februari 2010 nummer 1

INFORMATIEBEVEILIGING

Social Engineering: herstel de zwakste schakel

De opbouw van IB-patronen

Nominaties Artikel van het Jaar bekend

De uitdaging van online onderzoek

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

We hebben binnen de vereniging een klein probleem en het resultaat hebt u nu in handen: een dun nummer. En dat vinden we jammer. We hebben een grote en trouwe lezersschare en maar een kleine kring van schrijvers. Er is dus sprake van enige onbalans. Redenen zijn er vast vele. Niet onbelangrijk is de financiële crisis. Veel potentiële auteurs krijgen of hebben gewoonweg geen tijd om hun gedachten op papier te zetten.

De redactie heeft veel lijntjes naar interessante onderwerpen liggen, maar ja, wat er niet is, kun je niet plaatsen.
We zitten er volop achteraan, maar voor zowel schrijvers als redacteuren geldt dat het, naast de eer, vooral een kwestie is van vrijwilligerswerk. Afdwingen is niet haalbaar. Maar we zitten natuurlijk niet bij de pakken neer en we ontwikkelen goede initiatieven om meer bijdragen te krijgen. We gaan de boel meer aanjagen en we hebben ook wel wat over voor goede kopij. Zo zullen we binnenkort weer bekendmaken wat het beste artikel uit 2009 was. De auteur wordt beloond met een leuke beloning. Op pagina 23 treft u de shortlist met artikelen aan. Schroom niet om uw voorkeur aan ons bekend te maken.

We weten dat er veel professionals en aankomende professionals kunnen bijdragen aan het verder professionaliseren van het vakgebied. Als u daartoe behoort, aarzel niet om het ons kenbaar te maken. Artikelen over ontwikkelingen in het vakgebied, cases, uitleg van principes, samenvattingen van scripties et cetera. Wij zouden ze graag willen plaatsen.

En we hebben wat goede ideeën voor dit jaar. Zo gaan we aan de slag met een special over Cloud Security en we neigen naar een update van de privacy special, daar is permanent genoeg over te doen. Ook gaan we verder in op mobile security. Met al die nieuwe smartphones is er genoeg te onderzoeken. We vermoeden dat het ook zinvol kan zijn om een paar artikelen te wijden aan security binnen het onderwijs en dan niet zozeer het lespakket, maar eerder de instellingen. Het lijkt een redelijk onontgonnen gebied. Ook plaatsen we dit jaar een hele serie artikelen over social engineering van Jan de Boer van Capgemini. Hij zal elk nummer een paar interessante voorvallen presenteren.
We hebben nog lang niet alle ideeën voor artikelen ingevuld, dus als u denkt een bijdrage te kunnen leveren, aarzel niet!

Hoe dan ook, we hebben genoeg leuke ideeën en we zetten ons voor de volle honderd procent in dit jaar weer acht interessante nummers te publiceren. Doet u met ons mee?

Veel leesplezier gewenst,

André Koot
Hoofdredacteur

Binnen de redactie nemen we afscheid van Henk Meeuwisse. Door persoonlijke omstandigheden lukt het hem niet meer actief bij te dragen. We willen hem in ieder geval bedanken voor zijn bijdrage.

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
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

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

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

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

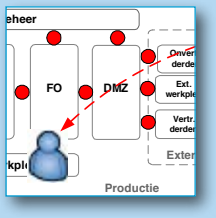
ISSN 1569-1063

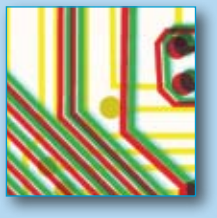
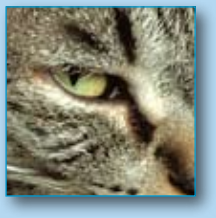
creative commons

PvIB
Platform voor InformatieBeveiliging

Inhoud





Herstel van de zwakste schakel

Auteur: Jan de Boer MSIT > Jan de Boer 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 via jan.de.boer@capgemini.com.

De resultaten van de diverse Social Engineerings Assessments verbaasden me enorm: wachtwoorden van kritische systemen, toegang tot hoog beveiligde locaties, inzage in criminele informatie, zelfs handvuurwapens kreeg ik eenvoudig in handen. In het merendeel van de gevallen was het enige dat ik hoefde te doen: er gewoon om vragen! In een serie van acht artikelen wordt ingegaan op de psychologische trucs die door Social Engineers gebruikt worden om slachtoffers te manipuleren. Waarom en hoe werken ze, hoe zijn ze te herkenen en wat is de beste verdediging?

Verbazing of verwondering

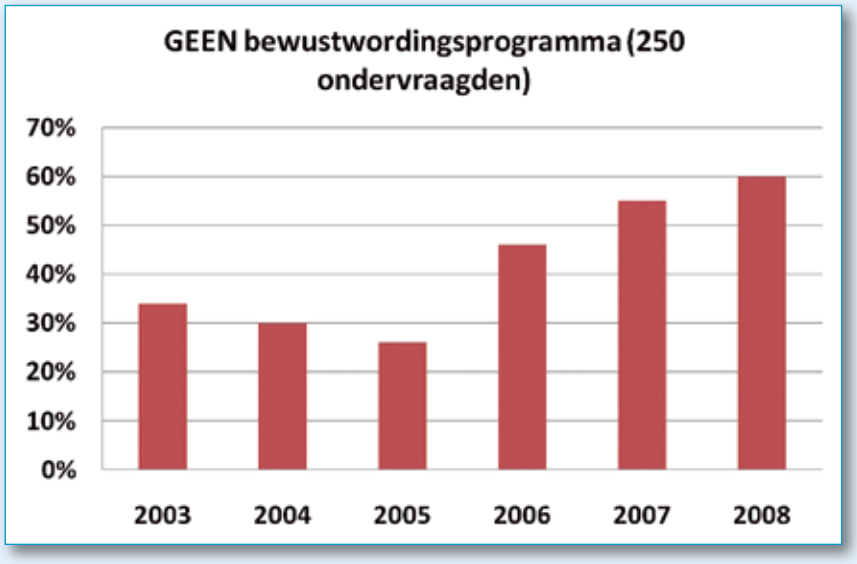
In de informatiebeveiliging wordt de mens steeds omschreven als de zwakste schakel. Ondanks alle inspanning, zoals firewalls, bewakingspersoneel, toegangscontrolesystemen, vercijfering en hoge hekken, kan een mens achter die hekken ertoe overgehaald worden indringers toe te laten tot gebouwen en informatie.

In mijn rol als security consultant heb ik een groot aantal security audits uitgevoerd in de vorm van Social Engineering Assessments, zowel binnen de publieke, als de private sector. Social Engineering (SE) kan omschreven worden als het manipuleren van mensen met het doel toegang te verkrijgen tot vertrouwelijke informatie. Daarbij wordt gebruikgemaakt van list, bedrog en psychologische trucs. De resultaten van deze bijzondere vorm van security audits waren soms schokkend: toegang tot een kluis met opiaten, geheugens van stemcomputers, een nachtkluis met paspoorten en rijbewijzen en procescontrolsystemen voor bruggen, sluizen en gemalen. Het meest extreme resultaat was het in ontvangst mogen nemen van vijf handvuurwapens, simpel met één telefoontje en een goed verhaal.

Ik ben er steeds meer van overtuigd geraakt dat de beveiliging niet in de firewall, de SafeWord tokens en de andere technische beveiligingsmaatregelen zit, maar in de mens zelf. Om deze reden heb ik ervoor gekozen om af te studeren voor de opleiding Master of Security in the Information Technology aan (destijds) EUFORCE van de Technische Universiteit Eindhoven[1] op het onderwerp Social Engineering: herstel van de zwakste schakel.

Tegen de doelbewuste manipulatie van mensen is geen technische maatregel bestand. De enige effectieve maatregel tegen SE is een bewustwordingsprogramma waarin aandacht wordt besteed aan dit onderwerp. Er is echter al een aantal jaren een trend te onderkennen waarbij steeds minder aandacht en geld beschikbaar is voor deze bewustwordingsprogramma's. Capgemini houdt jaarlijks een onderzoek onder tweehonderdvijftig CIO's en CISO's van bedrijven en overheden naar (informatie) beveiliging. Uit dit onderzoek (cijfers van 2008) blijkt dat:

- 16% van de ondervraagden aangeeft dat er informatie gestolen is met behulp van Social Engineering (het betreft 8% van de incidenten, een toenemende trend)
- 23% van de ondervraagden de dreiging die uitgaat van diefstal van informatie door middel van Social Engineering ervaart als reëel (vergelijk: fysieke inbraak 11%, phishing 19%)
- 60% aangeeft GEEN aandacht te schenken aan het beveiligingsbewustzijn van de medewerkers. Dit is opnieuw een verslechtering ten opzichte van het voorgaande jaar en wel met 5% (zie het diagram GEEN bewustwordingsprogramma). Er zijn signalen dat deze neerwaartse spiraal zich in 2009 stabiliseert of mogelijk zelfs verbetert, de cijfers zijn echter nog niet bekend.



1. Huidig: TiasNimbas, the business school of Tilburg University and Eindhoven University of Technologytk: Bewustwordingsprogramma's

Kakao Por & Harrison Keely via sxc.hu

De serie Spy op Discovery Channel

De theoretische beschrijving van social engineering technieken kan onderbouwd worden met de praktische ervaring van acht kandidaten die met de camera werden gevolgd, terwijl zij een (vergelijkbare) opleiding tot spion volgden.
In september en oktober 2005 werd bij Discovery Channel de serie Spy van tien afleveringen uitgezonden waarin acht Engelse kandidaten werden opgeleid en getraind voor het vak van spion. De opleiding werd gegeven door drie voormalige Amerikaanse en Engelse opleiders van de CIA en MI5. De kandidaten werden getraind in het gebruik van technische hulpmiddelen en achtervolgingstactieken, maar voornamelijk in het manipuleren van mensen zodat deze de opdrachten van een kandidaat zouden uitvoeren. Vooral dit laatste is vergelijkbaar met de werkwijze van een SE. Discovery Channel herhaalt regelmatig series. Mocht u in de gelegenheid zijn de serie Spy te volgen dan wordt dat van harte aanbevolen.

De artikelreeks

In een serie van acht afleveringen wordt ingegaan op het hoe en waarom van het menselijk gedrag en hoe daar misbruik van gemaakt kan worden door profiteurs. Met die kennis is het mogelijk te herkennen wanneer iemand je probeert te beïnvloeden, zowel privé als zakelijk. Maar de kennis van de psychologische mechanismen is ook in positieve zin bruikbaar als het gaat om zakelijke contacten of in de privésfeer.

De serie is bedoeld als bijdrage aan een reeds bestaand bewustwordingsprogramma van een organisatie, maar het is ook prima te gebruiken als zelfstandig bewustwordingsprogramma, inzetbaar voor risicogroepen, zoals secretaresses of bewakingspersoneel. De artikelen behandelen de psychologische mechanismen die door SE's gebruikt worden om tegenstanders te manipuleren. Er wordt ingegaan op de achtergrond van de werking ervan en er vindt een verduidelijking plaats aan de hand van voorbeelden uit de praktijk. Deze voorbeelden komen zowel uit de dagelijkse omgang met collega's, als uit de gehouden onderzoeken. Verder worden maatregelen aangedragen om een aanval te herkennen en af te slaan.

Daar waar vroeger gold dat de aanval de beste verdediging is, geldt in het informatietijdperk dat kennis de beste verdediging is: de kennis van je tegenstander zijn de 'wapens' en de aanvalstechnieken. Maar ook kennis van je eigen zwakheden is essentieel om effectieve tegenmaatregelen te kunnen nemen. Het doel van deze serie is dan ook het verhogen van de weerbaarheid tegen een mogelijke SE-aanval.

