mei 2008 nummer 3

Dossier: SAS70, de ins en outs

Verslag Black Hat Europe 2008

Beveiligingsprobleem: is it a monster?

RBAC, géén ICT-feestje

Welkom in Iebeetopia...

INFORMATIEBEVEILIGING

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Voor dit nummer was ik op zoek naar een leuke afbeelding bij een van de artikelen. Internet is wat dat betreft natuurlijk een onuitputtelijke bron van verbazing en vermaak. Het betreffende artikel was een van de drie artikelen uit het SAS70 dossier in dit nummer. Op jacht naar een plaatje dus. En daar geldt wel een belangrijke regel voor: de bijdrage moet wel plaatsbaar zijn op grond van de licentie van het plaatje. Gelukkig hebben we daar een eenvoudig hulpmiddel voor. Alle artikelen in dit blad worden gepubliceerd onder een Creative Commons licentie. We hebben daar enige tijd geleden al iets over geschreven. Kenmerk van de licentie is dat distributie van 'werken' mag, mits... En die mits is voor ons blad simpel: verspreiden mag onder bronvermelding en veredelen van het artikel betekent dat het aangepaste werk ook onder dezelfde licentie plaatsvindt. Voor ons betekent het dat we dan ook plaatjes kunnen plaatsen die onder deze licentie zijn gepubliceerd. De zoektocht begint gewoon op de site van Creativecommons.nl. Daar staat bovenaan een functie om te zoeken naar werken. Als zoekwoord voerde ik in: audit. Simpel en doeltreffend.

En ik vind op Flickr.com tientallen foto's van een schoothondje. Wie noemt zijn hondje nu Audit?

Dat was meteen een korte intro naar ons dossier over SAS70. Een hot topic, dat nog relatief onbekend is, hoewel het al meer dan tien jaar bestaat. Drie artikelen waarin we SAS70 belichten vanuit het perspectief van de serviceverlener (die de TPM verkrijgt), de auditor (die het onderzoek uitvoert) en de toeschouwer of klant (die wil weten hoe hij ermee om moet gaan). Charles Eijk beschrijft waarom CagGemini een SAS70 onderzoek liet uitvoeren. Reynold ten Hoor beschrijft hoe een onderzoek wordt uitgevoerd en ondergetekende beschrijft wat SAS70 voor een klant betekent.

We zijn daarnaast heel blij met de bijdrage van Wolter Pieters. Hij weet alles van 'Monsters'. Een wetenschappelijk beschouwing op ons vakgebied. Hij vertelde het verhaal op het security congres afgelopen najaar, maar het is te leuk om het niet op papier te hebben. Wat ook altijd leuk is, is Black Hat. Dit keer maar liefst drie redacteuren die daar rondkeken. Hun impressie is te vinden vanaf pagina 5. Een volgende redacteur, Rob Greuter, laat wat andere inzichten zien op pag. 23. En we zijn ook altijd blij met Paul Overbeek. Hij levert de Questafette (zie pagina 28/29).

En voor de liefhebbers tot slot op pagina 24 en volgende het eerste deel van een drieluik over RBAC van John Rudolph en Rob Kroneman.

Tot zover, veel leesplezier gewenst!

André Koot,
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Sandra Kagie (eindredacteur,
TOPpers Media bv, Berlicum),
e-mail: sk@toppers.nl

Redactieraad
Lex Borger (LogicaCMG)
Hans Buijtelaar (Belastingdienst)
Lex Dunn (Capgemini)
Ray Flinkerbusch (MDG Infosec)
Rob Greuter
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Gerrit Post (CPA)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Ontwerp/Vormgeving
Ron Toonen, TOPpers Media bv, Berlicum

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

Druk
Roto Smeets GrafiServices Eindhoven

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

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

ISSN 1569-1063

De security specialisten van HintTech ondersteunen organisaties bij het definiëren en opzetten van het security management proces. Zij bewegen zich in en rond het snijvlak van business en ICT.

Door gebruik te maken van hun expertise en ervaring, krijgt u inzicht in, en controle op uw informatiebeveiliging. Mede door gebruik van de GrIB methode, is HintTech in staat snel en adequaat informatiebeveiliging in uw organisatie op de kaart te zetten.

Meer informatie op www.hinttech.com/security

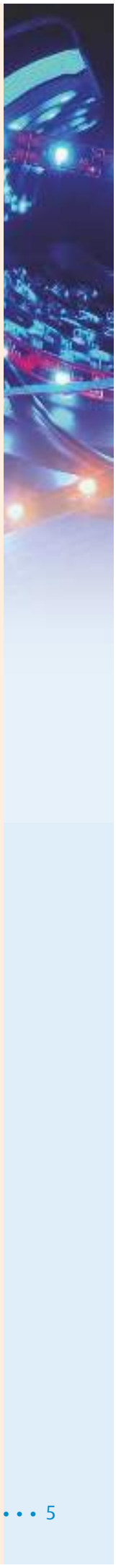
HINTTECH

DELFT | SAN FRANCISCO | NOVI SAD

www.hinttech.com | info@hinttech.com | + 31-(0)15-268 25 73

Black Hat Briefings 2008 – een impressie

Auteurs: Hans Buijtelaar (hans.buijtelaar@chello.nl), Lex Borger (lex.borger@logica.com) en Aart Jochem (aart.jochem@ictu.nl); allen leden van de redactieraad PvIB. Foto's: Lex Borger en Maarten Oosterink.



Donderdag 27 maart was het dan zover, de eerste dag van de beruchte briefings van Black Hat, dit keer de Black Hat Europe 2008 in Amsterdam. In twee dagen word je bijgepraat over de laatste stand van zaken aangaande hacking. Het programma bestaat uit twee tracks met in totaal 24 presentaties. Vrijdag na de laatste sessie konden we ons opmaken voor het schrijven van een artikel over deze briefings, maar uw 'reporters' zaten met een groot probleem: geen typemachine meer te vinden. Alleen zo'n machientje is waarschijnlijk opgewassen tegen hackers, al het andere is zo kwetsbaar als wat. Het moge dan ook duidelijk zijn dat het bijwonen van deze briefings de beste awareness sessie is die je kunt krijgen, ook al ben je nog zo gespecialiseerd in informatiebeveiliging. Hoe we deze dagen zijn doorgekomen...?

Proloog

Als informatiebeveiliger moet je een keer de Black Hat briefings hebben meegemaakt. Dus toen de uitnodiging bij het PvIB binnenkwam, waren er opeens voldoende schrijvers voor een artikel te vinden. Ter voorbereiding werden de verslagen van René Bense en Kelvin Rorive van de Black Hat briefings in 2005, van André Koot in 2006 en van Jim de Haas en Henk Bel in 2007 nog eens grondig doorgenomen. Wat opviel was dat deze schrijvers eenzelfde leerervaring hebben opgedaan: oprechte bewondering voor de technische knowhow bij de sprekers en een beter begrip van de dreiging die elk moment op kan doemen.

De eerste dag

De registratie verloopt vlot. Het feit dat je in het Engels wordt aangesproken, geeft direct al aan dat deze briefings tot ver over de landsgrenzen belangstelling genieten. Bezoekers komen van all over the world. Engels, Russisch, Chinees, Spaans, Italiaans, Duits, ... en nog een klein beetje Nederlands is er te horen deze dagen. Overigens geldt dat ook voor de sprekers die wereldwijd zijn geworven om ons als bezoeker bij te praten over de laatste hacks.

Jeff Moss, directeur van Black Hat neemt het openingswoord voor zijn rekening. Hij benadrukt dat Black Hat goed is voor het opdoen van technische kennis, maar dat het vooral ook een evenement wil zijn waar sociale interactie tussen sprekers en publiek onderling centraal staat. Om deze interactie te bevorderen wordt het "Speaker Meet and Greet" concept ingevoerd. Dit houdt in dat een spreker na zijn presentatie een uur lang in een aparte ruimte bevraagd kan worden door geïnteresseerden uit het publiek. De sfeer bij Black Hat is overigens zo dat naast deze meet en greet sessies vrijwel alle sprekers makkelijk aanspreekbaar zijn. Even een praatje maken met een spreker tijdens de koffie is geen enkel probleem. Na deze introductie is het de beurt aan de keynote speaker Ian Angell.

Digital Security: a Risky Business – Ian Angell

Ian, een bekend internationaal spreker, is Professor Information Systems aan de London School of Economics. De Times noemde hem ooit "the Angel of Doom" en dat geeft precies aan hoe hij over computertechnologie denkt: ondergeschikt aan de business, vaak veel te complex en zeker niet alleen de oplossing van veel problemen, maar juist ook vaak de oorzaak van veel problemen. Zeker voor het publiek is deze kijk verfrissend en prikkelend aangezien de meesten ICT als corebusiness zien. Waar doen we het eigenlijk voor? Ian komt niet met een echte oplossing, een visie hoe het anders zou kunnen, maar benadrukt wel dat de complexiteit omlaag moet.

Na de keynote beginnen de twee tracks met sessies. In het vervolg van deze samenvatting zullen we per sessie een korte samenvatting geven.

Client-side security – Petko Petkov

Petko, beter bekend als pdp, stelt dat een beveiligingsmodel zich niet alleen kan richten op de client of op de server, maar op beide. De wederzijdse afhankelijkheid tussen clients en servers is zo groot dat een veilige client en een veilige server niet automatisch leiden tot een veilige oplossing, de interacties tussen client en server moet ook in het beveiligingsmodel worden meegenomen. Na deze uiteenzetting neemt pdp het publiek in duizelingwekkende vaart mee van kwetsbaarheid naar kwetsbaarheid. Gevonden kwetsbaarheden in gmail, BT home hub, Flash, Second Life, Citrix en RDP, Skype, Firefox, Quicktime, Internet Explorer en Java passeren de revue. Niemand wordt gespaard en de les is dan ook dat elk stukje software kwetsbaarheden bevat waar de Hats (White, Grey en Black) actief naar op zoek zijn. Pdp, zichtbaar trots op gevonden kwetsbaarheden, vertelt dat er een verschuiving plaatsvindt in de zoektocht naar kwetsbaarheden door de Hats: het onderzoek richt zich meer en meer op de client om zodoende via een gecompromitteerde client de server aan te vallen. Na deze presentatie zijn de meeste bezoekers toe aan een flinke bak koffie.

Security Failures in Secure devices - Christopher Tarnovsky

Christopher neemt met ons de stappen door die nodig zijn om de geheimen bloot te leggen van embedded processors, zoals die in USB-tokens, autosleutels en smartcards worden gebruikt. Waar Karsten Nohl onlangs met polijsten de interne werking van de Mifare Classic smartcard ontcijferde, geeft Chriostopher aan de hand van tientallen voorbeelden weer hoe zijn aanpak werkt bij het kraken van chips: de chips worden ontdaan van behuizing en

beschermende lagen en met microscopisch kleine naalden worden data en instructies gelezen en gewijzigd. Hiermee worden algoritmes, data en sleutels ontdekt. Beveiligingen op de chip, zoals fuses, actieve maskers en lichtgevoelige sensoren worden hierbij omzeild. Tarnovsky geeft aan meer dan duizend chips te hebben onderzocht. Met zo'n tien exemplaren is hij in staat de meeste analyses af te ronden.

Attacking Anti-Virus - Feng Xue

Feng werkt voor Nevis Lab en is bij kenners beter bekend als Sowhat. Het onderwerp waarover hij spreekt, is "Attacking anti-virus". Anti-virus pakketten zijn complex en daardoor steeds vaker een interessant werkterrein voor hackers, aangezien complexiteit in relatie staat tot het aantal kwetsbaarheden. Bijkomend probleem is dat de meeste computergebruikers blindelings vertrouwen op de goede werking van anti-virus pakketten en de vraag is dus gerechtvaardigd of dit vertrouwen wel zo goed is. Een makkelijke oplossing is er overigens niet, aangezien anti-virus pakketten wel nodig zijn, maar zijn les is kritisch te blijven over alle genomen beveiligingsmaatregelen. De sessie van Feng geeft ook een andere kant van Black Hat aan: helaas zijn niet alle sprekers goed in staat een presentatie in het Engels te geven en voor niet alle sprekers geldt dat het geven van een presentie hun tweede natuur is, waardoor er wel eens onduidelijkheid bestaat over de bedoeling van de spreker; hetgeen soms leidt tot hilariteit. Gelukkig geldt deze handicap maar voor een kleine minderheid.

Cisco IOS Forensics – Felix 'FX' Lindner

Felix geeft aan dat er een monocultuur bestaat in componenten voor netwerkinfrastructuren. Cisco heeft een belangrijk marktaandeel en dus draaien veel core routers en switches op Cisco's IOS platform. Felix heeft de structuur van IOS onder de loep genomen: het bestaat uit één grote binary die rechtstreeks op de hardware draait, zonder beschermingslagen of privileges. Voor iedere configuratie is een aparte binary, er worden momenteel zo'n 10.000 versies ondersteund. Eigenlijk knap van Cisco dat ze dit stabiel weten te houden. Bekend is dat IOS een interessant aanvalsobject is, maar de vraag is: hoe kom je er achter dat de box gehackt is? IOS levert nauwelijks mogelijkheden voor analyse. Een crash kan alleen met een reboot worden hersteld, waarbij alle bewijzen verdwijnen. Crashlogs of SNMP MIBS bevatten nauwelijks zinnige gegevens, het onderscheid tussen functionele problemen of attacks is niet te maken. De enige optie is coredumps te analyseren. Felix heeft hiervoor een core dump analysis framework ontwikkeld, genaamd CIR (Cisco Information Retrieval). Dit framework stelt de gebruiker in staat uit de brij aan data nuttige informatie te destilleren voor verdere analyse.

