maart 2010 nummer 2

INFORMATIEBEVEILIGING

Social Engineering: wederkerigheid en onmiddellijke invloed

Generiek beveiligen en CRAMM

Het Business Oriented Autorisation Model

De mogelijke consequenties van virtualisering

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Het is maar goed dat deze winter voorbij is. Zolang het winterde, gebeurden er eigenlijk ook geen spannende dingen op ons vakgebied. Sneeuw en vorst zorgden voor stilstand. Maar gelukkig brak eindelijk de lente aan en ontwaakte ook ons vakgebied. En hoe: onze huidbacillen blijken unieke identificators voor onze identiteit. Kijk, dat is nou nog eens een fijne ontwikkeling: weg met al die dure techniek, weg met de centrale registraties, gewoon bacteriën. Je bent waar je naar stinkt. Ik had daar nooit zo bij stilgestaan, maar ik vind het wel mooi dat je in plaats van een bodyscanner ook gewoon een teckel kunt africhten. Veel vriendelijker. In ieder geval een organisch en duurzaam begin van het nieuwe seizoen.

Dit is dan ook wel een moment om even terug te kijken. Dit nummer is het laatste dat met de redactie door TOPpers wordt gemaakt. Vorig jaar hebben de redactie en het bestuur besloten om een groot aantal logistieke (hoofd)redactietaken uit te besteden. De reden is dat het maken van een nummer van dit blad nogal veel tijd van de vrijwilligers van de redactie vergt en het hele planningsproces te informeel werd. Daardoor kwam vooral zo rond het verstrijken van de deadline flink wat adrenaline vrij, die echter maar nauwelijks effect sorteerde. Om de balans tussen vorm en inhoud beter te krijgen hebben we besloten om het proces te professionaliseren en outsourcen. Na een onderzoek is besloten om het proces te laten begeleiden door MOS, het bureau dat ons ook al op andere gebieden ondersteunt. Dat betekent dat we waarschijnlijk wel een poosje moeten wennen aan de nieuwe samenwerking, waarvoor alvast onze excuses... We hopen en verwachten wel snel op orde te zijn en weer mooie bladen te kunnen maken.

Hoe dan ook past het om TOPpers (met name Monique, Peter en Daniël) te bedanken voor hun inzet!

In het vorige nummer heb ik uw hulp gevraagd bij het leveren van input voor dit blad. Die vraag heeft geresulteerd in diverse aanbiedingen. Leuk, en al bij voorbaat hartelijk dank daarvoor. Dat levert natuurlijk ook niet direct heel veel kopij op, vandaar dat ook dit nummer niet heel dik is, maar we zijn niet ontevreden!
Even een paar highlights uit deze uitgave: we gaan weer door met onze serie over Social Engineering door Jan de Boer. Ook aflevering twee kun je weer zo in je HRM toolkit opbergen! Een tweede praktijkartikel is het eerste van een interview in twee delen, dat Lex Borger had met Hans Alfons. Hans is niet alleen een collega van mij, maar hij is ook nog eens veel interessanter. Peter Hoogendoorn en Jean-Pierre Vincent behandelen autorisatiemodellen. Leuk om te weten dat dit artikel refereert aan de expertbrief Access Control architectuur. Kijk even op de site, van harte aanbevolen!

Er is gelukkig nog veel meer te lezen, maar mijn ruimte is op! Veel leesplezier,

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

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

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

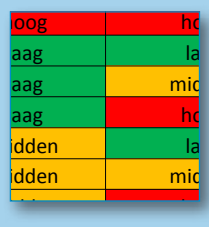
Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

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

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

ISSN 1569-1063

Inhoud



Virtualisatie: goede oude wijn in nieuwe, maar kwalitatief minder goede zakken

Auteur: Jan Tervooren > Jan Tervooren is eigenaar van het onafhankelijk adviesbureau Inframatica Consultants bv in Soest. Jan is tevens Region manager van Guide Share Europe (GSE), afdeling Nederland. GSE is een zelfstandige, non-profit gebruikersassociatie van bedrijven, organisaties en individuen die betrokken zijn bij ICT oplossingen in de ruimste zin van het woord. Jan is bereikbaar via jan.tervooren@inframatica.nl.

De laatste jaren kun je geen ICT-blad meer openslaan zonder ergens het woord virtualisatie tegen te komen. Virtualisatie wordt vaak verkocht als Haarlemmer Olie, een product waarmee zo ongeveer alle bestaande ICT-problemen kunnen worden opgelost. Vooral leveranciers van hard- en software springen hierop gretig in en ze geven hun producten een virtueel tintje in de hoop hun klanten ervan te overtuigen dat ze deze producten ook daadwerkelijk nodig hebben. Een aantal jaren geleden heeft men dat ook geprobeerd met Information Life Cycle Management (ILM), waarbij ik constateerde dat bestaande huis-tuin-en-keukenproducten voor bijvoorbeeld back-up plotseling werden aangeprezen als een 'ILM compatible oplossing'.

Dit artikel geeft een beeld van de historie van virtualisatie en de ontwikkeling ervan naar Cloud Computing, maar het relativeert ook het revolutionaire karakter dat aan dit concept wordt toegekend. Het geheel wordt beschouwd vanuit het oogpunt van informatiebeveiliging en de mogelijke consequenties van virtualisatie in de (verre) toekomst.

Heel lang geleden

Informatiebeveiliging is van alle tijden. Ook in het computerloze tijdperk werd informatie zorgvuldig opgeborgen en bewaakt om te voorkomen dat het in verkeerde handen terechtkwam. Het proces rondom informatiebeveiliging is in wezen nooit veranderd: de eigenaar van de informatie stelde de eisen op qua Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) en vervolgens ging iemand zich bezighouden met de uitvoering, door technische maatregelen te bedenken en daaromheen beheerprocessen te ontwikkelen.
De technische uitvoering van de beveiligingsmaatregelen zijn door de eeuwen heen echter wezenlijk veranderd. Het begon heel lang geleden met het opbergen van informatie op een geheime plaats in een grot, in het bos, in een hut, in een kast, in een verzegelde envelop, in een doos of kist, en veel later in een kluis, al dan niet met een cijferslot. Ook de back-up bestond toen al, want men kopieerde een tekening of document eenvoudig door het twee keer te creëren.

Een belangrijke eigenschap van informatiebeveiliging in die tijd was de gedachte dat men alle geheime stukken zoveel mogelijk op één centrale plaats wilde bewaren (denk hierbij ook aan schatkamers). Uit het oogpunt van beheer en kosten was dit meestal de beste oplossing. De bovenstaande manier van beveiliging was nog relatief simpel en tastbaar en was vooral gebaseerd op een fysieke locatie met fysieke bewaking.