Ken de 'wapens' van je tegenstander

De wapens die een SE ter beschikking staan, vallen in de categorie list en bedrog, misleiding, overtuigen, manipuleren, et cetera. Kortom; de toepassing van psychologische beïnvloedingswapens om resultaat te bereiken. Een aantal van deze wapens is zelfs zo sterk dat het 'slachtoffer' met een tevreden gevoel wordt achtergelaten, terwijl hij zojuist van zijn informatie is be-

Praktijkvoorbeeld 1

Ik stond om 06.50 uur voor het nog gesloten gebouw van de gemeente. Een vroege ambtenaar opende het gebouw en liet me vriendelijk binnen zonder iets te vragen. Ik had de hele dag de tijd om op de tien etages rond te neuzen en mijn voorbereidingen te treffen voor die avond. Als ik werd aangesproken, vertelde ik dat ik ARBO-coördinator was van de betreffende gemeente. Ik had allerlei ARBO-artikelen bij me om mijn rol te bevestigen. Tegen lunchtijd maakte ik buiten een praatje met de portier over zijn nare gewoonte; hij wilde stoppen met roken, maar dat lukte hem niet. Blijkbaar had ik een gevoelige snaar geraakt, want hij begon honderduit te vertellen. Toen ik merkte dat we een band hadden opgebouwd, vroeg ik hem naar de procedure van het afsluiten van het gebouw, omdat mijn laatste vergadering vermoedelijk pas 's avonds na 19.00 uur afgelopen zou zijn. Hij gaf me informatie over de sleutels, de lichtschakelaars, het telefoonnummer van de meldkamer en de procedure om de sluitronde aan te vragen. Die middag heb ik me verborgen in een ongebruikte vergaderkamer. Toen ik om 18.00 uur uit mijn schuilplaats kwam, was het gebouw leeg en kon ik in alle rust kantoren, bureaus, kasten en ladenblokken doorzoeken zonder gestoord te worden. Het resultaat was overweldigend.
Om 21.00 uur heb ik het lege kantoorpand verlaten en de sluitprocedure in werking gesteld om er voor te zorgen dat de veiligheid en vertrouwelijkheid van alle gemeentelijke gegevens gewaarborgd zou zijn.

roofd. De serie gaat in op deze psychologische beïnvloedingswapens en legt uit hoe mensen tijdens hun opvoeding, hun werk en hun verdere ontwikkeling leren omgaan met macht, gezag en autoriteit. Door kennis te hebben van deze wapens en de situaties waarin zij ingezet kunnen worden, ben je in staat het gebruik ervan te herkennen en tegenmaatregelen te nemen.

Bepaal de tegenmaatregelen

Bij het bepalen van de tegenmaatregelen is het van belang te herkennen welk type wapen wordt ingezet. Het heeft bijvoorbeeld geen zin om een kogelvrij vest aan te trekken als je bestookt wordt met traangas. In alle gevallen zal een slachtoffer alle mogelijke tegenmaatregelen moeten kennen en in staat moeten zijn ze in te zetten. Dat vereist kennis van de wapens en de tegenmaatregelen. Daarbij zullen zowel de preventieve maatregelen worden besproken, als de tegenmaatregelen die genomen kunnen worden om een aanval af te slaan. De belangrijkste algemene tegenmaatregel daarbij is het creëren van bewustzijn.

Oefen de tegenmaatregelen

Tegenmaatregelen zullen geen effect hebben als er niet geoefend wordt. Naast 'opzet en bestaan' van een serie tegenmaatregelen zal ook aandacht besteed moeten worden aan het aspect 'werking', door middel van praktische training of bewustwordingstrajecten.
Een waarschuwing bij een bewustwordingsprogramma op het gebied van SE is hier op zijn plaats. Uit onderzoek[2] is gebleken dat degenen die instructie hebben gehad om misleiding en onechte autoriteit te weerstaan, ervan overtuigd zijn dat zij iedere misleiding kunnen weerstaan. Zij zien zichzelf als 'onoverwinnelijk'. Pas na een tweede test werd de werkelijkheid (pijnlijk) duidelijk. Het is dus noodzakelijk om na de instructie een hernieuwde test of audit uit te voeren. Deze laat de personen die de training hebben gevolgd, inzien dat ook zij niet honderd procent bestand zijn tegen misleiding.

Psychologische aspecten, een korte inleiding

Waarom en hoe kan het menselijke gedrag zo sterk beïnvloed worden, dat een verzoek van een vreemde om vertrouwelijke informatie te verstrekken, wordt ingewilligd.
De serie van artikelen vormen een korte studie naar de psyche van de mens, de invloed die de opvoeding tijdens de jeugd heeft op ons gevoel voor gezag en autoriteit, de denk- en redenatiepatronen waarop besluitvorming op latere leeftijd is gebaseerd en de wijze waarop en de mechanismen waarmee deze aspecten beïnvloed kunnen worden.

Praktijkvoorbeeld 2

Bij een organisatie was de informatie in het onroerendgoedarchief over de plaatselijke horeca uiterst vertrouwelijk, het bevatte veel gegevens over criminele achtergronden van de eigenaren die kamers per uur verhuurden. De opdrachtgever gaf mij ondermeer de opdracht om te onderzoeken of het voor een buitenstaander mogelijk zou zijn onrechtmatig toegang tot dat beveiligde archief te krijgen.
Toen een medewerker tegen het einde van de dag naar buiten stapte, liep ik door de nog openstaande deur naar binnen zonder dat ik werd tegengehouden. Bij een secretaresse gaf ik aan dat ik de afdeling kwam controleren op de bestrijding van muizen (er hingen overal posters met de tekst 'Ruim je eten op in verband met de muizenplaag'). In korte tijd was iedereen bekend met het doel van mijn aanwezigheid en werd ik zelfs alleen achtergelaten toen de laatste medewerker vertrok. De beveiligingsbeambte die de sluitronde deed, geloofde mijn verhaal eveneens.
Mijn zoektocht naar de sleutels van het archief leverde niets op, alles was keurig afgesloten. Ik belde de volgende dag als de sleutelsmid van facilitaire zaken naar de afdeling. Ik begreep zogenaamd niet waarom er maar één extra sleutel van de betreffende archiefkast bijgemaakt hoefde te worden, want er waren maar twee sleutels verstrekt.
Ik wilde met alle plezier een paar extra sleutels laten bijmaken voor alle medewerkers. Daar was de betreffende medewerker erg blij mee. Toen ik vroeg hoe ze allemaal met dezelfde sleutel werkten, werd me verteld dat die in het pennenbakje in het ladeblok van Piet lag. De volgende dag ben ik op dezelfde wijze binnengeslopen, heb de sleutel uit de (open) bureaulade van Piet genomen en heb ik foto's van de vertrouwelijke dossiers gemaakt.

2. Brad Sagarin et al., Journal of Personality and Social Psychology. Dispelling the Illusion of Invulnerability: The Motivations and Mechamisms of Resistance to Persuasion, American Psychology Association Inc. 2002. Pages 526 – 541.

Praktijkvoorbeeld 3
Bij een organisatie moest onderzocht worden of het voor een buitenstaander mogelijk was om ongeautoriseerd toegang te krijgen tot gebouwen en vertrouwelijke informatie in dossiers, computers en netwerken. Met een zekere mate van spanning en een vrijwaringbewijs op zak, ben ik gestart met het inwinnen van telefonische informatie en heb ik vervolgens geprobeerd om toegang te krijgen tot de gebouwen. Ongeveer twintig minuten nadat ik ongeautoriseerd het gebouw was binnengegaan (de portier deed gewoon de deur open), kreeg ik van een vriendelijke secretaresse tijdelijk de beschikking over het kantoor van haar afwezige afdelingshoofd en logde ze onder haar naam in op het bedrijfsnetwerk om mij toegang te geven tot internet (en dus de bestanden en de mail, zowel die van haar, als van het afdelingshoofd!).

Er wordt een antwoord gezocht op de vraag hoe het mechanisme van de verleiding werkt en waarom mensen gevoelig zijn voor misleiding. Het antwoord is even simpel als complex:
"Mensen zijn menselijk en werken niet als een automaat. Maar soms handelen ze automatisch op bepaalde prikkels en dat maakt de zaak gecompliceerd."

Psychologische kortsluitingen
Gedragspatronen worden vaak gekenmerkt door een patroon dat steeds in dezelfde volgorde en op een identieke manier wordt doorlopen. Indien het patroon wordt opgeroepen, worden de handelingen op de gebruikelijke, identieke wijze uitgevoerd; een soort voorgeprogrammeerde 'kortsluiting'.

Psychologen hebben een hoeveelheid van deze voorgeprogrammeerde patronen, die we gebruiken wanneer we een mening vormen, onderzocht. De mens is zich meestal niet bewust van de automatische gedragspatronen waarover hij beschikt. Daardoor zijn we een gemakkelijke prooi voor mensen die wél weten hoe ze in elkaar steken; mensen kunnen daardoor gemakkelijk beïnvloed worden. Het geheim hiervan zit in de manier waarop iets aan ons wordt gevraagd en de manier waarop de beïnvloedingswapens gebruikt worden.

De meest belangrijke psychologische kortsluitingen die in de volgende artikelreeks behandeld zullen worden zijn:
- **Wederkerigheid**: de drang om te moeten compenseren wat andere mensen ons hebben gegeven. Door het gevoel te hebben iemand anders iets verschuldigd te zijn, wordt gemakkelijker aan een wederverzoek voldaan dan normaal.
- **Onmiddellijke invloed**: we gebruiken maar een klein gedeelte van alle beschikbare informatie om tot een besluit te komen. Bij besluitvorming onder druk vertrouwen we vaak op slechts één specifiek element van de beschikbare informatie.
- **Consistentie**: de drang om in overeenstemming te handelen met dat wat daarvoor is gedaan. Als we een mening verkondigen of een keuze maken, zijn we ook geneigd om in overeenstemming te handelen met voorafgaande soortgelijke keuzes.
- **Sociale bewijskracht**: ons oordeel over correct of incorrect gedrag hangt samen met het gedrag van anderen. Wanneer veel mensen een handeling op gelijke wijze uitvoeren, bestempelen we deze als correct.
- **Sympathie**: het niet voldoen aan een dringend verzoek is onvriendelijk. Als er druk wordt uitgeoefend door een herkenbare, moeilijke situatie te schetsen of door het noemen van de naam van een wederzijdse goede vriend, kan een verzoek al niet meer geweigerd worden.
- **Autoriteit**: vanaf de geboorte wordt ons bijgebracht dat gehoorzaamheid aan goede autoriteiten juist is. Doordat zij zoveel macht hebben, lijkt het vaak wijs om deze autoriteiten te gehoorzamen.
- **Schaarste**: sommige dingen gaan we meer waarderen naarmate er minder van beschikbaar is.

Profiteurs weten mensen te manipuleren door misbruik te maken van de hierboven beschreven kortsluitingen, zonder dat deze mensen hen ook maar één moment verdenken. De mens is van nature in zekere mate volgzaam en ziet het niet als een vorm van manipulatie.

SE-dreiging is actueel
Enkele jaren geleden is onder de secretaresses van Capgemini een enquête gehouden over SE. Hieruit bleek dat 82 procent van de secretaresses door onbekenden telefonisch om vertrouwelijke informatie was gevraagd. De beller gaf zich meestal uit voor een accountmanager of een consultant van een andere sector die bij een klant zat, of iemand die in opdracht van het hoofdkantoor in Parijs handelde.

Samenvatting
Mensen zijn zich doorgaans niet bewust van de manier waarop zij zich een mening vormen of reageren op een verzoek. Profiteurs kunnen daarvan misbruik maken. Door hieraan aandacht te besteden in een bewustwordingsprogramma, gericht op Social Engineering, kan de weerbaarheid tegen manipulatie vergroot worden. In de komende artikelen zal nader worden ingegaan op een aantal van deze psychologische trucs.

ISF 2009: de 20e verjaardag van de ISF-conferentie

Auteurs: Aart Jochem en Ella Broos > Aart Jochem is lid van de redactie van Informatiebeveiliging en werkzaam bij GOVCERT.NL. Hij is bereikbaar via aart.jochem@govcert.nl. Ella Broos is zelfstandig adviseur crisiscommunicatie en interim manager en bereikbaar via info@brooscommunicatie.nl

Het is een beetje zuur als je een jubileum wilt vieren in een jaar dat de buikriem aangetrokken moet worden. Je vrienden, die al twintig jaar gefêteerd zijn op mooie conferenties, komen vol verwachting naar Vancouver om het feestje te vieren. Wat doe je? Zorgen dat het inhoudelijk in orde is.