Iron Chef Black Hat: John Henry challenge

Voor velen is het hoogtepunt van de dag de strijd tussen mens en machine in de Iron Chef - John Henry Challenge. Twee teams van ieder twee personen proberen in 45 minuten tijd zoveel mogelijk kwetsbaarheden te vinden in hetzelfde stukje software. Het ene team maakt gebruik van code reviews (de mens) en het andere team maakt gebruik van zelfgeschreven tools (de machine). De strijd wordt vergeleken met het gevecht van Kasparov met Deep Blue. Daar waar het publiek de rest van de dag behoorlijk relaxed overkomt,

bemerk je nu een zinderende spanning. Uitgelegd wordt hoe code reviews worden uitgevoerd en welke tools gebruikt kunnen worden bij het vinden van kwetsbaarheden. Drie van de vier “strijders” werken voor Fortify Software en één voor Cigital, dus is er geen reden voor een strijd op leven en dood, maar deze exercitie is vooral interessant om te zien hoe in de dagelijkse praktijk kwetsbaarheden worden gevonden. Gestructureerd werken en discipline zijn hiervoor belangrijke randvoorwaarden. Beide teams vinden meerdere kwetsbaarheden en de scheidsrechter, het publiek, bepaalt dat beide teams tot winnaar worden uitgeroepen.

0-day Patch-Exposing Verdors (In)Security Performance – Stefan Frei & Bernard Tellenbach

Op een conferentie waarbij het Apple sentiment het duidelijk wint van het Microsoft sentiment is deze presentatie een duidelijke tegenstromer. Twee onderzoekers hebben alle Microsoft en Apple patches van de afgelopen jaren onderzocht op de tijd tussen de eerste publicatie van de betreffende kwetsbaarheid en het uitbrengen van de patch. Twee belangrijke conclusies: Ten eerste is het patchproces van Microsoft stabiel daar waar Apple nog steeds aan het leren is. Bij Apple is namelijk een trend zichtbaar dat steeds meer kwetsbaarheden gelijktijdig openstaan daar waar het aantal gelijktijdig openstaande kwetsbaarheden bij Microsoft producten redelijk stabiel is. De tweede conclusie die de onderzoekers trekken, is dat beide bedrijven duidelijk niet twee dingen tegelijk kunnen doen: rond de release van een nieuw OS loopt de tijd tot het maken van een patch namelijk flink op. Link: http://www.techzoom.net/risk.

The fundamentals of physical security – Deviant Ollam

De eerste dag eindigt met een bijzonder leuke presentatie van Deviant. Deviant werkt voor The Open Organization of Lockpickers. Dat ook de fysieke beveiliging te hacken valt, laat Deviant verschillende keren zien. Sloten blijken niet bestand te zijn tegen zijn handigheid. Een onderhoudende sessie is het gevolg, waarbij de aandachtige toeschouwer op het puntje van de stoel zit.

De tweede dag

Bij de start van de tweede dag valt op dat het nogal rustig is. Waarschijnlijk hebben velen even een bezoekje gebracht aan Amsterdam. Tenslotte ben je niet elke dag in Amsterdam… Wel jammer voor de eerste sprekers, aangezien de belangstelling voor de eerste sessie tegenvalt.

URI Use and Abuse – Nathan McFathers en Rob Carter

De presentatie van Nathan en Rob is een echte eyeopener: de URI’s *http://*, *ftp://* *en telnet://* zijn wel bekend, maar dat er zoveel meer URI’s zijn geregistreerd en worden ondersteund door de verschillende browsers is voor velen minder bekend. Denk hierbij aan aim://, *firefoxurl://* *en picasa://*. Deze URI’s zijn de in feite de springplank vanuit de browser naar de applicaties. De sprekers laten zien hoe eenvoudig het is om middels XSS (cross-side scripting) technieken de URI’s als springplank te gebruiken om een stack overflow, command injection of andersoortige aanval op te zetten richting de applicatie. Nogmaals, jammer dat er zo weinig publiek zat want deze presentatie was zeker de moeite waard.

Mobile Phone spying tools – Jarno Niemelä

Jarno geeft een snelle cursus over de software omgeving van een Symbian telefoon.Verschillende “spy tools” passeren de revue. Deze tools zijn veelal vrijwel onzichtbaar voor de gebruiker. Het schadelijke werk, zoals het doorsturen van SMS naar de aanvaller of het registreren van toetsaanslagen, is zodoende nauwelijks zichtbaar. Maar de leveranciers van de smartphones zitten ook niet stil. De Symbian S60 3th edition smartphone bijvoorbeeld gebruikt een beveiligingsmodel waarbij applicaties worden gecertificeerd Verder gelden de gewone “PC” regels, zoals: gebruik anti-virus en houd het OS up-to-date. Nog een wijze raad van Jarno: roep bij malware besmettingen de hulp in van je mobiele operator, je enige vriend in bange dagen. En dan nog een laatste raad voor de paranoïden onder ons: wil je er zeker van

zijn dat een telefoon veilig is voor malware besmettingen, zet hem dan uit en neem de batterij eruit, maar zelfs bellen wordt dan wel heel moeilijk...

LDAP Injection & Blind LDAP Injection – Chema Alonso & Jose Parada Cimeno

LDAP injection is een interessante variant op SQL injection. Door het wijdverspreide gebruik van LDAP, de directe koppelingen met web-applicatie formulieren en de eenvoudige syntax zou LDAP injection wel eens een belangrijke aanvalstechniek voor hackers kunnen worden. Deze techniek richt zich grotendeels op zoekfilters. Wildcards kunnen eenvoudig worden toegevoegd aan URL's en invulvelden. Met tools laat Chema zien hoe dit soort aanvallen uitgevoerd worden.

Malware on the Net – Iftach Ian Amit

Deze presentatie over crimeware is zeker de moeite waard. Ian vertelt dat de criminaliteit op het net steeds volwassener wordt, dat meer gerichte aanvallen op een specifiek doel te zien zijn en dat steeds vaker gebruik wordt gemaakt van technieken als dynamic code obfuscation om de aanval te versluieren. Dat de criminaliteit steeds volwassener wordt, weten we wel, maar code obfuscation is voor de meeste aanwezigen in de zaal toch wel nieuw. Als voorbeeld een javascript. Normaal gesproken kan het kwaadaardige deel van zo'n script relatief eenvoudig worden gedetecteerd. Door gebruik te maken van code obfuscation wordt het kwaadaardige deel versleuteld waardoor detectie veel moeilijker wordt. Het gebruik van code obfuscation wordt als één van de belangrijkste technieken gezien om malware aan de man te brengen.

DTRACE: The ... Swiss Army Knife – David Weston & Tiller Beauchamp

DTRACE is een kernel-based dynamic tracing framework van Sun. Met DTRACE is het mogelijk vrijwel elk aspect van een systeem te tracen waardoor het analyseren van problemen een stuk makkelijker wordt, waaronder problemen met stack overflows. On the fly kunnen zogenaamde probes worden opgezet waardoor de werking van een stukje van het systeem gemeten wordt. Daarnaast kunnen scripts worden gebruikt waarvan vele out-of-the-box worden geleverd. Het meest interessante aan deze tool is dat het nauwelijks met verlies aan snelheid en capaciteit gepaard gaat, wat het geschikt maakt voor toepassing in productiesystemen. DTRACE lijkt een onmisbaar tool te worden voor het uitvoeren van analyses tijdens een hack-poging, toch maar een tool om te volgen. Apple heeft het al standaard in de Mac zitten, wie volgt?

Antiphishing Security Strategy - Angelo Rosiello

Phishing is momenteel vooral gericht op banken en een klein beetje op overheidsorganisaties. Maar websites van de overheid worden wel weer vaak misbruikt als host (in Italië tenminste). Phishing ontwikkelt zich nog steeds door onder meer nog moeilijker herkenbaar te zijn: foute en goede content worden gemixed middels embedded links, URL's zijn onherkenbaar gemaakt, via malware wordt verkeer bestemd voor de originele site geredirect naar phishing sites, et cetera. Angelo legt uit hoe een pagina automatisch geanalyseerd kan worden om de gebruiker te waarschuwen voor phishing. AntiPhish (een plugin voor de webbrowser) voert deze controle uit op het moment dat gegevens worden ingevuld. Hierbij worden achttien kenmerken in de HTML-source geanalyseerd. Deze kenmerken worden vergeleken met de originele pagina en de gebruiker krijgt een waarschuwing bij afwijkingen.

Intercepting Mobile Phone/GSM Traffic – David Hulton & Steve

Deze onderzoekers tonen twee dingen aan. Ten eerste dat GSM verkeer eenvoudig uit de ether te ontvangen en te interpreteren is. Een Nokia 3310 met kabel of een generieke software gestuurde radio ontvanger bijvoorbeeld kunnen gebruikt worden om het GSM verkeer op te vangen. Als tweede tonen zij aan dat een theoretisch bedachte aanval op het GSM encryptie algoritme (A5/1) in de praktijk uit te voeren is met weinig meer dan een PC en een FPGA kaart. In dertig minuten is elke sessiesleutel te kraken, waarbij gebruikgemaakt wordt van een tabel met mogelijke sessiesleutels.

Bad Sushi – Beating Phishers at Their Own Game – Nitesh Dhanjani & Billy Rios
Deze presentatie geeft een interessante kijk op de wereld van de phishers. Nitesh en Billy laten zien hoe ze door analyse van phishing scams inzicht krijgen in het weglekken van gegevens, waar ze tijdelijk bewaard worden op publiek toegankelijke fora en guestbook sites en hoe er rangen en standen zijn onder de phishers. Script kiddies krijgen wat scripts van de gevorderden en doen in feite het echte werk. De gevorderden, ofwel de masterminds, krijgen ongemerkt een kopie van alle door de script kiddies gephishte data toegestuurd. Eenmaal doorgedrongen tot dit publiek laten Nitish en Billy zien hoe in deze wereld het bedrog zich voortzet in de interacties onder elkaar. Men licht elkaar op, leidt elkaar om de tuin en rooft elkaars informatie. It's a jungle out there.

Hacking Second Life – Michael Thumann
De man die vorig jaar Cisco's NAC uiteenrafelde met een attack-tree benadering heeft dit nu toegepast op Second Life. Diverse interessante aanvallen zijn te bedenken, maar enkele kunnen legaal worden uitgevoerd. Thumann's conclusie is dat de Second Life viewer (open source) relatief goed beveiligd is. Het aardigst is het scannen van websites in de echte wereld vanuit Second Life. Hiervoor heeft Michael de Nikto Vulnerability scanner gemigreerd naar Linden Scripting Language en gekoppeld aan een object in Second Life. Als het object wordt aangeraakt, start de scan en als een kwetsbaarheid wordt gevonden, krijgt de hacker een mailtje. Hij heeft het script beschikbaar gesteld onder de naam Slikto (natuurlijk). Verreweg de mooiste user interface voor een hacktool.

Investigating Individuals and Organizations Using Open Source Intelligence – Roelof Temmingh en Chris Böhme
Het beste van de tweede dag komt als laatste, de presentatie van Roelof en Chris. Vooral Roelof is een spreker waar het publiek op blijft wachten. Het onderwerp leent zich er natuurlijk ook voor: hoe makkelijk is het om informatie te achterhalen van individuen en organisaties door gebruik te maken van open bronnen? Roelof heeft al zijn kennis gestopt in Maltega, een applicatie waarmee je met enkele klikken op de muis inzichtelijk krijgt wie met wie contacten heeft door slim gebruik te maken van sociale netwerken, zoekmachines, maar bijvoorbeeld ook door eigenschappen van documenten te analyseren. Stel je vindt een document van iemand op het internet. De eigenschappen van dit document geven misschien wel een aanwijzing waar iemand werkt, of ander interessant materiaal. Dat er juridische consequenties zullen zijn moge wel duidelijk zijn. Roelof schetst een toekomst waarin virtuele en echte identiteiten niet meer te onderscheiden zijn: ook een virtuele identiteit heeft een e-mailadres en een actieve blog, dus de identiteit bestaat, toch? Door grote hoeveelheden virtuele gebruikers te laten leven op het net kunnen opinies en politiek beïnvloed worden. Dat zet je aan het denken.
Deze presentatie vormt in elk geval een prikkelend einde van de briefings.

Epiloog
Zoals in de inleiding al aangegeven zijn er 24 presentaties gegeven, waarvan je de helft kunt volgen. Het is erg jammer dat je die andere helft aan je voorbij moet laten gaan. De sprekers zijn vrijwel allemaal zeer deskundig en goed toegankelijk. De trend is duidelijk: de hacking scene gaat zich meer en meer bemoeien met applicaties. Al met al zijn deze twee dagen zeer leerzaam geweest en komen we graag nog eens terug.

Dus hebben we de verslagen van de voorgaande jaren nog eens doorgenomen en komen we tot een heldere conclusie: er is echt niets veranderd; oprechte bewondering en een beter begrip!

De 'global warming' van GSM encryptie
Het lezen over GSM encryptie – en het breken daarvan – is net als het lezen over de opwarming van de aarde. Ondanks het feit dat geleerden al tijden roepen dat het kan gebeuren, wordt er gedacht dat het zo'n vaart nog niet loopt.
GSM encryptie is gebroken en niet alleen theoretisch. Op de Black Hat conferenties in Washington DC en Amsterdam hebben twee onderzoekers aangetoond dat GSM verkeer eenvoudig te onderscheppen is met een Nokia 3310 of een USRP (universele radio met software sturing). Vervolgens breken ze de sessiesleutel in zo'n 30 minuten met goedkope apparatuur, waardoor alle communicatie beluisterbaar en zichtbaar wordt. Israëlische onderzoekers hadden al in 2003 zo'n aanval theoretisch beschreven.
GSM encryptie was van origine geheim, maar het algoritme is uiteindelijk gepubliceerd. Ross Anderson schreef in 1994 al dat het algoritme niet deugt. Sindsdien zijn er meerdere mogelijke aanvallen beschreven. Er is zelfs een nieuw algoritme ontwikkeld: Kasumi, ook bekend als A5/3. Kasumi wordt nog niet algemeen gebruikt.

Je kunt je natuurlijk afvragen hoe erg dit is. Omdat bij de aanval een gigantische opzoektabel wordt gebruikt (meerdere Terabytes), die nog niet eens volledig gevuld is, is honderd procent succes nu nog niet mogelijk. Dit is echter slechts een kwestie van tijd. Voor de particuliere telefoongebruiker heeft een mogelijke inbreuk op privégesprekken nauwelijks gevolgen. Maar wat vindt de zakelijke gebruiker hiervan? Ontkent hij de opwarming van de aarde nog steeds?
Wat kan er aan de encryptie van GSM gedaan worden? Gelukkig is het versterken van GSM encryptie eenvoudiger dan CO2 reductie. Een pleister op de wond is het vaker authenticeren van de telefoon. Dit verkort de geldigheidsduur van een sessiesleutel. Effectiever is om over te gaan op het gebruik van Kasumi als algoritme. Dit vergt wel infrastructurele aanpassingen in het netwerk en de telefoons.

