november 2009 nummer 7

INFORMATIEBEVEILIGING

Internationale normen voor IT beveiligingstechnieken

De juridische aspecten van digitaal onderzoek

Hoe veilig is PassWindow?

De kwetsbaarheden van browser plugins

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

De afgelopen maand was wel weer bizar. Als je de security kalender van het hele jaar bekijkt, dan is het best een rustig jaar. Niet veel bijzonders te doen. En dan komt de maand oktober en die is dan te kort. Hoe is het toch mogelijk dat alle congressen in Nederland in dezelfde weken worden gepland? Wie doet dat toch? Weten die planners niet dat er twaalf maanden in een jaar zitten en dat het heel vervelend is als je overal naartoe wilt, maar dat niet redt?

In oktober hadden we een Jericho-evenement, IIR Identity 2009, het GOVCERT-congres, ons eigen Security Congres in Ede en, als we nog een paar dagen in november meepakken, de Infosecurity beurs in Utrecht. Bovendien tussendoor hadden we ook nog eens de herfstvakantie. De overige PvIB-sessies, werkgroepen, seminars en leveranciers-presentaties et cetera, laat ik dan nog maar even voor wat ze zijn. Ik werd er niet vrolijk van. In die maand was ik regelmatig uithuizig en dat is best jammer, want ik word ook geacht productie te leveren voor mijn werkgever. Ik kon dus niet alles bijwonen, ik moest bijvoorbeeld GOVCERT laten lopen. Pech voor mij dan. In dit nummer hebben we wel een korte impressie van Maarten Oosterink, dat maakt gelukkig nog iets goed.

Wat we nog meer hebben: een artikel over de juridische aspecten van forensische onderzoeken door Erwin van der Zwan, een technisch artikel over browser plugins van Maarten Hartsuiker (onze eindredactie schrok van de inhoud), een analyse van een nieuwe authenticatiemethode door Andor Demanteau (Passwindow, levert dat een bijdrage?), een interessant artikel over de ontwikkeling van de ISO-normen door Jan Rietveld en ik heb zelf iets geschreven over BCM in de Cloud (ja, dat wordt nog een probleem). Bovendien heeft Berry last van een identiteitscrisis. Een divers programma, dunkt mij.

Enne, of ik dan nog even nog een artikeltje aan kan leveren? Dat was het mailtje van de eindredactie. Tja, daar zit je dan, een dag voordat het blad naar de opmaak gaat, met nog ruimte in het blad en heel veel ideeën voor leuke artikelen. Maar ja, net als andere auteurs; een gebrek aan tijd. We hebben besloten om het dan maar gewoon wat dunner te houden en niet zomaar een artikeltje aan te leveren. Dat werkt niet, we hebben toch ook een naam hoog te houden. En daarmee hebben we dus weer iets minder pagina's in dit nummer. Dat scheelt natuurlijk, want ook lezers hebben een gebrek aan tijd en hoe dunner een nummer, hoe sneller je een blad uit hebt. Zo eindig je toch met een vrolijke noot ;)

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
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)
Henk Meeuwisse (Sogeti)
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

Inhoud





Huidige ontwikkelingen bij JTC 1/SC 27

De internationale normcommissie voor IT beveiligingstechnieken

Auteur: Jan Rietveld > Jan Rietveld is secretaris van de NEN-commissie IT beveiligingstechnieken en is bereikbaar via jan.rietveld@NEN.nl.

Het belang van informatiebeveiliging blijft toenemen nu steeds meer organisaties online toegankelijk zijn en online zaken doen. Goede beveiligingstechnieken zijn dan ook verplichte onderdelen van de bedrijfsvoering voor deze organisaties. Dit heeft zijn invloed op de normen die worden ontwikkeld door de internationale normcommissie JTC 1/SC 27 IT Security techniques. De commissie IT beveiligingstechnieken van het Nederlands Normalisatie-instituut (NEN) werkt mee aan de normen van JTC 1/SC 27.

Sinds het artikel over ISO/IEC 17799 en BS7799 in het oktobernummer van 2005 (ISO/IEC 17799:2005 en BS7799-2:2000 herzien, door Ernst Oud en Jan Rietveld) van dit tijdschrift, zijn er veel nieuwe initiatieven voor normen op het gebied van informatiebeveiliging. De normcommissie is op dit moment verantwoordelijk voor meer dan honderdveertig normen. In dit artikel hoop ik duidelijk te maken voor welke onderwerpen de JTC 1-normcommissie normen maakt. In vogelvlucht wordt een overzicht gegeven van de veranderingen bij de normcommissie IT Security techniques.

Inleiding

De meest in het oog lopende veranderingen zijn natuurlijk het hernummeren van ISO/IEC 17799 naar ISO/IEC 27002 en de publicatie van de ISO/IEC 27001. Onder invloed van het toenemende belang van informatiebeveiliging werkt de normcommissie aan een serie basisnormen, die allemaal genummerd worden in de reeks 270xx. Hierover verschijnt in 2010 een zelfstandig artikel.

Minder bekend is de uitbereiding van de onderwerpen die door de normcommissie worden behandeld. Door het toenemende gebruik van internet is het beveiligen van privégegevens belangrijk geworden, net als Identity Management. Sinds 2008 zijn deze twee onderwerpen opgenomen in het onderwerpsgebied van de normcommissie. Verder wordt gekeken naar het maken van normen voor het beveiligen van biometrische gegevens en voor Information Security Governance (ISG).

Werkgroepen

Binnen de normcommissie zijn vijf werkgroepen actief die verantwoordelijk zijn voor deelonderwerpen.

Werkgroep 1: Information security management systems

Is alleen verantwoordelijk voor normen in de 270xx-serie, onder andere voor ISO/IEC 27001 en 27002. Ook werkgroep 4 (zie hieronder) beheert verschillende normen uit de 270xx-serie. Over de 270xx-serie en werkgroep 1 verschijnt volgend jaar een apart artikel. Ter informatie: namens NEN zijn ING en KPN lid van deze werkgroep.

Werkgroep 2: Cryptography and security mechanisms

Is verantwoordelijk voor normen op het gebied van encryptie, entiteit authenticatie, non-repudiation (onweerlegbaarheid), time-stamping (tijdstempel/prikklok), digitale handtekeningen, sleutelbeheer, message authentication codes (MAC's, bericht authenticatiecodes), hash-functies (door de cryptograaf in de NEN-commissie soms klutsfunctie genoemd) en mathematische en crypthografische technieken.
Er zijn recent normen verschenen op het gebied van sleutelbeheer (ISO/IEC 11770) en digitale handtekeningen (ISO/IEC 14888). Werkgroep 2 gaat werken aan normen voor groepgebaseerde cryptografie, threshold cryptografie en cryptografische technieken voor Digital Right Management. NEN heeft geen vertegenwoordigers in deze werkgroep.

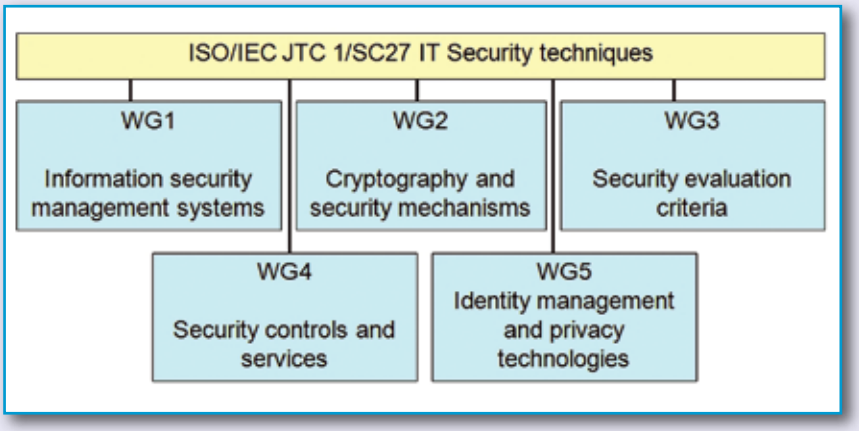
Werkgroep 3: Security evaluation criteria

Maakt normen voor de methodologie en administratieve procedures voor het evalueren van IT-beveiligingstechnieken. De werkgroep is onder andere verantwoordelijk voor ISO/IEC 15408 *Methodology for IT security evaluation* en ISO/IEC 15443 *A framework for IT security assurance*.

De werkgroep gaat werken aan normen voor het verifiëren van cryptografische protocollen en voor het documenteren van IT-beveiliging-evaluaties en op lange termijn aan normen voor het ontwerpen van veilige systemen. Werkgroep 3 werkt samen met de Common Criteria Development Board (CCDB). Als de Common Critieria veranderen, kan Werkgroep 3 besluiten haar normen aan deze veranderingen aan te passen. De voorstellen hiertoe worden weer voorgelegd aan de nationale normalisatie-instituten, dus ook aan de NEN-commissie. NEN heeft geen vertegenwoordigers in deze werkgroep.

Werkgroep 4: Security controls & services
Is opgericht voor het maken en onderhouden van normen op het gebied van Security controls and services. Deze normen helpen organisaties bij het implementeren van de normen uit de 270xx-serie. De werkgroep maakt normen voor bekende beveiligingsproblemen, maar probeert ook te anticiperen op aankomende of nog onbekende beveiligingsissues. Zo wordt gewerkt aan ISO/IEC 27032 *Cybersecurity* en aan normen om vast te stellen of er IT-beveiligingsproblemen zijn opgetreden. Bij deze werkgroep ligt een normvoorstel voor *Guidelines for identification, collection and/or acquisition and preservation of digital evidence*.
Enkele bestaande normen van deze werkgroep worden herzien en soms op nieuw genummerd in de 270xx-serie. Zo krijgt ISO/IEC 18028 IT *network security* als nieuw nummer ISO/IEC 27033. ISO/IEC 18044 *Information security incident management* wordt herzien en hernummert naar ISO/IEC 27035. Namens NEN zijn ING en KPN lid van deze werkgroep.

Werkgroep 5: Identity management and privacy technologies
Maakt normen met betrekking tot privacy, Identity Management en het beveiligen van biometrische gegevens. Zo liggen er voorstellen voor *A framework for access management en Access control mechanisms*. Er wordt gewerkt aan een *Privacy framework* en een *Privacy reference architecture*. Met betrekking tot biometrie wordt gewerkt aan een normen voor *Authentication context for biometrics* en *Biometric template protection*. Namens NEN is Philips lid van deze werkgroep.



Bij het maken van normen werken de werkgroepen zoveel mogelijk samen met andere ISO- en IEC-normcommissies en met andere organisaties die standaarden maken op het gebied van informatiebeveiliging. Bij nieuwe normvoorstellen wordt gekeken of bestaande standaarden als uitgangspunt kunnen dienen. Ook wordt nagegaan of er belangrijke standaarden zijn waar in het normdocument rekening mee moet worden gehouden.

Nederlandse inbreng
De leden van de NEN-commissie IT beveiligingstechnieken bepalen gezamenlijk het standpunt van NEN op de normen die internationaal ontwikkeld worden. Dit doen zij door commentaar te leveren op een normtekst en door het stemmen over ratificatie van normen. Organisaties die lid zijn van de normcommissies kunnen experts aanmelden voor de genoemde internationale werkgroepen en hebben zo invloed op de normdocumenten die verschijnen.

Het lidmaatschap van de NEN-commissie staat open voor Nederlandse belanghebbenden. Op het moment zijn de volgende organisaties lid: ABN Amro, Deloitte, Equens, Getronics, IBM, ING Bank, KEMA, KPN, Logica CMG, Ministerie van Economische Zaken, Philips, Rabo Bank, SIDN, TNO Telecom en Urenco. Voor het lidmaatschap van een normcommissie wordt een financiële bijdrage gevraagd waarmee de activiteiten van NEN, ISO, IEC en JTC 1 worden ondersteund.

Tot slot
Het gebruik van informatie technologie blijft toenemen en wordt niet beperkt door nationale grenzen. Om de digitale informatieverwerking in goede én veilige banen te leiden zijn internationale afspraken (normen) nodig. JTC 1/SC 27 zal dan ook een actieve commissie blijven. De NEN-commissie IT beveiligingstechnieken zal de komende jaren deze ontwikkelingen blijven volgen en commentaar leveren op de normvoorstellen, zodat internationale normen ontstaan die zo goed mogelijk aansluiten bij de Nederlandse situatie.

Informatie
Voor informatie over de NEN-commissie kunt u contact opnemen met de secretaris van de commissie: Jan Rietveld, email: jan.rietveld@NEN.nl, telefoonnummer (0156) 269 0376.

- Informatie over de documenten van de normcommissie vindt u via Technical Committees op de ISO-website: *www.iso.org*.
- Informatie over de NEN-commissie vindt u op *http://www.nen.nl/IT-beveiligingstechnieken*
- Sommige ISO/IEC JTC 1/SC 27-normen zijn kosteloos beschikbaar via: *http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm*.
- Geprinte versies van normen kunt u bij *NEN.nl* bestellen.
- Het artikel uit het oktobernummer van 2005 is te downloaden als PDF op de website van PvIB: *https://www.pvib.nl/download/?id=6473719&download=1*.

Is PassWindow wel echt zo veilig als de maker claimt?

Auteur: Andor Demarteau > Andor Demarteau is Security Consultant bij CapGemini en is bereikbaar via andor@nl.linux.org.

In dit artikel introduceert de auteur het authenticatiesysteem PassWindow en verdiept hij zich in de toepasbaarheid en de veiligheid ervan. Maar eerst wordt de achtergrond uitgelegd: wat is nu precies 1, 2 en 3 factor authenticatie en hoe doen we het nu? Daarna gaat Andor Demarteau in op PassWindow en analyseert het verschil tussen het product enerzijds en RSA-tokens en one-time pads anderzijds. Tot slot worden de toepassingsmogelijkheden van PassWindow beschreven.

Factor authenticatie

Je hebt drie verschillende authentiserende factoren nodig voor 3-factor authenticatie: De categorisatie gaat als volgt:

- iets dat je hebt: smartcard, token, PassWindow, et cetera.
- iets dat je weet: passwords, pincodes, andere geheime teksten en combinaties
- iets dat je zelf bent: een biometrisch kenmerk, bijvoorbeeld een vingerafdruk

Wat maakt een 2- of 3-factor authenticatie nu sterker dan één van deze drie factoren op zichzelf? Eén van de basisprincipes in de IT security is hoe meer verschillende gegevens je over iemand hebt en kunt gebruiken om diegene te identificeren, des te zekerder ben je ervan dat hij of zij het ook echt is. Daarop volgt dan de authenticatie van die persoon aan de hand van diezelfde gegevens. Overigens geldt dit ook voor fysieke beveiliging en toegangscontrole. Meer authentiserende gegevens maakt het lastiger voor hackers om in te breken door zich voor te doen als een geautoriseerde gebruiker.