Later

Met de komst van de eerste computers ontstonden al snel problemen, omdat informatie minder tastbaar werd. Het begrip data werd geïntroduceerd, hetgeen inhield dat gegevens werden opgeslagen als gaatjes in papier en later als magnetische nullen en enen. Om de informatie terug te halen uit de data, was apparatuur en programmatuur nodig.
In het begin speelde de fysieke locatie hierbij nog steeds een belangrijke rol. Immers, informatie bevond zich op media als een ponsband, een ponskaart, een magneetband of een magneetschijf, die werden opgeborgen in goed bewaakte gebouwen waar je niet zomaar kon binnenlopen. Omdat er ook wel eens nullen en enen omvielen of bij brand werden vernietigd, moest van elk belangrijk bestand een kopie worden gemaakt, die dan ook weer ergens anders moest worden opgeborgen en bewaakt. Omdat alle applicaties in één grote computer draaiden (het mainframe), die in datzelfde goed bewaakte gebouw stond, was ook toen de beveiliging toch nog relatief eenvoudig.

Nog later

Met de komst van de openbare computernetwerken begon de ellende pas goed. Informatie stroomde, al dan niet gecodeerd, door dunne kwetsbare koperdraadjes het goed bewaakte gebouw uit. Niemand had meer zicht op wat ermee in die boze buitenwereld gebeurde. Er werd een scala aan technische snufjes bedacht om te voorkomen dat iemand data kon aftappen, door ergens aan een lijn te snuffelen om er vervolgens de informatie uit te reconstrueren. Gelukkig hadden we nog wel die ene grote computer waar alle informatieverwerking op plaatsvond en door die ene computer goed te beveiligen waren meteen ook alle applicaties goed beschermd tegen het kwaad van buitenaf. Centralisatie bleek zo gek nog niet.

Nog niet zo lang geleden

Waar het fout is gegaan weet ik niet meer precies, maar ergens begin jaren tachtig kwam iemand op het idee, om iedereen zijn eigen computer te geven (Personal Computer) en af te stappen van de centralisatiegedachte. 'Gedistribueerde verwerking' noemden ze dat en de computers kon je in elke winkel op de hoek van de straat kopen voor weinig geld. De software was ontwikkeld door ene meneer Bill G., waarmee hij in eerste instantie de thuishobbyist enthousiast wist te maken met vooral veel vrolijk gekleurde schermpjes, icoontjes en grappig bedoelde bewegende poppetjes, die ongevraagd hulp aanboden. Bovendien kon je al die schermpjes zelf aanpassen en de hele kermis naar jouw persoonlijke voorkeur instellen. Daarmee kon je uren zoet zijn en het was vooral leuk, maar in het geheel niet nuttig.

Al gauw moesten die apparaten ook op het werk worden geïnstalleerd en werden ze later ook gebruikt om kritische applicaties te draaien. Omdat deze computers slechts één applicatie tegelijk konden verwerken, moest voor elke applicatie weer een nieuw doosje worden neergezet, met alle randverschijnselen er omheen, waaronder de beveiliging in de ruimste zin van het woord. Het 'serverpark' was geboren en (bijna) iedereen was enthousiast.

IT-managers dachten in het begin dat ze goed hadden gescoord omdat ze met goedkope computers hetzelfde werk konden doen als met die grote, dure, centrale computer. Bovendien was het bedienend personeel (beheerders) heel tevreden, want ze konden eindeloos kleurtjes veranderen, werkbalken wijzigen en met icoontjes spelen. Ook mochten ze na elke nieuwe versie van het besturingssysteem weer opnieuw naar een cursus, omdat niets meer hetzelfde was als bij de vorige versie. Beheerders vinden dit leuk, maar zakelijk is dit absurd en het brengt ook weer vele beveiligingsrisico's met zich mee.

Na enkele jaren stonden bij sommige bedrijven inmiddels honderden en soms zelfs duizenden van die apparaten te snorren, met daaromheen hele hordes aan beheerders die niet alleen de beveiliging in de gaten moesten houden, maar ook de stroomvoorziening van elk apparaat, de netwerkverbindingen, de back-up, de software updates, et cetera. Natuurlijk werd er van alles bedacht om het beheer te automatiseren, maar de kwetsbaarheid van de serverparken, en dus van de applicaties, werd steeds groter door de versnippering van de beveiligingsmaatregelen. Bovendien stegen de kosten voor het beheer, de fysieke ruimte, het energiegebruik, de warmteregulatie en natuurlijk de beveiliging naar ongekende niveaus en werd de capaciteit van elk apparaat slechts voor maximaal dertig procent benut. Voor deze wildgroei moest dus wel een keer een oplossing worden bedacht.

Heden

Ik heb niet kunnen achterhalen wie het eerst met de oplossing voor dit probleem is gekomen, maar ik kan me niet aan de indruk onttrekken dat dit een vijftigplusser of misschien wel een zestigplusser is geweest: **virtualisatie** bleek de ultieme oplossing om de wildgroei van de 'applicatiedoosjes' tegen te gaan.

Hoe werkt het?

- Men neme een grote, sterke computer;
- men installeert een hoofdbesturingssysteem met virtualisatiesoftware;
- men installeert onder het hoofdbesturingssysteem een heleboel andere besturingssystemen;
- men installeert binnen elk (virtueel) besturingssysteem telkens één applicatie;
- men zorgt vanuit het hoofdbesturingssysteem voor de centrale beveiliging en het beheer van alle onderliggende besturingssystemen en applicaties.

Op de een of andere manier komt bovenstaand verhaal mij heel bekend voor uit de tijd dat ik nog jong was, want ik durf nu wel te bekennen dat ik een zestigplusser ben met meer dan veertig jaar ervaring in de IT (dat woord bestond toen zelfs nog niet). Toen ik de eerste signalen opving over deze 'revolutionaire' en spraakmakende oplossing was mijn eerste gedachte: "Dit kan niet waar zijn".

Virtual Machine (VM) is een begrip uit de jaren zestig en was, en is nog steeds, gemeengoed bij de oudere IT populatie. Ik ben ermee opgegroeid en ik kon dan ook niet begrijpen dat we in de jaren tachtig de centralisatiegedachte onderuit begonnen te halen onder invloed van twee grote multinationals: Microsoft en Intel. Met name informatiebeveiligers moeten dit met lede ogen hebben aangezien. Naast of onder VM hadden we MVS (Multiple Virtual Storage), het huidig z/OS. Dit besturingssysteem is in staat om tienduizenden applicaties tegelijk te laten draaien onder het toeziend oog van één centrale beveiligingsapplicatie, die zowel de toegang tot bestanden, als tot functies voor het hele systeem regelt. Door het concept van Geographically Dispersed Parallel Sysplex (GDPS) is het bovendien mogelijk om daadwerkelijk 7x24x365 te draaien. Met slechts enkele beheerders en een minimale vloerbezetting kun je hiermee de hele wereld aan. Met nadruk wil ik stellen dat ik hier een pleidooi houd voor de genoemde concepten en niet voor de producten van de betrokken leverancier.

Het is een bekend verschijnsel dat ouderen vaak terugverlangen naar vroeger, maar dat de jeugd daar meestal heel anders over denkt. Het doet me dan ook deugd, dat de IT-wereld van nu heel druk bezig is om toch weer terug te gaan naar vroeger, waarbij we met één of enkele grote computers vanuit een goed bewaakt gebouw al onze applicaties kunnen draaien met een centrale voorziening voor beveiliging en beheer, waarbij bovendien de capaciteit van het apparaat optimaal wordt benut. Het is wel jammer dat virtualisatie wordt uitgelegd als iets heel revolutionairs, terwijl het in mijn beleving hele goede wijn is, die in totaal vernieuwde, maar kwalitatief mindere zakken wordt verkocht. Dat laatste leid ik af uit het feit dat er vaak toch maar één of een beperkt aantal applicaties kan draaien binnen één virtueel besturingssysteem. Dat dit efficiënter kan, moge duidelijk zijn.

