief gaat in op de trends van de afgelopen jaren. De klant wilde zekerheid hebben over de beveiliging van zijn informatie die door een IT-dienstverlener wordt beheerd. Van vertrouwen hebben in de beheerder is de trend over gegaan naar het aantonen dat de beheerder daadwerkelijk 'in control' is. De rol van de SLA en de daarin gemaakte afspraken worden benoemd evenals hoe de dienstverlener kan aantonen dat hij de dienstverlening beheerst uitvoert. Dit laatste kan door gebruik te maken van een managementverklaring, certificering van de dienstverlening op basis van ISO 27001 of gebruik te maken van een externe audit-organisatie voor een groep klanten om een TPM af te geven.

Dienstverleners werken vaker met partners in de levering van de dienstverlening. Het borgen van de informatiebeveiliging door standaardisatie van werkwijze en opslag van data (centraal of decentraal) en communicatie is dan essentieel. Hierbij wordt aangegeven dat een gecertificeerde partner (ISO 27001) een voordeel biedt en kostenbesparend is.

Uitvoerig wordt stilgestaan bij security-architectuur, waarbij de lezer inzicht krijgt in de samenstelling van de informatiearchitectuur. De definitie van de architectuur omvat de ontwerpprincipes voor het informatie object, de relaties en de interactie met de omgeving. Een voorbeeld hiervan is een informatiesysteem bestaande uit hardware, software en de applicatie.

*Elementen van de security-architectuur zijn security-services en de ontwerprichtlijnen*

Elementen van de security-architectuur zijn security-services en de ontwerprichtlijnen. De ontwerprichtlijnen hebben betrekking op de bescherming van gegevens op het niveau van informatie/data, de applicatie, de ondersteunende infrastructuur en de omgeving inclusief de culturele en fysieke aspecten. Security-services heeft ook betrekking op de borging, betrouwbaarheid, toepasbaarheid en de controleerbaarheid van de services. Hierbij moet ook aan de inrichting van de organisatie worden gedacht. Functies, taken, bevoegdheden en

verantwoordelijkheden. Er is een overzicht gegeven van algemene ontwerpprincipes voor de security-services die kunnen worden gebruikt.

Ontwerpprincipes voor beveiligde omgevingen zijn genoemd. Hierin wordt ingegaan op kenmerken die horen bij specifieke security-services. Op zes verschillende services worden de karakteristieken van de service benoemd. Een voorbeeld hiervan is beheer van de security-services.
Kenmerken van deze service zijn onder andere:

- centraal, decentraal, rapportage, logging, bewaking en alarmering;
- rollen en verantwoordelijkheden;
- eigenaarschap, verantwoordelijkheid en delegeren.

De hedendaagse uitdaging ligt in het feit dat delen van de informatie, services en infrastructuur worden beheerd door de business, vertrouwde partijen of zijn uitbesteed aan derde partijen. Contracten met deze partijen bevatten dan elementen om de eisen van de informatiebeveiliging te borgen.

Hoofdstuk 3 gaat in op de basisprincipes van het beheer van informatiebeveiliging. De basis voor het beheer ligt in het gebruik van het algemene managementproces in de vorm van de Demming-cirkel (Plan-Do-Check-Act). Hieraan is control toegevoegd om de toepasbaarheid voor informatiebeveiliging te verbeteren zodat compliancy en auditing zijn ingedekt. De uitleg van de Demming-cirkel en de toepassing op het beheer van informatiebeveiliging is verder uitgewerkt op de vier stappen in het model en de toegevoegde stap van control. Na de uitleg worden de activiteiten in de stap samengevat.

Gerhard Mars.

Het hoofdstuk wordt afgesloten met de management-review van het beheer, waarin de effectiviteit en de efficiëntie van de huidige implementatie en de beheersmaatregelen worden geëvalueerd. Een overzicht wordt gegeven van de input voor de management-review, gevolgd door de mogelijke output van de review in de vorm van besluiten en acties.
Tot slot wordt aandacht besteed aan de rapportage over het beheerproces van informatiebeveiliging. De lezer krijgt een overzicht voorgeschoteld van te rapporteren informatie en gebeurtenissen en in welke fase van de Demming-cirkel deze informatie beschikbaar is.