Alleen een wachtwoord of pincode is niet veilig genoeg. Beide kun je aan iedereen vertellen en (wat natuurlijk vaak genoeg gebeurd) opschrijven en ergens onder plakken. Denk maar aan de Post-its onder toetsenborden en bureaus.

Maar wat nu als je naast dat gegeven ook een smartcard nodig hebt? Als je dan je wachtwoord opschrijft en ergens achterlaat, hebben kwaadwillenden er nog niets aan. Ze moeten je ook nog je smartcard afpakken. Het omgekeerde gaat natuurlijk ook op: als je toegang hebt met alleen een badge zonder pincode, dan is het verliezen ervan voldoende voor de vinder om zichzelf toegang te verschaffen. Maar als er ook nog een pincode bij nodig is, dan moet je beide hebben wil je toegang kunnen verkrijgen.

En ja, ik weet dat een aantal lezers nu direct denkt aan het skimmen van bankpassen. Vaak lezen fraudeurs een pincode af door middel van een camera boven het keypad, waarmee ze de toetsaanslagen vastleggen. Een effectieve maatregel om dit te voorkomen is je hand af te dekken met bijvoorbeeld je portemonnee, zodat de camera niet kan zien welke knoppen in welke volgorde worden indrukt. Oké, het is een 'security through obscurity' maatregel, maar het is beter dan niets. Want als het hele apparaat gecompromitteerd is, kun je doen wat je wilt, dan helpt niets.

Iets dat je hebt

Zoals gezegd gaat dit puur om iets dat je bij je hebt (een bezit), waarmee je identificeerbaar bent. Dat kan een toegangsbadge, een paspoort, een nationale ID-card, maar ook een gewone sleutel zijn. Hoewel je met een sleutel bij je eigen voordeur of je auto niet uniek identificeerbaar bent (tenzij het de enige sleutel is), krijg je met die sleutel wel toegang tot je woning of je auto. Letterlijk gezien authenticeer je jezelf als legitieme gebruiker door het slot te openen.
Niet veilig genoeg? Dat klopt, als je wel eens een sleutel bent kwijtgeraakt, weet je daar alles van. Maar een toegangsbadge voor je werk is wat dat betreft net zo onbetrouwbaar als de sleutel van je woning. Dit op zichzelf is dus zeker geen sterke vorm van authenticatie.

Iets dat je weet

Die onbetrouwbaarheid geldt overigens voor alle drie de vormen als je ze op zichzelf staand gebruikt. Maar helemaal voor wachtwoorden! Sommige mensen ruilen hun gebruikersnaam en wachtwoord gewoon in voor een chocoladereep. In een artikel getiteld Passwords revealed by sweet deal, rapporteerde de BBC in april 2004 dat bij een onderzoek onder willekeurige reizigers in Liverpool Street zeventig procent bereid was hun inlog gegevens af te geven in ruil voor een chocoladereep. Erger nog; vierendertig procent gaf de inlog gegevens zelfs zonder het aanbieden van de chocolade af. Puur en alleen doordat de onderzoekers vroegen of hun wachtwoord iets te doen had met huisdieren, achternaam of favoriete voetbalclub.
Hoewel dit artikel ruim vijf jaar oud is, vermoed ik dat er wat dat betreft niet veel is veranderd. Een tweede onderzoek wees uit dat ruim negenenzeventig procent van de ondervraagden ongewild informatie gaf, waarmee identiteitsdiefstal mogelijk is. Tachtig procent van de ondervraagden heeft een hekel aan wachtwoorden en vraagt zich af of het niet anders kan *(bron: http://news.bbc.co.uk/2/hi/technology/3639679.stm)*.

Iets dat je bent

Biometrie, het meten van biologische kenmerken, wordt tegenwoordig veel gezien als dé oplossing voor alle authenticatie

alex_lee2001, via Flickr.com

problemen. De vraag is of dat zo is. Kijk bijvoorbeeld naar vingerafdrukken, een veelgebruikte biometrisch kenmerk dat gevoelig blijkt te zijn voor fraude. Dat werd pijnlijk duidelijk in april 2008 toen het Duitse hackerscollectief, Chaos Computer Club, de vingerafdruk van een minister op een folie meestuurde met het clubblad Datenschleuder. Het was hun protest tegen het opnemen van een vingerafdruk in het nieuwe paspoort, zo valt ondermeer te lezen op de site van Bruce Sneier onder de titel German Minister's Fingerprint Published *(bron: http://www.schneier.com/blog/archives/2008/04/german_minister.html)*.

Daarbij toonde het hackerscollectief twee belangrijke feiten aan:
- vingerafdrukken zijn te gemakkelijk te kopiëren.
- en, nog veel belangrijker, als dat is gebeurd, is het originele biometrische gegeven volledig onbruikbaar geworden voor de rest van het leven van de eigenaar.

Een ander interessant voorbeeld, wat dichter bij huis en ook van vorig jaar, is natuurlijk Albert Heijn met zijn vingerafdrukbetalingssysteem. Ook hier bleek het kinderlijk eenvoudig om de vingerafdruk van deelnemers aan deze vorm van betaling te kopiëren en op hun kosten vervolgens boodschappen te doen. Dat blijkt uit een artikel in het Algemeen Dagblad: AH opgelicht met rubberen vingerafdruk *(bron: http://www.ad.nl/binnenland/2410057/AH_opgelicht_met_rubberen_vingerafdruk.html)*.

En dan nog iets: biometrische gegevens veranderen door de tijd. Ook kleine dingen kunnen invloed hebben. Denk hierbij bijvoorbeeld aan een sneetje in de vinger, waar al dan niet een pleister overheen zit en een verkoudheid die invloed heeft op stemherkenning. Zo zijn er voor bijvoorbeeld irisscans, gezichtsherkenning en andere biometrische kenmerken ook vele veranderingen te bedenken. Toegegeven, een biometrisch kenmerk kun je niet kwijtraken, zoals een badge, of vergeten, zoals een toegangscode. Maar je kunt het wel kwijtraken als betrouwbaar gegeven als het gekopieerd en vervolgens misbruikt wordt.

Dat geldt in hoge mate voor vingerafdrukken. Je laat ze overal achter en daarmee is een vingerafdruk vele malen beroerder als authenticatiemethode dan het geeltje onder het bureau. Irisscans, handprintscans en andere, meer geavanceerde, biometrische methodes zijn navenant ook minder goed te kopiëren en daarmee bruikbaarder. Het nadeel is dat de apparatuur daarvoor weer duurder is en het daardoor niet of nauwelijks wordt gebruikt.

Biometrie is geenszins volledig slecht, kopieerbaar en dus onbruikbaar. Echter; bij gebruik ervan zal heel goed moeten worden gekeken naar de toepasbaarheid, de kosten, de mogelijke afwijkingen in de metingen en kopieerbaarheid van het biometrische gegeven.

Tokens en one-time pads

De meeste tokens zijn eigenlijk een digitale vorm van een one-time pad of OTP. Ze genereren namelijk een pseudorandom combinatie van cijfers of een combinatie van cijfers en letters die je slechts eenmalig kunt gebruiken voor het authenticatieproces.
De meeste tokens, RSA tokens of die van de

PassWindow

Is PassWindow wel echt zo veilig als de maker claimt?

banken, hebben een 2-factor authenticatie. Je hebt het token en een bijbehorende pincode nodig of, voor banken, je pas en pincode omdat die tokens universeel zijn. De voormalige Postbank (inmiddels ING) gebruikte voorheen papieren TANcode lijsten, die konden kwijtraken. Ook hier was een tweede authentiserende factor in de vorm van een wachtwoord nodig. Over de sms'jes van nu; meer dan een challenge/ response systeem is het niet. Het enige dat de bank eigenlijk weet, is dat de persoon die de gsm in handen heeft, de persoon is die de transactie wil doen.

De kracht van OTP zit in de eenmalige geldigheid van de code: mocht je authenticatiepoging in verkeerde handen terechtkomen, dan kunnen die gegevens niet zonder meer misbruikt worden om onrechtmatig toegang te verkrijgen.
Een zogenaamde 'replay attack' noemen is dus niet mogelijk.

De beveiliging van een OTP-systeem berust dus op twee principes: het niet herbruikbaar zijn van de logingegevens en, als een token met 2-factor authenticatie word gebruikt, op de betrouwbaarheid van het apparaat dat de OTP-code genereert.

Wat is PassWindow?
PassWindow is een systeem waarbij een transparant (deel van een) pasje op het beeldscherm wordt gelegd. In dit transparante deel is een 'onzichtbaar' patroon geprint. Doordat er op het scherm ook een patroon wordt getoond dat elke keer anders is, komt er in het transparante deel van het pasje een vier- tot zescijferige code tevoorschijn. Deze code kan voor online authenticatie worden gebruikt, bijvoorbeeld bij het online betalen met een creditcard.

Voordelen
De Australiër Matthew Walker bedacht PassWindow uit frustratie met alle moeilijke, dure en technische oplossingen, die wij als security professionals kennen. De basis voor zijn drive om een ander systeem te bedenken, kwam vooral voort uit het feit dat hij slachtoffer is geweest van online creditcardfraude. De afgelopen twee jaar is hij bezig geweest deze oplossing voor online authenticatie uit te werken. Volgens Walker's site (www.passwindow.com) is zijn systeem de beste oplossing voor online authenticatie.

De belangrijkste voordelen volgens hem:
- beveiliging tegen keyloggers en phishing-aanvallen, het systeem bereikt dat op dezelfde wijze als een OTP-systeem dat doet.
- gebruikers hoeven geen wachtwoorden meer te onthouden.
- beveiliging tegen social engineering, omdat het patroon niet via mail of telefoon overdraagbaar is.
- het is gemakkelijk patronen te vervangen bij verlies of diefstal, onder andere per post of per mail.
- de kaart is veilig in je portemonnee in plaats van een token die in het zicht aan een sleutelbos hangt.
- het is veiliger dan een sms omdat de patronen via SSL worden verzonden en niet over de onbetrouwbare lijnen van derden.

Op zijn site geeft hij er nog meer voordelen, maar voor dit artikel zijn dit de meest belangrijke punten. Andere voordelen, zoals de prijs van het systeem en het feit dat er geen cryptografie wordt gebruikt, wat weleens handig zou kunnen zijn in verband met bepaalde internationale wetgeving, zijn natuurlijk waar, maar zeggen niet zoveel over de beveiligingswaarde van het systeem. Cryptografie natuurlijk wel, maar niet vanwege de reden die de site opgeeft. Hoewel er dan wel weer SSL wordt gebruikt voor de verbinding. Wat verder opvalt, is dat de punten over social engineering en het makkelijk vervangbaar zijn van patronen elkaar tegenspreken.

PassWindow versus tokens
Ten opzichte van tokens heeft Walker eigenlijk maar één belangrijk voordeel: PassWindow is goedkoper en makkelijker te vervangen. Zeker als je gebruikers op afstand hun nieuwe patroon zelf laat printen en op de kaart laat plakken. Maar juist dat punt geeft ook een probleem: e-mail is nu niet bepaald het meest veilige

communicatiemiddel. En als je voor de e-mail optie kiest, dan is Walkers anti-phishing argument ook meteen om zeep geholpen.

Inderdaad, als je het goed doet zou SSL veiliger moeten zijn dan een sms-bericht. Aan de andere kant: sms een OTP, gebruik die eenmalig en je hebt in essentie hetzelfde bereikt.
En als je gebruikers inderdaad hun hardware token in het zicht aan hun sleutelbos laat dragen, dan ben je als bedrijf op het gebied van security awareness toch iets te kort geschoten. Maar grote kans dit soort gebruikers hun PassWindow pasje ook zo naast hun laptop leggen of in hun borstzakje stoppen, want elke keer die portemonnee opvissen en het pasje eruit halen en terugstoppen is ook zo'n gedoe.

In principe is er maar één reden waarom PassWindow nooit een vervanger van de token kan zijn: 1- versus 2-factor authenticatie. De PassWindow oplossing valt slechts in de categorie 'iets dat je hebt', terwijl tokens ook nog een pincode hebben en dus in de categorie 'iets dat je weet' zijn onder te brengen. Kortom; security technisch gezien is een token met pincode gewoonweg veiliger dan PassWindow.

PassWindow, waneer dan wel?
Maar is PassWindow dan onbruikbaar? Nee, dat niet. Als onderdeel van de categorie 'iets dat je hebt' is het zeker een revolutionaire en unieke oplossing, waar bijvoorbeeld de ING zijn voordeel mee zou kunnen doen als vervanger van die tancodelijsten of sms'jes.
Verder is het overduidelijk waar deze oplossing een flinke meerwaarde zal bieden. Namelijk precies op het gebied waar die frustratie van Walker is ontstaan: het voorkomen van creditcardfraude op internet. Huidige creditcards hebben een extra code op de achterkant ter verificatie dat je de echte kaarthouder bent. Helaas vragen tegenwoordig vrijwel alle online winkels die creditcards accepteren om deze code. Hiermee is het veiligheidsaspect waarvoor die code was ingevoerd volledig teniet gedaan, aangezien de winkelier nu het creditcardnummer plus verificatiecode heeft.

Als je de kaart zou uitrusten met een PassWindow die deze verificatiecode vervangt, heb je dat probleem simpel, efficiënt en goedkoop opgelost. Enige nadeel is dat bij elke transactie de online winkel aan de creditcardmaatschappij een patroon moet opvragen waarbij de kaarthouder zich kan identificeren als de legitieme eigenaar ervan (of in ieder geval diegene die de fysieke kaart op dat moment heeft). Maar aangezien er toch een verificatiestap wordt gedaan voordat de transactie door de online shop wordt goedgekeurd, is dat slechts trivaal.