Toekomst

Als we vorig jaar hét ICT-woord van 2009 hadden gekozen, dan was dat vrijwel zeker Cloud Computing geworden, want als vervolg op de virtualisatiehype, moeten de 'wolken' de ultieme oplossing bieden voor al ons ICT-leed. Vaak wordt hierbij de parallel met gas-, water- en elektriciteitscentrales getrokken, maar daar zit toch nog een belangrijk verschil in. Bij onze nutsvoorzieningen zijn wij immers slechts verbruiker van de geleverde eenheden (éénrichtingsverkeer), terwijl we bij Cloud Computing ook toeleverancier en eigenaar zijn van gegevens en verwerkingsalgoritmes (tweerichtingsverkeer).

Veel leveranciers gebruiken Cloud Computing als lokkertje om alle IT-activiteiten uit handen te geven, waarbij je alleen maar betaalt voor het gebruik van de resources en waarbij al het beheer, de beveiliging en het onderhoud voor je wordt geregeld. Dit noem ik dus 'Cloutsourcing' en dat is niets anders dan ordinaire outsourcing in (alweer) een nieuw jasje.
Is Cloud Computing dan alleen maar een nieuwe hype die in werkelijkheid niets inhoudt? Het antwoord hierop is duidelijk 'neen'. Het is wel degelijk een concept met

een duidelijk perspectief, dat in de toekomst overal gemeengoed zal zijn, maar wel met een geleidelijk acceptatie- en migratiepad met de nadruk op acceptatie.

Voor kleinere ondernemingen, zoals ons bedrijf Inframatica Consultants (twintig vaste medewerkers, tien externen en vijfentwintig opdrachtgevers) is de wolk een uitkomst. Al sinds zeven jaar hebben wij alles ondergebracht bij een Cloud-leverancier, die alles voor ons regelt, zodat wij ons volledig kunnen concentreren op onze kernactiviteit. Dit houdt dus in dat de hardware, de applicaties en de data in een Cloud beschikbaar zijn voor iedereen die over internet beschikt en is geautoriseerd voor het gebruik hiervan, afhankelijk van de rol die iemand binnen het bedrijf heeft. Ja, ja, zelfs wij hebben als klein bedrijf Role Based Access Control (RBAC) met succes geïmplementeerd.

Wij hebben dus niets te maken met onderhoud, virusscanners, back-ups, licenties, enzovoorts. We betalen een vast bedrag per maand en nog een extra bedrag per medewerker die toegang heeft tot het systeem en daarmee hebben we 7 x 24 uur, 365 dagen per jaar toegang tot het systeem en zijn applicaties, onafhankelijk van de locatie waar iemand zich bevindt. Natuurlijk hadden we die Cloud ook in eigen huis kunnen opzetten, maar dan heb je wel zelf de sores van het onderhoud, de back-ups, enzovoorts.

“Hoe zit het dan met de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van de data die is opgeslagen?”, hoor ik u vragen. Ja, dat is nou een kwestie van afwegen. Natuurlijk zei de leverancier dat dit allemaal perfect geregeld is en dat het allemaal in SLA’s wordt vastgelegd. Ben ik daarmee geholpen als het achteraf alsnog fout gaat? Schiet ik er wat mee op, als ik al mijn data kwijt ben, geen toegang heb tot het systeem, maar wel enige vorm van (geldelijke) schadevergoeding ontvang? Dat hangt dus sterk af van het belang van die data en het belang van die beschikbaarheid. Nou, ik kan u zeggen: Inframatica is niet ‘out of business’ als er iets vreselijk mis zou gaan. Ons voortbestaan is niet afhankelijk van onze IT, dus de keuze was toen eigenlijk niet zo moeilijk.

Bij de grote ondernemingen ligt dit verhaal heel anders als er wordt gekozen voor een Cloud buiten de deur. Als de gegevens van een grote bank of een verzekeringsmaatschappij in een wolk verloren gaan of in verkeerde handen komen, dan staat een eventuele schadevergoeding niet meer in verhouding tot de werkelijk geleden schade. Want wat moet je met die paar centen als je bedrijf failliet dreigt te gaan? Hier loopt nu de belangrijkste beer op de weg: men is nog niet bereid zomaar alle bedrijfsgegevens in een vreemde wolk te laten zweven. Dit heeft alles te maken met (het ontbreken van) vertrouwen en dat is in mijn beleving een kwestie van tijd. Hoeveel tijd? Ik denk nog minstens tien tot vijftien jaar.

Ooit kregen wij ons loon in een papieren zakje en dat werd vervolgens verdeeld over allerlei potjes op de schoorsteenmantel. Op enig moment waren wij bereid om dat geld af te staan aan een ‘provider’, die het voor ons beheerde en ons voorzag van overzichten waarmee we konden controleren of hij zijn werk wel goed deed. Zeg nou eerlijk: wie rekent nog na of de bank zijn werk wel goed doet? Wij geven al ons geld af en vertrouwen erop dat het goed beheerd wordt en dat we er altijd over kunnen beschikken. Dat geldt voor zowel particulieren, als voor bedrijven. Helaas heeft het afgelopen jaar geleerd, dat dit niet meer zo vanzelfsprekend is.

In mijn lange IT-loopbaan heb ik bij de opkomst van de magneetschijf nog meegemaakt dat bestanden die op tape stonden niet op schijf mochten worden gezet samen met bestanden van andere gebruikers. Men was bang voor vermenging van de verschillende bestanden en wilde een eigen schijf net als de eigen magneetband. Het heeft even geduurd voordat we dat vertrouwen van onze gebruikers hadden gewonnen en veel later moesten ze er zelf ook om lachen, dat ze zo bekrompen hadden gereageerd op de komst van die ‘enge’ schijven.

Ook met de introductie van het SAN was men in het begin sceptisch om een storage infrastructuur te moeten delen met andere applicaties, die op andere servers draaiden. Inmiddels is het SAN niet meer weg te denken uit onze ICT-wereld en hebben we (bijna) allemaal volledig vertrouwen in deze technologie. Ik ben ervan overtuigd dat er ooit een tijd komt dat we dat vertrouwen ook hebben als het gaat om het afstaan van onze kritische bedrijfsgegevens aan Cloud-providers. Wat dat betreft blijft de geschiedenis zich herhalen maar dan op andere niveaus.