Dat is wat het Information Security Forum te doen stond. Een gebalanceerd programma met toonaangevende sprekers, thought leaders en visionairs. Dat is grotendeels gelukt. Er stonden enkele grote namen op het podium, zoals Scott Charney en Bruce Schneier. En natuurlijk Howard Schmidt, de president en CEO van ISF, die enkele weken na de conferentie door president Obama werd benoemd als Amerika's nieuwe cyber security coördinator. Wel had de locatie een regionaal accent: de sprekers kwamen vooral uit Noord-Amerika.

De toekomst van informatiebeveiliging

De eerste plenaire spreker, Esther Dyson, opende de conferentie met een toekomstscenario: Report to the board in november 2019. Portee van het scenario is dat verzekeringsmaatschappijen zich gaandeweg meer gaan richten op het voorkomen van risico's, dan op het verdelen ervan. Verzekeringen spelen een rol in de beveiliging van producten en in het opstellen van normen. Uiteindelijk is in 2019 alles een financiële kwestie geworden. De verzekeringspremie is betaalbaar als je goedgekeurde producten gebruikt en conform de opgestelde normen je informatievoorziening inricht. Er is hoop: het internet is in 2019 een stuk veiliger geworden. Maar criminelen zijn er nog steeds en de cyberdreigingen bestaan vooral uit terreur. Dyson eindigt met een besluit voor het bestuur van ISF in 2019: samengaan met het Internationaal Insurance Forum (the new leaders), samengaan met een groep epidemiologen, of zelf doorgaan en je concentreren op cyberterreur en de bestrijding van internationale cybercrime organisaties.

Oefening

Dit jaar heeft ISF een oefening voorbereid, gericht op de respons op cyberdreigingen. Alle deelnemers aan het congres zijn ingedeeld in groepen van ongeveer acht personen. De groepen vormen het management van het IT-department van een internationale organisatie. Na het lezen van de algemene bedrijfsinformatie druppelen de berichten van nieuwsbulletins en e-mails binnen: de website van de organisatie is geschonden door een groep die zich voordoet als antiglobalisten. In rondes van dertig minuten kwam er steeds meer informatie binnen en ontstond het beeld van een brede aanval met malware en dDoS-aanvallen, keyloggers, et cetera. Een aantal van de incidenten die gerapporteerd werden, stonden los van de aanvalslijn en konden flink verstoren. Belangrijk was hoe te communiceren met de pers en de directie. In verschillende groepen werd toch snel gefocust op techniek en technische maatregelen. De oefening was leerzaam om te doen en het was interessant om met een nieuwe groep snel te moeten schakelen om tot resultaten te komen.

Anonimiteit van bits

Dit jaar was het plenaire podium vooral die van de discussies. De Europese vertegenwoordiger was Alexander Seger van de Europese Commissie en Bernhard Otupal van Interpol. Daarnaast waren Schmidt, Bruce Schneier en Mary Ann Davidson van Oracle van de partij. Seger, die naast cybercrime nu ook privacy en de informatiemaatschappij in zijn portefeuille heeft, vertelt dat privacy, nu en in de komende tijd, steeds meer verankerd zal worden in de Europese regelgeving. Organisaties die twijfelen om een data breach te rapporteren, moeten zich realiseren dat de reputatieschade van het niet rapporteren groter kan zijn dan de reputatieschade na rapporteren. Hij voorziet ook een actieve inzet om aanvallen op internet te traceren en de daders te straffen. Hij lokt hiermee een levendige discussie uit met Schneier, die beargumenteert dat anonimiteit een fundamenteel kenmerk van datacommunicatie is. Bits zijn immers anoniem. Daarom kun je op ieder niet-anoniem netwerk anonimiteit bouwen en zal het traceren van daders uiteindelijk op niets uitlopen. Ik voorzie hier het onderwerp van een nieuw essay van zijn hand.

Jericho en consumerization

Iedere, zichzelf respecterende, grote organisatie is tegen de grenzen van centrale beveiliging en aan gebruikers opgelegde beveiliging aangelopen en denkt na over de toepassing van de principes van Jericho en consumerization. Natuurlijk was ook dit een onderwerp op deze conferentie. We moeten echter de conclusie trekken dat in de praktijk nog een aantal hobbels te slechten zijn. Zo is er nog een probleem rond licenties van software: als medewerkers hun eigen laptops gebruiken, wie betaalt de specifieke licenties en hoe zit het juridisch en met support? Ook is duidelijk dat beveiliging zich vooral richt op preventie van incidenten. Incident respons in de heterogene omgeving die is ontstaan door de vrije keuze van platforms door medewerkers, is een silicon hell.

Op het podium naast de gastheer: Howard Schmidt, Bernhard Otupal en Alexander Seger

Beveiliging is geen optie

Tijdens het ontbijt serveert Bruce Schneier zijn visie op de ontwikkeling van de informatiebeveiligingsector. Tijdens zijn bezoek aan het GOVCERT-symposium in Rotterdam afgelopen jaar sprak hij over hetzelfde onderwerp en het is hoopgevend om te horen dat Schneier verwacht dat beveiligingsmaatregelen geen optie meer zijn, maar worden geïntegreerd in de standaardfuncties van systemen. Hij laat dit zien aan de hand van gedragsvoorbeelden van consumenten. Hij trekt een parallel met de auto-industrie: het is onacceptabel dat als je een nieuwe auto hebt gekocht de dealer je adviseert om zo snel mogelijk remmen te kopen bij een winkel verderop.

Everybody loves the cloud

Hoewel cloud computing zoals we dat kennen al enkele jaren praktijk is, begint het beveiligingsdenken pas langzaam vorm te krijgen. Het Amerikaanse standaardisatiebureau NIST is bezig hiervoor een standaardwerk te maken. Tim Grance licht een tipje van de sluier op. Hij stelt dat cloud computing, in essentie het delen van resources, fundamenteel in strijd is met het garanderen van beveiliging. Er zijn drie servicemodellen: Software as a Service, Platform as a Service en Infrastructure as a Service. Wat nog mist volgens Grance is Hype as a Service en Apologies as a Service. De belangrijkste probleemgebieden rond het beveiligen van cloud computing zijn: vertrouwen, multitenancy, encryptie en compliance. Ieder van deze aspecten zal ongetwijfeld binnenkort in dit vakblad voorbijkomen.

Thrustworthy computing

Het is verbazingwekkend hoe gemakkelijk Amerikanen spreken in het openbaar. Dat geldt zeker ook voor Scott Charney van Microsoft. Met een flair alsof hij zijn vrienden en familie toespreekt, legt hij ons nog eens uit dat om betrouwbaar informatie te verwerken, ieder aspect van de computer onder de loep moet worden genomen. Microsoft, king of desktop, heeft dit met de cliëntcomputer gedaan en is enkele jaren geleden al met het trustworthy computing concept gekomen. Het begint met veilig ontwerpen, bouwen en beheren van systemen en software. Hierop bouw je vertrouwde hardware, vertrouwde software, vertrouwde gegevens en vertrouwde gebruikers. Vervolgens wordt als één van de belangrijkste elementen het identity metasysteem gebouwd. Het gaat wat ver om hier de details te beschrijven, gelukkig heeft Microsoft deze goed gedocumenteerd en online.

De aanpak van de wereldwijde cyberdreiging

Shawn Henry van de FBI gaat in op de ontwikkeling van dreiging van cybercrime en aanvallen. Hij ziet een kloof tussen digital immigrants en digital natives in de mate van besef van risico voor veiligheid en privacy. De digital immigrants, die vanuit een ander perspectief internet gebruiken, zijn voorzichtiger dan de digital natives, die al hun hele leven deelnemen aan fora en chats. Ook ziet Henry drie groepen kwaadwillenden en voor de aanpak van een onderzoek is het belangrijk om zo snel mogelijk door te hebben met welke groep je te maken hebt: individuen en groepen van hackers, terroristische organisaties en de vooroplopende en ontwikkelende cyberstaten. Deze laatsten gebruiken hackertechnieken om de eigen ontwikkelende industrie te helpen.
Henry schat de schade op vele miljarden op jaarbasis. De sleutel tot de aanpak van cybercrime ligt in het grenzeloos samenwerken van opsporingsdiensten.

De ontwikkeling van ISF

ISF is in 1989 opgericht als European Security Forum en kreeg al snel een bredere basis. Hoewel de organisatie het afgelopen jaar door zwaar weer moest, is de financiële basis nog steeds gezond en is de organisatie professioneler en slagvaardiger geworden. Belangrijk is dat ISF actief de samenwerking zoekt met ISACA en de Japanese Network Security Association, om de basis voor de producten en raamwerken te versterken. Ook worden nu licentieovereenkomsten met organisaties afgesloten om praktisch aan de slag te gaan met de producten van ISF. Nogal een belangrijke verandering voor een organisatie die voorheen tamelijk gesloten was.

Volgend jaar weer? Als het even kan wel. ISF blijft een richtinggevende conferentie met voldoende feedback van professionals onderling. En het is volgend jaar weer in Europa.

PvIB activiteiten eerste helft 2010

Datum	Activiteit	Soort evenement
16-03-2010	Trends: virtualisatie en beveiliging	PvIB evenement
24-03-2010	IBO	PvIB/IBO evenement
15-04-2010	Masterclass: Wet Bescherming Persoonsgegevens (WBP)	PvIB evenement
20-04-2010	PvIB ALV	PvIB evenement
20-04-2010	BCM nog eens onder de loep Uitreiking Award Beste artikel van 2009	PvIB evenement
20-05-2010	Privacy in perspectief	PvIB evenement
02-06-2010	IBO - Esmeralda lezing	PvIB evenement
17-06-2010	Innovatieve bijeenkomst: softskills	PvIB evenement

Een bijzondere 'activiteit' is dat er in april een aparte special over Informatiebeveiliging verschijnt in het ondernemers-magazine ZAKELIJK dat in drie edities in Brabant verschijnt. Daarbij zal onder meer gebruikgemaakt worden van de kennis en de input van de redactie van InformatieBeveiliging. Er zal een relevante serie artikelen en een toelichting worden geplaatst.

Opbouw van IB-patronen

Auteur: Jaap van der Veen > Jaap van der Veen is strategisch architect Informatiebeveiliging bij het Ministerie van Financiën. Als auteur en lid van de expertgroep werkt Jaap mee aan het nieuwe NORA katern Informatiebeveiliging en hij is tevens trekker van de PvIB-community voor IB-patronen. Jaap is te bereiken via jaap.vanderveen@gmail.com.

Dit artikel behandelt het onderwerp Patronen voor Informatiebeveiliging en geeft een voorbeeld hoe een patroon is opgebouwd. Het is een vervolg op een eerder verschenen artikel in dit blad van maart 2009, Securitycafé geslaagd, en een artikel in het vorige nummer (8 van 2009), waarin de architectuuraanpak voor de patronen en een zoneringsmodel is besproken. In een volgend artikel later dit jaar behandelt Kees Terlouw een praktijkvoorbeeld van een patroon voor logging.

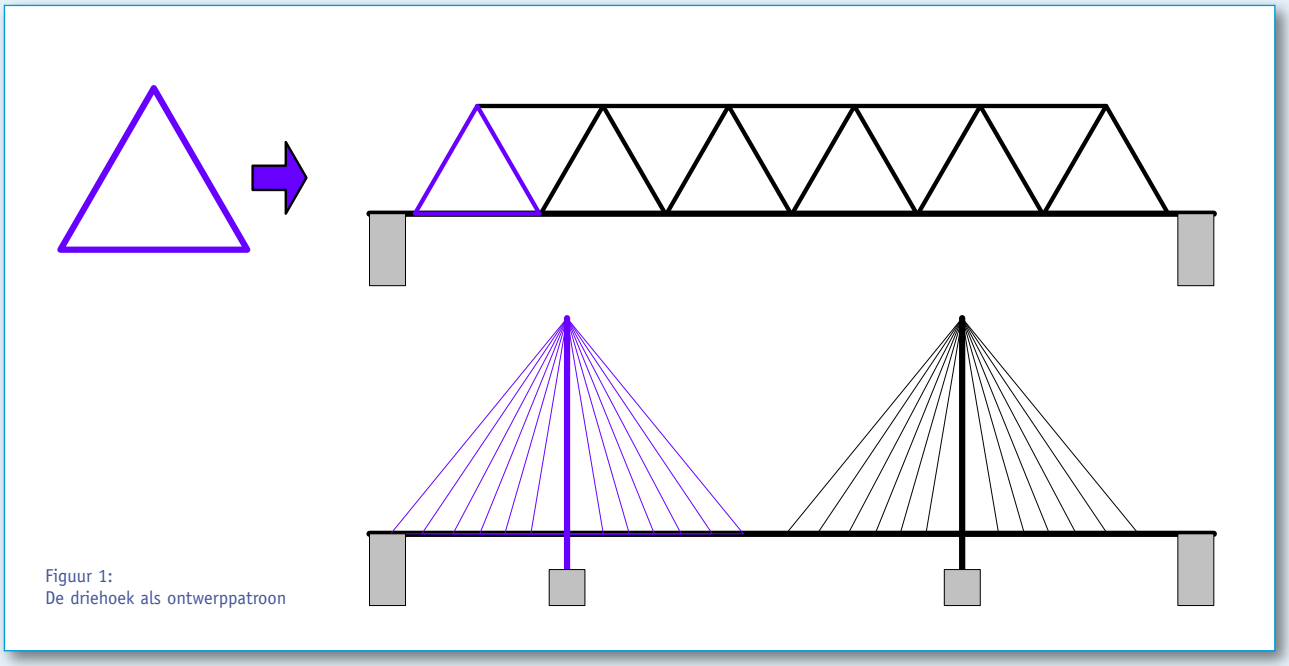
De patronencommunity van PvIB hoopt een bijdrage te leveren aan de communicatie tussen securityarchitecten en andere architecten bij het concretiseren van beveiligingsoplossingen in de ICT. Een patroon geeft daarbij snel inzicht in de oplossingsrichting die we als IB-ers kunnen hanteren.