In hoofdstuk 4 wordt ingegaan op de veranderingen van ITIL V3 en informatiebeveiliging. Voor de lezers die met de vorige versie van ITIL bekend zijn geeft dit hoofdstuk een goed inzicht in de veranderingen in V3. Uitgebreid wordt stilgestaan bij het service lifecyclemodel, de opbouw van de verschillende boeken en daarin voorkomende processen. V2 bevatte elf processen en een functie, V3 bevat vijfentwintig processen en vier functies. Dit is een behoorlijke uitbreiding! Deze vijfentwintig processen zijn nu gepubliceerd in vijf boeken, onderverdeeld in Service Strategie, Service Design, Service Transitie, Service Operation en Continual Improvement. De schrijvers gaan in op de rol, relatie en het effect van informatiebeveiliging op de processen. Bruikbare informatie wordt gegeven om bijvoorbeeld een security-strategie op te zetten waarvoor een aantal vragen zijn opgenomen. Binnen het financiële proces wordt aandacht besteed aan de opbrengsten vanuit security in plaats van de kosten. Het begrip ROSI (Return On Security Investment) wordt geïntroduceerd en hoe je dit kunt berekenen. Binnen het demand-managementproces wordt gesproken over de security baseline en het leveren van een hoger niveau van beveiliging. De rol van security-management in paragraaf Transitie, waarbij de security-manager lid is van het CAB en de beoordeling van de change vanuit security-oogpunt uitvoert. Per proces in de Service Transitie-paragraaf is door de schrijvers duidelijk aangegeven wat de relatie is tussen het proces en de informatiebeveiliging.

In de paragraaf continual service improvement wordt aandacht besteed aan het zeven-stappenmodel en hoe dit model te gebruiken is voor risico- en informatie-beveiliging. Onderdeel van service improvement is het rapporteren over de dienst-verlening op basis van afgesproken KPI's voor security zoals het niveau van de patchlevels, gedetecteerde aanvallen op het netwerk enz.

Service operation is de fase waarin het beheer van informatiebeveiliging verantwoordelijk is voor 'business as usual'. De vier functies in ITIL V3 zijn verantwoordelijk voor het uitvoeren van de operationele taken van informatiebeveiliging zoals het behandelen van gebeurtenissen waardoor informatie niet of beperkt beschikbaar is voor de business, de integriteit of vertrouwelijkheid van de informatie is beschadigd. In deze paragraaf wordt uitgebreid stilgestaan bij security-incidenten en het beheer hiervan. De vier functies in ITIL V3 worden toegelicht, de rol en relatie van service operation en informatiebeveiliging wordt besproken en het hoofdstuk wordt afgesloten met een korte terugblik op V3. V2 was opgezet voor het beheren van IT-infrastructuren, V3 bekijkt het beheer vanuit een service levenscyclusmodel. Waarbij de aansluiting wordt gezocht in het leveren van diensten die aansluiten bij de business-wensen en -behoefte.

*Dit boek is voor de doelgroep van de business- en IT-manager geschreven*

Hoofdstuk 5 gaat over het implementeren van informatiebeveiliging. Het hoofdstuk gaat in op het opzetten en/of verbeteren van informatiebeveiligingsbeheer. Hiervoor wordt het CSI-model gebruikt, wat eerder in hoofdstuk 4 is beschreven en onderdeel uitmaakt van het boek Continue Service Improvement (CSI). De lezer wordt met behulp van de stappen in het CSI-model door de cyclus van het implementeren c.q.