Van trust me en tell me naar show me

Auteur: Charles Eijck > Charles Eijck is werkzaam bij Capgemini Outsourcing B.V. als Quality Manager.
E-mailadres: Charles.Eijck@capgemini.com.

Wat heeft Capgemini Outsourcing B.V. (CgO) te maken met de Amerikaanse overheid? Veel meer dan op het eerste gezicht lijkt. Om mondiaal opererende klanten te kunnen bedienen moet CgO voldoen aan de strengste eisen. In dit geval zijn die afkomstig van de andere kant van de oceaan.

Nadat pijnlijk duidelijk werd dat beursgenoteerde bedrijven in Amerika hun aandeelhouders wisten te misleiden, soms leidend tot een onverwacht faillissement zoals bij Enron in 2002, waardoor 21.000 medewerkers op straat kwamen staan en het bedrijf een schuld van 20 miljard dollar achterliet, werd de roep om verandering groot.
Het is deze trieste gebeurtenis die het bestaan van de Sarbanes-Oxley Act (SOx) verklaart. In deze wet, ingediend door de senatoren Sarbanes en Oxley, stelt de Amerikaanse overheid eisen aan de manier waarop bedrijven de risico's in de administratie en de processen moeten beheersen. Die moeten deugdelijk en transparant zijn door de hele productieketen. Managers worden verantwoordelijk voor de integriteit van de financiële rapportage en kunnen bovendien persoonlijk aansprakelijk worden gesteld voor schade die voortvloeit uit een ondeugdelijke boekhouding. Ook als zij zelf niet de directe uitvoerders zijn van de controlemaatregelen, blijven zij wel verantwoordelijk voor de uitvoering.

Van SOx naar SAS

Ook als organisaties een gedeelte van de administratie, bedrijfsprocessen of het beheer van systemen bij een outsourcing-partner hebben ondergebracht, vereist SOx dat de organisatie hier zelf voor verantwoordelijk blijft ten aanzien van het voldoen aan wet- en regelgeving. Dientengevolge zal de accountant ook moeten nagaan of de outsourcing-partner voldoet aan wet- en regelgeving. Outsourcing partijen spelen hier handig op in door dit onderzoek in samenwerking met hun eigen accountant uit te voeren en de uitkomsten van dit onderzoek middels een rapport beschikbaar te stellen aan haar klanten. Hierbij onderkent men twee type rapporten:

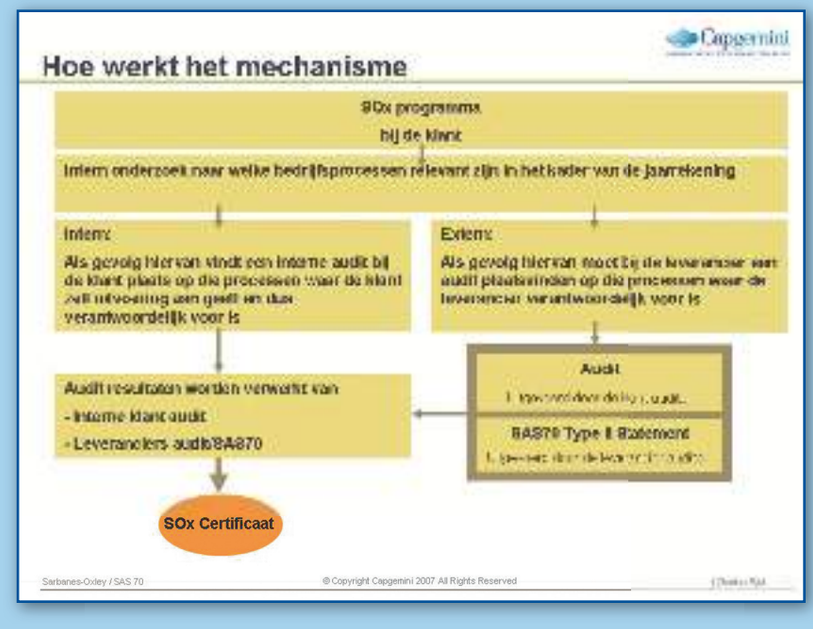
- SAS70 Type I: Dit rapport geeft een oordeel ten aanzien van opzet en bestaan;
- SAS70 Type II: Dit rapport geeft een oordeel ten aanzien van de werking over een periode van ten minste zes maanden.

De accountant van de klantorganisatie kan op het SAS70 Type II rapport steunen bij het beoordelen van de diensten die zijn ondergebracht bij de outsourcing partij.

Aangezien CgO een mondiale speler is met vestigingen in Amerika, Europa en India is een Controls Framework ontwikkeld in samenwerking met PricewaterhouseCoopers. Dit Controls Framework, bestaande uit 22 controle doelstellingen, is zodanig ontwikkeld dat het voor de totale IT-dienstverlening van CgO toepasbaar is. Hiermee zijn we in staat om wereldwijd, voor alle klanten, een identiek Controls Framework toe te passen hetgeen grote efficiency voordelen heeft voor CgO en dus kostenvoordelen voor de klant. Door het toepassen van dit raamwerk is het tevens mogelijk inzicht te geven in de genomen controlemaatregelen. Dit inzicht heeft de auditor van CgO nodig om een SAS70 verklaring af te geven en de auditor van de klantorganisatie om te beoordelen of hierop kan worden gesteund.

Extra kosten

CgO heeft een team van tussen de vijf en tien mensen samengesteld uit de bestaande operatie om alle voor SAS70 vereiste controles te testen en indien nodig bij te sturen. CgO ziet werken volgens de zorgvuldigheidseisen van SAS70 als een service element. Dat daar een prijskaartje aanhangt, is duidelijk. Tegelijkertijd denken we hard na over mogelijkheden



om de kosten naar beneden te brengen. Dit bijvoorbeeld door interne audits te laten uitvoeren waarbij het benodigde bewijsmateriaal intern al verzameld wordt. Dit bewijsmateriaal kan de auditor vervolgens gebruiken voor dossiervorming.

Hogere eisen welkom

De SAS70-'compliance' wordt door de buitenwereld min of meer aan CgO opgedrongen. Toch verwelkomt CgO de hogere eisen die aan de dienstverlening worden gesteld, aangezien deze hogere eisen moeten leiden tot een betere dienstverlening aan klantorganisaties. Het bezig zijn met SAS70 zal moeten resulteren in een betere risicobeheersing. Maar risicobeheersing, het streven naar een nul-fouten resultaat, leeft nog te weinig binnen de IT. Binnen CgO komen we hieraan tegemoet door de noodzaak van SAS-'compliance' continu onder de aandacht te brengen bij zowel medewerkers als het management.

Standaardisatie

Door de grote aandacht voor procesbeheersing en de noodzaak fouten uit te sluiten zien we ook het belang om onze dienstverlening voor onze klanten op een eenduidige manier uit voeren. Door zo min mogelijk uitzonderingen op de wijze van dienstverlening te laten ontstaan, is de kans op fouten geminimaliseerd en zijn ook de kosten voor het auditen van de processen ten behoeve van deze dienstverlening geminimaliseerd.
Als voorbeeld het Change Management proces. Dit proces wordt voor verschillende klanten op een identieke wijze uitgevoerd met identieke controles en bijbehorend bewijsmateriaal, met als gevolg dat een auditor het Change Management proces slechts één keer hoeft door te lichten.

Dat CgO ernaar streeft om de dienstverlening te standaardiseren, betekent overigens niet dat er geen maatwerk meer plaatsvindt. Dat blijft gewoon mogelijk. Maatwerk heeft niet alleen impact op de dienstverlenende organisatie, maar ook op de klantorganisatie. In een SAS70 rapport is dit terug te vinden als een 'User Consideration'.

Een voorbeeld hiervan is bijvoorbeeld de onderstaande User Consideration:
"The customer is responsible for authorizing Capgemini Outsourcing B.V. to establish access to customer systems."
Ofwel, de klant is verantwoordelijk om een geautoriseerde aanvraag in te dienen om een medewerker van CgO toegang te verschaffen tot één van zijn systemen.

Aan de hand van dit voorbeeld zie je dus dat een SAS70 rapport niet alleen impact heeft op de organisatie bij de dienstverlener, maar ook op de klantorganisatie. De klantorganisatie zal een autorisatieproces binnen haar organisatie moeten beschrijven en inrichten. De dienstverlenende partij

zal het verzoek conform een beschreven procedure in ontvangst moeten kunnen nemen en verwerken.

CgO heeft een hoge mate van standaardisatie van de dienstverlening doorgevoerd en het gedefinieerde SAS 70 framework is hierop goed toepasbaar. Door de optimale inzet van CgO-medewerkers is over het afgelopen jaar een 'clean statement' bereikt. Dit wil zeggen dat er geen afwijkingen ('deficiencies') in het rapport gemeld zijn.

Quality Dashboard

Eén manier waarop de organisatie geïnformeerd wordt over de status ten aanzien van alle controlemaatregelen (niet alleen ten aanzien van SAS70, maar ook ISO9001 en ISO27001) is door middel van een maandelijkse rapportage aan het management waaruit blijkt hoe het gesteld is met de 'compliancy'.

Hierin kan het management in één oogopslag zien waar zwakke punten in de organisatie zitten. Het is een driekleuren systeem; Groen betekent dat alles foutloos verloopt, Geel is voldoende, maar niet 100% en Rood is de alarmkleur. Fouten zijn nooit helemaal uit te sluiten. Dat beseft niet alleen CgO, maar gelukkig ook de klant, de accountant en de Amerikaanse regelgever.

In essentie zorgt een SAS70 rapport ervoor dat de Administratieve Organisatie en Interne Control (AO/IC) zodanig is inricht dat problemen snel zichtbaar worden, waardoor ook snel kan worden ingegrepen om fouten te herstellen en verdere schade te voorkomen. Tevens wordt ervoor gezorgd dat de fout niet nogmaals kan optreden.

Link

- *http://www.npn-online.com/news/fullstory.php/aid/84/SAS_70_garandeert_transparantie_en_gefundeerd_vertrouwen_bij_uitbesteding.html*

Is YOUR data leaking?

Data encryption protects your company's critical data if it ends up in the wrong hands. Data leakage prevention solutions save you from unintentional or malicious data threats inside your organization.

Working together, **SafeGuard® Enterprise** and **SafeGuard® LeakProof™** secure all your data—at rest, in motion, and in use.

Data Encryption
+ Data Leakage Prevention

Data Security 360° by Utimaco

utimaco®
The Data Security Company.

www.utimaco.com

‘SAS70 maakt interne controle transparant’

Drs. Reynold S.L. ten Hoor RE > Reynold ten Hoor is sinds 2000 IT-auditor bij PricewaterhouseCoopers en heeft ruime ervaring opgebouwd in het coördineren van audits voor het uitbrengen van onafhankelijke mededelingen (third-party assurance) waaronder SAS70 op het gebied van inrichting en beheer van ICT-omgevingen. Hij studeerde Economie aan de Universiteit van Maastricht en voltooide de opleiding IT auditing aan de Erasmus Universiteit in Rotterdam. E-mail: reynold.ten.hoor@nl.pwc.com.

In uitbestedingsituaties komt het regelmatig voor dat serviceorganisaties worden geconfronteerd met meerdere auditors van hun cliënten. Om zekerheid te verkrijgen over de uitbestede processen wordt door gebruikersorganisaties ‘the right-to-audit’ geëffectueerd waarmee generieke processen telkens weer door verschillende auditors worden onderzocht. Kan SAS70 soelaas bieden en overbodig onderzoek voorkomen? Dit artikel gaat in op de betekenis van SAS70, de verschillen ten opzichte van andere third-party mededelingen en de voor- en nadelen vanuit het gezichtspunt van de auditor.

Wat is SAS70?

De ‘Statement on Auditing Standards (SAS) No. 70 voor Service Organisaties’, is een algemeen geaccepteerde audit standaard die is ontwikkeld door het American Institute of Certified Public Accountants (AICPA). Deze standaard is een leidraad voor het uitbrengen van een third-party memorandum (TPM) over de interne beheersing van primaire en ondersteunende bedrijfsprocessen. SAS70 wordt met name toegepast in situaties waar de auditor (‘User Auditor’) voor een gebruikersorganisatie (‘User organization’) de financiële controle uitvoert waarvan deels processen zijn uitbesteed aan een Serviceorganisatie (‘Service organization’). De Serviceorganisatie brengt zelfstandig een SAS70 uit met een verklaring van de eigen auditor (‘Service auditor’), die gebruikt kan worden voor haar eigen verantwoording en waarop de User auditor kan steunen. De gebruikers van SAS70 rapportages bevinden zich in velerlei branches: van banken en verzekeraars tot telecom en industrie. De rapportage en bijbehorende verklaring worden gebruikt om zekerheid te krijgen over de kwaliteit van interne controle met betrekking tot de uitbestede processen. Voorbeelden van serviceorganisaties die deel uitmaken van de interne controleomgeving van gebruikersorganisaties zijn bijvoorbeeld datacenters, applicatie service providers en verwerkingscentra voor data zoals claims of andere transacties. Vandaag de dag dienen serviceorganisaties proactief aan te tonen dat adequate maatregelen zijn geïmplementeerd voor het beheersen van de risico’s in de omgevingen die zij voor hun cliënten beheren.

SAS70 biedt richtlijnen voor een onafhankelijke auditor (‘service auditor’) om een opinie te geven over de beschrijving van beheersmaatregelen van de serviceorganisatie door middel van een zogenaamd ‘Service Auditor’s Report’. SAS70 schrijft geen vastomlijnde set van doelstellingen en maatregelen voor die serviceorganisaties dienen uit te voeren. SAS70 werkt dus niet volgens een checklist en stelt geen normen voor beheersing, maar service auditors dienen wel de AICPA standaarden te volgen die voorschrijven op welke wijze onderzoek, kwaliteitscontrole en rapportage plaats dient te vinden. Hierdoor kan op de gerapporteerde uitkomsten worden gesteund door interne en externe partijen waaronder in het bijzonder de accountants van derde partijen.