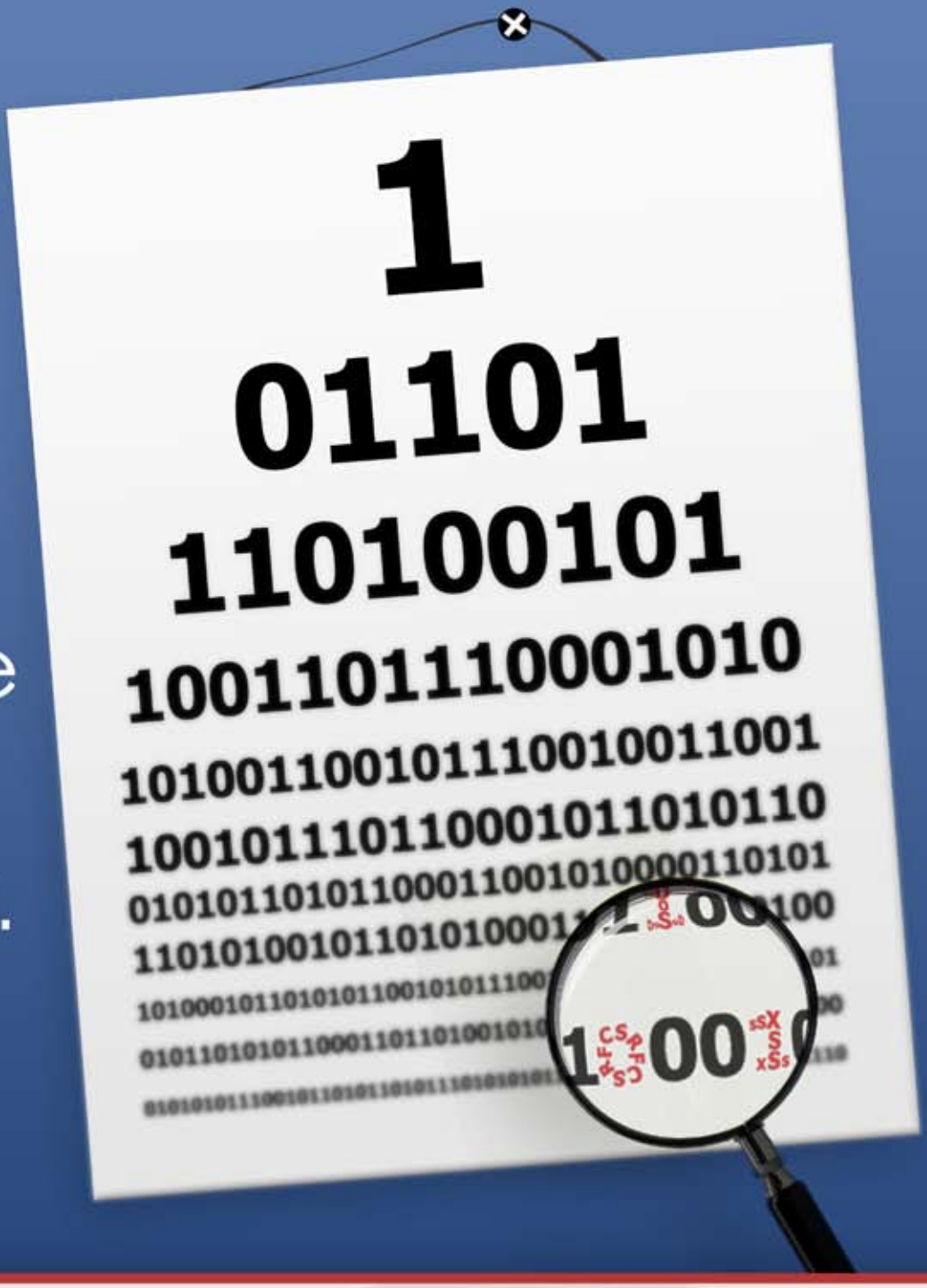
Grote creditcardgegevens diefstal, zoals die van meer dan honderddertig miljoen kaarten *(bron: http://news.bbc.co.uk/2/hi/americas/8206305.stm)*, zijn daarmee redelijk nutteloos geworden. Zonder de fysieke kaart en dus het PassWindow, waarmee de verificatiecode gegenereerd wordt, is het kaartnummer en de vervaldatum niet meer voldoende voor gebruik. Dit moet dan wel altijd en bij elke transactie gebruikt worden.

Eén van de andere punten die de maker aangeeft, namelijk ter vervanging van security vragen op sites als je je password vergeten bent, is eveneens een relevante toepassing. Het enige nadeel is wel dat je voor elke site een unieke en separate pas moet hebben met dat patroon erop. Dat werkt pas echt als een initiatief als OpenID (een unieke online ID per persoon, dat bruikbaar is voor alle daarbij aangesloten sites) echt van de grond komt.

PassWindow mark II
Een inherente zwakheid van dit systeem zal echter altijd het statische patroon blijven dat op de kaart zit. Je kunt dit vervangen natuurlijk, wat vooral per e-mail onveilig is, maar het blijft een kritiek punt. Hoe zouden we dit kunnen oplossen zonder het systeem te duur, te onhandig en gewoon weer een token te maken? Meest ideaal is dat ook het patroon op de pas wijzigt per transactie. Dat kan door een nieuw patroon op basis van tijd en een basispatroon te genereren. Dan ben je ook direct af van het (foto)kopiëren van de kaart en heb je elke keer een unieke oplossing. De kaart heeft dan natuurlijk wel een chip nodig. Nu hebben de meeste smartcards die tegenwoordig al, dus ook dat is niet echt een beperkende factor. Maar hoe de chip van stroom te voorzien, is wel een struikelpunt. De techniek staat nog in de kinderschoenen, maar er zijn ontwikkelingen gaande, waarmee stroom uit de radiogolven van wifi-accesspoints gegenereerd kan worden. En aangezien de meeste gadgets tegenwoordig zowel wifi, als bluetooth hebben en er weinig stroom nodig is, lijkt dit een goede oplossing voor de toekomst. Dat we daarmee het internet weer een stuk visueler maken en een deel van onze bevolking daarmee wederom een stap achteruit doet (inclusief mijzelf), daar gaat dit artikel niet over.

Conclusie
PassWindow is een uniek en nuttig systeem, maar vooral voor beperkt gebruik, waarbij een zwakkere vorm van authenticatie voldoet. Voor vervanging van authenticatie voor systemen waar nu tokens worden gebruikt met een pincode, of generieke met een smartcard met pincode, is het geen oplossing. Als je echter een oplossing zoekt om je huidige OTP-systeem op basis van lijsten of sms-berichten te vervangen, dan is PassWindow een goede keuze.
Het is en blijft echter een 1-factor authenticatie en als je het voor 2-factor wilt gebruiken, zal er altijd een wachtwoord, een pincode of een ander te onthouden gegeven aan moeten worden toegevoegd. Of biometrie natuurlijk: Albert Heijn zou de vingerafdrukbetalingen al een stuk veiliger kunnen maken door niet alleen de vingerafdruk te gebruiken, maar tegelijkertijd een PassWindow in de bonuskaart als extra authenticatie.

What you can't see **CAN** hurt you.



CODEFEND™, the unique fusion of leading technologies with human expertise is an innovative, ***outsourced Security Code Review Service***.

Flexible. Accurate. Efficient.

Incorporate **CODE**FEND™ into your software development lifecycle.

A Service by

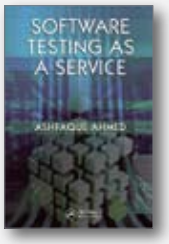
COMSEC Consulting
Information Security

CODEFEND™
Your Software SECURED.

Comsec Consulting BV | www.codefend.com www.comsecglobal.com | Tel: +31-10-2881010 | info@comsecglobal.com

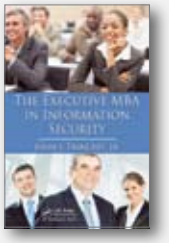
InZicht

Over deze rubriek > InZicht geeft een overzicht van recent verschenen en te verschijnen boeken en whitepapers in binnen- en buitenland, geselecteerd door de redactie. Onze bronnen voor de toelichting bestaan uit persberichten en internet, niet gegarandeerd onafhankelijke informatie. Actualiteit staat bij de inhoud van deze rubriek voorop.



Software Testing as a Service
Auteur: Ashfaque Ahmed
ISBN: 9781420099560
Uitgever: CRC Press
Druk: 1e druk, september 2009
Vorm: Hardback, 228 blz, Engels

In today's unforgiving business environment where customers demand zero defect software at lower costs - it is testing that provides the opportunity for software companies to separate themselves from the competition. Providing a fresh perspective on this increasingly important function, Software Testing as a Service explains, in simple language, how to use software testing to improve productivity, reduce time to market, and reduce costly errors.
The book explains how the normal functions of manufacturing can be applied to commoditize the software testing service to achieve consistent quality across all software projects. This up-to-date reference reviews different software testing tools, techniques, and practices and provides succinct guidance on how to estimate costs, allocate resources, and make competitive bids.



The Executive MBA in Information Security
Auteur: John J. Trinckes Jr.
ISBN: 978-1-4398-1007-1
Uitgever: CRC Press
Druk: 1e druk, september 2009
Vorm: Hardback, 352 blz, Engels

The Executive MBA in Information Security provides the tools needed to ensure your organization has an effective and up-to-date information security management program in place. This one-stop resource provides a ready-to use security framework you can use to develop workable programs and includes proven tips for avoiding common pitfalls - so you can get it right the first time.
Presenting difficult concepts in a straightforward manner, this concise guide allows you to get up to speed, quickly and easily, on what it takes to develop a rock-solid information security management program that is as flexible as it is secure.

Beautiful Security
Editors: John Viega, Andy Oram
ISBN: 978-0-596-52748-8
Uitgever: O'Reilly Media
Druk: 1e druk, april 2009
Vorm: Paperback & Ebook, 304 blz, Engels

In Beautiful Security, today's security experts offer a collection of essays that describe bold and extraordinary methods to secure computer systems in the face of ever-increasing threats. You'll learn how new and more aggressive security measures work - and where they will lead us. This far-reaching discussion takes you into the techniques, technology, ethics, and laws at the center of the biggest revolution in the history of network security.

Beautiful Security explores this challenging subject with insightful essays and analysis on topics that include:

- The underground economy for personal information: how it works, the relationships among criminals, and some of the new ways they pounce on their prey
- How social networking, cloud computing, and other popular trends help or hurt our online security
- How metrics, requirements gathering, design, and law can take security to a higher level
- The real, little-publicized history of PGP

The Myths of Security
Author: John Viega
ISBN: 978-0-596-52302-2
Uitgever: O'Reilly Media
Druk: 1e druk, juni 2009
Vorm: Paperback & Ebook, 264 blz, Engels

If you think computer security has improved in recent years, Myths of Security will shake you out of your complacency. Longtime security professional John Viega reports on the sorry state of security, with concrete suggestions for professionals and individuals confronting the issue.

Why is security so bad? Attacks are sophisticated, subtle, and harder to detect than ever. But, as Viega notes, few people take the time to understand the situation and protect themselves accordingly. This book tells you:

- Why it's easier for bad guys to 'own' your computer than you think
- Why anti-virus software doesn't work well - and one simple way to fix it
- Whether Apple OS X is more secure than Windows
- What Windows needs to do better
- How to make strong authentication pervasive
- Why patch management is so bad
- Whether there's anything you can do about identity theft
- Five easy steps for fixing application security, and more

The Myths of Security not only addresses IT professionals who deal with security issues, but also speaks to Mac and PC users who spend time online.

Continuïteit as a service

Auteur: André Koot > André Koot is werkzaam als informatiemanager bij Univé-VGZ-IZA-Trias en is hoofdredacteur van dit blad. Hij is bereikbaar via a.koot@unive.nl

Tegenwoordig is alles AAS: software, infrastructuur, platform, security, identity, storage. Steeds meer traditionele IT-zaken raken buiten zicht, we zijn steeds meer 'in de wolken'. Wat overblijft van het oude IT-vak is het bedenken en beheren van nieuwe dingen die nog niet in de wolk zijn opgenomen. Dat is geen fictie: steeds meer bedrijven gaan ertoe over hun legacy over te brengen naar de cloud. Maar er komen ook meer en meer 'niet legacy'-processen, denk aan HRM- en CRM-processen, die zich binnen de cloud afspelen. De cloud doet me een beetje denken aan die oude Blob, die science fictionfilm, die met de cloud werkelijkheid is worden. De cloud raakt zo alom aanwezig dat het ons leven steeds meer gaat beheersen en, geef toe, dat vinden we spannend, eng en leuk tegelijkertijd. Maar: hoe groter de geest, hoe groter het beest. Als alles in de cloud verdwijnt, hoe weten we dan dat alles wel goed gaat? In deze alom tegenwoordige mist is het zicht verdwenen.

De kritische lezer zal ons echter voorhouden dat er niets nieuws is onder de zon. Cloud computing is niets anders dan wat we vroeger ASP of Grid computing noemden en daarmee konden we redelijk goed uit de voeten. Feitelijk is clouden een vorm van outsourcing en daarmee hebben we op heel veel fronten al ervaring, zowel technisch als functioneel. We weten alles van het definiëren van eisen, het in contracten afdekken van risico's en het voorbehouden van het recht op audit. We blijven in control. Dat is wat mij betreft echter een al te simpele voorstelling van de problematiek, een iets te eenzijdige kijk op de cloud. Er is meer met de cloud aan de hand.

Laten we wel een onderscheid maken tussen de cloud en de cloud. Niet alles is even ondoorzichtig. Er bestaan zonder meer varianten die heel dicht aanliggen tegen de reguliere ASP- of outsourcingsoplossingen. Als je een afspraak maakt met een provider om specifieke services over te nemen, dan is dat gewoon outsourcing, Niet via huurlijnen, maar via het internet en dat is niet heel spannend. Het wordt eigenlijk pas spannend als de provider datzelfde ook gaat doen voor anderen en als die provider zelf weer diensten gaat afnemen van andere cloudproviders. En dat is helemaal geen unicum meer. Er zijn al CRM-providers die CRM-services aanbieden, die ze dan weer laten draaien op ergens in de cloud gehoste platforms. Denk maar aan Amazon's Elastic Comput (EC2). En wie weet waar het echte ijzer staat? Het lijkt zo simpel; gewoon een CRM-dienst afnemen en krijgen, maar wat er eigenlijk alleen nog specifiek is, is de factuur.