Wat is een patroon?

De eerste vraag is: wat verstaan we precies onder een patroon? De Open Group hanteert daarvoor de volgende definitie: "Een patroon is een abstractie van een probleem en de oplossing binnen een bepaalde context, waardoor de oplossing algemener inzetbaar wordt". Een bekend auteur van patronen is Erich Gamma *(literatuurverwijzing 1)*, hij hanteert de definitie "A pattern is a three-way relation between a certain context, and a certain configuration which allows these to resolve themselves". Een PvIB-vakgenoot, Aaldert Hofman, schreef *(literatuurverwijzing 2)*: "Een patroon is een relatie tussen een bepaalde context, een bepaald krachtenspel en een bepaalde configuratie die hiervoor een oplossing biedt". De Securitypatterns.org website *(literatuurverwijzing 8)* definieert tenslotte: "Een patroon is een generieke, herbruikbare oplossing voor algemeen voorkomende problemen bij het maken en onderhouden van veilige IT-systemen". In deze definities spelen de begrippen probleem, oplossing en context een centrale rol.

Eerste patronen

Het fenomeen patronen is voor het eerst beschreven door bouwkundig architect Christopher Alexander. Hij ontdekte dat er in bouwontwerpen bepaalde constructies voorkwamen die door hun gunstige eigenschappen steeds opnieuw gebruikt konden worden. Deze herbruikbare constructies noemde hij ontwerppatronen. De snelheid waarmee gebouwd kon worden, bleek sterk afhankelijk te zijn van de toepassingsmogelijkheid van de herbruikbare of prefab componenten en de documentatie die daarover is vastgelegd. Alexander publiceerde zijn ideeën over patronen voor het eerst in *The Oregon Experiment*, uit 1975, waarna hij nog een aantal publicaties uitbracht, waaronder zijn boek *The Timeless Way of Building*, uit 1979.



Figuur 1:
De driehoek als ontwerppatroon

Een mooi voorbeeld van een ontwerppatroon is een driehoek. De driehoek wordt door zijn unieke eigenschappen veel toegepast als 'bouwsteen' in bouwkundige constructies. De driehoeksconstructie is een voorbeeld van een ontwerppatroon voor constructies van bruggen zoals te zien is in Figuur 1. Door gebruik te maken van driehoeken in plaats van massieve- of rechthoekige vormen, kan met relatief lichte onderdelen een zeer sterke constructie gemaakt worden.

Worden patronen in de IT toegepast?

Er is inmiddels veel gezegd en geschreven over patronen sinds het boek van Alexander uitkwam, echter; in de informatietechnologie blijft het gebruik van patronen tot dusver beperkt tot het domein van softwareontwikkeling. Voor het aspectgebied informatiebeveiliging is van actief gebruik nog nauwelijks sprake. De redenen hiervoor zijn niet helemaal duidelijk. Een kritische succesfactor voor IB-patronen zou wel eens de praktijkgerichtheid kunnen zijn en de mate waarin ze echt als bouwsteen of 'praatplaat' kunnen dienen voor het gesprek tussen beveiliger en ontwerper of architect. Patronen zijn bedoeld voor ICT-architecten en -ontwerpers, IB-specialisten en IT-auditors. Een uitdaging voor auteurs van IB-patronen is dat men zich beperkt tot de *belangrijkste* problemen uit het vakgebied. Met dit doel in het achterhoofd zou je met een beperkte set van patronen moeten kunnen volstaan. Wat, gelet op het nog beperkte gebruik door de doelgroep, blijkbaar niet aanslaat, zijn dikke boeken en omvangrijke repositories op een hoog abstractieniveau. Daarbij komt nog dat de verbinding tussen architectuur (patronen) en de geldende normen niet altijd even duidelijk is.

Patronen als oplossing

In een artikel van Aaldert Hofman wordt *Time to Market* als belangrijkste drijfveer genoemd voor de toepassing van patronen. De visie is dat e-business en e-overheid bedrijven en overheden dwingt om veel sneller dan voorheen met nieuwe producten en diensten te komen, wat alleen lukt op basis van bestaande e-business oplossingen. Een voorwaarde is wel dat de beschikbare oplossingen voldoende flexibel zijn om ze snel aan te kunnen passen aan nieuwe behoeften van de klant. Omdat deze flexibiliteit vaak ontbreekt in de bestaande applicaties en infrastructuurontwikkelmethoden, zullen we de praktijk een handje moeten helpen met het methodisch toepassen van patronen in ontwerp- en realisatieprojecten.

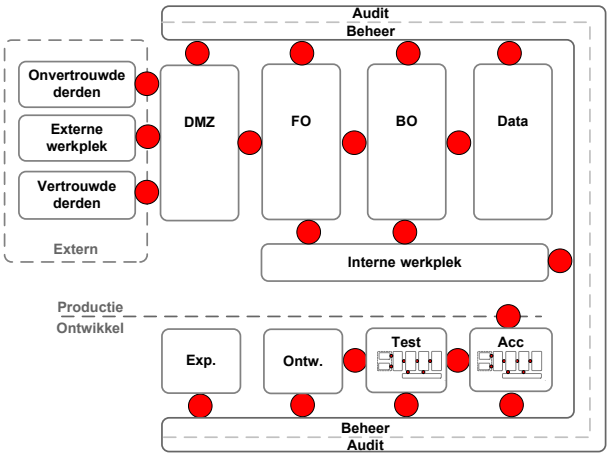
Een andere drijfveer voor de toepassing van patronen is reductie van *complexiteit* en *kosten*. Wat we daarmee bedoelen, is de kans die het werken met patronen ons biedt om onnodige diversiteit in de gekozen oplossingen te beperken. Diversiteit gaat altijd gepaard met complexiteit van applicaties en infrastructuur en met een (sterke) toename van beheerinspanningen en exploitatiekosten. Het streven moet zijn: 'eenvoud-enkelvoud'. Patronen kunnen daarbij een brug slaan tussen architecten, ontwerpers, bouwers en beveiligers en helpen bij het denken in standaardoplossingen.

De Open Security Architecture *(literatuurverwijzing 7)* spreekt van Visual Patterns, de kern van de OSA. Daarin worden beveiligingseisen en functionele eisen van usecases samengebracht. De patronen vormen de basisbouwblokken voor een specifiek IT-toepassingsgebied.

Patronen volgens de PvIB community

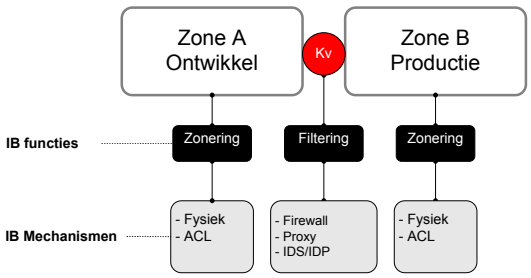
Een patroonbeschrijving kent volgens de Open Group negen vaste rubrieken. De uitwerking daarvan in de gepubliceerde patronen is grote lijnen steeds dezelfde. In de PvIB-community voegen we aan Open Group rubrieken nog enkele relevante IB-specifieke rubrieken toe: *criteria*, *normen* en *implicaties*. Tabel 1 geeft het template voor het beschrijven van een patroon.

Tabel 1: Template van een IB-patroon

Rubriek	Omschrijving
	Naam De naam moet een begrip zijn in het vakgebied of het doel van het patroon kort samenvatten
Criteria	Deze rubriek geeft aan welke van de IB-criteria (*beschikbaarheid, integriteit, vertrouwelijkheid* en *controleerbaarheid*) het meest relevant zijn voor de oplossing die het patroon moet bieden.
Context	Beschrijft de omgeving waarin het risico of het op te lossen probleem zich voordoet, bij voorkeur geschetst aan de hand van het zoneringmodel.
	 Figuur 2: Schets van de omgeving waarin het probleem zich voordoet

vervolg tabel 1 op volgende pagina

Opbouw van IB-patronen

Probleem	Welk risico moet worden gereduceerd? Wat gaat er mis waardoor risico's ontstaan?
Oplossing	Welke risicoreducerende (standaard) oplossing is er te geven? Hoe vindt de beheersing van risico's plaats?  Figuur 3: Schets van de oplossing
Afwegingen	Wat zijn de voor- en nadelen en welke doorslaggevende argumenten zijn gehanteerd voor de keuze van de uitgewerkte oplossing?
Voorbeelden	Een patroon bewijst zijn waarde door het bestaan van een aantal beproefde toepassingsvoorbeelden. Per oplossingstype kunnen verschillende varianten worden beschreven in een patroon.
Implicaties	Deze rubriek geeft aan welke impact de realisatie van een patroon heeft op het toepassingsgebied en wat de eventuele randvoorwaarden zijn. Met impact wordt bedoeld: wat moet de organisatie doen om gebruik te kunnen maken van de geboden oplossing van een patroon, oftewel: wat moet je doen om het voor elkaar te krijgen? Bij de implicaties beschrijf je ook de dynamiek van de oplossing, oftewel: wat zijn de gedragskenmerken tijdens operationeel gebruik?
Gerelateerde patronen	Van welke patronen is het functioneren van de oplossing van het beschreven patroon afhankelijk? Omschrijving van de relatie met andere patronen.
Normen	Indien relevant, wordt hier de verbinding gelegd van patronen met IB-normen. Normen zijn bedoeld om risico's (en problemen) te vermijden of te beheersen. Patronen daarentegen zijn bedoeld om problemen op te lossen en daarmee risico's te verminderen. In beide gevallen zijn maatregelen nodig om dit resultaat te bereiken. Sommige normen zijn al zo concreet in het beschrijven van maatregelen dat patronen daaraan niets toevoegen. Voor andere normen voegen patroonbeschrijvingen wel waarde toe en wordt hier de relatie gelegd. *(Zie normen Informatiebeveiliging ICT-voorzieningen, literatuurverwijzing 6)*

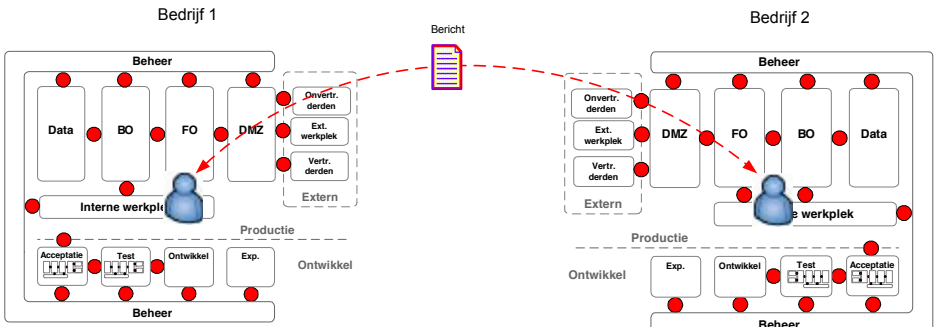
	IB functie	**Normen**	**Implementatie-richtlijnen**
	Functie <x>	Hfst. 5	§ 5.2- normtekst § 5.3- normtekst

Voorbeelduitwerking van een IB-patroon

Tabel 2 geeft een voorbeeld van een uitgewerkt patroon, waarin de rubrieken van de template zijn ingevuld voor de Elektronische Handtekening. De figuren spelen een belangrijke rol in patronen en de toelichtende tekst is beknopt. De PvIB-community gebruikt in haar contextbeschrijving bij voorkeur het beschouwingsmodel Zonering dat in het vorige nummer Informatiebeveiliging (2009, nummer 8) is toegelicht. Patronen moeten zo veel mogelijk zelfverklarend en zelfstandig leesbaar zijn zonder onnodige verwijzingen naar andere documenten.