Het vak van informatiebeveiliger zal zich tegen die tijd beperken tot het opstellen van de eisen en wensen en het inrichten van de processen. De achterliggende tooling en techniek zal geheel een verantwoordelijkheid zijn van de Cloud-provider. Compliance regels zullen in de toekomst hierop worden aangepast met een verschuiving van de verantwoordelijkheden naar de provider. Tot die tijd is het zeker raadzaam om voorbereidingen te treffen, door het inrichten van een ‘binnenwolk’. Bedrijven met grote, complexe en bedrijfskritische ICT-omgevingen kunnen dan intern ervaring opdoen met Clouds en profiteren direct van alle virtualisatietechnieken die nu en in de toekomst op de markt beschikbaar zijn.
Zodra het tussen de oren goed zit met het vertrouwen om alles bij een externe Cloudleverancier onder te brengen, is het een eitje om die migratie uit te voeren. Pas dan zal men echt met het hoofd in de wolken lopen, omdat van die Cloud-leverancier verwacht mag worden dat hij grote schaalvoordelen kan bieden, waardoor substantiële besparingen kunnen worden gerealiseerd. Persoonlijk verwacht ik dat er straks wereldwijd maximaal vijf grote aanbieders zullen overblijven die voldoende schaalvoordelen kunnen bieden.

Eén ding is hierbij zeker: alle verwerkingen zullen weer centraal plaatsvinden vanuit een goed beveiligd gebouw met wellicht het oude vertrouwde VM en MVS concept weer als basis.
Mocht u plannen hebben om iets met wolken te gaan doen, dan hoop ik dat u onderstaande tips ter harte neemt alvorens grote investeringen te doen of overhaaste beslissingen te nemen.

- Hoedt u voor de Cloudsourcing-leveranciers.
- Vraag uzelf af, wat de gevolgen kunnen zijn van een wolk met kritische bedrijfsgegevens die door derden wordt beheerd.

- Technisch kan (bijna) alles, maar laat u vooral niet door techniek leiden.
- Ga lekker oefenen met een 'binnenwolk' zonder dat u zich hoeft te bekommeren over de invloed van een mogelijke 'donderwolk' buiten de deur.
- Streef naar open standaardoplossingen, want een vendor lockin ligt altijd op de loer.
- Een businesscase helpt u bij de onderbouwing.
- Vraag naar ervaringen en adviezen van onafhankelijke derden.
- Laat u niet gek maken met SaaS, PaaS en IaaS, want dat doet alleen een DwaaS (Dombo without any architectural Sense).

Conclusie

Grote, gevirtualiseerde en goedbeveiligde computers ontmantelen en er kleine systemen voor terugplaatsen, die we vervolgens door middel van virtualisatie weer gaan opschalen tot grote computers, is eigenlijk wel een heel merkwaardige vorm van evolutie. Virtualisatie is niets nieuws en als in de jaren tachtig niet iedereen zo hard achter de hype van decentralisatie was aangehold, hadden we nooit al die losse doosjes in onze rekken gehad. Door de gebrekkige beveiliging zijn hackers (te) vaak in staat geweest om computers te kraken en informatie te stelen of door te verkopen.

Natuurlijk heeft de down sizing ons ook goede dingen gebracht, want kleinere bedrijven konden met relatief lage kosten toch een volwassen IT-omgeving realiseren. Met name de komst van Unix en later Linux heeft zeker een positieve bijdrage geleverd aan de ontwikkeling van IT, maar helaas zijn we op sommige terreinen te ver doorgeschoten.

Voor de toekomst denk ik dat Cloud Computing een serieuze zaak wordt, waar we allemaal mee te maken gaan krijgen, maar waarmee we niet over één nacht ijs mogen gaan. Kleinere ondernemingen kunnen nu al profiteren van de schaalvoordelen met een beperkt risico door deel te nemen in een externe Cloud, maar voor bedrijven die volledig afhankelijk zijn van hun ICT, zal het nog wel even duren voordat zij zich helemaal overgeven aan een Cloud-leverancier.

Het devies is: neem de tijd, volg de ontwikkelingen, praat met onafhankelijke deskundigen en loop vooral niet te snel met uw hoofd in de wolken.

Boekpresentatie Information Security Management with ITIL V3

Auteur: Lex Dunn CISSP ISSMP > Lex Dunn is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is één van de redacteuren van het blad Informatiebeveiliging en editor van een schriftelijke CISSP cursus. Hij is bereikbaar via lex.dunn@capgemini.com.

Op 2 maart jl. was een groot deel van informatiebeveiligend Nederland te vinden in het Diligentia Theater in Den Haag om, op uitnodiging van Verdonck, Klooster & Associates, de presentatie van het nieuwe boek Information Security Management with ITIL V3 bij te wonen. De bijeenkomst werd geopend door Wim Schimmel, directeur/partner bij VKA. Hij memoreerde aan het eerste Security Management boek in de ITIL-reeks van elf jaar geleden. Ten aanzien van de komende verkiezingen, het Binnenhof was per slot van rekening vlakbij, hoopte hij dat informatiebeveiliging niet op de lange baan geschoven zou worden en dat privacy de nodige aandacht zou krijgen.

Dick Brandt, Information Security Officer bij TNT Post, vroeg zich in zijn presentatie af: "Waar heb dat nou voor nodig?" Een vraag die Sjef van Oekel, alias Dolf Brouwers, zich rond 9 april 1973 ook stelde toen hij een plan lanceerde voor een klassieke radiozender op de Noordzee. Brandt vroeg zich af wat ITIL nu eigenlijk is. Naast de Turkse naam voor de langste rivier in Europa (de Russische Volga, of zoals wij hem kennen: Wolga) is ITIL de Information Technology Infrastructure Library, een initiatief van de Engelse overheid, dat ondertussen is uitgegroeid tot een defacto standaard voor het inrichten van IT beheer in Europa. Daarin heeft Information Security Management een plaats, alhoewel Brandt de rol van security ziet verschuiven richting de business managers. Maar of de security rollen ook uit zullen sterven, zoals de boordwerktuigkundige met de komst van de Airbus 300, valt nog te bezien. Dan zal er nog wel wat aan de 'taal' moeten gebeuren: ITIL is nu vooral een taal voor techneuten.


Dick Brandt

Over het boek merkte Brandt op dat het vooral pragmatisch gebruikt moet worden. Ook Jacques Cazemier merkte in een eerder artikel al op: "Alomvattende volledigheid is leuk voor een boek, maar niet voor de praktijk." Het doel is risico's te beperken tot een aanvaardbaar niveau en in de huidige cultuur van 'bewijs wat je zegt', is dit nieuwe boek zeker bruikbaar.
Alexander Kist, bestuurslid bij ITSMF, de vakorganisatie voor IT beheer in Nederland, gaf de aanwezigen een inleiding IB onder het motto 'How to bluff your way into (IT) security'. Hij had dit al eerder gedaan over ITIL V3, op Youtube is een leuk filmpje daarover te vinden.

De term information security geeft zo'n 434.000 hits op Google, dus er wordt kennelijk het nodige over gezegd en geschreven. Maar voor 'dummies' was de presentatie van Kist een goede achtergrond om te kunnen meepraten. Op ludieke wijze kwamen de bekende termen over het voetlicht. Voor de meeste aanwezigen natuurlijk gesneden koek, maar wel iets om over na te denken, omdat informatiebeveiligers regelmatig met mensen om de tafel zitten die al die vaktermen niet kennen.