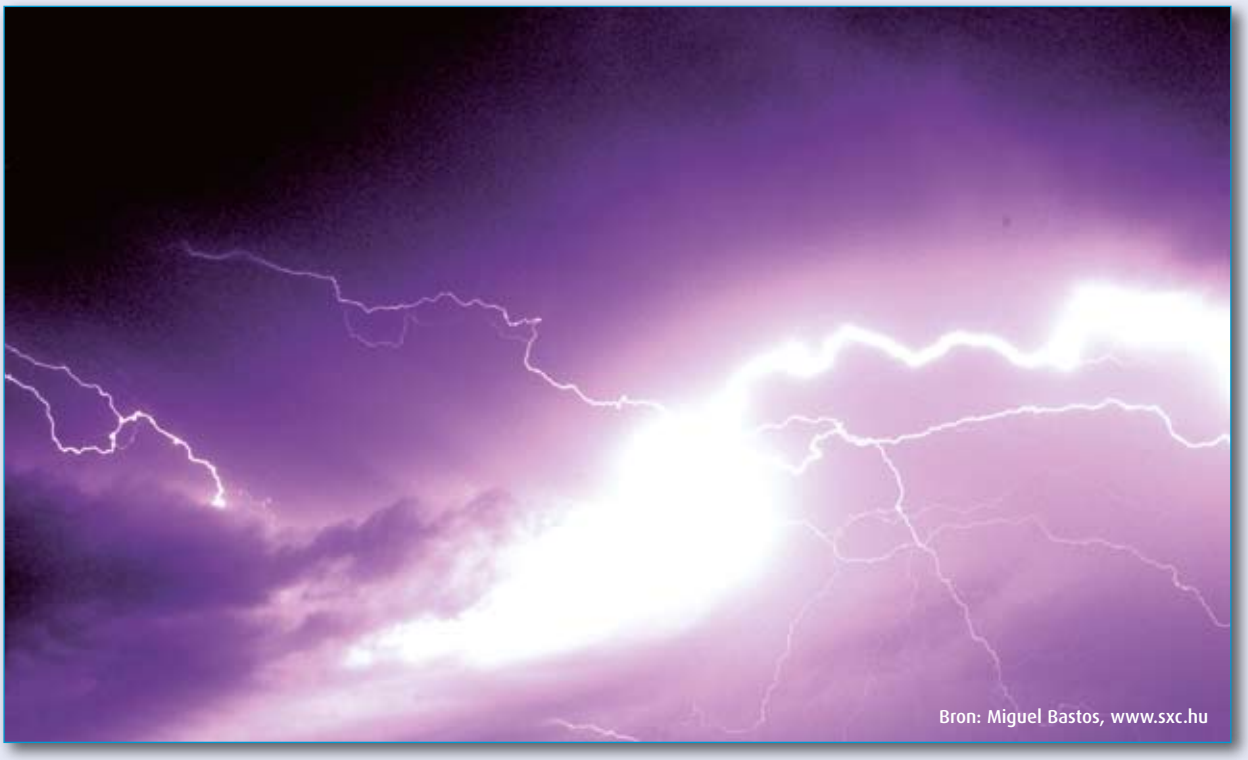
We kunnen voor een dergelijke casus meteen al legio security gerelateerde vragen stellen. Hoe zit het met de privacy, met de access control, met het change management van de applicatie, met het beheer? Gelukkig zijn de meeste van dergelijke vragen vergelijkbaar met de traditionele outsourcingsomgevingen. De meeste van de problemen worden in de reguliere contracten afgehandeld. Afspraken rondom ISO-certificeringen, audits, TPM's en SAS70's zijn gemeengoed.

Maar de kern van de AAS is nu juist dat de contractpartner niet in alle gevallen de partij is die feitelijk die dienst levert. Dat kun je in contracten wel proberen af te dekken, maar feit is dat AAS in is omdat door de structuur van de cloud de prijs/prestatieverhouding in orde is. Extra waarborgen eisen is strijdig met de mogelijkheid van hergebruik die de productiviteit ten goede komt. Het onderaannemerschap dat we in diverse traditionele bedrijfstakken kennen, bestaat niet in de cloud. Als de ene ijzeraanbieder te duur is, dan verplaatsen we de virtuele platforms toch gewoon naar een andere? Dat betekent dat we slachtoffer worden van de willekeur van onze providers.

Even terug naar de risico's. De meeste risico's zijn redelijk in beeld. Met autorisaties, toegangscontroles en audits kunnen we betrekkelijk eenvoudig inzicht krijgen in de problemen. Er is inmiddels heel wat informatie over security in de cloud (ik heb in een vorig nummer wat links gegeven). Maar een groep risico's is eigenlijk helemaal niet inzichtelijk, namelijk de risico's op het gebied van continuïteit. De cloud is in sommige gevallen een oplossing voor continuïteit. We hebben het immers over gevirtualiseerde, op webservices gebaseerde omgevingen die via het internet toegankelijk zijn. Dat betekent achtereenvolgens dat de beschikbaarheid van ijzer geen probleem is (gewoon verplaatsen van images), dat schaalbaarheid een kwestie is van meer ijzer en dat de beschikbaarheid van het internet de grens is van de bereikbaarheid van de dienst. Allemaal prima. Maar de cloud is niet zomaar een oplossing voor continuïteit. Er spelen specifieke problemen en daarvoor zijn nog niet altijd oplossingen voorzien. Sterker nog; partijen als Gartner hebben geen pasklaar advies.

Even kort enkele specifieke cloud-gerelateerde continuïteitsproblemen en oplossingsrichtingen. Hierbij wil ik wel aanmerken dat dit geen wetenschappelijk verantwoorde opsomming is. Het is verbazingwekkend hoe weinig er geschreven is over cloud (SAAS) en BCM.

- De serviceprovider valt weg: gewoon contractueel afhandelen, net als ASP en outsourcing toch?
  Helaas. Bij ASP en outsourcing is meestal bekend wat het onderliggende applicatielandschap is en hoe de onderliggende gegevensmodellen eruit zien. Je kunt periodiek bijvoorbeeld een dump van de omgeving en de gegevens maken en zelf het landschap herbouwen. Dat is niet zo



Bron: Miguel Bastos, www.sxc.hu

bij SAAS. Als de provider wegvalt, zou al die kennis ook wel eens kunnen wegvallen. Modellen en datastructuren zijn van de SAAS provider en daar kun je niets mee als de provider wegvalt. De minimale oplossing is het periodiek dumpen van gegevens (zowel de transacties als de beheerdata en logging) in een verstaanbaar formaat. Neem dit op in het contract. Een alternatieve maatregel is Escrow, maar ja, de changes op SAAS-applicaties kunnen zich wel eens heel frequent afspelen. Escrow is er nog niet als een service, een gat in de markt, dunkt me. Gartner vindt het een interessant idee om de provider te vragen om de applicatiecode vrij te geven als open source software, maar de vraag is of een provider zijn business zo wil publiceren. Het valt te proberen... Alternatief is de contractuele overeenkomst waarbij je zelf het recht hebt om de applicatie in huis te draaien in het geval van een calamiteit bij de cloud-provider.

- Niet de SAAS-serviceprovider, maar de onderliggende infrastructuur of de platformleverancier valt weg.
  Mag je uitgaan van de traditionele onderaannemerschapsrelaties? Is het genoeg om de SAAS-provider contractueel aan te spreken? Nee, dat kost veel te veel tijd. In het cloud-tijdperk moeten we ook cloud-maatregelen treffen. Het zekerstellen van data en code is wel vitaal, maar daarbij moet minimaal contractueel geregeld worden dat er een uitwijk vanwege de SAAS-provider kan plaatsvinden. Het is niet voldoende om bij niet-beschikbaarheid de SAAS-provider aan te spreken, het uitwijken door de SAAS provider moet als preventieve maatregel meegenomen worden.

- Wat is een incident of een calamiteit op grond waarvan je aanspraak op de contractvoorwaarden kunt maken? Definieer dat vooraf in het contract.

- Dat je als organisatie altijd in staat moet zijn de eigen applicatie te kunnen benaderen, is evident. Zorg dan ook voor bereikbaarheid van het internet (en dus jouw cloud-omgeving) voor de eigen medewerkers. Beschikbaarheid is niet duur, maar zorg er wel voor dat de medewerkers bij de cloud-omgevingen terecht kunnen. Alternatieven als toegang via UMTS-achtige kanalen zouden overwogen moeten worden.

- Beschikbaarheid buiten het reguliere netwerk om betekent niet alleen technische maatregelen, maar ook functionele. En dat brengt wel een beheerlast met zich mee, want identiteitenbeheer is in de cloud minstens zo belangrijk als in de fysieke wereld. Federatie en Identity 2.0 kunnen wel eens heel belangrijk gaan worden.

- Dat laatste geeft wel meteen aanleiding om ervoor te waken dat SAAS-oplossingen ingebed zijn in de eigen keten van bedrijfsprocessen. Als zo'n SAAS-proces instort, zou de hele keten wel eens kunnen falen. Het is om meer dan één reden zinvol om niet te integreren: tot op de dag van vandaag zijn er eigenlijk nog geen industriestandaarden waardoor je delen van bedrijfsprocessen kunt verleggen naar de cloud. Tot nog toe zijn cloud-processen point solutions. Vanuit de optiek van continuïteit is dat misschien maar beter ook.

- En natuurlijk gelden nog steeds de standaard beheersmaatregelen, zeker bij cloud-applicaties. Denk aan degelijke inkoopvoorwaarden, het uitvoeren van penetratietests en het overleggen van SAS70 type 2 verklaringen.

  De onzekerheid rondom continuïteit is op dit moment groot. De vraag is dan ook of het voor bedrijfskritische toepassingen verstandig is om nu in de cloud te stappen. Een afweging rondom de continuïteitsrisico's en -waarborgen vooraf lijkt dan ook zinvol. De hier bovenstaande aandachtspunten zouden bij de overweging een rol moeten spelen.

Browser plugins

Auteur: Maarten Hartsuijker > Maarten Hartsuijker is Security Officer bij de ANWB, business consultant bij het Competence Center Security van Getronics en helpt organisaties vanuit zijn bedrijf Classity Informatiebeveiliging met veelzijdige beveiligingsvraagstukken en audits. Maarten is te bereiken via pvib@classity.nl.

De afgelopen maanden zijn we veelvuldig geconfronteerd met kwetsbaarheden in browser plugins. In dit artikel een korte statusupdate.

Van DOS-box naar browser

Wie de werkplek van eind jaren negentig vergelijkt met de werkplek van nu, moet de verschillen zijn opgevallen. DOS-boxen en terminal emulatoren zijn een uitstervend ras geworden, verdrongen door de alles kunnende browser. En de mogelijkheden van browsers blijven toenemen. Applicaties worden steeds verder verrijkt en we bieden ze het liefst vanaf een centraal platform aan. Want waarom zou je de moeite doen applicaties naar clients te distribueren, als je ze ook op een high-availability server pool kunt installeren en onderhouden? Ontsloten via een webinterface die werkplekken anyplace en anytime kunnen benaderen.

Alhoewel dit alles mooi klinkt, is er ook een schaduwzijde aan deze ontwikkeling. Om alle verschillende soorten, centraal gepubliceerde, applicaties te kunnen verwerken, is de werkplek inmiddels een verzamelbak voor interpreteer-programmatuur geworden. We hebben Quicktime nodig voor filmpje X, Windows Media Player voor filmpje Y. We gebruiken een Java runtime omgeving om webstart of Java-archiefapplicaties op te starten. Veel websites maken inmiddels gebruik van Flash voor een gelikte user-experience en alsof dat nog niet genoeg is, probeert Microsoft met Silverlight de markt te veroveren. Open je in een website een presentatie of een PDF-bestand, dan verwacht je als gebruiker dat de noodzakelijke Acrobat Reader en office componenten de documenten direct aan je tonen.

Het benaderen van webapplicaties met een browser klinkt dus eenvoudig, maar voor een juiste werking ervan is er op de werkplek vaak een omvangrijke selectie aan plugins nodig. Deze plugins moeten over het algemeen aanvullend geïnstalleerd worden. En hoewel de verschillende wormen, virussen en trojans ons de afgelopen jaren hebben geleerd om onze werkplekken beter te beschermen, beperkt deze bescherming zich vaak tot een antivirus-pakket en een WSUS-server[1]. De installatie van beveiligingsupdates van plugins is over het algemeen afhankelijk van het opnieuw bouwen en distribueren van een softwarepakket. Of de updates worden overgelaten aan de gebruiker, die onderin zijn scherm er aan wordt herinnerd dat er een update beschikbaar is (maar dat het niet verplicht is om deze te downloaden en te installeren). Doordat organisaties, wat betreft de beveiligingsupdates van browser plugins (en andere cliëntsoftware), vaak nog niet voldoende 'in control' zijn, is de software afgelopen jaren een geliefd aanvalsobject geworden.

Wat betekent dit concreet? Hieronder volgen een aantal voorbeelden van het risico dat je met het niet wegnemen van de kwetsbaarheden als organisatie loopt.

Adobe Flash Player

Een klein jaar geleden werd er op grote schaal misbruik gemaakt van een kwetsbaarheid in de Adobe Flash Player. Hackers besmetten tienduizenden websites met scripts die de bezoekers van de websites doorstuurden naar een webpagina waarop

1. *WSUS is een voorziening waarmee (security) updates van Microsoft-producten kunnen worden gecontroleerd, gepland, gedistribueerd en geïnstalleerd.*

een flash-object was geplaatst. Als de werkplek van de gebruiker een oude flash player bevatte, dan werd er automatisch een programma geïnstalleerd op de werkplek. Hackers konden hierdoor dezelfde rechten krijgen als de eigenaar van de pc en daarmee de pc overnemen.

Maatregelen

Als gebruikers voor hun werk geen flash nodig hebben en geen administrator-rechten op hun werkplek hebben, is het verstandig de werkplekken niet van deze browser-plugin te voorzien. Is flash noodzakelijk? Zorg er dan voor dat werkplekbeheerders de updates voor deze software in de gaten houden en tijdig over de werkplekken verspreiden.

Welke versie is er op mijn werkplek actief?

Bedrijven die een software inventory oplossing hebben, kunnen hierin de op de werkplekken geïnstalleerde versies opzoeken. Is een dergelijke oplossing niet voor handen? Kijk dan op *http://www.classity.nl/check-flash-version.html*.