Zie tabel 2 op volgende pagina.

Tabel 2: Voorbeeldpatroon

Rubriek	Omschrijving
	Elektronische Handtekening
Criteria	Integriteit en Controleerbaarheid
Context	In de wereld van vandaag worden gegevens steeds meer door computersystemen verwerkt, waarbij papieren documenten vervangen worden door elektronische berichten. Gebruikers van deze berichten rekenen daarbij wel op dezelfde zekerheden over de identiteit van zender en ontvanger en de onveranderlijkheid van de gegevens zoals ze gewend zijn bij de verwerking van papieren documenten. De toevoeging van een elektronische handtekening aan een bericht (document, e-mail, bestand), biedt de ontvanger de mogelijkheid om de identiteit van de ondertekenaar van het bericht te verifiëren. Tevens kan hij de integriteit (juistheid, volledigheid) van het bericht controleren (dus dat het ongewijzigd is sinds het is verzonden). Dit patroon richt zich op situaties waarbij het bericht los van enige context of andere beveiligingsmechanismen wordt beschouwd.
	 Figuur 4: Omgeving elektronische handtekening
Probleem	Tijdens het transport en de opslag vormt het onopgemerkt *wijzigen* van berichten (of het wijzigen door onbevoegden) een risico. De ontvanger heeft geen garantie dat het bericht integer is en dat het bericht afkomstig is van de identiteit die als ondertekenaar bij het bericht staat vermeld (authenticiteit).
Oplossing	De elektronische handtekening geldt als bewijs van een wilsuiting wanneer het voldoet aan de eisen in de Wet Elektronische Handtekening (WEH), die inhouden: *"Wanneer de zender een bericht voorziet van een elektronische 'verzegeling', waaruit de ontvanger met zekerheid kan afleiden dat het bericht ongewijzigd is en afkomstig is van de genoemde zender, dan fungeert dat 'zegel' als een elektronische handtekening"*. De elektronische handtekening is inmiddels ook toepasbaar als wettig bewijs, met dezelfde juridische waarde als een gewone (fysieke) handtekening. In art.3:15a lid 4 van het Burgerlijk Wetboek wordt de elektronische handtekening als volgt omschreven: *"Een elektronische handtekening is een handtekening waarvan de elektronische gegevens zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel van authenticatie"*. De wet onderscheidt daarbij drie varianten, die als 'zekerheidsniveau' kunnen worden gebruikt: 1. Gewone elektronische handtekening 2. Geavanceerde elektronische handtekening 3. Gekwalificeerde elektronische handtekening Per niveau wordt daarmee bereikt: 1. Authenticatie van elektronische gegevens 2. Niveau (1) + Identificatie van eigenaar + Data integriteit + Onweerlegbaarheid van creatie 3. Niveau (2) + kwalificatie van certificaat, uitgegeven door een bij de OPTA ingeschreven vertrouwde derde partij, meestal Trusted Third Party (TTP) genoemd. Het laagste zekerheidsniveau (1) garandeert alleen de authenticiteit van het bericht. Daarvoor kan een controlegetal (hash) aan het bericht worden toegevoegd of een pincode of wachtwoord worden gebruikt voor het bevestigen van de transactie. Zekerheidsniveau (2) en (3) zijn qua techniek identiek en ze zijn beiden gebaseerd op een x.509 Public Key Infrastructure (PKI)- certificaat en ze zijn gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen. Het verschil is de garantie omtrent het PKI-certificaat voor identificatie van zender en ontvanger. Figuur 5 schetst de processtappen voor een operationele toepassing. Over het algemeen valt het 'zetten' van de digitale handtekening uiteen in twee delen, wat leidt tot een unieke relatie tussen het bericht en de handtekening en het biedt daarmee herleidbaarheid. 1. Vastleggen van de unieke kenmerken van het bericht (in een hash) 2. Verbinden van de unieke identiteit van de zender aan de hash.

vervolg tabel 2 op volgende pagina

De unieke identiteit van elektronische handtekeningen kan met behulp van verschillende mechanismen worden verbonden met het controlegetal, waarvan de bekendste zijn:

- Symmetrische cryptografische sleutels = vooraf uitgedeeld door regiepartij
- Asymmetrische cryptografie o.b.v. PKI = uitgedeeld door een TTP.

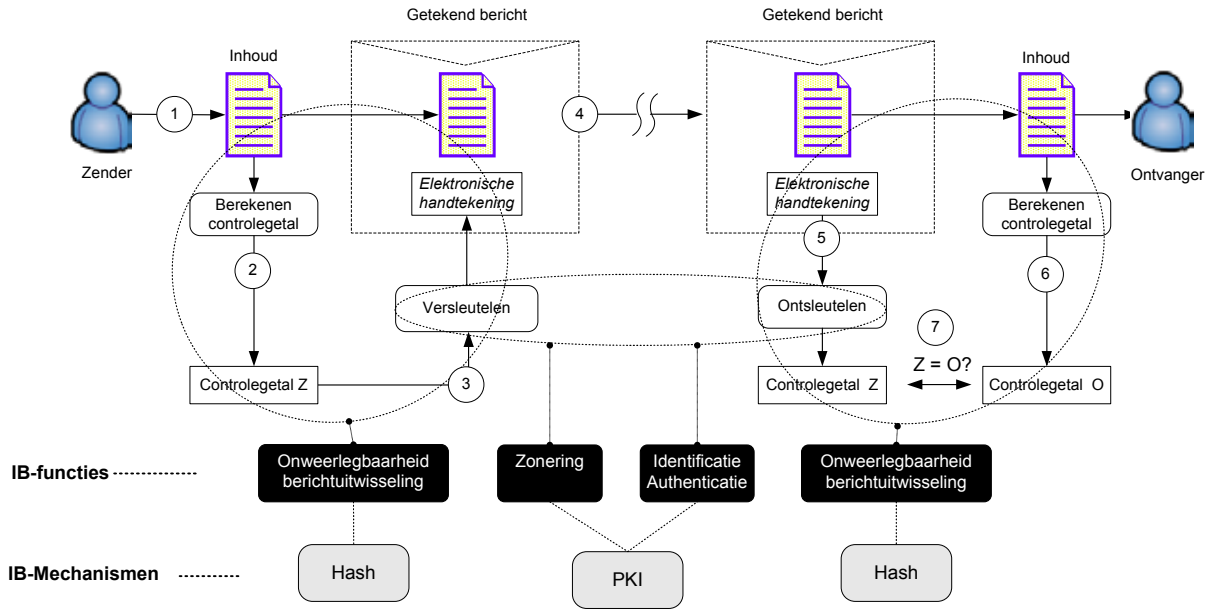
De mate van zekerheid die uit de toegepaste methode voortvloeit, wordt sterk beïnvloed door de kwaliteit van:

- Aard en toepassing van algoritmen en methoden en met name van:
  - Toevalsgetallen
  - Uniciteit en lengte van sleutels en toegangscodes
- Sleuteluitgifte-, distributie- en bewaarprocessen en middelen
- Kwalificatie van de certificaatuitgifte

Tabel 3 geeft aan welke verbanden er bestaan tussen het zekerheidsniveau, de toegepaste sleutels en wie er door zender en ontvanger wordt vertrouwd.

Tabel 3: Zekerheidsniveau en vertrouwen

Zekerheidsniveau	Sleutelmodel	Proceskwaliteit	Zender en ontvanger vertrouwen:
1: Laag, onzekere bewaartermijn	Symmetrisch	Gedeelde encryptiesleutels	Eigen organisatie, of partner
2: Middel, onzekere bewaartermijn	Asymmetrisch	PKI service of private PKI	Eigen organisatie of partner
3: Hoog, gegarandeerde bewaartermijn	Asymmetrisch	PKI 0verheid	Overheid of gecertificeerde partij



Figuur 5: Processtappen voor zekerheidsniveau 2 en 3

Oplossing

De uitgeschreven processtappen gelden voor de toepassing van PKI.

1. De zender stelt een bericht op.
2. Over de inhoud van het bericht wordt een controlegetal berekend, de hash. Voor de berekeningsmethode van de hash wordt een standaard algoritme gebruikt, dat door elke infrastructuur die deze standaard ondersteund is toe te passen.
3. Het controlegetal wordt versleuteld met de *private key* van de zender en bij de al dan niet versleutelde berichtinhoud gevoegd als een elektronische handtekening. Versleutelen van de inhoud van het bericht is mogelijk. Dit maakt verder geen deel uit van het patroon voor elektronische handtekening.
4. Het bericht wordt compleet met handtekening verstuurd.
5. Van het bericht wordt de handtekening ontsleuteld met de *public key* van de zender, waarna het controlegetal (Z) van de zender herkenbaar wordt.
6. Van de inhoud van het bericht wordt aan de ontvangstkant opnieuw een controlegetal (O) berekend.
7. Tenslotte wordt het meegestuurde controlegetal (Z) vergeleken met het controlegetal (O). Wanneer deze getallen precies gelijk zijn, dan is daarmee bewezen dat:
   - De inhoud van het bericht niet is gewijzigd
   - Het bericht afkomstig is van de zender van de overeenkomende public key en daarmee heeft de zender zich bij de ontvanger geauthenticeerd.

Daarmee is het bericht geverifieerd.

vervolg tabel 3 op volgende pagina

Afwegingen	In deze oplossing wordt vanwege de eenvoud alléén het controlegetal versleuteld, waarmee in combinatie met de private key de integriteit van het bericht én de identiteit van de zender kan worden aangetoond. Wanneer vertrouwelijkheid van het bericht ook vereist wordt, kan het bericht zelf ook worden versleuteld, maar dit maakt geen onderdeel uit van de elektronische handtekening. Vanuit het gebruikersperspectief spelen de vragen: • Welke sleutel moet voor deze toepassing gebruikt worden? • Hoe wordt vastgesteld dat de juiste data getekend worden? • Kan in deze omgeving de gekozen handtekening veilig geplaatst worden?		
Voorbeelden	**Zekerheidsniveau 1:** • Het indienen van een belastingaangifte met DigiD • Het gebruik van een wachtwoord om een document te ondertekenen **Zekerheidsniveau 2 en 3:** • Uitwisselen van akten tussen notarissen en het kadaster. • E-facturering		
Implicaties	• De keuze voor de elektronische handtekening impliceert dat organisaties een keuze maken voor een bepaald niveau van beveiliging en het gewenste zekerheidsniveau voor de handtekening. Afhankelijk van dat niveau moeten de verschillende partijen beschikken over de juiste technische hulpmiddelen (cryptografie en rekencapaciteit) en organisatie-inrichting (sleutelbeheer). • Beoogde levensduur van de bescherming. Een handtekening moet over dertig jaar nog steeds betrouwbaar zijn! • Kosten (her-) uitgifteproces van certificaten.		
Gerelateerde patronen	• PKI, dat als mechanisme gebruikt wordt voor identificatie en authenticatie van zender en ontvanger • Bestandsarchivering, dat mogelijkheden biedt om bestanden na archivering terug te kunnen halen om de integriteit, authenticiteit en oorsprong van het bestand aan te kunnen tonen.		
Normen	Zie normen Informatiebeveiliging ICT-voorzieningen *(literatuurverwijzing 6)*		
	IB functie	Normen hoofdstuk	Implementatierichtlijnen
	Zonering	Hfst. 5	§ 5.4- Sterkte van de encryptie § 5.5- Vertrouwelijkheid sleutels
	Onweerlegbaarheid berichtuitwisseling	Hfst. 7	§ 7.1- Implementatierichtlijnen
	Identificatie, authenticatie, autorisatie	Hfst. 8	§ 8.2- Authenticatie