In een korte presentatie gaf Jacques Cazemier, één van de auteurs en Principal Consultant bij Verdonck, Klooster & Associates, vervolgens een overzicht van de huidige stand van zaken met betrekking tot informatiebeveiliging. Uit een onderzoek van Joey Roetman van de Haagse Hogeschool bleek dat de hele ISO 27002 vaak zonder meer als baseline wordt gebruikt en dat de baseline dus weinig tot niet geba-

Louk Peters, Jaques Cazemier en Paul Overbeek

seerd is op reële risico's (meestal beveiliging 'omdat het moet'). Ook kwam uit het onderzoek naar voren dat er nauwelijks rapportage is te vinden over informatiebeveiliging en zo die er al is, er weinig mee wordt mee gedaan. Het gebruikte vakjargon is daaraan misschien debet. Het sluiten van de Plan-Do-Check-Act cyclus (of die nou linksom of rechtsom wordt weergegeven) ontbreekt vaak (de ACT fase). Het nieuwe boek kan bijdragen aan een verbetering hiervan, ook bij organisaties die hun beheer niet met ITIL hebben opgezet.

Tot slot werd het nieuwe boek Information Security Management with ITIL V3 door Ivo van Haren, CEO bij Van Haren Publishing gepresenteerd en aan de auteurs Jacques Cazemier, Paul Overbeek en Louk Peters overhandigd.
Tijdens de afsluitende borrel was er nog ruimschoots gelegenheid om te netwerken en met de auteurs van gedachten te wisselen. Een uitgebreide beschrijving van het boek kunt u in één van de komende nummers als boekbespreking tegemoet zien.


Alexander Kist

Links
- Het boek is onder andere verkrijgbaar via de website van de uitgever (Van Haren Publishing): http://www.vanharen.net/product_info.php?products_id=835&language=nl
- Meer informatie over ITIL V3 kunt u vinden op: http://www.itil-officialsite.com/
- De website van het ITSMF in Nederland vindt u op: http://www.itsmf.nl/
- ITIL is ook de Turkse naam voor de Wolga: http://en.wikipedia.org/wiki/Volga_River
- Filmpje van Alexander Kist op Youtube: http://www.youtube.com/watch?v=TlqIGhn1C58

Het Business Oriented Autorisation Model

Auteurs:Peter Hoogendoorn en Jean-Pierre Vincent > Peter Hoogendoorn is werkzaam bij Achmea Pensioenen als Group information security manager en belast met het invoeren van governance op dit gebied. Hij is bereikbaar via peter.m.hoogendoorn@achmea.nl. Jean-Pierre Vincent is Managing Security Consultant bij Capgemini en hij is thoughtleader identity en access management binnen de interne security community. Hij is bereikbaar via jean-pierre.vincent@capgemini.com.

Veel, met name grotere, organisaties zijn druk met het beter en efficiënter beheren van de autorisaties van hun medewerkers. Om dit doel te bereiken wordt vaak een centrale identiteit en een access management organisatie ingericht en een centraal autorisatiemodel vastgesteld. Van het autorisatiemodel staat vaak al van begin af aan vast dat het een model moet worden op basis van RBAC. RBAC kent echter een aantal belangrijke risico's. Die risico's liggen zowel in het denken over RBAC, als ook over hoe een organisatie de invoering van RBAC ter hand neemt.

Dit artikel beschrijft hoe een autorisatiemodel kan worden ontwikkeld, waarbij zaken als de RBAC-risico's tot een minimum kunnen worden beperkt, de kosten voor autorisatiebeheer aanzienlijk kunnen worden teruggebracht en de gebruikersvriendelijkheid voor de business wordt geoptimaliseerd.

Nog steeds zijn autorisatieprocessen bij veel grote bedrijven niet eenduidig. De autorisatieprocessen vergen veel inspanning, ze vragen een lange doorlooptijd en ze brengen daarom hoge kosten met zich mee. Deze situatie betreft niet alleen het snel en flexibel kunnen verstrekken van de juiste autorisaties bij de in-, door- en uitstroom van medewerkers (medewerkerlifecycle), maar ook het snel en efficiënt inzicht kunnen geven in de verstrekte autorisaties aan de medewerkers in controleprocessen en bij audits.

Organisaties zijn zich ervan bewust dat het doorvoeren van verbeteringen in de autorisatiebeheerprocessen kunnen leiden tot besparingen in de beheerkosten en het sneller en gebruiksvriendelijker kunnen faciliteren van de business in de medewerkerslifecycle. Door het opzetten van een identity en access managementprogramma wordt de bestaande situatie verbeterd. Een dergelijk programma begint meestal met een onderzoek naar een juist identity en access managementsysteem, een optimale IAM-procesinrichting, een bij de organisatie passend autorisatiemodel en een implementatieaanpak. Dit artikel geeft richtlijnen voor het ontwerpen van een optimaal autorisatiemodel.

Verschillende typen autorisatie modellen

In de afgelopen jaren zijn er verschillende typen autorisatiemodellen ontwikkeld. In de Expertbrief Access management, deel 2: Architectuur, worden verschillende typen autorisatiemodellen beschreven. Ieder type autorisatiemodel heeft zijn eigen voor- en nadelen of vindt zijn toepassing in een bepaald type omgeving (bijvoorbeeld federatief). Wanneer we hier de focus beperken tot de toegang van medewerkers op systemen binnen een organisatie, dan zien we in de praktijk dat het RBAC-model nog steeds zeer populair is. Andere modellen krijgen wel steeds meer aandacht, maar het praktisch toepassen, lijkt nog steeds maar beperkt mogelijk door onder andere het ontbreken van goede tooling.

RBAC kent echter een aantal risico's, waarmee we in ons te ontwerpen autorisatiemodel rekening willen houden:

- Omdat iedere medewerker over een net even andere set aan autorisaties lijkt te beschikken, is het moeilijk om groepen medewerkers aan één of meerdere rollen te koppelen. In de praktijk groeien rollenmodellen uit, tot een onoverzichtelijke rollenstructuur en worden daardoor niet te beheren.
- Snelheid en flexibiliteit in het verstrekken van autorisaties verdwijnen als gevolg van de onoverzichtelijkheid. Vooral het wijzigen van de inhoud van rollen wordt een complex proces, zeker als een mutatie maar voor een deel van de gekoppelde medewerkers bedoeld is. Roleengeneerings activiteiten en goedkeuringsprocessen kosten dan veel inspanning.
- De business begrijpt niet meer aan welke rollen zij hun medewerkers moeten koppelen, er zijn te veel rollen en de verschillen in rollen onderling zijn soms miniem.

Bovenstaande risico's kunnen niet simpelweg aan enkele eenvoudige oorzaken worden toegeschreven. Dan zou het probleem al lang geleden zijn opgelost. Bedrijven hebben vaak een relatief grote hoeveelheid aan applicaties en systemen. Er zijn veel applicaties met een ingewikkelde rolgeba-

seerde autorisatiestructuur en zelfs de huidige generatie applicaties kennen nog de nodige complexiteit op dit gebied.

Zoals we deze risico's in ons autorisatiemodel willen beperken, willen we ook de uitvoeringskosten zo laag mogelijk houden. Dat betekent dat we autorisaties automatisch willen kunnen toekennen, waar dat zonder risico's mogelijk is. Dit geautomatiseerd toekennen heet Rule Based Access Control. Rules kunnen worden toegepast op losse autorisaties of op rollen. Sommige autorisaties willen we in verband met de risico's zeker niet geautomatiseerd toekennen, óf omdat ze gevoelig zijn, óf omdat de gegevens waarop de automatische toekenning is gebaseerd niet betrouwbaar zijn. Deze willen we als losse autorisatie handmatig kunnen toekennen en niet opnemen in een rol. In omgevingen waar veel medewerkers een gelijke set aan autorisaties hebben, biedt Role Based Access Control echter wel goede beheermogelijkheden. Een optimaal autorisatiemodel is dus opgebouwd uit een combinatie van verschillende autorisatiemodellen.