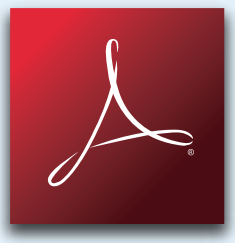
Adobe Acrobat Reader

Van medio 2008 tot eind 2008 constateerde Microsoft een enorme toename in misbruik van de Acrobat Reader. Ook dit jaar blijft dit product niet buiten schot. Eind maart bracht Adobe een beveiligingsupdate voor de software uit. De betreffende fout werd op dat moment op internet al weken actief misbruikt. Dit concept herhaalde zich in oktober 2009, toen Acrobat ruim een week voordat Adobe zijn beveiligingsupdates had gepland weer actief werd aangevallen. Net

als de fout in Flash kunnen ook deze fouten ertoe leiden dat, zonder enige gebruikersinteractie, een hacker op een werkplek inbreekt. Door een kwaadaardig PDF-bestand in een website te verwerken (embedden) raakt een werkplek van een gebruiker, die toevallig op de verkeerde website terechtkomt, besmet. Ook het openen van een via e-mail verspreid PDF-bestand kan tot een gecompromitteerde werkplek leiden.

Maatregelen

Doordat hackers er vaak in slagen om hele gewone websites van kwaadaardige PDF-bestanden te voorzien (bijvoorbeeld door programmeerfouten in een UGC-interface[2] of kwetsbare CMS-software[3]), is het erg lastig om gebruikers te instrueren over websites die wel of niet veilig zijn. De oplossing moet dus voortkomen uit een goede technische ondersteuning. Het verwijderen van PDF-software is door de grote acceptatie van het PDF-documentformaat over het algemeen geen optie. Overstappen naar een andere 'reader' kan tijdelijk helpen, maar is resource-intensief en vaak op termijn niet effectief omdat ook in deze software fouten geconstateerd kunnen worden. Antivirus-programmatuur op de gateway en/of de client helpt vaak deels:



helaas blijven virusprogramma's door hackers te gemakkelijk te misleiden. Het (tijdelijk) blokkeren van PDF-bestanden afkomstig van internet kan de dreiging doen afnemen, maar is erg gebruikersonvriendelijk. Daarnaast voorkom je er over het algemeen niet mee dat er over versleutelde kanalen alsnog een kwaadaardig bestand doorglipt. Het meest effectief is ook hier om werkplekbeheerders in staat te stellen snel nieuwe updates over werkplekken uit te rollen.

Welke versie is er op mijn werkplek actief?

Bedrijven die een software inventory oplossing hebben, kunnen hierin de op de werkplekken geïnstalleerde versies opzoeken. Is een dergelijke oplossing niet voor handen? Kijk dan op *http://www.classity.nl/check-acrobat-reader-version.html*.

Java Runtime Environment

De Java Runtime Environment (JRE) is een browser plugin die gebruikers in staat stelt centraal aangeboden programmatuur op de eigen werkplek uit te voeren. Lang werd verondersteld dat de sandbox van de JRE deze onkwetsbaar maakte voor beveiligingsfouten. Helaas is de afgelopen jaren het tegendeel bewezen en vormt ook de JRE een aanzienlijk risico voor de betrouwbaarheid van werkplekken met een internetverbinding. Momenteel ondersteunt Sun de JRE versies 1.5 en 1.6. Maar ook versie 1.4 is vanwege de ondersteuning van legacy applicaties bij bedrijven vaak nog in gebruik. Eind maart 2009 werden er niet minder dan zestien beveiligingsfouten in JRE 1.4, 1.5 en 1.6 bekend. Voor de versies

2. *User Generated Content: een onderdeel van een website waar gebruikers zelf website-content kunnen plaatsen. Hackers struinen het internet af naar dit soort websiteonderdelen, in de hoop er kwaadaardige content te kunnen plaatsen.*
3. *Content Management Systeem: de schil om de website heen, van waaruit berichten in de website worden geplaatst.*

Your Player Version:	WIN 10,0,32,18
Debug Player:	No
Operating System:	Windows Vista
Video Capable:	Yes
Audio Capable:	Yes
Local File I/O Enabled:	Yes

1.5 en 1.6 kwamen updates beschikbaar, maar omdat versie 1.4 in december end-of-life is verklaard, wordt deze verouderde JRE alleen nog tegen betaling geactualiseerd. Gevolg: alle gebruikers die een Java web-start applicatie vanaf internet starten (in een 'jnlp' webstart-bestand kan een hacker aangeven welke JRE hij voor het starten wil gebruiken) of in hun browser een oude Java plugin hebben geactiveerd, zijn kwetsbaar voor diverse security fouten. Voor een deel van de zestien fouten zijn al proof-of-concept exploits geschreven, waarmee wederom via het bezoeken van een kwaadaardige website de werkplek op het bedrijfsnetwerk door een hacker op internet kan worden overgenomen.

Maatregelen

Omdat veel bedrijven nog oude Java-software gebruiken, heeft Sun geprobeerd om de beveiliging van Java, in combinatie met de webbrowser, aan te scherpen. Browsers met een recente Java-versie, zullen ook standaard deze recente versie gebruiken. Staat er dus een JRE 1.4.2_19 en een JRE 1.6.0_17 op de werkplek, dan start de browser versie 1.6.0_17. Omdat er echter applicaties zijn die via de browser werken maar alleen JRE 1.4.2_xx ondersteunen, heeft Sun een functie moeten maken die de browser ertoe dwingt een oudere Java versie te gebruiken. Deze functie (die met zogenoemde CLSID's werkt) is functioneel een uitkomst, maar voor hackers geldt natuurlijk hetzelfde. Als ze een grotere kans willen hebben dat ze succesvol een kwetsbaarheid kunnen misbruiken (exploiteren), dan forceren ze dit door het CLSID van de Java 1.4.2 of 1.5 familie op te geven dat hun kwaadaardige applet met de oude software wordt gestart. Het is dus aan te raden om CLSID's die naar kwetsbare Java versies verwijzen uit de browserconfiguratie te halen en alleen de Java-versie die van de laatste beveiligingsupdates is voorzien aan de browser te koppelen.

Daarnaast kan op centrale proxy servers vaak worden ingesteld dat het ophalen van JAR-, JNLP- of CLASS-bestanden van willekeurige internetpagina's niet is toegestaan. Specifieke, 'vertrouwde' sites kunnen eventueel in een uitzonderingslijst worden opgenomen.

Welke Java-versies gebruikt mijn browser?

Door met een werkplek naar *http://www.classity.nl/check-java-version.html* te browsen, kan worden opgevraagd welke Java-versie een hacker vanuit een website kan oproepen. Oplossingen zoals de Corporate Software Inspector van Secunia kunnen systeembeheerders binnen omvangrijke bedrijfsomgevingen inzicht geven in de gebruikte software versies.

Vergelijkbare problematiek

De drie hierboven beschreven dreigingen staan niet op zichzelf. Fouten in programmatuur als Word, Excel, Powerpoint, Quicktime, Windows Media Player en Silverlight kunnen tot vergelijkbare problemen leiden. En voor programmatuur die niet direct vanuit de browser aangesproken kan worden, maar wel bestanden opent die via e-mail of een USB-stick de werkplek bereiken (WinRar, Winzip, Winamp, iTunes, et cetera) geldt het beschreven scenario in mindere mate uiteraard ook.

Misbruik in ontwikkeling

Waar we in het verleden zagen dat hackers vooral inbraken op werkplekken door misbruik te maken van fouten in het besturingssysteem, zien we op dit moment dat inbraken via applicaties die content tonen enorm aan het toenemen is. De statistieken uit het laatste Microsoft security intelligence rapport[4] geven hier ook een goed beeld van. De oorzaak van deze verschuiving zit ongetwijfeld in het feit dat we als organisaties inmiddels redelijk in staat zijn om ons besturingssysteem van updates te voorzien. De noodzaak om dit proces te optimaliseren, is de afgelopen jaren bijna overal wel naar voren gekomen. Aan eenieder de uitdaging om de focus de komende jaren te verbreden richting applicaties.

Met name voor organisaties die erg incident gedreven zijn, is dit geen gemakkelijke opgave. Daar waar een leverancier als Microsoft het framework meelevert om al haar software vanaf één plek te onderhouden (en waar we ons dus grotendeels achter een technische oplossing kunnen verschuilen), is een oplossing voor andere softwarepakketten minder vanzelfsprekend. Alhoewel Firefox inmiddels besloten heeft om ook de plugins mee te nemen in het softwareonderhoud, is dit bij andere browsers nog niet het geval. Bedrijven met Internet Explorer blijven in hun gevecht tegen kwetsbare software dus afhankelijk van een procesmatige aanpak. Het continu detecteren, beoordelen, prioriseren, plannen en uitvoeren van de juiste beveiligingsupdates zijn daarbij de sleutelwoorden. De noodzaak tot actie is in ieder geval evident, want kun je het je als organisatie wederom veroorloven om op dit onderdeel door schade en schande wijs te worden?

4. http://www.microsoft.com/downloads/details.aspx?familyid=AA6E0660-DC24-4930-AFFD-E33572CCB91F&displaylang=en

Foto: Peter Nielsen, www.sxc.hu

Besnuffeld door de baas

De juridische aspecten van preventief monitoren en digitaal onderzoek

Auteur: Erwin van der Zwan > Erwin is Sr. Security Advisor bij het Nationale Adviesorgaan voor Kritische Infrastructuur. Hij is per email bereikbaar via evdzwan@gmail.com

Dit artikel beschrijft verschillende juridische aspecten ten aanzien van het verzamelen en gebruiken van elektronische gegevens bij het (preventief) controleren van elektronische gegevens of als onderdeel van een incidentopvolging. Als voorbeeld wordt ingegaan op het doorzoeken van de computerbestanden en de e-mail van een werknemer door de werkgever en enkele uitdagingen bij digitaal forensisch onderzoek en de bewijskracht van elektronische gegevens. De verwijzingen in dit artikel zijn te vinden op pagina 24.

De juridische aspecten van digitaal onderzoek

ICT vervult een prominente rol in het dagelijks leven, bij het uitvoeren van bedrijfsprocessen en het bedienen van allerlei complexe processen in vitale infrastructuren. ICT is diep ingebed in de samenleving. Vandaag de dag bewaren we al onze gegevens en kennis wel ergens elektronisch en zijn we aangewezen op de beschikbaarheid en de integriteit van ingewikkelde computersystemen en telecommunicatienetwerken. Helaas kennen we ook de keerzijde van ICT, waarbij personen ICT-middelen misbruiken of inzetten voor illegale activiteiten of het uiten van hun (politieke) ongenoegen. Daarnaast worden ICT-voorzieningen gebruikt voor het voorbereiden of uitvoeren van (strafbare) handelingen, zonder dat de computerfaciliteiten zelf hierbij een doel of middel zijn. Denk bij dit laatste aan bijvoorbeeld e-mail en telefoneren (VoIP), waarbij de computer alleen is gebruikt als communicatiemiddel.

Omdat ICT zo belangrijk is, besteden we aandacht aan continuïteitsplannen en informatiebeveiliging. Natuurlijk zijn deze vastgelegd in het bedrijfsbeleid en in de bedrijfsvoering georganiseerd en geborgd. De beveiligingscyclus omvat elementen voor het analyseren van risico's, het vaststellen, uitwerken en implementeren van maatregelen, opleiding en training, operationeel beheer en evaluaties. Echter; hoe te handelen als het toch misgaat, is vaak nog een onderbelicht aspect. Dit wordt versterkt doordat het gros van de maatregelen zich focust op technische (ICT) preventieve oplossingen. De wijze waarop beveiligingsincidenten kunnen worden gedetecteerd, blijft in veel omgevingen een grijs gebied. Het is dan ook niet verwonderlijk dat in veel organisaties incidentherkenning en opvolging nauwelijks worden geadresseerd. De rol en de (on)mogelijkheden van digitaal forensisch onderzoek worden vaak evenmin onderkend.

Wat is digitaal forensisch onderzoek? Digitaal forensisch onderzoek laat zich beschrijven als een gestructureerd onderzoek naar illegale activiteiten volgens bewezen methoden, waarbij informatie op elektronische middelen wordt verzameld, wordt veiliggesteld en wordt geanalyseerd en gepresenteerd op een juridisch verantwoorde wijze ten dienste van de rechtspraak. Het gaat hier dus om een objectieve waarheidsvinding van wat er is gebeurd, waar, wanneer, waarmee (hoe), met welk gevolg en (indien mogelijk) door wie. Een forensisch onderzoek beantwoordt nooit vragen waarom iemand iets heeft gedaan en stelt ook nimmer een schuld vast.

Het onderzoek kent meestal fasen voor de voorbereiding, het veiligstellen van sporen, het analyseren en het presenteren van de resultaten (zie figuur pag. 19). De aldus verkregen bevindingen moeten eventueel

gebruikt kunnen worden in een civiele of strafrechtelijke procedure. De forensisch onderzoeker moet zich onder meer afvragen hoe om te gaan met het incident, waar digitale sporen kunnen worden aangetroffen, wie allemaal een rol speelt, wie beslissingen mag nemen, waar de verantwoordelijkheden liggen en wat de juridische kaders zijn. Daarnaast moet worden beschouwd of er überhaupt sprake is van een wederrechtelijk handelen en van opzet, hoewel deze vaststelling ook na het (initiele) onderzoek mag plaatsvinden *(verwijzing 1)*. Is er binnengedrongen in een computersysteem (WvSr art.138a), wordt er een stoornis veroorzaakt (WvSr art.161sexies/septies), zijn er gegevens beschadigd (WvSr art.350a/b) of zijn er gegevens getapt (WvSr art.139c/d/e) *(verwijzing 2)*?

Terwijl de onderzoeker zich over deze vragen buigt, wordt een onderzoeksstrategie bepaald. Deze moet met de opdrachtgever worden besproken en goedgekeurd. Tevens kan het noodzakelijk zijn in dit stadium ook de ondernemingsraad te informeren over het onderzoek. Het plan van aanpak moet aandacht besteden aan de in te zetten onderzoeksmiddelen en een afweging geven, waaruit blijkt dat deze voldoen aan de principes voor proportionaliteit (evenredigheid van doel en middelen) en subsidiariteit (gematigdheid bij de inzet van middelen en methoden) *(verwijzing 3)*.