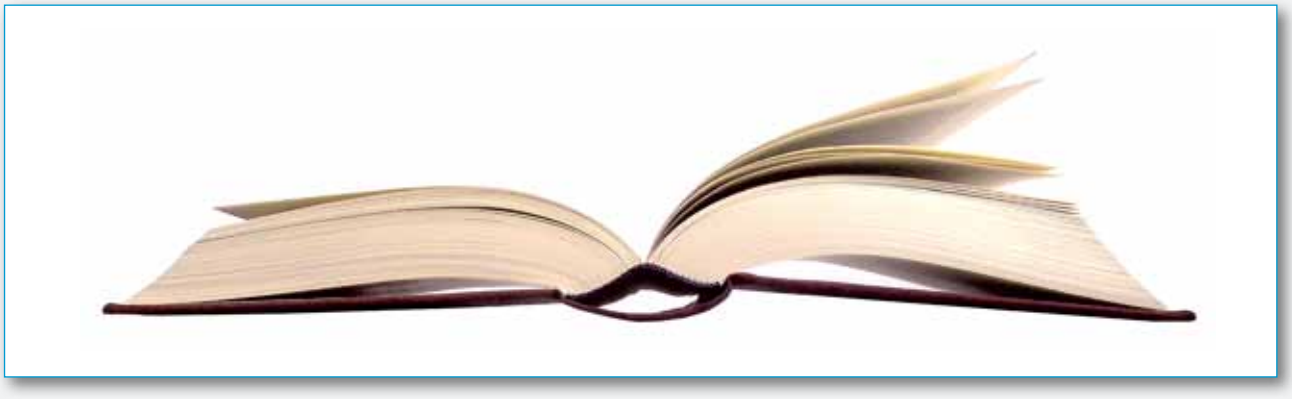
verbeteren van informatiebeveiliging in de organisatie geleid. De afleiding naar het model is mijns inziens niet geslaagd. De stappen en de bijbehorende vraagstelling komen ook in andere verbeteringsmodellen voor en zijn niet specifiek op het CSI-model van toepassing.
Om de aandacht te krijgen en te houden op informatiebeveiliging is het nodig dat bij de medewerkers bewustzijn wordt gecreëerd over dit onderwerp en het toepassen hiervan als onderdeel van ons dagelijkse werk. Een bewustzijnsprogramma voor de implementatie en een continue programma, en de rol van het management hierin, is het onderwerp van de volgende paragraaf.
Communicatie over informatiebeveiliging is een belangrijk middel om de medewerkers te bereiken en de betrokkenheid van het management is noodzakelijk om het niveau te behouden. Een eenmalige campagne is weggegooid geld, een continue programma brengt de boodschap over. Denk hierbij aan de reclames die ons dagelijks bereiken.

Het organiseren van informatiebeveiliging en de benodigde structuur van de informatiebeveiligingsorganisatie is het onderwerp in paragraaf 5.3. Ingegaan wordt op de structuur van de organisatie, de indeling naar strategisch, tactisch business en IT en de operationele kant zowel in de business als IT.
De rollen die hieruit naar voren komen zijn op strategisch, tactisch en operationeel niveau voor beide kanten benoemd en uitgewerkt in voorbeeld profielen, inclusief de plaats in de organisatie. Kort aandacht wordt besteed aan de volwassenheid van informatiebeveiliging en de rollen die passen bij volwassenheidsniveau van de organisatie. Dit is een goede handreiking voor bedrijven die al informatiebeveiliging geïmplementeerd hebben om inzicht te krijgen of hun informatiebeveiligingsorganisatie past bij hun IB-volwassenheidsniveau. In een van de volgende paragrafen in dit hoofdstuk wordt nog uitgebreid stilgestaan bij volwassenheidsniveaus. Vanzelfsprekend wordt er ingegaan op de governance en de IB-organisatie.
Governance wordt besproken en de rol van de lokale en internationale wet- en regelgeving zoals Sarbanes-Oxley (SOx) en de code Tabaksblatt worden aangehaald. Kort wordt ingegaan op het belang van governance en de rol van informatiebeveiliging hierin. Tot slot wordt aangegeven dat met een combinatie van frameworks, governance mogelijk gemaakt wordt. Als voorbeeld wordt ITIL in combinatie met ISO 27001 genoemd.
Het aantonen dat je 'in control' bent kan alleen maar goed gebeuren door te documenteren en te registreren. Hiermee wordt aantoonbaar dat je erover na hebt gedacht (ontwerp) en door de registratie kun je ook aantonen dat je het zo doet. Documenteren vindt plaats op drie niveaus: strategisch, tactisch en operationeel. Met enkele voorbeelden wordt dit gedocumenteerd en een handreiking gegeven in een tabel hoe documenten in het framework worden geplaatst.