Voor een SAS70 mededeling van het type I, maakt de auditor een beoordeling van de toereikendheid van de beheersmaatregelen in aansluiting op de ontworpen beheersdoelstellingen (opzet). Ook wordt voor elke maatregel de nodige bewijslast vastgelegd om aan te tonen dat de beheersmaatregel in praktijk wordt uitgevoerd conform het ontwerp (bestaan). Voor een SAS70 van het type II volgt naast de werkzaamheden voor opzet en bestaan tevens een uitgebreide testronde om de werking van de maatregelen aan te tonen over een vooraf vastgestelde periode van minimaal een half jaar. In de rapportage van een type II verklaring wordt een omschrijving opgenomen van de uitgevoerde testactiviteiten en de resultaten hiervan. Ten behoeve van het opstellen van de uiteindelijke verklaring dient de auditor de opgetreden deficiënties te beoordelen, te onderzoeken in hoeverre hiervoor compenserende maatregelen aanwezig zouden kunnen zijn en ten slotte zorgvuldig af te wegen of deze tekortkomingen resulteren in het wel of niet behalen van de gedefinieerde beheersdoelstellingen.

‘SAS70 maakt interne controle transparant’

Toelichting

- Opzet - Procedures of werkinstructie waarin is weergegeven hoe een beheersmaatregel in ontwerp plaats zou moeten vinden (bijvoorbeeld autorisatieprocedure, procedures voor de verwerking van claimaanvragen).
- Bestaan - Documentatie waaruit blijkt dat een beheersmaatregel in praktijk wordt uitgevoerd conform opzet (bijvoorbeeld rapportages, logbestanden, checklists, wijzigingenregistraties et cetera).
- Werking - Het door middel van deelwaarnemingen aantonen van de werking van een beheersmaatregel over een langere periode (bijvoorbeeld rapportages over de maanden januari t/m juni, registraties van een aantal dagen).

Het belangrijkste verschil met andere TPM’s is dat de definitie van beheersdoelstellingen en -maatregelen die worden gebruikt door de serviceorganisatie zelf wordt samengesteld in plaats van een set van normen die door de gebruikersorganisatie wordt opgelegd. Het voordeel is dat hierdoor het raamwerk geheel kan worden afgestemd op de eigen organisatie en de manier waarop de beheersmaatregelen worden uitgevoerd.

Bijkomend voordeel boven een andere TPM is dat een SAS70 algemeen aanvaard wordt omdat richtlijnen zijn opgesteld ten aanzien van testwerkzaamheden, kwaliteitscontrole en rapportage. Het SAS70 rapport staat voor een grondig, diepgaand onderzoek van de beschreven beheersdoelstellingen en -maatregelen in de voor de financiële administratie relevante processen door een onafhankelijke accountant en auditor. De eisen in sectie 404 van de Sarbanes-Oxley wetgeving van 2002 maken SAS70 rapportages nog belangrijker in relatie tot het proces van rapporteren over de effectiviteit van interne controle ten behoeve van de financiële rapportage.

Gezichtspunt van de auditor

Als onafhankelijke auditor begeleidt PricewaterhouseCoopers cliëntorganisaties in het samenstellen van een raamwerk voor SAS70 onderzoeken. Dit raamwerk bestaat uit een definitie van beheersdoelstellingen voor elk van de risico’s die zijn geïdentificeerd binnen de processen die in scope zijn. Aansluitend worden door de cliënt de nodige beheersmaatregelen geformuleerd om de gedefinieerde beheersdoelstellingen te kunnen realiseren. Als voorbereiding is het samenstellen van dit raamwerk van groot belang. Is het raamwerk te uitgebreid dan verliest de lezer al snel het overzicht. Wordt het raamwerk te beperkt gedefinieerd dan verliest het de diepgang die nodig is om de gewenste transparantie te bieden.

Het uiteindelijke doel van de SAS70 rapportage is een zodanige transparantie te bieden aan de afnemende organisaties dat zekerheid wordt gegeven over de uitvoering van de voor de betreffende organisatie relevante processen. Als voorbereiding op het SAS70 onderzoek is het daarom van groot belang om de scope nauwkeurig vast te stellen, bestaande uit de objecten van onderzoek (welke processen, applicaties, onderliggende platformen en databases worden onderzocht), de aspecten die hiervan worden beoordeeld (Juistheid, Volledigheid, Validiteit, Toegangsrestricties) en de te hanteren normen (algemeen versus specifiek van aard).

Objecten van onderzoek

De uitvoering van processen door de serviceorganisatie is naast het leveren van kwaliteit gericht op efficiëntie en het behalen van schaalvoordelen, met als gevolg dat de applicaties van de klanten waarvoor het onderzoek wordt verricht veelal zijn ondergebracht op IT-omgevingen die ook met andere klanten worden gedeeld. Om die reden zullen niet alle objecten die beheerd worden voor de serviceorganisatie in scope zijn. Voor het uitvoeren van testen voor de cliënten in scope is het dus van belang om duidelijk in kaart te brengen welke platformen, systemen en databases in het onderzoek moeten worden meegenomen. Bovendien gelden voor de verschillende technologische platformen veelal verschillende procedures en werkwijzen voor het onderhoud en het productiebeheer. Door een nauwkeurige scoping uit te voeren kan worden gespecificeerd welke procedures van toepassing zijn.

Aspecten van onderzoek

Om te kunnen bepalen of het raamwerk van beheersdoelstellingen en -maatregelen toereikend is voor de mate waarin de serviceorganisatie transparantie wil geven over de mate van interne controle, dient te worden onderzocht of de aspecten van de informatievoorziening die van toepassing zijn op het betreffende proces, zijn afgedekt door een beheersdoelstelling. Vervolgens zullen de gedefinieerde beheersmaatregelen aan moeten sluiten op de doelstellingen zodat de relevante aspecten voldoende zijn afgedekt. Op het hoogste niveau wordt gekeken naar de aspecten *juistheid*, *volledigheid*, *tijdigheid*, *validiteit* en *toegangsrestricties*. De definitie hiervan is opgenomen in het kader. Deze begrippen kunnen nog verder doorvertaald worden naar specifiekere deelaspecten.

Definitiekader

- Juistheid - Transacties worden voor het correcte aantal/ bedrag ingevoerd en bij de juiste rekening;
- Volledigheid - Alle transacties zijn ingevoerd en geaccepteerd voor eenmalige verwerking;
- Tijdigheid - Transacties worden binnen het juiste tijdsbestek (boekingsperiode) verwerkt;
- Validiteit - Slechts geautoriseerde transacties die daadwerkelijk hebben plaatsgevonden worden verwerkt;
- Toegangsrestricties - Toegang tot vertrouwelijke data en fysieke bedrijfsmiddelen wordt op gepaste manier beperkt tot geautoriseerd personeel en gegevens worden beschermd tegen ongeautoriseerde wijzigingen.

Normenkader

Tot slot rest nog de keuze voor de te hanteren normen. Een voordeel van het gebruik van bestaande normen als Cobit voor de ICT-processen, is dat deze

algemeen aanvaard en bekend zijn. Bedrijfsmatige processen zijn echter veelal specifieker van aard en alleen van toepassing op de eigen organisatie. Hiervoor dienen dan ook specifieke normen te worden geformuleerd die in lijn zijn met de eisen die aan de processen worden gesteld.

Knelpunten

Hiermee komen we gelijk op een belangrijk aandachtspunt van SAS70. Het blijft namelijk de vraag welke normen het best gehanteerd kunnen worden om de gewenste zekerheid te verschaffen. Het is voor een gebruikersorganisatie die processen aan meerdere partijen heeft uitbesteed moeilijk om zekerheid te verkrijgen over de betrouwbaarheid van die omgevingen indien hiervoor verschillende normen worden gehanteerd die nauwelijks zijn te vergelijken. Maar de voornaamste knelpunten bij het uitvoeren van een SAS70 onderzoek liggen toch op het vlak van communicatie. Voor het bereiken van een goede invulling van een SAS70 is communicatie in de vorm van samenwerking tussen enerzijds de proceseigenaren in de serviceorganisatie en anderzijds de onafhankelijke auditor essentieel. Beeldvorming over hoe een beheersmaatregel in praktijk gestalte heeft gekregen, is veelal meer complex dan aanvankelijk in opzet was beschreven. In de werkelijke uitvoering heeft een beheersmaatregel vaak betrekking op verschillende applicaties en platformen en zijn hier meerdere personen of afdelingen bij betrokken. Ook blijkt dat maatregelen in praktijk per operationeel of technisch aandachtsgebied een verschillende invulling hebben gekregen en verschillende wijzen van testen vereisen. Van standaardisatie is geen sprake, de invulling en betekenis van SAS70 kan onderling maar ook per jaar verschillen.

Transparantie

Toch is SAS70 een waardevolle manier om de nodige transparantie te bieden aan klantorganisaties. Indien het raamwerk zorgvuldig is samengesteld, geeft SAS70 gedetailleerd inzicht in hoe interne controle is vormgegeven binnen de serviceorganisatie en de manier waarop bepaalde beheersingsrisico's zijn afgedekt. Het kan de verdeling van onderlinge relaties en verantwoordelijkheden in de totale keten van bedrijfsprocessen verder verduidelijken. Bovendien biedt SAS70 een gestructureerde mogelijkheid om op jaarlijkse basis verbeteringen of organisatieveranderingen door te voeren. SAS70 wordt door accountantsorganisaties onderling algemeen geaccepteerd in het kader van de jaarrekeningcontrole en wordt gezien als een volwaardige mogelijkheid om verantwoording af te leggen aan derden. SAS70 kan daarom worden gezien als een 'kwaliteitskeurmerk' voor zowel de huidige afnemers als potentiële cliënten van gebruikersorganisaties.

Checklist voorbereiding SAS70

- ✓ Zijn alle relevante risico's binnen de processen die in scope zijn, in kaart gebracht?
- ✓ Is voor elk van de gedefinieerde risico's een heldere beheersdoelstelling geformuleerd?
- ✓ Zijn de beheersmaatregelen 'SMART' geformuleerd, zodat duidelijk is welke verantwoordelijke functionaris welke activiteit verricht en met welke frequentie? (SMART staat voor Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden.)
- ✓ Zijn alle testactiviteiten ten aanzien van het aantonen van opzet, bestaan en werking van de beheersmaatregelen duidelijk gedefinieerd?
- ✓ Is het SAS70 traject bij zowel het management als procesmedewerkers toegelicht? (draagkracht en motivatie)
- ✓ Zijn proceseigenaren benoemd die de verantwoordelijkheid voor de (tijdige en correcte) uitvoering van de beheersmaatregelen dragen?

Voordelen van SAS70 vanuit verschillende gezichtspunten

Serviceorganisatie

- Biedt transparantie van de interne controleomgeving;
- Gestructureerde mogelijkheid om interne controle te (her)definiëren en op jaarlijkse basis verbeteringen door te voeren;
- Hulpmiddel om organisatieveranderingen door te voeren;
- Verduidelijken van de verdeling van onderlinge relaties/ verantwoordelijkheden in de keten;
- Flexibiliteit in het opstellen van normen op basis waarvan de interne beheersing wordt getoetst;
- Kan worden gezien als een 'kwaliteitskeurmerk' voor zowel huidige afnemers als potentiële cliënten.

Gebruikers organisatie

- Transparantie van de leveranciersorganisatie en de manier waarop bepaalde beheersingsrisico's zijn afgedekt;
- Duidelijk overzicht van beheersmaatregelen en inzicht in eventuele tekortkomingen en de betekenis daarvan;
- Algemene (internationale) acceptatie door accountants van belanghebbende partijen in het kader van de jaarrekeningcontrole;
- Volwaardige mogelijkheid om verantwoording af te leggen aan derden.

Auditor

- Uniforme standaard van rapporteren over interne controle en de wijze waarop beoordeling van opzet, bestaan en werking van interne beheersing geschiedt;
- De beheersmaatregelen zijn geformuleerd door de serviceorganisatie en volgen de wijze waarop de organisatie is vormgegeven;
- Vanuit SAS70 rapportage kan zekerheid ontleend worden ten behoeve van de jaarrekeningcontrole;
- De serviceorganisatie is gemotiveerd om geschikte maatregelen te definiëren en correcte werking hiervan aan te tonen.

SAS70, wat heb je eraan?

Auteur: André Koot > André Koot is CISO bij Univé-VGZ-IZA-Trias en hoofdredacteur van het blad Informatiebeveiliging.

Vroeger, toen was het simpel. Als je een IT-organisatie was, die IT-diensten leverde, liet je gewoon een EDP auditor langskomen om een technical audit of een system audit uit te voeren. Het rapport met bevindingen resulteerde al dan niet in een actieplan en het volgende jaar werd hetzelfde opnieuw uitgevoerd. In auditermen leek dat wel op een gegevensgericht onderzoek. Dergelijke onderzoeken zijn niet efficiënt, wel effectief, ze bieden namelijk inzicht, maar alleen ten aanzien van het onderzochte object.

In het midden van de jaren negentig van de vorige eeuw ontstond niet alleen het nieuwe vakgebied Operational Audit dat zich ging richten op interne beheersing, maar gingen ook IT auditors zich bezighouden met een nieuwe tak van sport, de procesgerichte onderzoeken. Je zou kunnen zeggen dat daarmee de concurrentie met het nieuwe vakgebied Operational Auditing werd aangegaan, maar de echte aanleiding was dat de invoering van ITIL binnen de IT-organisaties ook leidde tot de wens om inzicht in de IT-processen te krijgen. Effectiviteit en efficiency van de procesgang werden onderwerp van controle. Een ontwikkeling als het INK kwaliteitsmodel speelt een grotere rol. En grotere IT- dienstverleners ontdekten vervolgens het instrument TPM, het Third Party Memorandum, waarmee de kwaliteit van de dienstverlening aangetoond kon worden. De dienstverlener kon het TPM rapport als een soort keurmerk hanteren bij het acquisitieproces. Voordien kon elke klant van een dienstverlener zelf een audit laten uitvoeren, maar het is duidelijk dat naarmate het aantal klanten toeneemt, de auditlast ook toeneemt. Door het TPM instrument hoeft elke dienstverlenende organisatie maar één keer een audit te laten uitvoeren. De besparing is evident.