Is de onderzoeker eenmaal klaar om aan de slag te gaan, dan komen er nog veel uitdagingen op zijn of haar pad. Eén aspect is dat iedere stap in het onderzoek, door zijn wisselwerking met de omgeving, juist ook invloed zal hebben op het te onderzoeken materiaal *(verwijzing 4)*. Het eerste vraagstuk dient zich dan ook meteen aan wanneer besloten moet worden hoe het materiaal veilig te stellen. Stel dat het een desktop computer betreft: zet men de machine uit en neemt men deze mee? Of moeten we de machine aan laten staan, zoals deze wordt aangetroffen en als zodanig gaan onderzoeken? Bedenk tevens dat gegevens niet alleen op de harde schijf (het vaste geheugen), maar ook in tijdelijke werkgeheugens of bijvoorbeeld I/O buffers aanwezig kan zijn. Niet alleen is de vluchtigheid van de gegevens een uitdaging voor de onderzoeker, ook de enorme diversiteit van mogelijk aan te treffen computerapparatuur en programmatuur is een uitdaging. Windows, Unix, Linux, Apple en vele andere besturingssystemen kunnen worden aangetroffen, met evenzoveel verschillende bestandstructuren en media, zoals computers, personal digital assistants (pda's), mobiele telefoons, usb-sticks, cd-rom's, dvd's, navigatiesystemen, e-mail servers, printerservers, et cetera. Hoe bepaal je waar mogelijke relevante sporen kunnen worden aangetroffen? Hoe wordt alle relevantie informatie tijdig veiliggesteld?

De vele technologische uitdagingen vallen buiten het bereik van dit artikel. Wel is het van essentieel belang te weten dat, vanaf het allereerste moment dat het onderzoek aanvangt, de integriteit en betrouwbaarheid van de (technische) materialen die worden veiliggesteld, wordt gewaarborgd en kan worden aangetoond. De geschetste diversiteit aan vindplaatsen, plaatst de onderzoeker hierbij voor een uitdaging om aantoonbaar te maken dat de verkregen informatie uit het onderzoek een correcte representatie is van de werkelijk aangetroffen gegevens. De bewijslastketen (chain of evidence) moet onafhankelijk kunnen worden gecontroleerd.
Bij het afhandelen van een beveiligingsincident wordt getracht te leren om herhaling te voorkomen. Daarnaast kan het nodig zijn om juridische stappen te zetten tegen betrokken personen of kan het gebeuren dat strafrechtelijke maatregelen tegen het bedrijf volgen. Bij iedere incidentopvolging moet dan ook de vraag worden gesteld of (digitaal) forensisch onderzoek vereist is. Incidentopvolging en waarborging van de bedrijfscontinuïteit kan op gespannen voet staan met het forensisch onderzoek. Het laatste heeft tot doel om een waarheidsvinding naar de feiten, zoals die zijn gepleegd, uit te voeren. De eerste reacties bij een incident zijn echter vaak gericht op het beperken van schade en het waarborgen van de continuïteit. Bij de handelingen die hiervoor moeten worden verricht, kunnen mogelijk (elektronische) sporen worden vernietigd.

Een voorbeeld
Helaas vindt in de praktijk niet ieder onderzoek plaats als onderdeel van een (gecoördineerde) incidentopvolging. De mogelijke scenario's waarbij digitaal forensisch onderzoek gewenst is, zijn talrijk omdat ICT de ene keer het doel en de andere keer slechts een (communicatie) hulpstuk was. Forensisch onderzoek kan helpen om de daders te achterhalen en de schade in te kunnen schatten. Wanneer mogen de servers weer online? Wie heeft de bevoegdheid om beslissingen te nemen?

Regelmatig betreffen de voorkomende situaties verdenkingen tegen, of betrokkenheid van, eigen medewerkers of ingehuurd personeel. Bijvoorbeeld het verrichten van arbeid voor anderen, toegang (trachten te verkrijgen) tot informatie waarvoor men niet bevoegd is (bedrijfsspionage), fraude en andere criminele activiteiten. Laat je in een dergelijk geval een systeembeheerder de e-mail van een collega, die verdacht is van betrokkenheid, nakijken op sporen? Bovendien beperkt een onderzoek zich lang niet altijd tot een forensisch onderzoek van de geautomatiseerde werken. Zo kan het noodzakelijk zijn dat er aanvullend recherchewerkzaamheden moeten worden uitgevoerd, zoals het verrichten van interviews met de betrokken personen.

In de rest van dit artikel wordt als voorbeeld gekeken naar een situatie waarbij de

systeembeheerder, in opdracht van de directie, een computer van een medewerker van het bedrijf moet onderzoeken. Hierbij wordt gezocht naar documenten en e-mails waaruit zou kunnen blijken dat de medewerker zich heeft beziggehouden met nevenactiviteiten en/of handelingen die het bedrijf zou kunnen schaden.

Het elektronisch briefgeheim

Voor papieren post bestaat sinds de negentiende eeuw het grondwettelijk briefgeheim (Grondwet art. 13 lid 1). Dat houdt in dat de overheid en de openbare vervoerders van poststukken niet zomaar de post mogen inzien of onderscheppen. Alleen op grond van wettelijke uitzonderingen, zoals een machtiging van de rechter-commissaris (WvSv art.101) *(verwijzing 5)* of een sterk vermoeden dat er direct gevaar kan bestaan (bijvoorbeeld een bombrief), mag een brief worden geopend door een opsporingsdienst. Artikel 13 lid 2 van de Grondwet regelt het telefoon- en telegraafgeheim: "Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen". Op grond van dit artikel mag een opsporingsdienst dus niet zomaar telefoongesprekken afluisteren en brieven van burgers openen of kopiëren. Willen zij dat toch, dan zullen zij de rechter ervan moeten overtuigen dat zij daartoe het recht hebben op grond van wettelijke bepalingen. Communicatie per brief, per telefoon of per telegraaf is dus in principe vertrouwelijk. Afluisteren van dergelijke communicatiemiddelen is strafbaar. Andere vormen van communicatie staan niet in de grondwet genoemd. Een grondwetswijziging eind jaren negentig om dit te veranderen, sneuvelde. Dat wil echter niet zeggen dat e-mail vogelvrij is.

Voor e-mail leek in eerste instantie dus geen briefgeheim te gelden *(verwijzing 6)*. In 1997 werd dit als zodanig ook gemeld door de toenmalige minister van Justitie *(verwijzing 7)*. Echter; in een nota aan de Tweede Kamer (in vergaderjaar 2004-2005) schrijft de minister van Justitie dat uitwisselen op elektronische wijze per e-mail tussen individuele personen een vorm van besloten communicatie is, beschermd onder artikel 13 van de Grondwet *(verwijzing 8)*. Bovendien zijn voor het afluisteren van elektronische communicatie en het doorzoeken van gegevensdragers, als onderdeel van de wetten over computercriminaliteit, aparte bepalingen in het Wetboek van Strafrecht en Strafvordering opgenomen.

Aanbieders van telecommunicatiediensten hebben een geheimhoudingsplicht voor de e-mail van en naar hun klanten. Schending van de geheimhouding door internet service provider (ISP) medewerkers is strafbaar gesteld op grond van de Wet Computercriminaliteit. Het opzettelijk en wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van gegevens uit een telecommunicatiewerk of computer, als die gegevens niet voor de tapper bestemd zijn, wordt bestraft met maximaal één jaar cel (WvSr art.139c). In WvSr artikel 273d, wordt nog eens expliciet vastgelegd dat een medewerker van een telecombedrijf (inclusief ISP's) die opzettelijk en wederrechtelijk van gegevens kennisneemt van klanten, daarvoor maximaal anderhalf jaar cel kan krijgen. Dit geldt ook voor beheerders van niet-openbare telecommunicatie en computernetwerken zoals bedrijfsnetwerken.

Het aftappen of opnemen is niet strafbaar als dit gebeurt 'ten behoeve van de goede werking van een openbaar telecommunicatienetwerk' of in opdracht van politie of justitie. Een systeembeheerder mag bijvoorbeeld wel in de uitgaande e-mail van een klant kijken als deze zo veel e-mails verstuurt dat het systeem instabiel wordt. De ISP kan natuurlijk afspraken maken met de klant over wanneer zij in de e-mail van de klant mogen kijken. Zo kan een provider een automatische virusscan uitvoeren op uitgaande e-mail of binnenkomende ongewenste reclame of spam tegenhouden.

De schrijver van een e-mail kan via zijn auteursrecht optreden tegen ongewenste publicatie *(verwijzing 9)*. Bij het publiceren (of doorsturen) van een e-mail wordt immers een kopie gemaakt, en dat mag niet zonder toestemming. Bovendien is een e-mail een ongepubliceerd werk. De maker van een ongepubliceerd werk heeft het exclusieve recht te beslissen of, en zo ja waar en hoe, het voor het eerst gepubliceerd wordt.

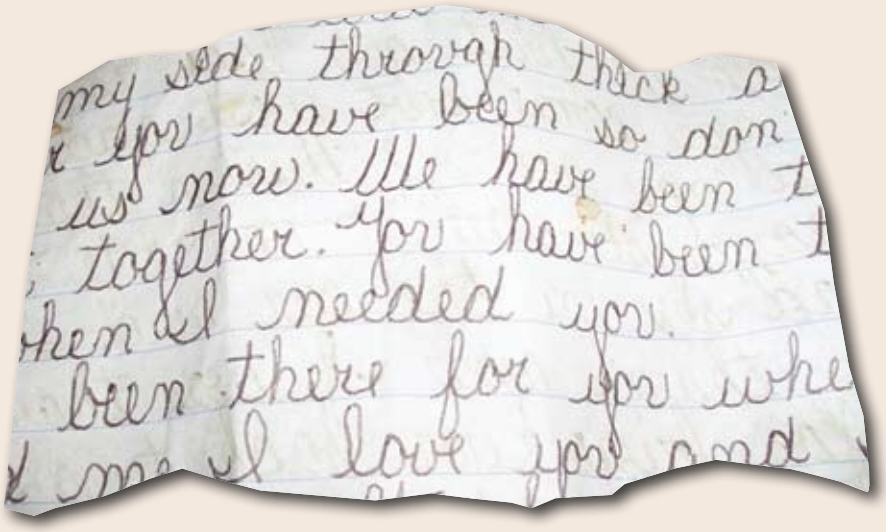


Foto: Digital Sextant, via Flickr.com

Privacy van de werknemer

De privacy van de werknemer gaat onder normale omstandigheden boven het bedrijfsbelang bij het monitoren of vastleggen (loggen) van internet- en computergebruik. De werknemer mag een redelijk niveau van privacy verwachten op de werkplek. Dat geldt ook voor internetgebruik. Pas bij een redelijk vermoeden van wangedrag mag de werkgever gaan observeren.

Bedrijfsmiddelen zoals internettoegang en e-mail zijn beschikbaar gesteld omdat ze nodig zijn voor het werk. Ze zijn eigendom van de werkgever en deze mag dus eisen

Foto: Vince Alongi, via Flickr.com

stellen aan het gebruik daarvan. De werkgever heeft natuurlijk geen plicht om werknemers gebruik te laten maken van internet. Van de werknemer mag worden verwacht dat hij verantwoordelijk, professioneel en integer omgaat met de bedrijfsmiddelen die hij krijgt.

Dat privacy wel degelijk bestaat op de werkplek, werd ook besloten door het Europese Hof voor de Rechten van de Mens *(verwijzing 10)*. Ook bij internetgebruik op de werkvloer mag men enige privacy verwachten. Het moet wel gaan om gebruik waarbij men een zekere privacy mocht verwachten. Bij het versturen van een e-mail is dat duidelijk het geval. Maar wie een bericht plaatst op een openbaar toegankelijk discussieforum, dat bijvoorbeeld via Google te vinden is, moet niet gek opkijken als zijn werkgever daarmee aan komt zetten. Het is geen schending van de privacy als de werkgever dat bericht vindt en de persoon in kwestie er op aanspreekt. Bij een bedrijf moet de ondernemingsraad haar instemming geven over de inhoud van een internetreglement. Artikel 27(1)(k) van de Wet op de Ondernemingsraden zegt namelijk dat instemming van de ondernemingsraad nodig is bij 'een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen'. Een reglement over internetgebruik is zo'n regeling.

Controle door de werkgever

De werkgever mag niet ongecontroleerd in detail bijhouden (monitoren of loggen) hoe werknemers hun internetfaciliteiten gebruiken. Wat en waarom er wordt gecontroleerd, moet zijn vastgelegd in een reglement. Het bijhouden van wat werknemers doen, is een verwerking van persoonsgegevens *(verwijzing 11)*. Dat mag alleen met een legitiem doel. Bovendien moet er zijn vastgelegd wat er bijgehouden wordt, waarom dat wordt gedaan en wat er met de gegevens gebeurd. Ook hebben werknemers een recht van inzage in wat er over hen is vastgelegd.

Monitoren en loggen moet zo veel mogelijk anoniem gebeuren. Pas als daarna wangedrag boven tafel komt, is het toegestaan uit te zoeken wie daarvoor verantwoordelijk is. Wel moet de werkgever daarbij uitkijken dat ook andere werknemers niet onnodig gecontroleerd worden. Voor monitoren en loggen betekent dit dat gedetailleerde logs over computer- en internetgebruik van alle werknemers niet zomaar bijgehouden mogen worden.

Doorzoeken van de bedrijfscomputer en e-mail

De systeembeheerder kan technisch heel veel. Alle e-mails lezen, alle bestanden op de netwerkschijven openen en met een beetje moeite zelfs meelezen met elke chat via bijvoorbeeld MSN. Dat mogen zij echter niet zomaar. Het eerder genoemde artikel 273d van het Wetboek van Strafrecht verbiedt beheerders van een netwerk om opzettelijk en wederrechtelijk kennis te nemen van vertrouwelijke communicatie van gebruikers. Hoewel dit artikel primair handelt over openbare telecommunicatienetwerken, zegt lid 2 'Het eerste lid is van overeenkomstige toepassing op de persoon werkzaam bij een aanbieder van een niet-openbaar telecommunicatienetwerk of een niet-openbare telecommunicatiedienst'. Hieronder valt ook een bedrijfsnetwerk. Het sleutelwoord is 'wederrechtelijk'. Uit nieuwsgierigheid e-mails lezen, is dus niet toegestaan. Berichten inzien mag alleen als dat strikt nodig is voor de goede werking van het netwerk. Zit er bijvoorbeeld een virus in een e-mail, dan kan dat een rechtvaardiging zijn om de inhoud te lezen. Al was het maar om te kijken of het virus met succes is verwijderd en de bijlage nog leesbaar is. De beheerder is dan wel geheimhouding verplicht over de inhoud. Een belangrijke eis is dat er een reglement is waarin staat onder welke omstandigheden men kennis mag nemen van mailboxen van medewerkers.