Volwassenheidsniveaus in informatiebeveiliging wordt verder uitgewerkt voor security- en risicomanagement. Hierbij wordt uitleg gegeven aan de niveaus en de kenmerken van de niveaus. Ook wordt ingegaan om te groeien naar een hoger niveau en hoe dit tot stand kan komen.
De schrijvers geven in de een na laatste paragraaf van het boek inzicht in de valkuilen en de succesfactoren voor de implementatie van informatiebeveiliging. Deze informatie is op basis van ervaringen vanuit implementaties opgesomd. De benoemde valkuilen zullen voor de meesten van ons nieuw zijn. Dit geldt ook voor de succesfactoren.

De bijlagen gaan in op managementstandaarden, hierin is onder andere een referentietabel opgenomen tussen ITIL V3 en Cobit. De mogelijkheden voor certificatie. Een aparte bijlage bevat een referentietabel tussen ITIL V3 en ISO 27001 en ten slotte zijn een literatuuroverzicht en internetlinks opgenomen voor de lezer. In de tekst van het boek wordt hiernaar verwezen.

**Conclusie**
Dit boek is voor de doelgroep van de business- en IT-manager geschreven, maar voor iedere geïnteresseerde aan te bevelen als meer inzicht in ITIL V3 en informatiebeveiliging wordt gewenst. De inleiding tot informatiebeveiliging komt door de compactheid van het boek niet altijd even helder over en lijkt van de hak op de tak te springen. Dit wordt door de schrijvers ruimschoots goedgemaakt door een heldere en duidelijke uiteenzetting te doen van informatiebeveiligingsbeheer en veranderingen in ITIL V3.
De praktische aanwijzingen voor de lezer om zelf aan de slag te gaan, wat je in deze serie best practice mag verwachten, vallen echter tegen.
De informatie over de implementatie van informatiebeveiliging is bruikbaar als achtergrondkennis maar hierin wordt weinig praktische informatie gegeven over het daadwerkelijk implementeren van informatiebeveiliging. Een meerwaarde was geweest als de implementatie op basis van een (fictieve) praktijksituatie was uitgewerkt.



# De trend van kleine alleskunners

De afgelopen jaren hebben in het teken gestaan van miniaturisering en mobilisering. Het resultaat van deze ontwikkelingen zien we dagelijks in het straatbeeld terug. Mensen die in de supermarkt naar huis bellen om nog maar even zeker te weten welke pindakaas ze moeten meenemen. Twitteren in de wachtkamer van de tandarts (wel nieuwsgierig wat in dat bericht stond), mobiel werken in de trein, mobiel werken in de auto, mobiel werken op de fiets. Zelfs bij het uitlaten van de hond wordt niet geschroomd een e-mailtje te versturen.