Een groot bezwaar van het TPM instrument is dat het leidt tot een verklaring, maar dat voor de verschillende klantengroepen de waarde van die verklaring verschilt. Voor de ene klant is de TPM nuttig, voor de ander interessant. De reden hiervoor? Het gehanteerde normenkader. Het is niet altijd duidelijk welk normenkader wordt gehanteerd. En als dat al wel duidelijk is, dan is het de vraag of het normenkader wel van toepassing is en of de verklaring dus wel het niveau van beheersing weergeeft dat gewenst is.

SOx en CobiT hebben vanaf 2002 geleid tot een ware hausse op het gebied van audits. SOx compliancy als doel, COSO en CobiT als hulpmiddel en sinds enkele jaren SAS70 als richtsnoer. Dat er in het kader van SOx compliancy gekozen wordt voor een standaard ligt voor de hand. SOx kent globale werking en moet ook op een globale manier worden vastgesteld.

Toch is niet alles glashelder als het gaat om SAS70. De zorg wordt geuit vanuit de ISACA. Dat is niet heel verwonderlijk:

SAS70 is in 1992 ontwikkeld door de Audit Standards Board van AICPA, het Amerikaanse NIVRA, verantwoordelijk voor onder meer de jaarrekeningcontroles. Het framework werd gehanteerd voor het beoordelen van de beheersing van service verleners. Dus niet specifiek voor het beoordelen van de beheersing van IT-dienstverleners. Het is ook niet ontwikkeld ten behoeve van de SOx audits, het kwam toevallig heel goed uit dat SAS70 daarvoor toepasbaar bleek.
ISACA is van origine het instituut van IT auditors, verantwoordelijk voor toetsing van IT- omgevingen. Opmerkelijk is dat ISACA ook via een gerelateerd instituut (ITGI) de ontwikkelaar is van het CobiT framework. Hier doet zich dan ook een interessant fenomeen voor: de IT auditors zeggen hoe je processen moet beheren, de RA's hoe je beheerprocessen moet toetsen.

In het blad Information Systems Control Journal van ISACA beschrijft Silka Gonzalez (zij bezit alle relevante certificeringen) knelpunten en aandachtspunten ten aanzien van de SAS70 verklaring zoals zij die in haar beroepspraktijk opmerkt.

Zij concludeert ten aanzien van:

• Type I rapporten
Dergelijke rapporten zeggen niets over de feitelijke gang van zaken bij een service organisatie. Zonder testen kun je wel iets roepen over opzet en bestaan, maar de waarde is beperkt (en daar staat natuurlijk de lagere kostprijs van het onderzoek tegenover). Het is dan ook van belang om expliciet te vragen om een type II onderzoek. SAS70 zegt in het algemeen dus niet genoeg.

• Type II rapporten
Het kan wel eens zo zijn dat voor een klant de onderzochte beheersdoelstellingen niet de meest relevante zijn. De service provider bepaalt immers zelf welke beheersdoelstellingen getoetst moeten worden. Ook de diepgang van het onderzoek kan wel eens onvoldoende zijn. Gonzalez geeft het voorbeeld dat bij een vraag om het autorisatiemechanisme te onderzoeken uitsluitend wordt gekeken naar de kwaliteit van het wachtwoordenbeleid, terwijl er meer aandachtspunten bestaan als het gaat om toegangscontrole. Een positief rapport zou hierdoor een vals gevoel van beheersing kunnen geven.

In het algemeen onderkent zij daarnaast de volgende risico's:

- Er is meer te onderzoeken dan alleen de beheersdoelstellingen en –maatregelen zoals die in SAS70 worden aangegeven. Wet- en regelgeving gaat verder, zo zou bijvoorbeeld misschien ook aandacht geschonken moeten worden aan de Wet Bescherming Persoonsgegevens.
- Het onderzoek vergt specifieke kennis. Toetsen van IT-beheersmaatregelen vergt IT-kennis. Een auditor zonder actuele kennis van het IT-vakgebied zou tekort kunnen schieten bij de beoordeling van de steeds complexere infrastructuren en architecturen.
- AICPA en de PCAOB (Public Company Accounting Oversight Board, de Amerikaanse toezichthouder voor SOx auditors) hebben volgens Gonzalez onvoldoende aandacht voor richtlijnen rond het proces van uitvoering van een audit van een IT-organisatie. Er is meer begeleiding bij de uitvoering nodig.

Het klantperspectief van SAS70

Hoe moet je nu een SAS70 verklaring op waarde schatten?
Gonzalez biedt de volgende richtlijnen om de SAS70 verklaring te beoordelen:

- *De auditor:* Kun je vaststellen wie de auditor was en of die voldoende gekwalificeerd is om het onderzoek uit te voeren?
- *Het type rapport:* Is een type I rapport echt voldoende? In de regel is een type II rapport toch een minimum vereiste om zeker te weten dat de voorgeschreven maatregelen ook werken.
- *Wat waren de controleobjecten?* Zijn de beoordeelde controledoelstellingen ook de doelstellingen waar je op zou moeten vertrouwen? Ontbreken er wellicht noodzakelijk te toetsen doelstellingen in de opdracht? (zie figuur 1, objecten van onderzoek)
- *Scope en diepgang van het onderzoek:* niet alleen de onderzoeker moet een goede technische kennis hebben om de toets uit te voeren, ook de beoordeling van de toets vergt de juiste technische bagage. Eventueel zou een derde het onderzoek moeten beoordelen.
- *Onderaannemers:* omvat de SAS70 ook de werkzaamheden die bij de dienstverlener zelf weer door derden worden uitgevoerd? En wordt daarbij het relevante normenkader en de relevante scope en diepgang ook bereikt?
- *Datum van het rapport:* is het onderzoek wel voldoende recent? Een bevinding van een jour oud zou wel eens niet meer actueel kunnen zijn. En let er ook op dat het onderzoek de financiële verslagperiode voldoende afdekt.
- *Andere uitgevoerde onderzoeken:* Zijn er buiten de SAS70 toetsen ook andere onderzoeken uitgevoerd (penetratietests bijvoorbeeld)?
- *Juridische aspecten:* Let erop dat de contracten met derden over het juiste soort verklaringen gaan. Wordt er bijvoorbeeld gesproken over een type II onderzoek en niet over een security scan.

Bovendien moet je in uitbestedingscontracten altijd de mogelijkheid openhouden om zelf een onderzoek uit te (laten) voeren.

Het is ook zinvol om de kwalificaties van de auditor te beoordelen. SAS70 is afkomstig uit de financial audit omgeving en richt zich dus op beheersing. Maar beheersing van een IT- omgeving is niet te vergelijken met de beheersing van andere dienstverlenende organisaties. Niet elke auditor bezit de juiste kwalificaties.

Conclusie

Het is nuttig om even van een afstand naar het SAS70 instrument te kijken. Voor veel organisaties is het de heilige graal om zonder veel eigen inspanning een goed oordeel over kwaliteit te krijgen. Zo'n SAS70 onderzoek lijkt bij uitstek een aanvulling op de bestaande SLA's en DAP's, dat lijkt vanzelf goed te gaan. Maar in de werkelijkheid van alledag is het nuttig om ook die jacht naar de heilige graal kritisch te volgen. Je blijft ook in geval van een SAS70 zelf verantwoordelijk voor het beantwoorden van de vraag of alle relevante beheerprocessen beheerst zijn.

Figure 1—Areas of Controls

Application System	Transactions
• System development, implementation and maintenance • Application documentation • Quality assurance	• Recording • Data transmission • Reporting • Calculations

Security	Computer Operations
• Logical security • Physical security • Environmental controls • Operational recovery • Segregation of duties	• System processing • Operations support

Silka Gonzalez concludeert het volgende: In het geval van outsourcing is het van groot belang dat de juiste waarborgen bestaan ten aanzien van de eigen beheersdoelstellingen. En door outsourcing ontstaat natuurlijk een nieuw risico, namelijk het ontbreken van eigen toezicht en dus het ontbreken van inzicht.
Het enkel bouwen op een SAS70 verklaring lijkt wat naïef. Je kunt echt wel eisen stellen aan de rapportage, om een beeld te krijgen van de uitgevoerde controles voor wat betreft de scope en diepgang.

Externe bron:
Artikel: SAS 70 Reports - What Do They Really Tell You? Van Silka Gonzalez, Information Systems Control Journal, Issue 2, maart 2008 (uitgave van ISACA)

De monsterlijke trekjes van beveiligingsproblemen

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

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

Pangolins en tweelingen

Bron: estherase via Flickr

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

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

Plastic en gentech

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

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

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

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

Sub-monsters

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

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

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

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

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

Perceptie en werkelijkheid

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

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

Foto: Jerzy Kociatkiewicz

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

Monsterbezwering

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

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

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

Assimilatie

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

De monsters van de stemcomputer

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

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

Monsters voorkomen?

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

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

Samenvatting/conclusie

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

URLs

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

Literatuur

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

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

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

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

InZicht

<Over deze rubriek> InZicht geeft een overzicht van recent verschenen en te verschijnen boeken en whitepapers in bnnen- 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.

Secrets Stolen, Fortunes Lost
Auteurs: Christopher Burgess, Richard Powers
ISBN-10: 1597492558
Uitgever: Syngress
Druk: 1e druk, 21 mei 2008
Vorm: Paperback + e-book, 300 blz, Engels

Secrets Stolen, Fortunes Lost biedt de lezer een fascinerende reis naar de donkere kanten van het informatietijdperk, geopolitiek en globale economie, waarbij corporate hacking, industriële spionage, oplichting, georganiseerde misdaad en aanverwante problemen opnieuw belicht worden. Uiteraard wordt in dit boek uitvoerig uit de doeken gedaan hoe een solide en effectieve bescherming tegen al deze dreigingen ontwikkeld kan worden. Er wordt tevens bijgebracht wat men dient te weten van deze dynamische en globale fenomenen (wat gebeurt er, wat kost het), hoe bouwt men een effectief programma dat solide bescherming biedt en in welke mate is bijvoorbeeld de corporate cultuur van invloed op het succes van zo'n programma.

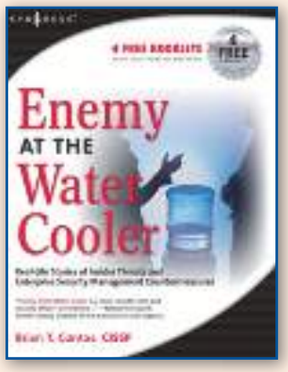
No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing
Auteurs: Johnny Long
ISBN-10: 1597492159
Uitgever: Syngress
Druk: 1e druk, 24 december 2007
Vorm: Paperback + e-book, 480 blz, Engels

Informatie is macht. Een groeiende meerderheid van informatie is digitaal opgeslagen. De industrie zet dan ook hightech elektronische beschermingssystemen in om al deze informatie zo veilig mogelijk te stellen. De auteur wordt als professionele hacker betaald om zwakheden in deze systemen te vinden en uit te buiten. Het doel is altijd gelijk gebleven: onttrek informatieve geheimen via welke tools of methodieken dan ook. De geheimen en methodieken om vele van deze hightech systemen te omzeilen zijn inmiddels wel zo'n beetje gevonden en eigenlijk weinig bijzonder. Wel bijzonder zijn de grote effectiviteit hiervan, nog immer! Dit boek neemt u mee in deze social engineering wereld aan de hand van vele voorbeelden en feiten.

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance
Auteurs: Tony Bradley, Anton Chuvakin, Anatoly Elberg, Brian J Koerner
ISBN-10: 1597491659
Uitgever: Syngress
Druk: 1e druk, 8 maart 2008
Vorm: Paperback + e-book, 448 blz, Engels

Deze titel voorziet in alle informatie die nodig is om PCI Data Security Standards te doorgronden en juist te interpreteren om vervolgens effectieve beveiliging op de netwerkinfrastructuur toe te passen waarmee compliance met PCI bereikt kan worden. Het belang van dit boek zit hem voornamelijk in de nadruk die wordt gelegd op het implementeren van de PCI controls als onderdeel van het gehele proces.

Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures
Auteurs: Brian Contos
ISBN-10: 1597491292
Uitgever: Syngress
Druk: 1e druk, 23 augustus 2006
Vorm: Paperback + e-book, 304 blz, Engels



Contos heeft een helder en prettig leesbaar boek gebracht waarin diepgaand wordt gekeken naar de risico's die 'insiders' kunnen introduceren. Opgeleukt met vele praktijkvoorbeelden zorgt de auteur voor belangrijke lesstof voor zowel de security management organisatie als voor directieleden. Tegenmaatregelen worden uitvoerig toegelicht ter handreiking van instrumenten om goed voorbereid te zijn op dit type dreigingen.

Get Informed! Kom 3 juni alles te weten over informatie-beveiliging

ICT staat centraal in elk bedrijfsproces. Een storing of calamiteit kan desastreus zijn. Iedere organisatie moet daarom voor hun primaire bedrijfsprocessen de continuïteit kunnen garanderen. Met ruim 25 jaar ervaring in informatiebeveiliging zijn we bij Getronics PinkRoccade als geen ander in staat om onze klanten op maat te bedienen conform de laatste wet- en regelgeving. Die know how willen we graag met jou delen op dinsdag 3 juni.

Interesse in Security & Continuity Services?
Kom dan naar ons zwaarbeveiligde datacenter aan de Fauststraat 1 te Apeldoorn voor een aantal inspirerende sessies met specialisten van Security & Continuity Services en bezoek onze informatiemarkt. Verder is er gelegenheid om te sparren over nieuwe en innovatieve technieken, en te bespreken wat jouw mogelijkheden zijn bij de marktleider op het gebied van informatiebeveiliging.

Programma dinsdag 3 juni in Apeldoorn.

16.00 - 17.00	Ontvangst met informatiemarkt
17.00 - 17.30	Security: noodzaak, hoofdzaak of bijzaak?
17.30 - 18.00	A day in the life of James Bond
18.00 - 19.00	Buffet met informatiemarkt
19.00 - 19.30	Business Continuity Services zorgt er voor dat de klant kan blijven werken, nu én in de toekomst
19.30 - 20.00	Hacken; het was nog nooit zo eenvoudig
20.00 - 21.00	Afsluiting met informatiemarkt

Meld je aan via enjoyfreedom.nl

Getronics PinkRoccade

Wake up!