Hergebruik bestaande structuren binnen een organisatie

Zeker wanneer een organisatie is voorzien van een goed ingerichte governance, die verankerd is in de architectuur, zijn er vaak meerdere structuren aanwezig binnen de organisatie. Structuren zijn bijvoorbeeld de organisatiestructuur of het functiehuis. Meestal zijn deze structuren goed uitgewerkt, worden ze goed beheerd en worden ze begrepen door iedereen in de organisatie. Voor een model dat is gericht op de business ligt het dan ook voor de hand om een dergelijke structuur te hergebruiken voor het autorisatiemodel.

Om de operationele kosten rond het gebruik en het beheer van een autorisatiemodel zo laag mogelijk te houden, moeten we als basis de meest stabiele structuur hergebruiken. De grootte en de diversiteit van een organisatie speelt hierbij een rol. Bekijken we een organisatie vanuit een bedrijfskundige bril en gaan we op zoek naar de meest stabiele structuren, dan zien we dat dit verschilt afhankelijk van de plaats in de organisatie. Binnen de verschillende onderdelen van een organisatie zijn andere structuren stabiel en/of bruikbaar om als basis te dienen voor een autorisatiemodel. Na de volgende alinea lichten we een paar modellen toe.

Daarnaast is het belangrijk de organisatie te zien als een eenheid van werkende mensen, met ieder hun eigen taken en verantwoordelijkheden, die hun activiteiten uitvoeren binnen bestaande processen of projecten en die middelen nodig hebben om hun activiteiten te kunnen uitvoeren. Die middelen zijn, naast wellicht fysieke middelen, onder andere de autorisaties. Het is voor de medewerkers dan ook van belang dat ze flexibel en snel de, voor het werk benodigde, middelen ter beschikking krijgen op zodanige wijze dat die middelen ook voldoen aan security- en beleidseisen.

"Most of the security violations in authorisations is caused by people who just want to do their jobs."
Bruce Schneier

De businessorganisatie

In het uitvoerende deel van de organisatie is de vraag om snel de juiste autorisaties te verkrijgen het hoogst, hier is verlies van tijd direct te vertalen naar het verlies van geld. Deze uitvoerende businessonderdelen zijn dan ook het meest belangrijk voor de organisatie. Hier gaan we opzoek naar een stabiele structuur. In deze tijden van reorganisatie en crisis is het behoorlijk onrustig in de businessonderdelen. Zowel de organisatiestructuur, als de benaming en/of inhoud van functies zijn in deze tijden weinig stabiel. Door wie en waar (binnen of buiten de organisatie) de activiteiten worden uitgevoerd, veranderd continu. De business gaat echter door en dus moeten de businessprocesactiviteiten nog altijd worden uitgevoerd. De activiteiten binnen een businessproces zijn dus een stabiele factor. Willen we een stabiel autorisatiemodel opzetten voor de business, dan moeten we deze baseren op de activiteiten in de businessprocessen. Termen als 'activiteiten' en 'businessprocessen' zijn termen die men in de business ook goed verstaat. Het baseren van het autorisatiemodel op deze termen heeft als direct voordeel dat de business eenvoudig in staat is het autorisatiemodel te begrijpen.

De projectenorganisatie

Zoeken we in een projectenorganisatie naar een stabiele structuur dan komen we al gauw uit op de taken van medewerkers binnen het project. Om aan de verwachting van de taken invulling te geven, wordt van de projectmedewerkers bepaalde activiteiten verwacht. Om deze te kunnen uitvoeren zijn autorisaties nodig. Binnen een project lijkt het daarom handig de projecttaken van de projectmedewerkers te koppelen aan de betreffende activiteiten en hun activiteiten te koppelen aan autorisaties.

De beheerorganisatie

Ook bij beheerorganisaties zijn de functies van medewerkers de meest stabiele structuur. Hoewel bijvoorbeeld richtlijnen als ITIL prima de processen beschrijven voor de ICT-beheerorganisatie, blijkt deze structuur maar moeilijk toepasbaar op een autorisatiemodel voor een beheeromgeving. Dit komt omdat taken gericht zijn op een verantwoordelijkheid voor het toepassen van kennis in verschillende processen. Bijvoorbeeld een servicedeskmedewerker moet calls afhandelen voor een proces dat divergeert naar ieder aanwezig platform in de organisatie. De activiteiten van de servicedeskmedewerker zijn dus procesoverstijgend. Het lijkt derhalve handig om activiteiten te relateren aan de functie van de medewerker. De benodigde autorisaties worden dan weer gerelateerd aan de activiteiten die bij die functie horen.

De organisatiestructuur

Grote organisaties zijn ingedeeld in verschillende bedrijfsonderdelen. Sommige autorisaties zijn uitsluitend afhankelijk van het bedrijfsonderdeel waarvoor de activiteiten worden uitgevoerd. Denk bijvoorbeeld aan logo's en templates. In dat geval moeten alle medewerkers die voor dat bedrijfsonderdeel werkzaam zijn van de betreffende autorisaties worden voorzien. Het toekennen van autorisaties gebeurt dan op basis

van het organisatiemodel. Aangezien dat gegevens zijn van de medewerkers die actief in HR-systemen wordt onderhouden, kunnen deze autorisaties (los of via een rollenstructuur) vaak eenvoudig geautomatiseerd worden toegekend.

Uitzonderingen

Er zijn altijd medewerkers met uitzonderlijke autorisaties. Een voorbeeld daarvan is medewerkers met een handicap. Zij hebben soms andere hulpmiddelen nodig om de activiteiten te kunnen uitvoeren. Het verdient aanbeveling de autorisaties die zij daarvoor nodig hebben te koppelen aan de betreffende, speciale wijze van uitvoeren van de activiteiten.

De opzet van een autorisatiemodel op basis van de verschillende structuren en modeltypen

Wanneer de meest stabiele structuren in de verschillende onderdelen van een organisatie zijn geïnventariseerd, kan het autorisatiemodel worden ingericht. Naast het selecteren van structuren moeten ook autorisatiemodeltypen worden vastgesteld.

Er kunnen meerdere modeltypen naast elkaar worden gebruikt, als dat het de beheerbaarheid van het model ten goede komt. Het mixen van Rule en Role Based Access Control is een al eerder gesuggereerd voorbeeld. Deze mix wordt ook wel aangegeven met RRBAC. Maar ook combinaties met Claims Based Access Control is mogelijk, mits bijvoorbeeld het beheer van identity-entitlements goed is geregeld, zowel aan de HR-kant, als aan de doelsystemen-kant. De entitlements dienen dan ook gebaseerd te zijn op de gegevens die worden gehanteerd binnen de geselecteerde structuren. Meer informatie over Claims Based Access Control is te vinden in de Expertbrief Access management, deels 2: Architectuur.