Het mobiele verkeer is in twee jaar tijd meer dan verdrievoudigd. T-mobile gaf aan dat het dataverkeer momenteel 200 terabyte per maand is. De verwachting is dat iedere klant in 2015 meer dan 14 gigabyte dataverkeer zal genereren. Ik ga u niet vervelen met een paar cijfers van 25 jaar geleden, maar neem van mij aan dat de maat vol is. Mobiel is helemaal in en de gevolgen daarvan zijn ook duidelijk te zien. De computerfabrikanten rollen over elkaar heen om de mooiste netbook (u weet wel, zo'n laptop van maximaal 10 inch groot) te leveren. Iedere telefoonfabrikant geeft minimaal twee keer per jaar een nog mooiere, snellere en meer geavanceerde gsm uit. TV-kijken op een gsm is al heel normaal (2 inch beeldscherm in vergelijking met het 52 inch beeldscherm bij mij thuis is wel grappig), navigeren, fotograferen, internetten, twitteren, e-mailen, muziek luisteren, video's kijken en niet te vergeten bellen kan ook nog (tenminste als je die functie weet te vinden). De verkoopcijfers van laptops hebben inmiddels de verkopen van de desktop overklast. En de desktop zal wellicht helemaal gaan verdwijnen. De meteropnemer loopt met een PDA rond en ook de installateur doet zijn bestellingen met een PDA. De keukenmonteur heeft een gps in de auto waarmee de planningsafdeling kan kijken of er misschien nog extra klant in de route past en of de geplande route de volgende keer moet worden bijgesteld omdat de monteur te vroeg thuis is. Het aspect privacy laat ik maar even buiten beschouwing omdat de hoofdredacteur mij slechts een pagina tekst toestaat.

Dat juist in deze tijd de uitvinder van de PDA in de etalage staat, is op z'n zachtst gezegd wonderlijk te noemen. Als je vroeger geen Palm had dan hoorde je er niet bij. Als je vandaag een Palm hebt hoor je er ook niet bij maar dan om een hele andere reden.
TomTom en andere verkopers van navigatiesystemen zullen het lastig krijgen nu onder andere Nokia zich ook op de navigatiemarkt heeft gestort. Alleen dan gratis geleverd. Waarom een tweede kastje kopen als je mobieltje hetzelfde kan? De fabrikanten van MP3-spelers zullen het, om dezelfde reden, ook lastig gaan krijgen. Waarom met twee kastjes rondlopen als je het met één kastje afkan? Dat laatste is niet helemaal waar want de MP3-spelers met het Applelogo erop vinden nog gretig aftrek. Zowel de IPod Nano, IPod classic (geen idee wat er classic aan is) en de IPod touch gaan als warme broodjes over de toonbank. De IPod touch is eigenlijk een IPhone zonder telefoniefaciliteiten en goedkoper. De IPhone is een bekend verhaal: verkoopsucces nummer één van Apple en de eigenaar is te herkennen aan het continu spelen met zijn IPhone als hij niet op zoek is naar een stopcontact om zijn bijna lege accu weer nieuwe energie te geven. Om het succes van de IPhone nog meer glans te geven wordt deze telefoon binnenkort multitasking (u leest het goed, de huidige IPhone kan maar een ding tegelijk) en om de aandelen van Apple nog een verdere boost te geven hebben we nu een machine op de markt die vier keer zo groot is als de IPhone en eigenlijk hetzelfde is. Deze IPad is sinds april in Amerika te koop en er zijn zelfs sites die de actuele verkoopaantallen doorgeven: http://labs.chitika.com/ipad/. Het miljoen zal inmiddels gepasseerd zijn. Misschien dat de IPad (en de ongetwijfeld komende imitaties) de laptop uit de markt gaat drukken maar aan voorspellingen durf ik mij niet te wagen.
Houden de fabrikanten een beetje rekening met de beveiliging van de gegevens op hun draagbare apparaten? Nee, dat doen ze niet. Ondanks het feit dat je alle data op het mobieltje kunt zetten is er nauwelijks standaard beveiligingssoftware op de mobieltjes aanwezig. Bestandje X wordt gewoon even op de e-mail gezet, of via Bluetooth even over geblazen. Mobieltje weg, dan zijn je bestandjes ook weg, dat is pech. Mijn vrouw zal mij wel weer een notoire doemdenker vinden maar ja. Ben ik tegen die nieuwe ontwikkelingen? Nee hoor. Op de IPad na heb ik ook alles in huis en doe dus vrolijk mee met deze trend. Heb ik ook alles beveiligd tegen verlies? Dat antwoord moet ik u schuldig blijven omdat mijn tekst op is.

Groeten,
Berry

SOPHOS


# SECURITY SO COMPLETE YOU FEEL INVINCIBLE

WORRY LESS. ACCOMPLISH MORE. WWW.SOPHOS.COM

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

CRYPSYS data security