Auteur: Rob Greuter > Rob Greuter is security consultant en redacteur van het blad Informatiebeveiliging.
Hij is bereikbaar via e-mail: op rob.greuter@kpn-officedsl.nl

Het is opmerkelijk hoe licht er nog altijd wordt gedacht over informatiebeveiliging zodra werkzaamheden buiten de werkomgeving plaatsvinden. De industrie is al jaren bezig te migreren van bescherming van de gebruiker tegen allerlei dreigingen, naar het beschermen van bedrijven tegen gebruikers. Bedrijven verzuimen echter massaal gebruikers verstandig te faciliteren en te informeren. Hoezo hoor ik u mompelen, telewerken regelen wij via hightech secure remote access technologie met daarop een strakke policy die uiteraard vergezeld gaat van een sterke authenticatie.

Klopt helemaal, secure remote access projecten worden tegenwoordig gelukkig behoorlijk professioneel aangepakt, daar lijkt niets mis mee. Toch zijn er valkuilen die een sterk groeiende dreiging vertegenwoordigen. Een actueel voorbeeld hiervan zijn de (moderne) DSL routers die uw goedbedoelende en o zo voorzichtige werknemers van haar internetproviders meegeleverd krijgen. Deze zijn namelijk grotendeels zo lek als een mandje, voor een leek nauwelijks enigszins veilig te configureren. Voorts migreren wij massaal naar Wireless routers. Erg handig en efficiënt, maar wederom vaak krankzinnig slecht veilig te configureren. Als de fabrikanten en providers dan ook nog nauwelijks de zeer noodzakelijke firmware updates beschikbaar stellen, is een beroerd plaatje ontstaan.

Het is helaas nog veel erger. Om diverse redenen wordt telewerken toegestaan vanaf machines die niet in eigendom zijn van werkgevers of worden toch Administrator rechten beschikbaar gesteld. Het gevolg is dat veel telewerkers op hun particuliere of zakelijke machines vele tientallen applicaties draaien en naar believen kunnen surfen. Voor de gemiddelde gebruiker is het onmogelijk zelf bij te houden welke applicaties wanneer een update vergen en hoe dit actualiseren precies uitgevoerd dient te worden. Windows update wil nog wel lukken, maar alle overige applicaties bijhouden kan en doet men gewoon niet.

Kom op mensen, word wakker! De kans dat er ellende in uw netwerk en data wordt geïnjecteerd via de thuisroute is enorm aan het toenemen en is hard op weg een aantrekkelijke weg te worden voor kwaadwillenden omdat het zo eenvoudig is! Informeer dus uw telewerkers (en liefst alle medewerkers) fatsoenlijk over hoe thuis een en ander veilig te krijgen en te houden en ondersteun daar waar mogelijk met aanvullende tools. En neen, dit hoeft niet direct geld te kosten (!), enkele voorbeelden:

Secunia Personal Software Inspector (gratis)
Dit pakketje houdt bij welke applicaties al of niet op het juiste patch niveau zitten en geeft bij problemen precies aan welke update er nodig is, waar deze is op te halen en welke eventuele aanvullende instructies uitgevoerd dienen te worden.
https://psi.secunia.com

Sxipper (gratis)
Dit is een browser extensie gebaseerde Web SSO oplossing die doet wat hij belooft en die alle toegepaste credentials versleuteld opslaat. Formulieren worden nauwkeurig ingevuld, wachtwoorden worden beheerd en het inloggen geschiedt vervolgens veilig, transparant en snel.
Nooit van gehoord zegt u? Kan kloppen. Sxip is opgericht door Dick Hardt, zeg maar de uitvinder van de Identity 2.0 terminologie. (De zakelijke versie van Sxipper is onlangs verkocht aan TriCipher). Er is overigens wel een nadeeltje aan verbonden, enkel de Firefox browsers worden ondersteund.
http://www.sxip.com

TrueCrypt (gratis)
Een open-source encryptie tool waarmee gebruikers naast interne harde schijven ook alle rondslingerende USB flash drives en externe harde schijven gemakkelijk en goed kunnen versleutelen.

Defendius Labyrinth Security Lock
Voor de paranoïde medewerkers is onderstaand slot een hele aardige!

Role Based Access Control: een procesbenadering

Auteurs: John Rudolph en Rob Kroneman > John Rudolph (CISA, CISM, CISSP) heeft meer dan vijftien jaar ervaring in informatiebeveiliging en auditing. Zijn technisch specialisme is het IBM z/OS platform. Naast technische advisering houdt John zich bezig met Risk Management, Operational Security Management, Business Continuity Management, Identity and Access Management, implementaties van Information Security Management Systems en het geven van trainingen op het gebied van informatiebeveiliging. John is lid van verschillende internationale vakverenigingen.

Rob Kroneman (CISA, CISM, lead auditor ISO27001) is al meer dan vijftien jaar werkzaam in het vakgebied informatiebeveiliging. Als professional heeft Rob Kroneman uitgebreide ervaring in Informatiebeveiliging gerelateerde disciplines, op zowel operationeel, tactisch en strategisch niveau, waarbij de nadruk ligt op management van informatiebeveiliging, review van informatiebeveiligingsrisico's en -maatregelen en informatiebeveiligingsbeleid.

Rob Kroneman (rob.kroneman@irc2.com) en *John Rudolph* (john.rudolph@irc2.com) zijn beiden als senior consultant werkzaam voor Information Risk Control.

Vanuit autorisatiebeheer is het vaak moeilijk aan te tonen dat de juiste autorisaties aan de juiste personen zijn toegekend. Van de verschillende modellen die hiervoor gebruikt worden[1] neemt Role Based Access Control inmiddels een belangrijke plaats in. Met dit artikel tonen wij aan dat het zeer goed mogelijk is om RBAC procesmatig te benaderen, waarbij de verantwoordelijkheid voor de RBAC-processen bij de organisatie zelf belegd kan worden. Met andere woorden: in onze visie is RBAC géén ICT-feestje.

Voor de inrichting van de RBAC-processen, de inrichting van een governance-structuur inclusief de onderliggende managementrapportages introduceren wij een methodiek geënt op het meten van de organisatie-volwassenheid ten aanzien van Identity and Access Management. De geïntroduceerde methode heeft van ons de naam IAM[3] (Identity and Access Management Maturity Model) meegekregen.

Inleiding

Voor grote, maar vaak ook voor kleinere bedrijven, is het proces van het beheren van gebruikers en aan hen toegekende bevoegdheden minimaal een grote uitdaging te noemen.
Dit geldt zowel voor de bedrijfsmatige kant als voor de ondersteunende ICT-kant van de organisatie.
Onderstaand een aantal voorbeelden van de problematiek waarmee autorisatiebeheer wordt geconfronteerd:

- Tijdens controle op bestanden waarin accounts van gebruikers worden geregistreerd, komt het met zeer grote regelmaat voor dat hier accounts in staan, of nog steeds actief zijn, van medewerkers die al enige tijd het bedrijf hebben verlaten.
- Vaak zijn de bevoegdheden toegekend aan reeds vertrokken medewerkers nog niet ingetrokken.
- Medewerkers veranderen van functie en nemen bevoegdheden behorend bij hun vorige functie met zich mee.
- Het duurt lang voordat nieuw in dienst gekomen medewerkers kunnen beschikken over accounts voorzien van de juiste autorisaties om de voor hun functie noodzakelijke informatiesystemen te kunnen benaderen.

Vanuit de literatuur wordt het onderdeel Access Management van Identity and Access Management vaak vanuit de technische infrastructuur benaderd[2]. Acces Management wordt beschouwd als logische toegangsbeveiliging, uit te voeren door de ICT-afdeling. Dit is een terechte invalshoek omdat bevoegdheden die de organisatie aan één bepaalde medewerker geeft, vertaald moeten worden naar technische autorisaties op systeemniveau die ook op dat niveau beheerd dienen te worden.
De verantwoordelijkheid van de ICT-afdeling ligt in het uitvoeren van technisch beheer over autorisaties: het onderhouden van koppelingen van autorisatiegroepen met objecten enerzijds en van koppelingen van user IDs met autorisatiegroepen anderzijds.
Waar de ICT-afdeling verantwoordelijk is voor de uitvoering van het technische autorisatiebeheer, is de business zelf verantwoordelijk voor het definiëren van businessrollen en het juist doorlopen van een aanvraagproces om aan medewerkers de voor hun rol benodigde autorisaties toe te laten kennen.
Wet- en regelgeving stellen eisen aan de bedrijfsvoering. Een voorbeeld hiervan is de SOx wetgeving, waar ook Nederlandse organisaties zich in toenemende mate mee geconfronteerd zien. Om aan een aantal van deze eisen te kunnen voldoen, is het noodzakelijk dat aangetoond kan worden dat uitgegeven autorisaties correct zijn. Dat houdt in dat ze overeenkomen met de bevoegdheden die bij een bepaalde functie horen of dat er een formele goedkeuring is gegeven voor het aanbrengen van technische autorisaties. Dit aantoonbaar 'in control' zijn van een organisatie is daarmee een grote drijfveer voor IAM geworden. Veel organisaties denken daarom aan de invoering van IAM of zijn hiermee al bezig. Kijkend naar de Access Management component zien we dat er meer en meer een keuze voor het RBAC-model wordt gemaakt.

Invoering van RBAC is op zich geen eenvoudige opgave. Een aantal redenen hiervoor:

- De complexiteit van de systeeminfrastructuur: meestal maken informatieverwerkende systemen niet gebruik van slechts één systeemomgeving, maar hebben ze connecties met meerdere interne (en vaak

[1] Een aantal modellen voor autorisatiebeheer zijn: Mandatory Access Control, Discretionary Access Control en non-Discrectionary Access Control (waaronder RBAC).
[2] Zie o.m. het artikel "De (on)beheersbaarheid van toegangsbeveiliging" – KPMG 2005
[3] Dit begrip is vergelijkbaar met de audit-term IST-SOLL. Dit zijn kwalitatieve begrippen waarbij de actual state de huidige status van het RBAC-proces weergeeft en de desired state de door de organisatie gewenste procesinrichting weergeeft.

ook externe) systeemomgevingen. Elke omgeving kan andere eisen stellen aan de representatie van user accounts en aan de manier waarop bevoegdheden worden vertaald naar autorisaties.

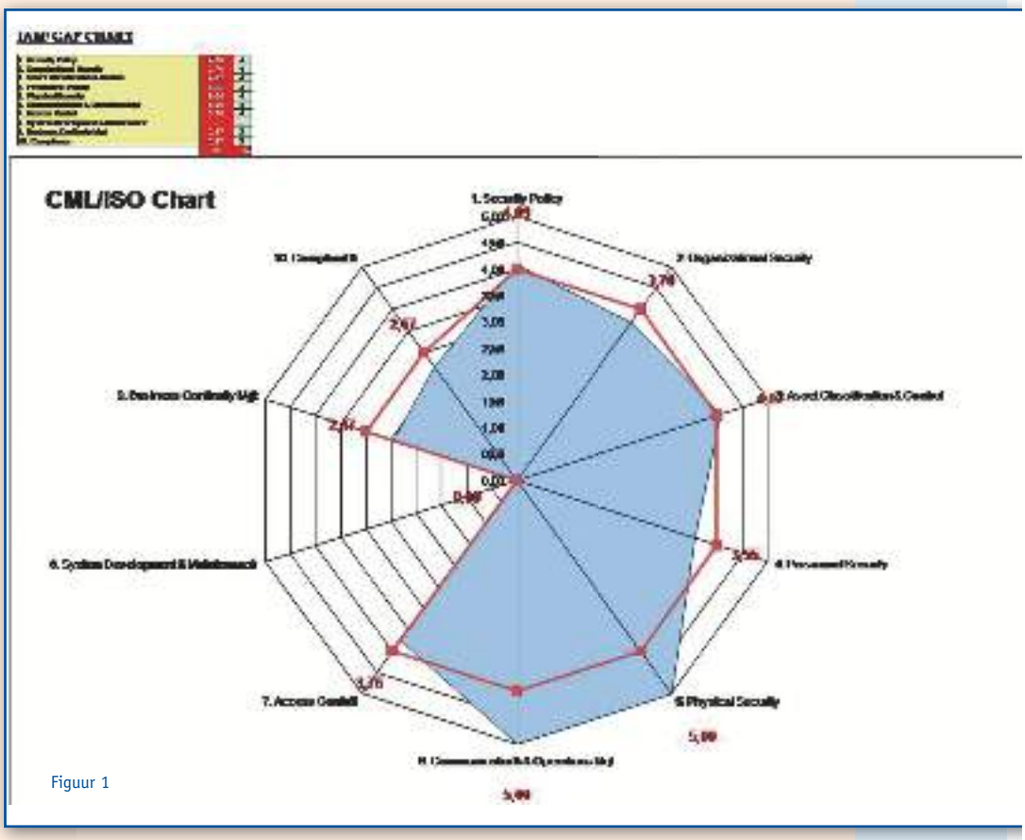
- De complexiteit van de applicatie-infrastructuur: applicaties maken vaak gebruik van gegevens en informatie die uitgewisseld of bewerkt wordt door andere applicaties. Die applicaties kunnen op dezelfde of andere systeemomgevingen en platformen draaien en kunnen hun eigen eisen stellen aan de manier waarop bevoegdheden naar autorisaties worden vertaald.
- De organisatie beschouwt functionele bevoegdheden die medewerkers nodig hebben om hun taken naar behoren uit te kunnen voeren. Deze functionele bevoegdheden moeten vertaald worden naar technische autorisaties op systeem/applicatie niveau. Andersom moeten bestaande technische autorisaties vertaald worden naar functionele bevoegdheden. De vertaling van functionaliteit naar technische componenten is vaak een uiterst moeizame taak.
- Brongegevens zijn vaak niet integer of onvolledig. Dit is zeker het geval wanneer autorisatiegegevens, behalve opgeslagen in externe security files, ook binnen applicaties moet worden onderhouden. Voor identiteitsgegevens kunnen meerdere systemen in gebruik zijn.
- De verantwoordelijkheid voor het onderhoud van brongegevens is vaak bij verschillende organisatieonderdelen belegd. Synchronisatie van deze gegevens binnen de organisatie is hierdoor een uitdaging op zich.