Een medewerker, een systeembeheerder of een directeur van een bedrijf mag dus niet

Foto: Stephanie Hofschlaeger, www.sxc.hu

zonder meer in zakelijke en privé e-mail kijken. Het stelselmatig volgen of waarnemen van de activiteiten van een persoon, zeker als hierbij mogelijk een inbreuk op de persoonlijke levenssfeer optreedt, is een opsporingstaak en daarmee voorbehouden aan bevoegde autoriteiten. Als een officier van justitie het bedrijf daartoe bevel geeft, moet de beheerder meewerken en dan kan hij dus mogelijk wel kennisnemen van de inhoud van de mailbox. Op eigen houtje gaan snuffelen naar eventueel bewijs van (illegale) activiteiten mag niet.

Als de betrokken persoon van een overtreding wordt verdacht, bijvoorbeeld als er al andere aanwijzingen zijn dat de medewerker nevenactiviteiten verrichte die in strijd zijn met zijn arbeidsovereenkomst of van onbetamelijk of strafbaar gedrag, mag de bedrijfsleiding wel gericht gaan monitoren - mits dat geregeld is in een reglement dat de goedkeuring van de OR heeft. Komt er dan bewijs naar voren, dan mag dat worden gebruikt. Gaan 'vissen' zonder aanleiding is in principe niet toegestaan en het bewijs dat men zo vindt, mag meestal niet worden gebruikt in bijvoorbeeld een ontslagprocedure.

Veel onderzoeksmethoden zijn afgeleid van de mogelijkheden waarover de opdrachtgever beschikt vanuit de contractuele relatie die de opdrachtgever heeft met de onderzochte persoon, of omdat de opdrachtgever als rechthebbende wordt aangemerkt in de zin van het Burgerlijk Wetboek en uit dien hoofde een onderzoek kan instellen in geval van onregelmatigheden. De opdrachtgever heeft bepaalde belangen en die kunnen rechtvaardigen dat hij een onderzoek instelt. Verschillende onderzoeksmethoden betekenen in voorkomende gevallen dat inbreuk wordt gemaakt op de privacy van de onderzochte persoon. Om die reden is normering van onderzoeksmethoden en -middelen noodzakelijk. Bovendien geldt als basisregel dat de beginselen van proportionaliteit en subsidiariteit in acht worden genomen. Tevens zal voorafgaand aan de inzet van de onderzoeksmethode moeten worden bepaald tot welk resultaat dit moet kunnen leiden. Daarmee wordt beoogd te voorkomen dat gegevens worden

vergaard die niet strikt noodzakelijk zijn voor de uitvoering van de onderzoeksopdracht.

Wanneer een bedrijfscomputer wordt doorzocht, dient de desbetreffende medewerker en de OR te worden geïnformeerd over het onderzoek *(verwijzing 12)*. Als bij het onderzoek bestanden of e-mailberichten worden aangetroffen die duidelijk herkenbaar zijn als privé, dienen deze bestanden en berichten in principe ongemoeid te worden gelaten *(verwijzing 13)*.

Wanneer een bestand of e-mailbericht ontoegankelijk is gemaakt, bijvoorbeeld door versleuteling (encryptie), kan de betrokken persoon (door de werkgever) niet verplicht worden om het bestand of het bericht te ontsleutelen, of om zijn wachtwoord af te gegeven *(verwijzing 14)*. De opdracht om de ontoegankelijkheid op te heffen, kan wel aan een derde worden gegeven door de politie of justitie.

Als een particulier onderzoeksbureau *(verwijzing 15)* optreedt in het verlengde van de rechthebbende van een geautomatiseerd werk *(verwijzing 16)*, zoals een aan de medewerker beschikbaar gestelde computer of het bedrijfscomputernetwerk, is onderzoek, waarbij de gegevens op bijvoorbeeld een server of een harde schijf worden benaderd, geoorloofd. Er is dan geen sprake van 'wederrechtelijk binnendringen' in de zin van artikel 138a van het WvSr. Evenmin is er sprake van gekwalificeerde computervredebreuk *(verwijzing 17)*, als het inkijken in de gegevens gevolgd wordt door het overnemen van de gegevens en deze voor een ander wordt vastgelegd (ontvreemden van gegevens).

Ook wanneer een particulier onderzoeksbureau wordt ingeschakeld, blijft het de verantwoordelijkheid van de opdrachtgever om de gebruikers in algemene zin te informeren dat handelingen op computers, op computernetwerken en/of het gebruik van computerdiensten worden vastgelegd en onder welke omstandigheden de vastgelegde gegevens in de geautomatiseerde voorzieningen kunnen worden onderzocht.

Security Monitoring

Hoewel een zekere mate van 'privatisering' van de werkplek dus is toegestaan, kan ook een continue bewaking van de computernetwerken worden ingezet. Een werkgever kan zich zo wapenen tegen het uitlekken van bedrijfsgeheimen of voor het detecteren van cyberaanvallen. Controle op naleving van afspraken op verboden gebruik (policy compliance) alleen rechtvaardigt echter niet een continue controle en de daarmee gepaard gaande, verregaande inbreuk op de persoonlijke levenssfeer van de werknemer. In de regel zal de controle op naleving van de afspraken slechts steekproefsgewijs mogen geschieden. Echter; als een werknemer of een groep werknemers ervan worden verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. Op grond van artikel 8f Wet Bescherming Persoonsgegevens heeft een werkgever een gerechtvaardigd belang en mag dit eventueel worden uitbesteedt aan een derde partij. Hierbij dient de controle zo veel mogelijk geautomatiseerd (content-filtering) plaats te vinden en moeten de privacybelangen van de betrokkenen in acht worden genomen.

Bewijsmiddelen

Boek II, Titel VI, derde afdeling van het Wetboek van Strafvordering behelst de strafvorderlijke bepalingen over het strafrechtelijk bewijsrecht *(verwijzing 18)*. Noodzakelijk voor het aannemen van het bewijs door de rechter is dat de bewijsmiddelen wettig en overtuigend zijn. Wettige bewijsmiddelen zijn de eigen waarneming van de rechter, verklaringen van de verdachte, een getuige of een deskundige en schriftelijke bescheiden benoemt in het Wetboek van Strafvordering *(verwijzing19)*. Andere geschriften kunnen alleen als bewijsmiddel dienen, als deze gelden in verband met de inhoud van andere bewijsmiddelen.

Het bewijs moet rechtmatig verkregen zijn en voldoen aan de minimumregels voor bewijs. Als dat niet het geval is, kan bewijsuitsluiting volgen. Er mag geen ongerede twijfel over het bewijsmateriaal bestaan. Voor het bewijs mag bijvoorbeeld geen gebruik worden gemaakt van meningen of gissingen, van verklaringen van medeverdachten *(verwijzing 20)* of van bewijsmateriaal waarvan de verdediging gemotiveerd aanvoert dat het onbetrouwbaar is, zonder dat er een motivering door de rechter tegenover staat. Gemotiveerde verweren van de verdediging met betrekking tot de betrouwbaarheid van bewijsmateriaal moeten door de rechter gemotiveerd worden verworpen. Gebeurt dat niet, dan mag het bewijsmateriaal niet worden gebruikt. Dergelijke verweren kunnen bijvoorbeeld betrekking hebben op de betrouwbaarheid van een verklaring, van een ingeschakelde deskundige, van diens toegepaste onderzoeksmethode of van de onzorgvuldige hantering van een (onderzoeks) methode. Ook kan de betrouwbaarheid van de uitkomst van een (elektronische) meting of elektronische informatie gemotiveerd worden betwist, tengevolge waarvan de rechter daarvan onder bepaalde omstandigheden geen gebruik mag maken *(verwijzing 21)*.

Bewijskracht van elektronische gegevens

Uit het voorgaande blijkt dat elektronische gegevens als zodanig niet in de opsomming van wettige bewijsmiddelen zijn opgenomen. De gegevens zullen derhalve in een proces-verbaal of een ander geschrift moeten worden opgenomen om als bewijs in een strafzaak te kunnen worden gebruikt. Een in de wettelijke vorm door een bevoegde ambtenaar opgemaakt proces-verbaal over diens waarneming van gegevens van een computer of gegevensdrager zou in beginsel kunnen gelden als schriftelijk bewijs in de zin van art. 344 lid 1 onder 2 WvSv. Andere geschriften, inhoudende de gegevens uit een computer of gegevensdrager, zouden kunnen gelden als bewijs in de zin van art. 344 lid 1 onder 5 WvSv. Voor de waardering van dit bewijs is van belang hoe betrouwbaar de waargenomen gegevens worden geacht. De forensisch onderzoeker zal de integriteit van de onderzochte gegevens te allen tijde moeten kunnen aantonen.

Conclusies

Het opzetten en uitvoeren van een digitaal forensisch onderzoek vereist specialistische kennis en deskundigheid. Het onderzoek moet aan objectieve waarheidsvinding doen. De uitvoering moet onafhankelijk en gedegen plaatsvinden. Middelen worden gematigd en evenredigheid aan het doel ingezet.

Een systeembeheerder die in opdracht van de directie een computer of e-mail van een eigen medewerker van het bedrijf moet onderzoeken, laat zich vaak niet omschrijven als een gedegen en onafhankelijk digitaal forensisch onderzoek. Als de beheerder zonder verdere aanleiding de computer onderzoekt op de aanwezigheid van documenten, waaruit zou kunnen blijken dat de medewerker zich had beziggehouden met handelingen die het bedrijf zou kunnen schaden, lijkt dit veel op 'vissen naar be-

wijsmateriaal'. Bovendien zal de betreffende medewerker geïnformeerd moeten worden over dit onderzoek. Als de beheerder vervolgens een e-mail bericht aantreft dat duidelijk herkenbaar is als verzonden van een privé e-mailadres naar een ander privé e-mailadres, dient dit bericht in eerste instantie ongemoeid gelaten te worden. Als de systeembeheerder toch dit bericht leest en overlegt aan de directie, kan er sprake zijn van inbreuk op de privacy en persoonlijke levenssfeer en daarmee schending van de Wet Bescherming Persoonsgegevens. Als desondanks de directie de inhoud van dit bericht vervolgens hanteert om aan te tonen dat de medewerker zich schuldig heeft gemaakt aan nevenactiviteiten, omdat in het (privé) e-mailbericht hiervan melding zou worden gemaakt, kan worden betwist dat het hier om rechtmatig verkregen bewijsmateriaal gaat. Het een en ander hangt er echter af van de vraag of er al aanwijzingen waren dat de medewerker nevenactiviteiten verrichte die in strijd waren met een arbeidsovereenkomst. Als dat zo is, dan mag de bedrijfsleiding gaan monitoren - mits dat is geregeld in een reglement dat de goedkeuring van de OR heeft. Komt er dan bewijs naar voren, dan mag dat wel worden gebruikt. Gaan 'vissen' zonder aanleiding is in principe niet toegestaan, en bewijs dat men zo vindt, mag meestal niet worden gebruikt in procedures.

Verwijzingen

1. Het rapport Van herkenning tot aangifte: Handleiding Cybercrime. Den Haag, 08-2006. v2.0 van GOVCERT. NL geeft een uitgebreid overzicht van mogelijkheden en aandachtspunten.

2. Wetboek van Strafrecht. s.l.: Koninkrijk der Nederlanden, 03-03-1881.

3. Juridische aspecten van forensisch digitaal onderzoek. Westerhoud, Marcel. s.l.: Platform voor Informatiebeveiliging, 02 2008, Vol. 1.

4. Locard's Exchange Theory

5. Wetboek van Strafvordering. s.l.: Koninkrijk der Nederlanden, 15-01-1921.

6. Verbeek, Mr.J.P.G.M. E-mail moet vallen onder het briefgeheim. Nationaal Programma Informatietechnologie en Recht. s.l.: NRC Handelsblad, 12-7-1997.

7. Verbeek, Mr.J.P.G.M. E-mail moet vallen onder het briefgeheim. Nationaal Programma Informatietechnologie en Recht. s.l.: NRC Handelsblad, 12-7-1997.

8. Minister van Justitie. Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). Den Haag: s.n., 2005. Kamerstukken II 2004/05, 26671 nr.10.

9. Engelfriet, Arnoud. Elektronisch briefgeheim: de stand van zaken. Ius mentis. (Online) ICT-jurist Arnoud Engelfriet, 2008. http://www.iusmentis.com.

10. Zie het Copland-arrest, COPLAND v. THE UNITED KINGDOM - 62617/00 (2007) ECHR 253, 3 April 2007.

11. Wet bescherming persoonsgegevens. s.l.: Koninkrijk der Nederlanden, 06-07-2000. Staatsblad 06-07-2000, 302.

12. Notificatie is onder andere verplicht op basis van artikel 33 en 34, Wet Bescherming Persoonsgegevens, op het moment van vastlegging of wanneer de gegevens voor de eerste maal worden verstrekt aan derden.

13. Van de gegevens kan slechts kennis worden genomen voor zover de gegevens klaarblijkelijk van de desbetreffende medewerker afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, of indien zij klaarblijkelijk tot het begaan van het feit hebben gediend of klaarblijkelijk met betrekking tot die gegevens het feit is gepleegd. De term 'klaarblijkelijk' betekent in dat verband dat alleen van die gegevens kan worden kennisgenomen waarvan van buitenaf, bijvoorbeeld aan de hand van de adressering of de herkomstgegevens van het e-mailbericht, duidelijk is dat ze van de medewerker afkomstig zijn of voor hem bestemd zijn.

14. Nemo-tenetur beginsel

15. Het verrichten of aanbieden van recherchewerkzaamheden zonder vergunning van de minister van Justitie is verboden. Zowel het betreffende beveiligingsbedrijf als de ingezette particuliere onderzoekers dienen te beschikken over een vergunning en vallen onder de Wet particuliere beveiligingsorganisaties en recherchebureaus.

16. Volgens art. 80sexies WvSr wordt onder een geautomatiseerd werk verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.

17. Art. 138a lid 2 Wetboek van Strafrecht.

18. Artikelen 338 – 344a, Wetboek van Strafvordering.

19. Artikel 344, Wetboek van Strafvordering.

20. Volgens de wet zijn dat enkel degenen die samen met de verdachte op dezelfde aanklacht, in dezelfde instantie, tegelijk terecht staan.