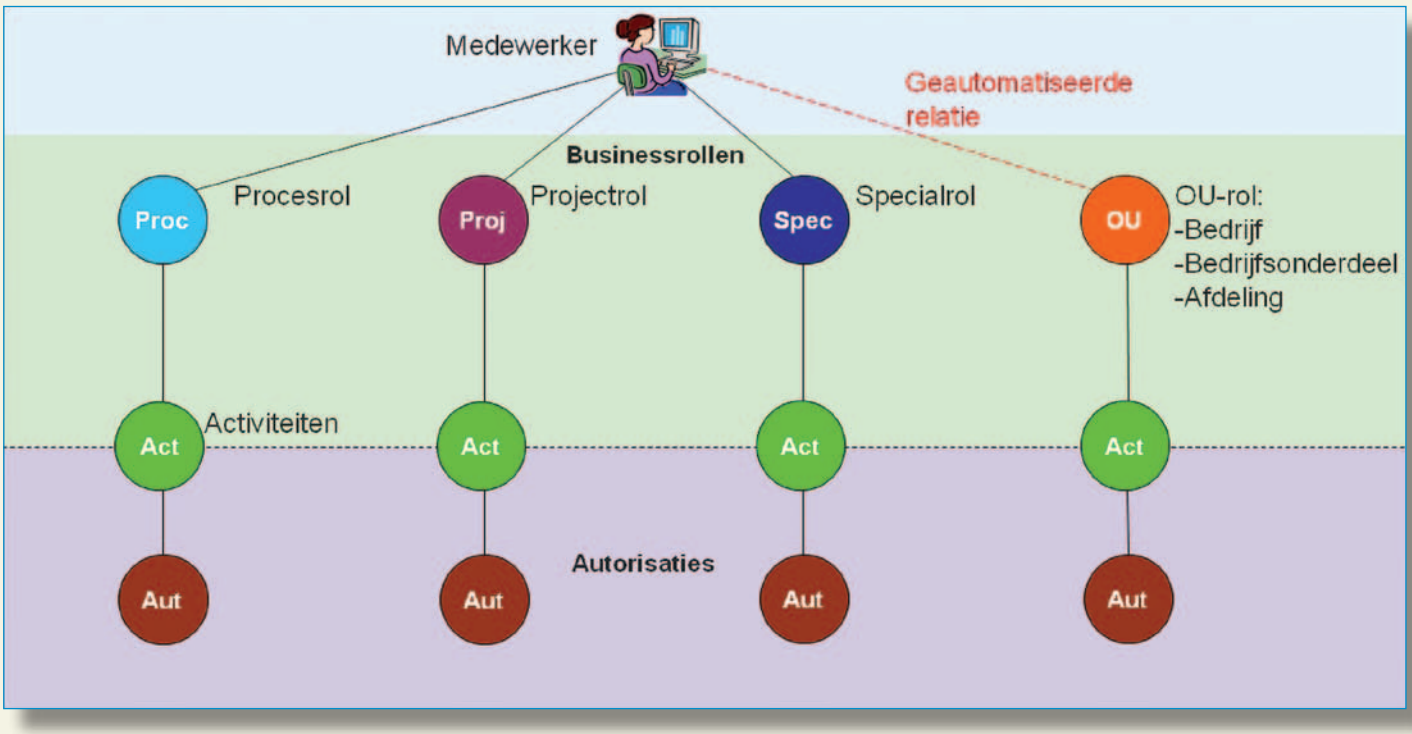
Een voorbeeld van een Business Oriented Autorisation Model op basis van de vier beschreven structuren en modeltype RRBAC, is weergegeven in figuur 1.

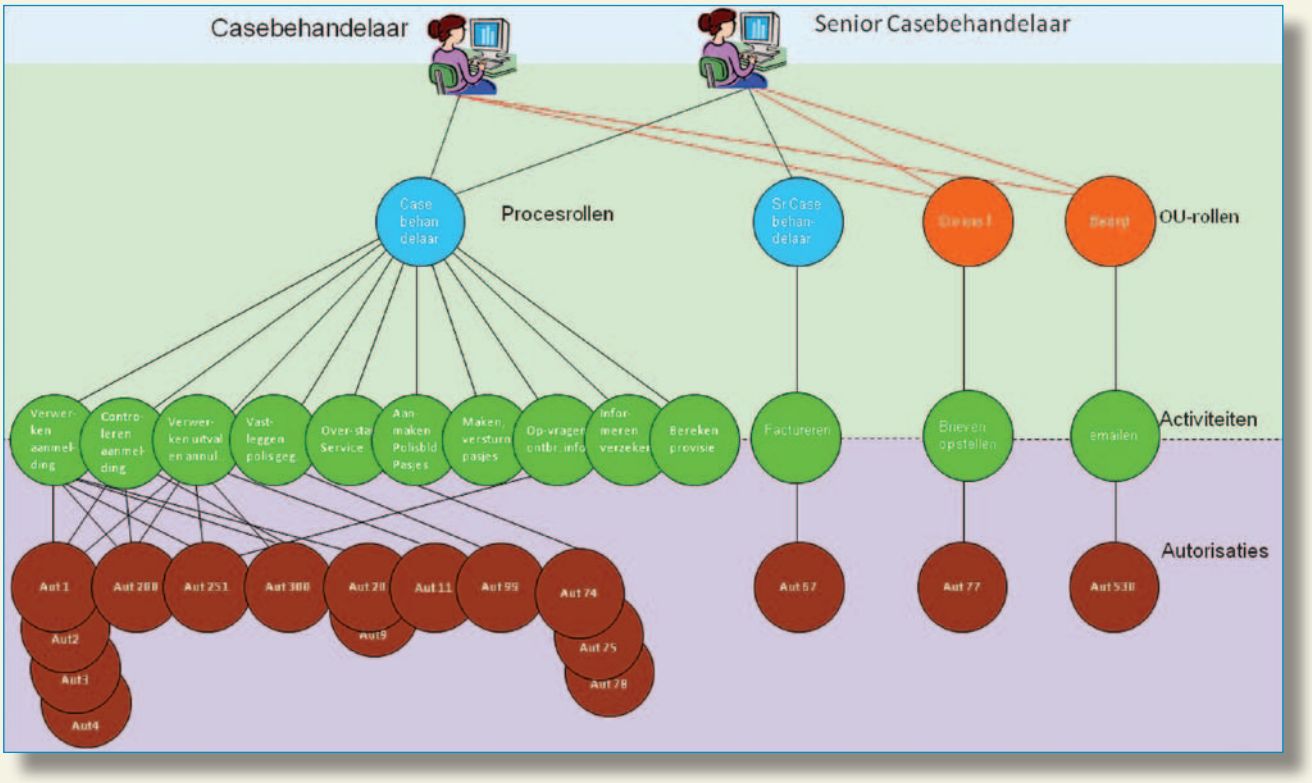
Praktische opmerkingen

Pas Rule Based Access Control toe wanneer de benodigde gegevens beschikbaar en betrouwbaar zijn. Hierop kunnen eenvoudig regels worden gedefinieerd voor het automatisch verstrekken van autorisaties. In de praktijk kom je hier overigens nauwelijks autorisaties tegen waarin functiescheidingscriteria een rol spelen.
Pas Role Based Access Control toe bij autorisaties die wel aan functiescheidingscriteria moeten voldoen.