Bestaande methoden en technieken worden meestal ingezet bij het initieel inrichten van een RBAC-structuur. Voor een procesmatige benadering van IAM en RBAC zijn vaak geen kwaliteitscriteria opgesteld.
Gebaseerd op CobiT, CMM en ISO 2700x hebben wij een methode ontwikkeld om de RBAC- processen te sturen, te meten en te voorzien in kwalitatieve (management)rapportages. Onze methode heeft als naam IAM (Identity and Acess Management Maturity Model) en is bruikbaar voor de volgende aandachtsgebieden:

- Het uitvoeren van GAP-analyses tussen de actual en desired state ;
- Het uitvoeren van trendanalyses op de volwassenheid van het proces. Doordat we de volwassenheid van bijvoorbeeld een implementatie nauwkeurig meten, kunnen we als trend de verbetering of verslechtering weergeven in een managementrapportage;
- Het aantonen van voortgang bij het inrichten van RBAC-processen;
- Het aantonen van verbetering in de kwaliteit van de geboden diensten op het gebied van RBAC;
- Het definiëren van metrics;
- Het stellen van prioriteiten bij implementatie van RBAC-processen.

IAM in het kort

Om te kunnen meten waar een organisatie staat voordat aan een IAM (of, in het kader van dit artikel verbijzonderd naar RBAC) traject begonnen wordt, wordt IAM al ingezet om via een nulmeting de huidige mate van volwassenheid van een organisatie ten aanzien van IAM (of RBAC) vast te stellen. Dit wordt gedaan door de relevante CobiT en ISO27002 controls op het gebied van IAM of RBAC te selecteren.
Voordat er nu aan een traject begonnen wordt, wordt er samen met de organisatie vastgesteld waar de prioriteiten liggen. Dit kan op basis van een aangeleverde risicoanalyse, een bestaand audit rapport of/en op basis van een eisen- en wensenlijst.
Voor deze controls zijn maturity levels gedefinieerd, gebaseerd op een aantal CobiT Controls. Per control zijn een aantal vragen gedefinieerd om vast te stellen wat de organisatievolwassenheid op het gebied van deze control is.
Afhankelijk van het doel van het traject wordt samen met de organisatie bepaald waar zij zou willen staan of naar toe zou willen groeien ten aanzien van de implementatie van deze controls. In feite is dit de definitie van de desired state.
De resultaten van het onderzoek worden met het door de organisatie gewenste resultaat samengevoegd. Op basis daarvan wordt het verschil tussen de actuele en gewenste situatie bepaald en kan een strategie worden gekozen om van de huidige naar de gewenste situatie te komen.
We zijn nu met IAM in staat te bepalen wat er in het traject gedaan zou moeten worden om het geconstateerde verschil te dichten. Als voorbeeld toont het schema (zie figuur 1) de onderzoeksresultaten in het rood en de gewenste resultaten in het groen. Dit spiderdiagram kan daarnaast worden gebruikt tijdens het traject om voortgang te visualiseren.



Figuur 1

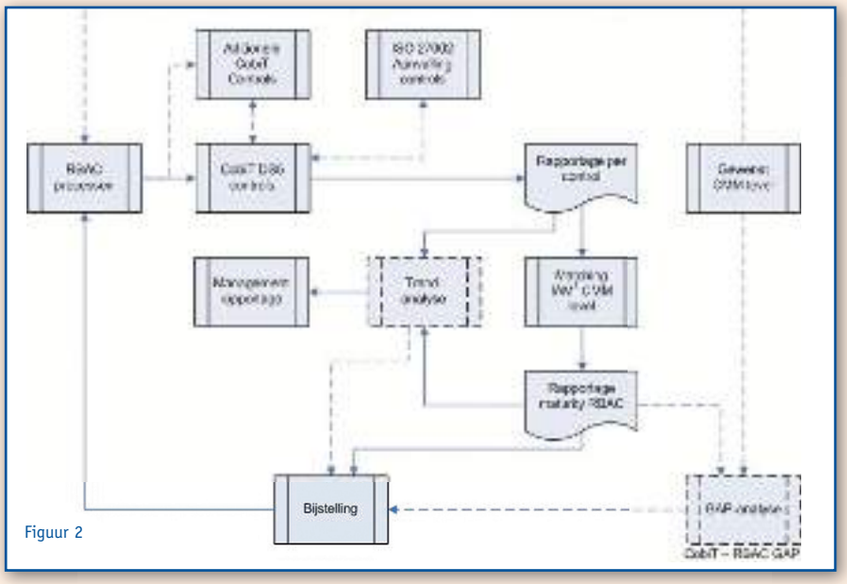
In een later stadium is het mogelijk onze methode te gebruiken om compliancy te meten en te rapporteren. Het spiderdiagram kan daartoe gepresenteerd worden met CobiT- of ISO compliance als uitgangspunt

CobiT als vertrekpunt

In de literatuur zijn de uitgangspunten, voorwaarden en standaarden rondom RBAC, ook als beheerproces, vaak genoeg beschreven[4]. Op zich hebben wij daar niet zoveel aan toe te voegen.

Onze benadering is anders. In dit artikel nemen wij CobiT als vertrekpunt. Wij hebben hiervoor gekozen omdat CobiT vanuit ICT sterk op de organisatie is georiënteerd vanuit een procesmatig perspectief. De uitgangspunten van CobiT zijn dat ICT-componenten en resources zodanig bestuurd worden vanuit vier logisch bij elkaar horende categorieën van processen dat de organisatie op basis van stuurinformatie haar doelstellingen kan bereiken. Vooral vanuit compliancy-oogpunt is het belangrijk verantwoording te kunnen afleggen over de totale bedrijfsvoering waarbij de CobiT controls richtlijnen bieden die als meetlat zeer goed bruikbaar zijn.

Met andere woorden: wij willen de RBAC-processen beschouwen als onderdeel van de totale governance. ICT-processen, componenten en informatie zijn slechts ondersteunend aan organisatiedoelstellingen.



Figuur 2

Daar waar CobiT per onderscheiden proces een aantal gedetailleerde maatregelen kent, kan aanvullend de ISO 27002 gebruikt worden voor het benoemen van additionele maatregelen (indien noodzakelijk).

Een ander aspect dat aan de orde komt, is de mate van volwassenheid waarmee de processen zijn ingericht. Een algemeen aanvaard hulpmiddel om de mate van volwassenheid te beoordelen, is het Capability Maturity Model (CMM). Aan de hand van de beoordeling van de volwassenheid kunnen vervolgens procesverbeteringen of -bijstellingen gerealiseerd worden.

Het procesmodel dat wij voorstaan en dat in dit artikel besproken wordt, is in figuur 2 schematisch weergegeven.

Deel twee van dit artikel (wordt geplaatst in nummer 4 van dit jaar) gaat in op de RBAC-processen, gevolgd door een (niet-uitputtende) selectie van relevante controls. Dit wordt gevolgd door een beschrijving van CMM levels, die in onze visie horen bij de wijze waarop de geselecteerde controls moeten zijn geïmplementeerd.

In deel drie van het artikel (verschijnt in nummer 6 van dit jaar) wordt vervolgens onze rapportagemethode beschreven en geven wij onze uiteindelijke conclusies over de wijze waarop wij RBAC als proces benaderen.

[4] Zie de Studie Role Based Access Control, door Platform Informatiebeveiliging, versie 1.0, november 2005

Agenda

15/05/2008
Themabijeenkomst
Onderwerp: Bewaren en bewijzen in de praktijk
Organisatie: PvIB
Locatie: nog niet bekend
Tijdstip: nog niet bekend

17/06/2008
Themabijeenkomst
Onderwerp: Security & Pervasive computing
Organisatie: PvIB
Locatie: nog niet bekend
Tijdstip: nog niet bekend

18/06/2008
Vijfde bijeenkomst IBO, inclusief diner
Onderwerp: nog niet bekend
Organisatie: PvIB
Locatie: nog niet bekend
Tijdstip: nog niet bekend
Deze voorinformatie is bestemd voor de leden van het PvIB die gekozen hebben voor het Management Pakket. Het Informatie Beveiliging Overlegorgaan (IBO) is een informele en interactieve bijeenkomst.

VOORAANKONDIGING
8/10/2008
Security congres 2008
Organisatie: PvIB - NOREA - ISACA
Locatie: Spant! in Bussum
Tijdstip: 12.00 - 22.00 uur

Heet van de naald:
Fred van Noord nieuwe voorzitter PvIB

De eerste reguliere algemene ledenvergadering van het PvIB werd op dinsdag 22 april gehouden in 't Spant in Bussum, dit voorafgaand aan de themasessie over de WBP. Op de ALV werd bekendgemaakt dat Fred van Noord het voorzitterschap van het PvIB overneemt van Jo Koppes.

Een bloemetje voor Gerrit Post

Dit feit kunnen we natuurlijk niet ongemerkt laten passeren. In het volgende nummer van Informatiebeveiliging dan ook een dubbelinterview met beide heren. Hierin wordt natuurlijk teruggekeken op de fusie, maar ook vooruitgekeken naar de toekomst.

Vincent Alwicher heeft vanwege zijn drukke werkzaamheden zijn secretariaatsfunctie neergelegd. Zijn rol wordt overgenomen door Hans Linschooten, die deze functie ok al eerder bij PI voor zijn rekening nam. Vincent en Jo blijven overigens wel als bestuurslid aan.

Gerrit Post nam tijdens de ALV afscheid als lid van het bestuur. Gerrit was de vertegenwoordiger van de redactie in het bestuur. Zijn rol wordt overgenomen door een ander redactielid, Hans Buijtelaar. Beiden blijven gelukkig wel lid van de redactie.

PvIB gaat banden met onderwijs versterken

Het moment lijkt gunstig om de banden met de opleidingswereld voor informatiebeveiliging nauwer aan te halen. Onderwijsinstellingen timmeren de laatste tijd nadrukkelijk aan de weg en komen regelmatig in de media met activiteiten van hun studenten. Jaarlijks zijn er vele inzendingen van scripties die meedingen naar de Joop Bautz Award. Het PvIB vindt het belangrijk om de jonge talenten voor het vakgebied te interesseren en te betrekken bij de activiteiten.

De activiteiten zijn het logische vervolg op het boek 'Functies in de Informatiebeveiliging' en de tweejaarlijkse Opleidingenmarkten. Beoogd wordt duurzame contacten te ontwikkelen teneinde de beroepsvorming van de informatiebeveiliger te stimuleren. Het gaat om universitaire, hbo en masters (post-hbo- en postdoctoraal)-opleidingen die een gerichte bijdrage leveren aan de vorming en ontwikkeling van informatiebeveiligers. De functies in het boek 'Functies in de informatiebeveiliging' vormen hierbij de referentie.

Pilot

Daarnaast wordt een pilot gedaan met vier onderwijsinstellingen waardoor studenten de gelegenheid krijgen om themabijeenkomsten en bijeenkomsten van de Young Professionals bij te wonen. Gestart wordt met de Academie ICT & Media te Zoetermeer en de Universiteit van Amsterdam. Studenten kunnen op deze manier starten met het opbouwen van een netwerk met professionals en ze maken kennis met actuele issues die spelen in de beroepspraktijk.

PvIB-leden op hun beurt krijgen op deze wijze de gelegenheid contacten aan te knopen met jonge professionals die op hbo- en academisch niveau worden geschoold. Het biedt de gelegenheid om voor vraagstukken uit de praktijk, stage- of afstudeeropdrachten te formuleren die door studenten kunnen worden uitgevoerd waarbij zij worden begeleid door professionals uit de praktijk. Het PvIB wordt door deze genoemde contacten bovendien beter op de hoogte gehouden van de inhoud en kwaliteit van de opleidingen, met toegevoegde waarde voor de praktijk. Het imago als kenniscentrum voor informatiebeveiliging wordt zo bevorderd door toegang tot nieuw ontwikkelde kennis.

Meer informatie/ideeën

Voor informatie en ideeën met betrekking tot mogelijke manieren om de banden met de opleidingswereld aan te halen, kun je terecht bij Fred van Noord, Piet Goeyenbier, Bart Bokhorst en/of Ambreen Gointhi.

Welkom in Iebeetopia...

Dr. Ir. Paul L. Overbeek RE

Naam:
Dr. Ir. Paul L. Overbeek RE
Functie:
Combineert een eigen praktijk met docentschapen aan de universiteiten Eindhoven en Amsterdam. Voor meer informatie: www.ois-nl.eu of Paul.Overbeek@ois-nl.eu.
Vindt ten aanzien van de stelling:
Informatiebeveiliging is te veel met de verkeerde dingen bezig.

"Vandaag is het feest in ons land, Iebeetopia. Vrolijke vlaggetjes flankeren de fanfare. Alle kameraden hebben hun mooiste kleren aangetrokken. Want het is vandaag precies tien jaar geleden dat Nick Leeson, een van de kameraden van het eerste uur, de Barings Bank liet ploffen. In die dagen leed ons volk zwaar, maar nu hebben we zijn boodschap begrepen! En ja, hebben wij niet allen de lessen van Nick aan onze borst gekoesterd? Wie kent niet het elfde gebod 'Gij zult uw functiescheiding eren'? Het geeft een warm gevoel iedere dag opnieuw te doorleven hoe diep dit gebod in onze cultuur is geworteld.

Fijn, zo'n lichtpuntje na de herdenking gisteren, van de OTAP-ongevallen. Eerst werd een lange rij namen voorgelezen van gevallenen door falende testprocedures. Veel namen uit het toch al zwaarbelaste Apeldoorn. En spandoeken: 'Leuker kunnen we het niet maken'. Ook slachtoffers van het falende veiligheidssysteem van de A73-tunnels waren aanwezig. Met de meesten gaat het al weer een stuk beter. Er was een korte confrontatie met de mensen die het systeem zo lichtvaardig hadden geaccepteerd. De meesten kregen een taakstraf en moesten hun IB-bewijs opnieuw halen. Van de hoofdschuldigen is hun inschrijving in het register geschrapt. Er was een mooie toespraak van de staatssecretaris voor IB over 'Acceptatie, eigenaarschap en verantwoordelijkheid'.