21. Zie in dit verband arrest HR 12 maart 1996, NJ 1996, 511

Het Govcert symposium 2009

Auteur: Maarten Oosterink > Maarten Oosterink werkt als managing consultant bij Capgemini en is bereikbaar via maarten.oosterink@capgemini.com.

Met alweer de achtste editie achter de rug, begint het Govcert symposium zo langzamerhand een vertrouwd en gewaardeerd begrip te worden onder informatiebeveiligers, die op enigerlei wijze verbonden zijn met Nederlandse overheidsdiensten of computer emergency response teams (CERT's). Net als vorig jaar was het symposium neergestreken in het WTC in hartje centrum van Rotterdam.

Govcert, de in 2002 opgerichte overheidsdienst die zichzelf ten doel stelt om Nederlandse overheidsdiensten van informatie, kennisdeling en kunde te voorzien over informatiebeveiliging, houdt sinds haar oprichting een jaarlijks symposium. Het doel hierbij tweeledig. Primair is het symposium bedoeld voor haar - met een duur woord - constituents. Dit zijn de deelnemende overheidspartijen: een bonte verzameling van overheidsorganen, variërend van ministeries tot kleine gemeenten en zelfstandige bestuursorganen als de OPTA en de AFM. Als tweede doel is er het uitwisselen van informatie en netwerken tussen de diverse CERT's en beveiligingsorganisaties (overheid en non-profit) waarmee Govcert samenwerkt, ook in internationaal verband.

Dit maakt dat er altijd al een spagaat te ontdekken is geweest tussen zeer lokale onderwerpen en de meer mondiale en specialistische onderwerpen. Elk jaar wordt de kloof tussen deze onderwerpen overigens steeds minder groot. Het feit dat alle presentaties inmiddels in het Engels zijn en er duidelijke parallel tracks zijn, maakt dat waarschijnlijk elke bezoeker onderhand zijn plek wel weet te vinden.

Hierbij hoort overigens wel de kritische noot dat dit betekent dat er aan beide kanten van de doelgroepen ingeleverd is. De Engelse taal lijkt toch lastig voor sommige, meer senior mensen uit de kringen van de overheid. Aan de andere kant van het spectrum zijn de technische presentaties geringer in aantal en minder diepgaand van niveau. Het is niet geheel duidelijk of hier bewust naar gestreefd is, maar het effect is in ieder geval dat er veel minder techneuten uit de overheidshoek te vinden zijn en meer beleidsmakers. De echte techneuten die er (nog) zijn, zijn veelal mensen uit de (internationale) CERT gemeenschap.

Opvallend is overigens dat een zeer groot deel van de circa vijfhonderd bezoekers nog steeds internationaal is, ondanks de recessie. Internationaal betekent hier niet alleen Amerikanen of Engelsen, maar dankzij de groei van het aantal CERT's in alle landen van de wereld echt internationaal. Dus naast de 'frequente' bezoekers uit de hoek van US-CERT en Department of Homeland Security (DHS) waren er veel mensen van CERT's uit landen als Australië, Japan, Denemarken, Frankrijk en Finland.

Inhoudelijk was het congres verdeeld over twee dagen, waarbij elke dag ingeleid en afgesloten werd met een aantal keynote presentaties. Daartussen was elke dag een viertal 'tracks' naar onderwerp, waarbij elk onderwerp vier of vijf presentaties kenden. Hierbij werden alle delen telkens onderbroken door networking breaks of lunch, waardoor er meer dan voldoende tijd was voor gesprekken met collega's of andere bezoekers. Op het intermenselijke vlak was er ook het social event op de avond van de eerste dag, gevolgd door een buffet/diner in restaurant Parkheuvel. Het social event bestond uit een vijftal activiteiten waar bezoekers uit konden kiezen, variërend van een wandeling door Rotterdam met gidsen tot een ritje op een Solex of Segway. Het eten na afloop was prima, de muziek binnen wat luid voor een netwerkgelegenheid.

Dat een gratis symposium niet meteen een indicator voor de kwaliteit van de sprekers is, bewees Govcert ook dit jaar met keynote sprekers als David Rice en niemand minder dan Bruce Schneier. Zo bracht Schneier ons een blik op de toekomst van security, waarbij dit volgens hem een integraal onderdeel zal worden van het IT productaanbod, mede dankzij ontwikkelingen als Cloud Computing. Onderwerpen als de psychologie van de koper (risk aversiveness versus risk seeking behaviour, prospect theory) en een blik op andere meer volwassen bedrijfstakken, zoals de auto-industrie, passeerden de revue. De presentatie was overigens niet nieuw, Schneier heeft gelijksoortige presentaties al meerdere malen ten gehore gebracht.

Zoals gezegd waren de parallel presentaties verdeeld naar onderwerp, waarbij thema's als Threats, Society & Security en Law Enforcement gehanteerd werden. Opvallend was dat bijna een kwart van de presentaties het 'No Press' stempel droeg. Daar waar er vroeger 'Law Enforcement only' sessies waren, zijn deze vervangen door sessies waar alleen de pers niet meer welkom is. Ondergetekende heeft een poging gedaan om iemand van de pers te vinden - ze zouden herkenbaar moeten zijn aan gele keycords - maar is daar niet in geslaagd. Een andere observatie is dat met het verdwijnen van zowel de meer technisch inhoudelijke alsmede de 'Law Enforcement only' sessies het aantal bezoekers vanuit deze hoeken inderdaad zienderogen is afgenomen, er is duidelijk een verschuiving zichtbaar in het publiek. Dat overigens voor de meerderheid 'business casual' gekleed ging. De paardenstaarten en Thinkgeek t-shirts waren op één hand te tellen.

Het gaat te ver om de inhoud van de presentaties in dit artikel te behandelen. Bovendien mag over een deel van de presentaties geheel niets openbaar gemaakt worden. Een aantal presentaties is te vinden op de site van Govcert (zie Links). Zonder inhoudelijk in te gaan op de presentaties kan gesteld worden dat het niveau nog steeds goed is en voor een ieder die zich in overheidsland met informatiebeveiliging bezighoudt interessante onderwerpen te vinden zijn. Wat dat betreft is Govcert er voor de achtste maal in geslaagd om een goed georganiseerd tweedaags evenement neer te zetten, dat qua inhoud en netwerkgelegenheden zeker niet onderdoet voor symposia die hiervoor soms honderden euro's of meer vragen.

Over de auteur
Maarten Oosterink werkt als managing consultant bij Capgemini en richt zich hierbij op IT security, specifiek op het gebied van infrastructuur en process control (SCADA). Ook heeft hij een tijdens het symposium een presentatie gegeven over process control security.

Links
- Bruce Schneier over de psychologie van security: *http://www.schneier.com/essay-155.html*
- Govcert Symposium: http://www.govcert.nl/symposium/

Laatste zat ik op een mooie zondagochtend in de tuin samen met vrouw en dochter te eten en we kregen het over internet. Mijn dochter was sinds een paar dagen helemaal enthousiast over het twitteren. Ik had er weleens van gehoord, maar na de eerste beschrijving had ik niet het gevoel dat twitter iets aan mijn bestaan kon toevoegen. Mijn dochter vertelde enthousiast over de twitterberichten van twee van haar grote helden die verslingerd zijn aan dit medium: Marco Borsato en Paul de Leeuw.

's Avonds heb ik eens even gekeken naar twitter en ik vroeg mezelf af waarom mensen geïnteresseerd zouden zijn in mijn belevenissen. Ik kan me zelfs niet voorstellen dat er iemand interesse heeft voor het dagelijkse leven van de twee eerder genoemde BN'ers, maar dat kan natuurlijk ook een kwestie van leeftijd zijn. De twitterberichten hebben niet alleen de lengte van een sms-bericht, ze hebben ook dezelfde nietszeggende inhoud. Ik heb nog even de twitters van ene Justin Halpern gelezen, die de mopperige belevenissen van zijn vader twittert en die nu dagelijks 250.000 lezers heeft. De twitterdienst trekt momenteel zeven miljoen bezoekers per maand, wat een groei is van 1382 procent ten opzichte van een jaar geleden.

Omdat ik toch achter mijn pc zat, besloot ik om eens te kijken op de twitter-site. Even gezocht op de naam van mijn dochter, maar helaas ging dat niet lukken. Blijkbaar had ze haar eigen naam niet gebruikt en dan wordt het volgens mij helemaal lastig om twitteraars (ik weet dat het geen Nederlands is, maar het woord twitteren is dat ook niet) te vinden. Ik besluit mijn eigen naam te zoeken, dus die typ ik in, ik druk op enter en dan slaat me de schrik om het hart. Ineens zie ik dat mijn scherm zich vult, terwijl ik 'no results' had verwacht. Ik zie op mijn scherm een aantal kenmerken, die wel heel erg op die van mij lijken.

Ineens begint mijn pc te rinkelen. Ik probeer te achterhalen waar dit geluid vandaan komt en ik realiseer me dan dat mijn wekker afloopt. Zwetend zit ik op de rand van mijn bed en ik verbaas me weer over het realiteitsniveau van mijn dromen. Ik sta op en na een paar bakken koffie besluit ik toch eens te kijken in hoeverre mijn dromen gebaseerd zijn op werkelijkheid. Al snel blijkt dat de uitdrukking 'dromen zijn bedrog' niet altijd de waarheid weergeeft. Het komt wel degelijk voor dat iemand besluit onder een andere naam te twitteren en daarbij meningen op het internet plaatst die je helemaal niet deelt, of, nog erger; waar je fel tegen bent.

Hoe voorkom je nu dat anderen gebruikmaken van jouw naam of van de naam van je werkgever? Daar kan ik vrij kort over zijn: dat kun je niet voorkomen en je kunt het ook niet stoppen. Vraag de NOS maar wat ze kunnen doen tegen de nepaccounts die allerlei fake berichten op internet achterlaten. Behalve de accounts te laten verwijderen, is dat verder niet veel. Ook onze bekende viroloog Ab Osterhaus, die de Mexicaanse griep nogal heeft gepromoot, kwam ineens zijn naam tegen op twitter, terwijl hij er honderd procent van zeker is dat hij geen account heeft. Daarmee kun je iemands reputatie behoorlijk beschadigen. Nu is het door mij gebruikte voorbeeld niet zo gelukkig omdat deze persoon heel goed in staat is zijn eigen reputatie onderuit te halen.

Zijn er dan helemaal geen positieve dingen te noemen over twitter? Jawel hoor, nieuws gaat nog sneller rond, alleen heb je geen idee over de betrouwbaarheid van de nieuwsberichten. Fileoverzichten en andere, snel wisselende, informatie is heel handig op te vragen, maar ook daarvan is het niet altijd duidelijk in hoeverre de informatie betrouwbaar is. Eén van de eerste lessen die ik leerde, toen ik mijn eerste schreden zette in de ICT wereld, was wel dat informatie alleen informatie is, als deze betrouwbaar is.

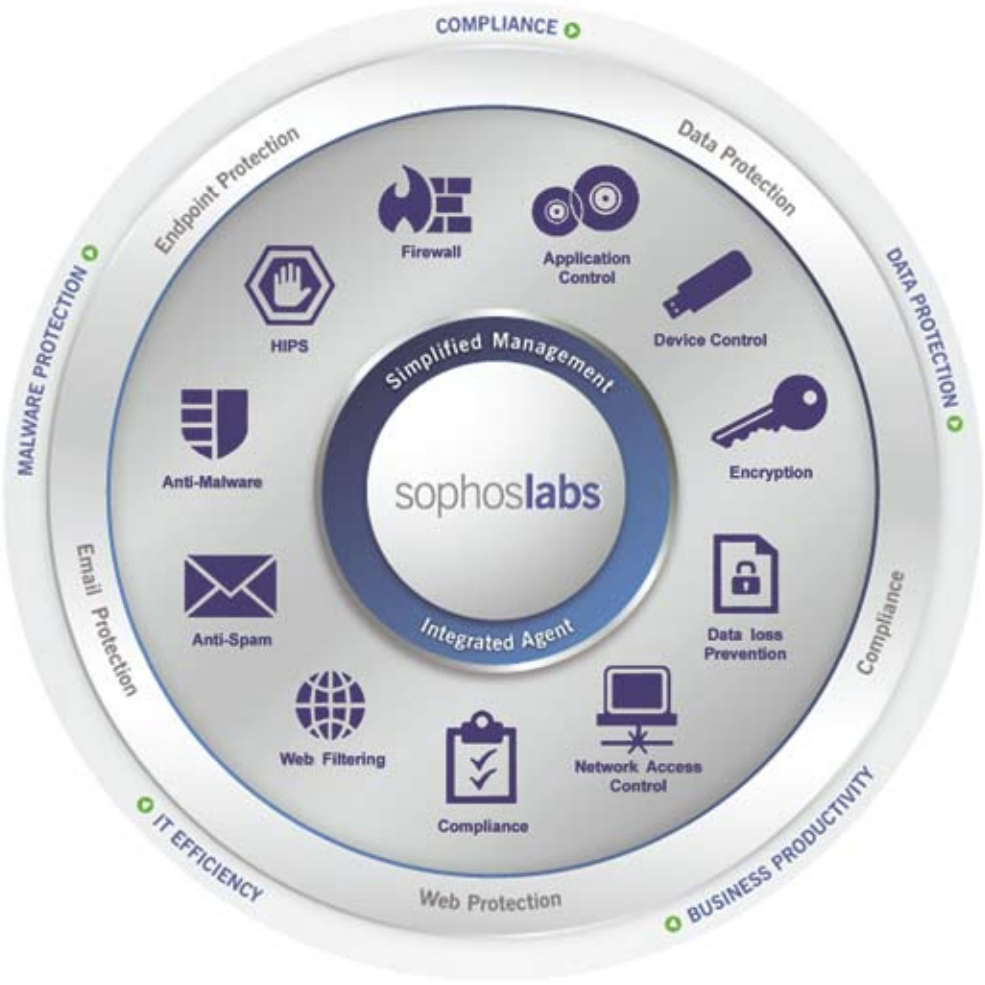
Misschien dat het ietwat overbodig is, maar mochten jullie mijn naam ineens zien verschijnen op twitter, dan durf ik jullie nu al te garanderen dat iemand mijn naam heeft gebruikt, dan wel misbruikt en dat hij mij min of meer heeft gestolen.

Tot twitter,
Berry

SOPHOS

secured.

Complete to compete!



Protect your data simply anywhere!

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

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

CRYPSYS data security