Conclusie

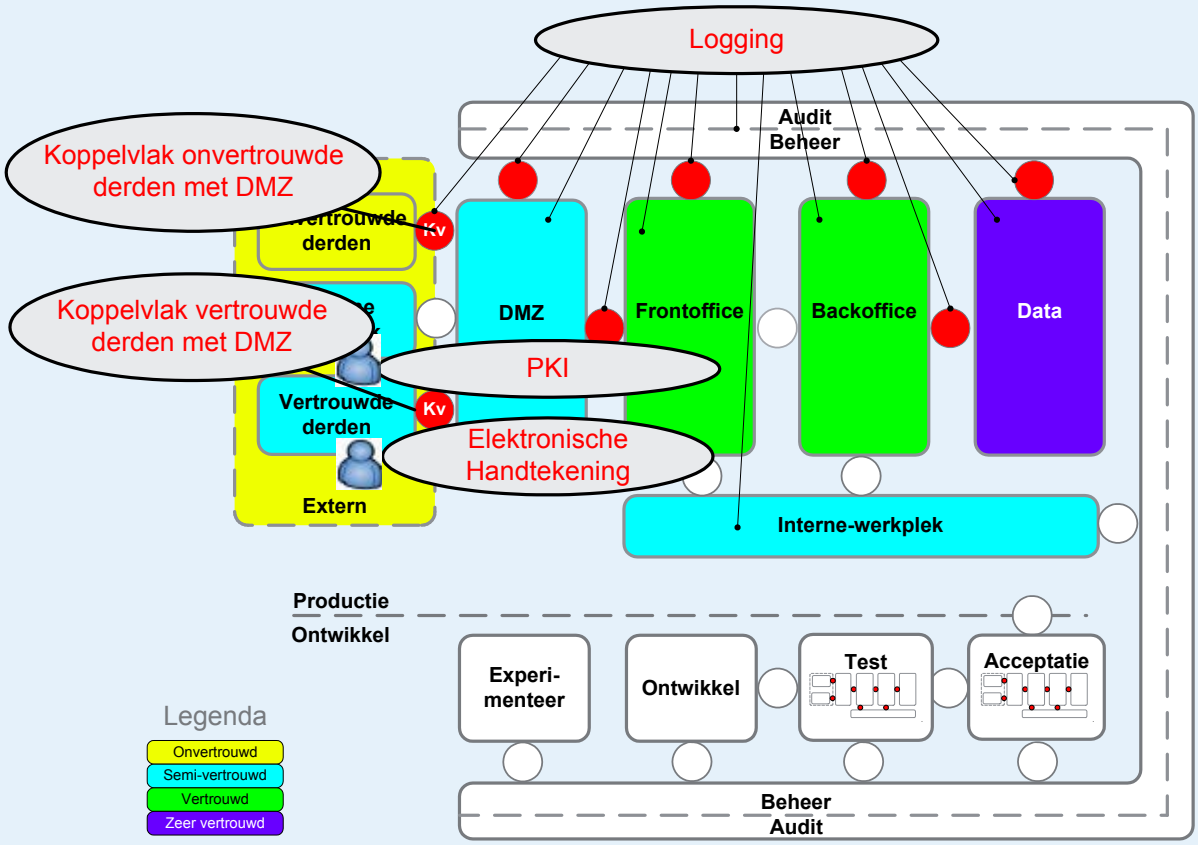
- De uitwerking van een patroon beperkt zich tot een schets van een standaardoplossingsrichting, op basis van een template (Tabel 1).
- IB-patronen benoemen IB-functies en -mechanismen voor de oplossing van het probleem.
- Patronen staan op zichzelf, maar de relatie met andere patronen is expliciet gemaakt.
- Patronen zijn product- en leverancierson-afhankelijk.
- Toepassingsvoorbeelden en implicatiebeschrijvingen zijn een onmisbare verbinding met de praktijk.

Afbeelden van het werkgebied van patronen

In het vorige nummer is in het artikel over de IB-architectuuraanpak het beschouwingsmodel Zonering toegelicht. Dat model schetst de zones in het ICT-landschap van een gemiddeld grote organisatie. Figuur 6 laat zien hoe dit zoneringmodel als overzichtsplaat gebruikt kan worden om te laten zien waar patronen werkzaam zijn in hun omgeving. Sommige patronen, zoals logging en Identity & Access Management (IAM) vinden bijna overal in het ICT-landschap hun toepassing. Het werkgebied van die patronen beelden we om die reden op een andere manier af dan patronen die werkzaam zijn in een keten, zoals de elektronische handtekening of PKI.

PvIB-Patronen community

Zoals in het vorige nummer al genoemd, is sinds maart 2009 een groep deskundigen actief bezig met het samenstellen en verbeteren van IB-patronen. De deelnemers van nu zijn: Jaap Arbouw (Vts Politie Nederland), Ralf Boersma (Achmea), Bart Bokhorst (MinFin/ICTU), Rinus Braak LNV, Jan Breeman BKWI), Boris Goranov (zelfst.), Cees Louwerse (gepens.), Jan van Prooijen (zelfst.), Hanno Steenbergen (Vts Politie Nederland), Kees Terlouw (Vts Politie Nederland), Jos van der Veeken



Figuur 6: Werkgebied van patronen

(zelfst.), Jaap van der Veen (MinFin; hoofdredactie en trekker), Renato Kuiper en André Beerten.

Door deze groep is een lijst opgesteld van kandidaatpatronen die met prioriteit uitgewerkt zullen worden, waaronder patronen voor IAM. De patronen logging, PKI en elektronische handtekening zijn inmiddels goedgekeurd door de community en beschikbaar op *www.IBPedia.nl*. Aan een reeks van andere patronen wordt gewerkt. Van elk type koppelvlak, waarvan er in Figuur 6 maar twee zijn uitgelicht, werkt de community uit wat de belangrijkste verkeersstromen en protocollen zijn die het koppelvlak (gecontroleerd) doorlaat.

Aan de slag met patronen!

We hopen dat u zich na het lezen van dit artikel afvraagt: kan ik nu ook aan de slag met IB-patronen? Het antwoord is: jazeker! Enerzijds omdat er al veel artikelen geschreven zijn over IB-patronen *(zie ook de literatuurverwijzingen 4 en 5)*. Veel daarvan is vrij toegankelijk op het internet. U kunt zich daarop oriënteren en ervaren of het werkt.

Anderzijds omdat u van harte wordt uitgenodigd om mee te denken en te schrijven met de PvIB-patronen community en in de praktijk te testen of de patronen voldoen aan uw eisen. Internationaal bestaat er ook een Security Patterns Community, onder leiding van Marcus Schumacher *(literatuurverwijzing 3)*.

Hoewel IB-patronen nog volop in ontwikkeling zijn, is het zeer de moeite waard om deze aanpak te verkennen en het vakgebied IB met uw kennis en ervaring te verrijken!

Literatuurverwijzingen

1. *Design Patterns: elements of reusable object-oriented software.* Erich Gamma et al, 1995 Addison Wesley Longman.
2. *Verkort uw Time to Market met Security Patterns* door Ir.A. Hofman en ir. J.G Sluiter; Cap Gemini 2001.
3. *Security Patterns: Integrating Security and Systems Engineering;* Markus Schumacher e.a. 2006.
4. *Security Patterns: 10 years later,* Koen Yskout, Thomas Heyman e.a; Katholieke Universiteit Leuven 2008
5. *A survey on security patterns*: Nobukazu Yoshioka e.a; National Institute of Informatics 2008.
6. *NORA Best Practice Informatiebeveiliging Normen ICT-voorzieningen 2009*.
7. *OSA, de Open Security Architecture*: www.opensecurity.org.
8. www.Securitypatterns.org. Het belangrijkste doel van deze website is 'het samenbrengen van securitypatterngebruikers', om een forum te vormen voor patronen en om het overkoepelende werk aan IB-patronen te verbeteren.

De uitdaging van online onderzoek

Auteur: Ing. Alwin Hilberink, CISSP > Alwin Hilberink is Forensisch ICT expert op de politieacademie en te bereiken via ah@cybercops.nl.

Een erg actuele stelling van de vorige schrijver, Marcel Lavalette: *'Levert een digitaal forensisch onderzoek op een systeem dat niet offline is gegaan of mag gaan wel sluitend bewijs?'* Niets is zo veranderlijk als digitale gegevens. Ook al zou men stellen dat een handeling met een bepaalde computer is gedaan, dan nog moet er een gebruiker aan deze handeling worden gekoppeld. Vaak is het sluitend bewijs dan ook een combinatie van bewijs dat zowel digitaal, als tactisch verkregen wordt. Sluitend bewijs op een persoon gericht, is vaak niet uit alleen digitaal onderzoek te halen. Ik zie digitaal onderzoek vaak als ondersteuning binnen een groter geheel, maar soms is het digitale bewijs binnen een onderzoek doorslaggevend.

De probleemstelling

Tot voor enige jaren geleden was het gebruikelijk een computer altijd offline te onderzoeken. In de laatste jaren is het vaak gebleken dat dit niet altijd mogelijk is, of dat er (meer) bewijs te vinden was in online systemen. Een voorbeeld hiervan zijn servers die, als ze uitgezet worden, de bedrijfsvoering ernstig in gevaar kunnen brengen. Verder zijn vluchtige gegevens, zoals het werkgeheugen, een nieuw ontdekte bron van gegevens en eventueel bewijs geworden.

Wat een extra uitdaging vormt bij online onderzoek is dat de gegevens dynamisch zijn en in tegenstelling tot bij een offline onderzoek kunnen veranderen gedurende het onderzoek. Een voorbeeld hiervan is dat op een mailserver e-mail kan blijven binnenkomen en dat daardoor misschien voor het onderzoek belangrijke mail wordt overschreven. Wat verder meespeelt, is dat de datum en het tijdstip van de bestanden nog steeds aangepast kunnen worden, wanneer een gebruiker een document bewerkt en gedurende het onderzoek opslaat. De tijdslijn kan hierdoor afwijkingen vertonen. Als gevolg hiervan kan de formulering van het aangetroffen bewijs en de eventuele oorzaak erg moeilijk zijn, want deze dient wel exact te zijn. Als fanatieke ICT-er wil een onderzoeker nog wel eens conclusies trekken, die meestal juist zijn, maar niet in elke denkbare situatie. De formulering van het gevonden bewijs en de betekenis ervan maakt de conclusies vaak moeilijk leesbaar voor een niet ICT-er. De vraag wat dit nu betekent, dient altijd gesteld te worden.

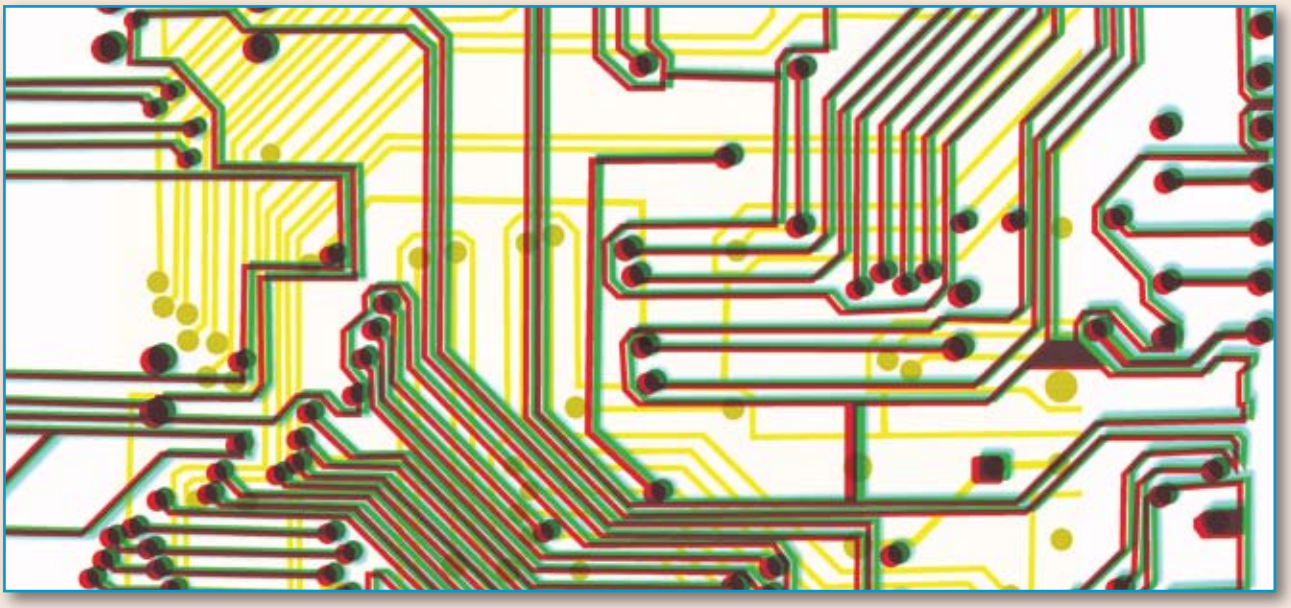
Daarnaast verricht je als onderzoeker handelingen op het systeem die ook wijzigingen van de gegevens met zich kunnen meebrengen, zoals het draaien van de onderzoekstools. Zelfs het klikken binnen Windows kan grote veranderingen met zich mee brengen.