Morgen is het ook weer feest. We weten nog niet wie of wat er in het zonnetje wordt gezet, we vieren de 'kraak van de dag'. Ons motto is: na de 'waan van de dag' komt de 'ween van de week'.

Onzin natuurlijk. In 2008 doet Jérôme Kerviel precies hetzelfde als Nick tien jaar geleden. En zo ook die handelaar in graan die meer dan honderd miljoen euro liet verdampen. Toegangspassen die elders allang zijn gekraakt, worden hier nog gewoon ingevoerd. En als vervolgens dezelfde kraak in Nederland wordt herhaald, slaat de paniek toe. Testprocedures falen voor het derde jaar op rij. Testprocedures voor de guillotine in de Franse Revolutie waren beter dan die van vandaag voor software.

Als ik vandaag op een fabriek over een hekje struikel en mijn enkel verstuik, komt de arbeidsinspectie. Als u een medicijn gebruikt, worden de effectiviteit en de bijwerkingen gevolgd. En als er een nieuw type auto op de markt komt, dan heeft deze een type-test glorieus doorstaan. Maar als ik vandaag een whiplash en gebroken been overhoud aan een door ICT veroorzaakt ongeluk dan lachen we dat weg. Of als ik door een gebrekkige riskmanagement-applicatie vijf miljard euro kan laten verdampen. Zelfs als er 700.000 mensen verplicht worden hun kostbare tijd te investeren in het 'spelen-voor-backup' voor onze 'overbelastingdienst' wordt dat als een fact-of-life ervaren. Dezelfde fouten worden herhaaldelijk, keer op keer en telkens weer opnieuw gemaakt...

Het profiel van de gemiddelde professional in de informatiebeveiliging is dat van de 'self-educated' professional, die door schade en schrammen, op basis van ruime

praktijkervaring, zijn kennis en ervaring heeft opgedaan. Er is een beperkt, gelukkig groeiend, cohort met enige opleiding. Veel van de IB-professionals draaien mee in een ICT-organisatie en geven dan bijvoorbeeld opvolging op beveiligingsincidenten. Veel van het werk is operationeel. Men staat op ruime afstand van de primaire bedrijfsprocessen. Het gaat veel over maatregelen en weinig over risico's of beheersing. De IB-professional wordt dan ook nog vaak gebruikt als schaamlap om de eigen verantwoordelijkheid af te kunnen schuiven. De IB-professional had een glorieuze rol kunnen spelen in het SOX-circus, dat toch ook helemaal over beheersing van risico's gaat. In veel gevallen stond hij echter langs de kant, hij stond erbij en keek ernaar. Fred Steenwinkel heeft helemaal gelijk met zijn stelling: 'Informatiebeveiliging is te veel met de verkeerde dingen bezig'. De professional van vandaag moet denken in termen van echte risico's voor de organisatie, functionaliteit en toegevoegde waarde. Niet vanaf de zijlijn, ook niet vanuit de ivoren toren, maar met beide benen in de modder. De hele wereld schreeuwt om betere beveiliging, en vanuit de beroepsgroep - ook vanuit het PvIB - is er een oorverdovende stilte.

Er zijn wel lichtpuntjes. We gaan best vooruit, maar het gaat nog te 'ad hoc' en ik zie te weinig visie. De fase waarin we ons nu bevinden, is een tijdelijke. Verdere professionalisering binnen de beroepsgroep is noodzakelijk. Dat dat snel mogelijk is, hebben de IT-auditors, in slechts vijftien jaar professionaliseringshistorie, laten zien.

Op weg naar verdere professionalisering zijn er vele hobbels te nemen. Ik kom hier met een aantal doelstellingen, die echt morgen nog niet gerealiseerd zullen zijn.Ten eerste moet de kwaliteit van de professional transparant zijn. Daar hoort bij: erkenning van zijn opleiding, van zijn praktijkervaring, persoonlijke integriteit en een professionele houding ten aanzien van (het bijhouden van) de ontwikkelingen in het vakgebied. Ten tweede moet er een cultuur komen waarin we onderling kunnen leren van fouten. Immers: iedere fout is al een keer gemaakt. En ten derde moet er een soort 'inspectie' komen die onderzoek doet bij ongevallen. Een soort Van Vollenhoven die aanbevelingen doet met een uitstralend effect op de hele sector. De sector moet zichzelf veel serieuzer gaan nemen, om erger te voorkomen. Dat betekent: zorgvuldiger werken (tussentijdse verantwoording en acceptatie) en durven leren van elkaar (Best & Bad Practice Sharing, Learning From Incidents). Ik zou zo graag zien dat onze sector zijn verantwoordelijkheid neemt en ook dat er zo een betere zelfreinigende werking ontstaat.

Tot slot, onderzoek en opleiding voor het aanstormende talent tot IB-professional is noodzakelijk, aan universiteiten, hogescholen en mbo-opleidingen. Maar, misschien nog wel de belangrijkste, informatiebeveiliging dient ook als vanzelfsprekend onderdeel ingebed te zijn in de normale curricula. Immers, vrijwel iedereen, van welke discipline ook, heeft hiermee te maken en heeft een generieke basiskennis nodig.

U kent de uitdrukking 'dom geboren en nooit iets bijgeleerd'. Deze is volledig op ons van toepassing. De mechanismen voor structurele verbetering ontbreken. Noem het governance, noem het oversight, of noem het een ouderwetse gilde-structuur. Hier ligt een verantwoordelijkheid en een kans voor de beroepsverenigingen.

Even terug naar het begin. IB-topia is vandaag de dag een eiland. De IB-topianen zijn van zeer diverse pluimage en ze letten goed op elkaar. De bewoners blijven een beetje rondhangen op dat eiland. Volgens de niet-eilanders zitten ze daar ook wel goed. Communicatie met de wereld vindt plaats door hard te roepen vanaf de kustlijn. Meestal hebben de IB-topianen geen idee of er echt wordt geluisterd. In de toekomst zou ik graag zien dat er bruggen komen, met tweerichtingsverkeer, en dat de IB-topianen uitzwermen over de wereld en alle talen spreken.

Ik geef het stokje over aan Arie van Bellen, Directeur van ECP.NL. ECP.NL viert dit jaar haar tiende verjaardag als neutraal platform tussen de sectoren voor de stimulering van de digitale economie en de samenleving. Een van de thema's binnen ECP.NL is authenticatie. De stelling die ik aan Arie mee wil geven is: 'Authenticatie is de sleutel voor het internet'. Succes!"

Geeft het estafettestokje door aan:
Arie van Bellen, Directeur van ECP.NL.

Met de vervolgstelling:
Authenticatie is de sleutel voor het internet

Auteursinstructie artikelen Informatiebeveiliging

Dit blad is een uitgave van het Platform voor InformatieBeveiliging (PvIB), de beroepsvereniging van professionals op het gebied van Informatiebeveiliging. De redactie is altijd actief op zoek naar bijdragen. Schrijven voor dit blad is niet moeilijk, maar kost natuurlijk wel tijd. En is gebonden aan een paar regels. Laten we die regels gewoon eens even publiceren. Wellicht kunnen we u prikkelen om ook eens een bijdrage te leveren. Niet alleen nuttig voor uw medeleden, maar ook voor uzelf!

De doelgroep van Informatiebeveiliging bestaat uit personen die zich beroepsmatig direct of indirect bezighouden met de beveiliging van de informatievoorziening binnen en/of tussen organisaties en individuen. Hierbij kan worden gedacht aan information security officers, information security managers, IT-management (zoals hoofden rekencentrum, automatisering), alsmede aan vertegenwoordigers van het business management die in toenemende mate met informatiebeveiliging te maken krijgen. Verder behoren adviseurs en EDP-auditors tot het lezerspubliek. Het opleidingsniveau van de doelgroep is hbo en universitair. Informatiebeveiliging zoekt een balans tussen maatschappelijk relevante issues enerzijds en praktijkgerichte achtergrondartikelen anderzijds.

Presentatie en stijl

We gaan ervan uit dat de doelgroep bestaat uit drukbezette functionarissen die weinig tijd hebben en die bovendien worden overstelpt door allerlei leesvoer. Het is dus van belang artikelen te schrijven vanuit de volgende standpunten:

- De artikelen zijn praktisch van aard. De onderwerpen dienen zoveel mogelijk te worden verduidelijkt met voorbeelden en praktijksituaties. Het praktisch gehalte wordt verder extra verhoogd door het opnemen van praktijkadviezen, schema's, checklists, conclusies en tips. Deze "krenten in de pap" zullen van het basisartikel worden onderscheiden door een opvallende lay-out.
- Eventuele theoretische artikelen dienen zoveel mogelijk de relatie te leggen met de praktijk.
- Artikelen zijn geen advertorials. Ze zijn authentiek werk dat beoogt kennis te delen, zonder een expliciete commerciële bijbedoeling.
- Het gebruik van kleurenillustraties (let op de licentievorm bij niet zelf gemaakte illustraties: public domain of een Creative Commons licentie) wordt van harte aanbevolen.

De tekst moet een overzichtelijke opbouw hebben. Formuleer vlot, kort, helder, kernachtig en foutloos. Vermijd zeer specialistisch vakjargon of afkortingen die niet voor iedereen duidelijk zijn. De praktijk is leuk en boeiend: ook een wat luchtige behandeling kan soms de juiste zijn.

Een artikel kent globaal een vaste structuur. Deze opbouw is als volgt:

- Kop van het artikel: maximaal 6 woorden;
- Auteursnaam of –namen: (titulatuur), voorletter(s) of voornaam en achternaam;
- Over de auteur: in 1 à 2 regels wordt vermeld waar de auteur werkt et cetera;
- Aantal woorden per pagina: 750, inclusief illustraties;
- Een artikel beslaat doorgaans vier pagina's, circa 3000 woorden. Maar kan afwijken indien dit nodig is om het verhaal goed te kunnen brengen.

Aanleveren van het artikel

Indien mogelijk het artikel aanleveren als Word-bestand, zonder opmaakkenmerken (dus als platte tekst). In de tekst kunt u aangeven wat als tabel of kolom opgemaakt dient te worden. Mocht u een ander tekstverwerkingspakket gebruiken dan graag het bestand opslaan en aanleveren als ASCII-bestand (dus zonder codes). Ten behoeve van de website vragen we auteurs tevens een abstract van het artikel aan te leveren (tussen 100 en 200 woorden).
Als het van belang is voor een beter begrip van het artikel, dan vragen we om de lezer enkele URL's aan te reiken.

Foto's, figuren, tekeningen en tabellen moeten bij voorkeur in aparte bestanden aangeleverd worden. Probeer de figuren zo simpel en duidelijk mogelijk te houden.
We ontvangen het liefst één figuur per A4.
Afbeeldingen ontvangen we graag in .jpg, .eps of .pdf. De resolutie dient minimaal 300 dpi op een formaat van 10 bij 15 cm (drukwerkkwaliteit) te zijn.
Bij aanlevering van een tabel verzoeken wij om een tabel zonder opmaakkenmerken aan te leveren, zodat de tabel eenvoudig passend is te maken in de huisstijl.

Publicatievorm en licentie

Het streven van het PvIB om kennis ten behoeve van leden te verzamelen en weer te delen, heeft ertoe geleid dat de publicaties van het PvIB worden vrijgegeven onder de Creative Commons Share-alike licentie *(http://creativecommons.org/licenses/by-sa/3.0/nl/)*.
Dat betekent dat het de lezer vrij staat het artikel te gebruiken, ook voor commerciële doeleinden, maar dat altijd bronvermelding moet plaatsvinden en dat afgeleide werken ook weer onder deze zelfde licentie moeten worden verspreid. Daarmee bewerkstelligen wij het effectief delen van de kennis.

Voor 2008 hebben we nog vijf nummers voorzien waarbij de volgende data van belang zijn.

Nr.	Kopij inleveren	Verschijnt		Thema
4	19 mei	25 juni	Week 26	Divers
5	30 juni	6 augustus	Week 32	Privacy (Special of dossier)
6	25 augustus	1 oktober	Week 40	Divers
7	29 september	5 november	Week 45	Virtualisatie (Special of dossier)
8	3 november	10 december	Week 50	Divers

SEMINAR OPEN SECURITY

Open ICT leidt vaak tot grote discussie, zeker als de term ‘security’ daarbij in beeld komt.

Open = tegenstelling van veilig en vertrouwd?
Ben je veiliger met een slot getest door één leverancier? Of is het juist verstandiger je beveiliging te laten testen door een horde ‘inbrekers’?

Voor antwoord op al uw vragen
Op het gebied van security in relatie tot Open Standaarden en Open Source komt u naar het Seminar Open Security op 3 juni 2008

Meer informatie en inschrijving
www.mediaplaza.nl Kies in het menu Security Plaza en ga in de agenda naar Seminar Open Security.

Graag tot ziens op dinsdag 3 juni!

media plaza
waar inspiratie innovatie wordt

Sophos Endpoint Security & Control

One client, one lab, one update, one vendor

inclusief Network Access Control

endpoint **security and control**

THE STRENGH OF ONE

Eén oplossing met gratis thuisgebruik

Sophos Endpoint Security biedt in één licentie bescherming tegen malware (zoals virussen, spyware en adware) en ongewenste applicaties, maar is ook voorzien een client firewall en host intrusion prevention.

Eén management console

Vanuit één console verzorgen wij de volledige uitrol, configuratie, updates en rapportage. Zo heeft u alle controle over malware, firewall en ongewenste applicaties zoals P2P en VOIP software, spelletjes en messengers.

Eén licentie

Wij bieden via één licentie ondersteuning voor meer dan 25 operating systems zoals Windows, OSX en Linux, maar ook voor Windows Mobile en nog vele andere operating systems zoals NetWare, Solaris en NetApp.

Meer info op: www.sophosbenelux.com/endpointsecurity

Sophos is één van de marktleiders op het gebied van geïntegreerde oplossingen die internetbedreigingen tegen gaan. Het bedrijf ontwikkelt software tegen virussen, spyware, spam en policy-misbruik, voor bedrijven, onderwijsinstellingen en de overheidssector.

SOPHOS
secured.