Er zijn dus een aantal problemen te definieren, die direct of indirect met elkaar te maken hebben. Soms is er gewoonweg niet de mogelijkheid om een systeem offline te onderzoeken en is het bewijs alleen te vinden in de vluchtige gegevens.

Welke mogelijkheden zijn er?

Als ik zo de problemen opsom, lijken sommige onoverkomelijk, maar ik denk dat dit zeker niet het geval is. De belangrijkste vereiste voor de onderzoeker is dat hij weet welke veranderingen hij teweeg kan brengen met een specifieke handeling, zeg maar de impact op de gegevens.
Dat hoeft niet per se de impact op het eventueel aanwezige bewijs te zijn. Zo kan een onderzoeker het beste een onderzoekstool gebruiken die een zo min mogelijke

Alwin Hilberink



hoeveelheid data verandert. Als bijvoorbeeld het geheugen van een computer met grote waarschijnlijkheid belangrijke gegevens bevat, dan kan een onderzoeker beter het geheugen veiligstellen met een tool die een kleine footprint heeft. Hierdoor is de kans kleiner dat belangrijke gegevens overschreven worden in het geheugen. Toch kunnen er situaties zijn waarin het bijvoorbeeld nodig is om ter plekke te analyseren of een systeem interessant is om te onderzoeken.
In een grote vestiging met duizend systemen is het niet haalbaar om op elk systeem een uitgebreid onderzoek uit te voeren, maar wil de onderzoeker weten welke systemen interessant kan zijn.
Dit kan voor een deel door tactische aanwijzingen worden gedaan, maar ook technisch gezien zijn er mogelijkheden.

Bij offline onderzoeken moet je vluchtige gegevens, zoals geheugendata, missen en dus online onderzoek is een mogelijkheid die we zeker moeten benutten als die zich voordoet. Op dit moment ben ik bezig met een vooronderzoek voor mijn dissertation van een opleiding die ik volg aan de Universtity College Dublin, met als onderwerp Memory Forensics. Ik wil hier met name aandacht besteden aan het zoeken naar Best Practice voor onderzoeken binnen het geheugen, het in kaart brengen van de nu al beschikbare (open source) onderzoekstools en in welke situatie deze het best ingezet kunnen worden.

Het geheugen heeft geen duidelijke bestandstructuur zoals een besturingsysteem als Windows dit heeft. Het gevolg hiervan is dat het moeilijker leesbaar is. Wat er in het geheugen wordt geschreven, is vaak ook niet te controleren door een gebruiker en dit aspect zorgt er vaak voor dat er veel waardevolle informatie te vinden is in het geheugen. Ook gegevens die op de harde schijf versleuteld zijn, worden soms in het geheugen onversleuteld opgeslagen.

In bepaalde onderzoeken, zoals hacking, is het nodig te weten welke services er draaien, wat deze doen en hoe ze communiceren. Dergelijke gegevens zijn moeilijk of soms onmogelijk te achterhalen als het systeem offline is. In die gevallen is het beter het systeem draaiende te houden, eventueel in een gecontroleerde omgeving, en zo het onderzoek uit te voeren.

Conclusie
De stelling of een online onderzoek wel sluitend bewijs oplevert, is dus alleen per casus te beantwoorden en ik ben van mening dat dit ook geldt voor offline systemen, hoewel hier de kans op fouten kleiner is voor de onderzoeker. Het is dan ook belangrijk om digitaal onderzoekers ook hier op te trainen en ze te laten bijblijven met de veranderingen binnen dit werkveld. De gevolgen van een verkeerde beslissing kunnen rampzalig zijn voor het eventuele bewijs. Toch zou ik in steeds meer situaties online onderzoek willen toepassen, omdat het vaak een schat aan informatie oplevert, die we anders misschien missen.
Een simpel voorbeeld is de registry van een Windows computer. Die bestaat alleen maar in het geheugen en wordt na elke restart opnieuw aangemaakt. De ontwikkelingen, zoals cloud computing en virtualisatie, zorgen ervoor dat steeds meer onderzoeken op online systemen uitgevoerd gaan worden, omdat we anders simpelweg geen of onvoldoende bewijs zullen vinden.

Per situatie zal een onderzoeker een onderzoeksplan moeten ontwikkelen en dit tijdens het onderzoek moeten bijstellen om het maximale uit een onderzoek te halen. Ik ben van mening dat het voor een onderzoeker niet uitmaakt of dit een offline of online systeem is. Voorwaarde is dat de onderzoeker voldoende getraind is, zodat hij weet wat zijn handelingen voor gevolgen kunnen hebben en deze altijd kan verantwoorden als dat nodig is.

Ik geef het estafettestokje door aan Sebastiaan Back, Strategist bij McAfee, met de vervolgstelling: *'Moet een IT Security fabrikant zorgen voor voldoende bescherming tegen cybercriminelen?'*

Overzicht verschenen artikelen in 2009

Titel	Auteur(s)	Trefwoord(en)	Paginanummer
Nummer 1, februari 2009, met het Browser Dossier			
Multifunctionele printers: vaak onveilig!	Eric Luiijf	ENISA rapport documentenstroom	4
Verslag NICC-event: Are you in control?	Patrick Borsoi	Security event NICC	5
Forensische softwarepakketten	Serdar Gürcan	Onderzoek forensische software	7
May I have your votes, please!	Henk Meeuwisse	Nominaties Artikel van het Jaar	9
De evolutie van de browser	Ferry den Dopper	Evolutie browsers	10
(in)Security 2.0?	Rob Hofker	Browser dossier	14
Browser Security Handbook	Lex Dunn en André Koot	Browser dossier	18
Slecht SSL beheer maakt uw webdiensten onbereikbaar	Kick Willemse	Browser dossier	20
Vriendensites op herhaling	Marco Smitshoek	Browser dossier	22
Questafette: .nl is het veiligste domein ter wereld	Roelof Meijer	Veilig domein	26
Boekbespreking: Identity Crisis	André Koot	Boekbespreking	28
Nummer 2, april 2009			
Claims based acces control	André Koot	Veilige webtoepassingen binnen SOA	4
Boekbespreking: Thinking outsite of the BoK	Lex Borger	Boekbespreking	9
Securitycafé geslaagd!	Jaap van der Veen	Verslag Securitycafé	10
Barcelona: ISF 19th Annual World Congress	Mario de Boer, Lex Borger en Aart Jochem	Verslag ISF 2009	12
Vertrouwen in beveiliging, is beveiligen met vertrouwen	Andor Demarteau	Trust management	15
InZicht	Rob Greuter	Boekbesprekingen	19
The human firewall of behavioral information security	Michiel Dan en Kevin Wessels	Gedragsintentie medewerkers	20
Kennisdeling binnen PvIB	Erno Duinhoven	Expertbrieven	23
Questafette: 'Zet DNSSEC op de agenda - met het wachten op elkaar is niemand gediend	Olaf Kolkman	DNSSEC voor een veiliger DNS	24
Extra aandacht voor Security en Architectuur en het ExD	André Koot	Komende specials IB	26
Kennis maken én kennis delen		IBPedia	27
Even voorstellen… Mario de Boer en Tom Bakker		Redactieleden IB	28
Joop Bautz Information Security Award: Maak het de vakjury lastig!	Kelvin Rorive	Award voor beste scriptie	30
De achterkant van beveiliging	Berry	Column	31
Nummer 3, mei 2009			
Identity In The Fog - New Radar Needed	Stuart Boardman en Michael Boley	Extended Enterprise, Web 2.0 & Internet based IT services	5
CIO Platform Nederland, een kennismaking	Hendrikus Beck	CIO platform	9
Publieke Identity Providers: kip en ei?	André Koot	DigiD	10
Wat het convergeren van de fysieke en logische beveiliging voor uw organisatie kan betekenen	David Ting	Onvoldoende beveiligde systemen	12
Boekbespreking: Zen and the Art of Information Security	Lex Borger	Boekbespreking	14
Het Business Continuity Management proces, de paradox	Sjoerd Vredenberg en Tim Willems	BCM	15
Economische crisis vraagt om het economisch borgen van informatiebeveiliging	Saïd El Aoufi	Investeren in informatiebeveiliging	20
Verkiezing Artikel van het Jaar: en de winnaar is…	Leo van Koppen	Verkiezing Artikel van het Jaar	22
Artikel van het jaar 2008: de monsterlijke trekjes van beveiligingsproblemen	Wolter Pieters	Winnaar verkiezing Artikel van het Jaar	23
De normatieve impact van ambient technology en converging technologies: Privacy en (veel) meer	Anton Vedder	Ethiek en nieuwe technologie	26
Functionarissen in de Informatiebeveiliging	Tom Bakker	Overzicht IB-functies	29
Automatisering of IT?	Berry	Column	31
Nummer 4, juni 2009: Special Architectuur en Security			
Beveiliging en architectuurraamwerken: de rol van audits	Saïd El Aoufi	De rol van audits	4
InZicht	Rob Greuter	Boekbesprekingen	9
Interview met Alexander Baas, CIO SNS Bank	Lex Borger	Interview	10
Open Security Architecture: een open source architectuur	André Koot	OSA	12
Beveiligingsarchitectuur in Jericho-stijl	Aaldert Hofman	Jericho principes	15
Interview met een (B)ISA	Tom Bakker	Functionarissen in de informatiebeveiliging	20
Architectuurprincipes versus projectmatig opportunisme	Lex Borger	Spanningsveld tussen architecten en projectmedewerkers	22
Toegang tot patiëntgegevens	Leon van der Kragt	Toegang tot patiëntgegevens	25
Het SABSA(r) Model	Lex Borger	Risicomanagement in SABSA	32
Compromis	Berry	Column	35

Titel	Auteur(s)	Trefwoord(en)	Paginanummer
Nummer 5, juli 2009			
AutoNessus: herhaaldelijk scannen realiseert gemak	Frank Breedijk	Uitvoeren en verwerken van scans	4
Een terugblik op Black Hat Europe 2009	Lex Borger	Verslag Black Hat 2009	8
Questafette: de beveiliging van IP-routing is een aanfluiting	Remco van Mook	IP-routing	12
Anonimiteit versus verantwoording op het internet	Ellen Wesselingh	Schending van rechten op internet	14
Een interview met Amichai Shulman, CTO en oprichter van Imperva	Mario de Boer	Interview	19
Een terugblik op de European Identity Conference in München	Bavo de Ridder	Verslag European Identity Conference	22
Boekbespreking: The Pragmatic CSO door Mike Rothman	Lex Borger	Boekbespreking	26
Cryptogebruik: werken met vertrouwelijke informatie in het buitenland	Edwin van Buuren	Cryptografie	27
De Spaanse zon	Berry	Column	30
Nummer 6, oktober 2009			
Groeiende cybercriminaliteit kost bedrijfsleven en overheid handen vol geld	Matthijs van der Wel	Cybercriminaliteit	4
De Leidraad voor de uitwisseling van gevoelige informatie van NAVI	Hans Muller en Erwin van der Zwan	NAVI	8
Functies in de informatiebeveiliging: Jeroen van Duuren van Edutel	Tom Bakker	Functionarissen in de informatiebeveiling	11
Questafette: de veelheid aan specifieke IT-security certificeringen doet eerder afbreuk dan dat het wat toevoegt	Marcel Lavalette	IT-security certificeringen	12
Het GOVCERT.NL Cybercrime trendrapport 2009 laat geen verbetering van de veiligheid van internet zien	Ton Slewe en Ella Broos	Trendrapport cybercrime	15
Verslag van het PvIB-seminar over het Elektronisch Patiënten Dossier	André Koot en Erno Duinhoven	Seminar EPD	18
Voorkom schijnveiligheid door een veilig ontwerp	Kees Hogewoning	Schijnveiligheid	20
DEMO architectuurmethode met securityparagraaf	Yuri Bobbert	DEMO	22
Goed verzekerd?	Berry	Column	27
Nummer 7, november 2009			
Internationale normen voor IT beveiligingstechnieken	Jan Rietveld	JTC 1/SC 27 IT Security techniques	4
Hoe veilig is het nieuwe authenticatiesysteem PassWindow?	Andor Demarteau	PassWindow	6
InZicht	Rob Greuter	Boekbesprekingen	11
BCM en de cloud	André Koot	Cloud computing	12
De kwetsbaarheden van browser plugins	Maarten Hartsuijker	Browser plugins	14
De juridische aspecten van digitaal onderzoek	Erwin van der Zwan	Juridische aspecten van digitaal onderzoek	17
Een verslag van het GOVCERT symposium 2009	Maarten Oosterink	Verslag GOVCERT	25
Diefstal van mijzelf	Berry	Column	27
Nummer 8, december 2009			
De ontwikkeling van eID in Europa	Elisabeth de Leeuw	eID	4
De aanpak van cybercriminaliteit: verdeel en heers	Henk-Jan van der Molen	Malware	6
Integriteit bekeken vanuit het oogpunt van informatiebeveiliging	Pieter IJfs	Betrouwbaarheid, vertrouwelijkheid en integriteit	11
Process control security en SCADA security: een realitycheck	Maarten Oosterink	SCADA Security	14
Verslag Information Security and Risk Management Conference	Tom Bakker	Verslag ISACA	16
Inzicht in informatiebeveiliging door security game	Marcel Spruit	Security game	18
De NORA als architectuuraanpak voor IB-patronen	Jaap van der Veen	IB-patronen, deel I	21
Controle of privacy?	Berry	Column	27

PvIB
Platform voor InformatieBeveiliging

Artikel van het Jaar 2009

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.

Vorig jaar hebben we voor het eerst een auteur beloond voor de bijdrage van een heel goed artikel. De deskundige, onafhankelijke jury vond dat Wolter Pieters een dikke pluim verdiende voor zijn artikel over monsters.

La Plume van Belgapixel via Flickr.com

We hebben gemerkt dat het initiatief positief werd ontvangen, het smaakte naar meer. Van verschillende kanten hoorden we wel dat het jammer was dat er maar één award werd uitgereikt. Die kritiek namen we ons als redactie ter harte en we reiken dit jaar dan ook niet één prijs uit (ter waarde van maar liefst 500 euro), maar drie, waardoor de jury zich minder bezwaard hoeft te voelen als het een nek-aan-nekrace blijkt te zijn. Ook de nummers twee en drie krijgen een (iets kleinere) beloning.

We hebben de jury van vorig jaar gevraagd om opnieuw een oordeel te vellen. De jury bestaat dus wederom uit:

- Leo van Koppen - vanuit het onderwijsveld (Haagse Hogeschool)
- Kees Hintzbergen - lezer van dit blad (3-Angle)
- John Rudolph - een ervaren, maar niet genomineerde auteur (Wipro Technologies)

Een ander puntje van kritiek kwam van deze jury: hoe is de shortlist bepaald? Wat waren de criteria? Voor dit jaar heeft de redactie dezelfde werkwijze gevolgd als vorig jaar. Dat ging als volgt: iedere redacteur mocht vijf artikelen nomineren. Er mocht niet worden gekozen uit de vaste en de redactionele artikelen (wat jammer is bijvoorbeeld de Questafette-auteurs en columnist Berry). Alle genomineerde artikelen vormden de longlist. Elk artikel dat door meer dan één redacteur werd genomineerd, kreeg een plaats op de shortlist. Dat leverde ook dit jaar weer een interessant overzicht op en een iets langere lijst dan vorig jaar.

De criteria waren ook voor de redacteuren hetzelfde als vorig jaar. Elk artikel werd beoordeeld op:

1 Opzet artikel
   a. Is het een feitenrelaas, een opiniërend artikel of staan feiten en mening door elkaar (laatste scoort niet).
   b. Doel van artikel - waar gaat het over en is dat duidelijk?
   c. Begin van het artikel - vormt het een prikkel om verder te lezen?
   d. Conclusie of samenvatting van het artikel - waar ging het nu over en stemt dat overeen met de gewekte verwachtingen?
   e. Is het 'wie, wat, waar, wanneer en waarom' gehalte duidelijk aanwezig?

2 Leesbaarheid (helder, begrijpelijke taal, lengte zinnen, toelichtende illustraties)
   a. Het niveau (wetenschappelijk, praktijkcase).
   b. De stijl (serieus van aard, satirisch).

3 Benadering van de doelgroep (interessant voor alle lezers of voor een kleine groep).

4 Het vernieuwende gehalte. Hebben we dit al vaker gehoord, is het een nieuwe of goedgedocumenteerde variant op bekend thema of geeft het juist nieuwe inzichten; *out of the box thinking*?

5 Zet het de doelgroep aan het denken?

Naar de mening van de redactie zijn met name het vierde en het vijfde criterium van doorslaggevende aard, mits een artikel ook de toets der kritiek volgens criteria één tot en met drie kan doorstaan. Maar de redactie heeft die aspecten minder zwaar laten wegen en als het goed is, hebben de redacteuren die aspecten al in de redactieslag gewogen.

Dit is de shortlist, in chronologische volgorde:

2009 no. 1: *Vriendensites op herhaling*
Marco Smitshoek

2009 no. 2: *Claimed based access control*
André Koot

2009 no. 4: *De rol van audits (beveiliging en architectuur raamwerken)*
Saïd El Aoufi

2009 no. 4: *IB-architectuur in Jericho stijl*
Aaldert Hofman

2009 no. 4: *Toegang tot patiëntgegevens*
Leon van der Krogt

2009 no. 5: *Anonimiteit versus verantwoording op het internet*
Ellen Wesselingh

2009 no. 6: *Interessante discussies over Elektronisch Patiënten Dossier*
André Koot en Erno Duinhoven

2009 no. 7: *BCM en cloud: Continuïteit as a Service*
André Koot

2009 no. 7: *De juridische aspecten van preventief monitoren en digitaal onderzoek*
Erwin van der Zwan

2009 no. 8: *Een architectuuraanpak voor IB-patronen*
Jaap van der Veen

Het is een mooie lijst met goede artikelen en ik mag me vereerd en gevleid voelen met zoveel nominaties. En nee, ik heb niet op mezelf gestemd…

We hebben nog geen publieksprijs, maar wat let ons om daar iets aan te doen? Als we genoeg reacties/stemmen krijgen, kunnen we daar vast iets mee doen! Mail me gerust.

Waar moet dat heen?

Keira Bishop via sxc.hu

Ik zit op mijn zolderkamer te werken aan een document dat ik moet opleveren en peinzend kijk ik door mijn zolderraam op zoek naar inspiratie. Het regent buiten en de wind giert om het huis; het zal wel weer druk zijn op de weg. Even mijn vaste website opstarten die grafisch het fileleed toont en ja hoor, heel Nederland staat weer vast. Gelukkig heeft mijn werkgever het 'nieuwe werken' geïntroduceerd en kan ik vanuit huis mijn werk doen. Mijn eigen koffie, mijn eigen bureaustoel en lekker in de pyjama achter mijn toetsenbord zitten.

Om mijn werk te kunnen doen, heeft mijn werkgever mij een laptop ter beschikking gesteld en een draagbaar apparaat waarop mijn agenda te zien is, mijn mail wordt binnengehaald en internetsites goed te bekijken zijn. Daarnaast kan het ding ook nog bellen. Is mijn werkgever vernieuwend bezig? Ja, maar tegelijkertijd is het nieuwe werken een trend die niet meer te stoppen is. Binnen de grote bedrijven is dit fenomeen zich al aardig aan het settelen. Eigenlijk kan het ook niet anders, want nieuwe werknemers zijn echt niet van plan om van negen tot vijf op kantoor te zijn. Die werken wel op momenten dat het hen uitkomt.

Ik heb altijd een vaste opstelling op mijn werkkamer, rechts staat de laptop van mijn baas en links staat mijn eigen laptop.
Tot grote verbazing van mijn vrouw staan ze altijd tegelijkertijd aan en ze vraagt zich af waarom dat zo is, want ik ben zo'n man die maar één ding tegelijk kan doen.
De reden is eenvoudig: mijn werkgever heeft zijn best gedaan de laptop zo goed mogelijk te beschermen tegen onheil van buitenaf. Veel beveiligingsmaatregelen zijn er getroffen om de data die ik van mijn werk meeneem te beschermen tegen vreemde ogen. Ik ga niet alle maatregelen noemen, maar neem maar van mij aan dat dit moderne apparaat heel wat controles moet uitvoeren, voordat ik er op aan het werk mag.

Aan de linkerkant staat mijn eigen laptop die zeer gebruikersvriendelijk is en die precies naar mijn zin is ingericht.
Het besturingssysteem is een ander dan op mijn werk, maar ik kan alle websites bezoeken die ik wil en ook andere software, die ik vaak tijdens mijn werk gebruik, staat me ter beschikking. Ik heb de machine ook zo geconfigureerd dat ik de mail op mijn werk kan bekijken. Als ik thuiskom en mijn mail even wil bekijken, pak ik ook altijd mijn eigen machine, omdat deze sterk mijn voorkeur heeft. Op mijn bureau tref je ook twee telefoons aan, één van de werkgever, die is uitgerust met een mobiele variant van de software die ook op de bedrijfslaptop staat en mijn privételefoon, die toevallig is uitgerust met een mobiele variant van de besturingssoftware die op mijn eigen laptop staat. Ik vind dat plezierig werken.

Ik ben inmiddels grijs en ik accepteer deze situatie ook wel, maar ik sprak een aantal maanden geleden met een nieuwe collega op onze helpdesk. Ik had een probleem met mijn bedrijfslaptop en hij zou dat verhelpen. Terwijl hij naar het scherm keek, spraken we over de beheersintensiteit van de laptops, de grote hoeveelheid laptops die de afgelopen periode zijn uitgerold en de enorme kosten die dit met zich mee brengt. Ik zei tegen mijn redder in nood dat ik mijn laptop wel wil inleveren en tegen een onkostenvergoeding mijn eigen laptop wil gaan gebruiken. Datzelfde geldt voor mijn telefoon, ik zet het simkaartje wel om en ik gebruik mijn privételefoon. Onder het toetsen vertelde hij me dat hij ook niet goed werd van de kostbare voorzieningen die bij ons in het bedrijf worden verstrekt. Grijnzend liet hij mij zijn telefoon zien en die kwam mij wel heel bekend voor. Inmiddels was mijn laptop klaar en we zaten te wachten tot de machine opstartte. Ik bedankte de technicus en gaf hem aan dat ik mijn laptop een andere keer wel zou brengen.

Dat was vier maanden geleden en de enige machine op mijn bureau staat nu recht voor me. En dat bevalt me prima. De telefoon van mijn werkgever ligt nu in de onderste bureaulade en zelfs mijn kinderen hebben daar geen belang bij, ondanks het feit dat ik hem toch een jaar met plezier heb gebruikt. Nu alleen de vergoeding van mijn baas nog en we zijn allemaal weer gelukkig.

Groeten,
Berry

Verlies uw USB stick, maar nooit uw data!

De voordelen van SafeStick

- Automatische back-up & recovery
- Snelste en veiligste encrypted USB stick
- Remote delete en password reset
- Timer lockdown en brute force protection
- Geen extra software nodig

Zelf SafeStick proberen? Neem contact op via (0183) 62 44 44 voor een evaluatie stick.
De prijzen van SafeStick kunt u vinden op www.crypsys.nl/shop

SafeStick®

CRYPSYS Data Security B.V. - Benelux Distributeur van SafeStick
Edisonweg 4 - 4207 HG Gorinchem - Postbus 542 4200 AM Gorinchem

CRYPSYS data security