Een medewerker kan hier, al dan niet geautomatiseerd, aan meerdere rollen worden gekoppeld uit de verschillende structuren. Iedere rol is gerelateerd aan één of meerdere activiteiten. De activiteiten vormen hier als rol de interface tussen business en techniek. Enerzijds zijn deze gekoppeld aan één of meerdere technische autorisaties, anderzijds krijgen ze de benaming uit de betreffende structuur (zie Naamgevingsconventieregels verderop in dit artikel). Indien echt 'businessgericht' wordt gewerkt, wordt ook iedere technische autorisatie voorzien van een functionele naam. In figuur 2 wordt een voorbeeld gegeven van dit autorisatiemodel, toegepast op een businessproces.

Figuur 1. Een voorbeeld van een Business Oriented Autorisation Model op basis van vier stabiele structuren en type RRBAC.





Figuur 2. Een uitgewerkt voorbeeld van een Business Oriented Autorisation Model voor een businessproces.

Hergebruik eigenschappen uit de gekozen structuren

Als de gekozen structuren op een juiste manier in de organisaties zijn ingebed, kunnen beleid, verantwoordelijkheden en middelen voor het autorisatiebeheer worden hergebruikt. Dat levert een aanzienlijke kostenbesparing en meer efficiëntie op. Taken, verantwoordelijkheden, kennis en belang liggen nu alle bij de meest direct betrokkenen in de structuur. Enkele voorbeelden:

- Hergebruik functiescheidingsregels
  Op businessprocesniveau worden de functiescheidingsregels vastgesteld. Deze kunnen één op één worden overgenomen.

- Overnemen procuratieregels
  Procuratieregels uit de businessprocessen kunnen één op één worden overgenomen in het autorisatiemodel. Indien procuratiegegevens in een administratie worden bijgehouden, kan deze worden gebruikt bij het geautomatiseerd verstrekken van de juiste autorisatieniveaus. Voor meer informatie, zie artikel RBAC Next Generations, IB december 2007.

- Naamgevingsconventieregels overnemen
  Op vastgestelde structuren is vaak ook een naamgevingsconventie van toepassing. Deze kan één op één worden overgenomen en waar nodig worden uitgebreid naar middelen (autorisaties). Dit betekent dat de taal wordt gesproken zoals die in de betreffende structuur wordt gehanteerd. Dat is een belangrijk aspect in het verkrijgen van begrip van de betreffende businesspartij.

- Taken beleggen bij de verantwoordelijken in de structuur
  Taken die horen bij het onderhouden van het autorisatiemodel (als eigenaarschap) kunnen worden belegd bij de betreffende taken in de structuur. Indien gewenst kunnen taken worden gedelegeerd naar een meer technische serviceafdeling. Een voorbeeld is het beleggen van het eigenaarschap van de relatie tussen medewerker en autorisatie. Aangezien de structuureigenaar (proceseigenaar, projectmanager, teamleider) de eindverantwoordelijkheid heeft voor kosten en efficiëntie van zijn structuur, is deze persoon ook de juiste kandidaat voor het eigenaarschap van deze koppelingen, bijvoorbeeld als rol- of rule-eigenaar in een RRBAC-oplossing. Het aanbrengen van de koppelingen binnen zijn structuurscope vindt onder zijn eindverantwoordelijkheid plaats. Het uitbreiden van de bestaande businesstaken met de relatief beperkt benodigde aandacht voor autorisaties, bespaart op FTE's in de autorisatiebeheerorganisatie. De controle of er gehandeld wordt binnen de beleidsregels dient uiteraard te worden gehandhaafd. Hiervoor zijn tegenwoordig ook goede tools beschikbaar.

Het koppelen van centraal autorisatiemodel aan doelsysteem-autorisatiemodellen

Net zoals de typen autorisatiemodel van doelsystemen kunnen verschillen, verschillen ook de gekozen doelsysteem-autorisatiemodellen. Wanneer een centraal autorisatiemodel en modeltype moet worden gekoppeld aan de vele doelsystemen die doorgaans in een grote organisatie aanwezig zijn, gaat dat gepaard met het doen van concessies. Een voorbeeld is dat de beschikbare autorisatiegroepen in een doelsysteem meer toegang geven dan dat voor een activiteit nodig is.

Een eerste vraag die in een dergelijke situatie moet worden beantwoord, is of het bestaande autorisatiemodel van het doelsysteem gehandhaafd moet blijven. Voor

complexe systemen is het antwoord veelal 'ja', omdat het uitgewerkte autorisatiemodel vaak zeer complex is en het teveel werk is om een nieuw autorisatiemodel op te zetten. Het doen van concessies leidt over het algemeen niet tot de verstrekking van onnodige autorisaties. Het is alleen wel zaak om concessies zoveel mogelijk consistent te doen en goed te administreren. Een voorbeeld van een concessie is bijvoorbeeld dat één autorisatie van een doelsysteem voorziet in de autorisaties die nodig zijn voor meerdere activiteiten. Een concessie kan dan zijn om de autorisatie alleen te koppelen aan de eerste activiteit, of juist om de autorisatie van het doelsysteem te koppelen aan alle activiteiten waarvoor de autorisatie van toepassing is.

Het koppelen van verschillende typen autorisatiemodellen kan een stuk lastiger zijn. Het koppelen van een centraal RBAC-model aan een CBAC-model in een doelsysteem vraagt om een specifiek ontwikkelde interface. Het verdient aanbeveling om het centrale autorisatiesysteem met standaard protocollen te laten communiceren naar doelsystemen. Eventuele conversieproblemen, zowel op technisch niveau als op autorisatiemodeltype-niveau, worden afgevangen door een specifieke conversie-interface.

In figuur 3 wordt een voorbeeld gegeven van het koppelen van bron- en doelsystemen aan een centraal ingevuld en operationeel autorisatiemodel.

Het volume van het ingevulde autorisatiemodel versus uitvoeringskosten

Vaak is het volume van een ingevuld autorisatiemodel nog al eens onderwerp van discussie. Bijvoorbeeld mag in een Rol Based Access Control oplossing het aantal rollen niet te groot worden. 'Hoe meer rollen, hoe meer onderhoudskosten' is vaak het devies. Deze mening zou overigens ook gelden voor andere typen autorisatiemodellen. Het is echter maar beperkt waar. De meest belangrijke factor is namelijk hoe snel een mutatie op een rol, een rule, een entititlement, et cetera kan worden doorgevoerd. Als de inspanning die hiervoor nodig is nihil is, mag het aantal best groot zijn. Dit kost minder inspanning en het werkt sneller dan andersom. Bij een business gericht autorisatiemodel is dit het geval. Het aantal rollen, rules en entititlements is gelijk aan het aantal gedefinieerde activiteiten in de gekozen structuren. Dat kunnen er best veel zijn. Het aanbrengen van een mutatie kost echter altijd minimale inspanning, omdat de mutatie precies de doelgroep bedient en de betrokkenen in het mutatieproces medewerkers zijn uit de directe businessomgeving en daarom kundig zijn in de te nemen overwegingen.

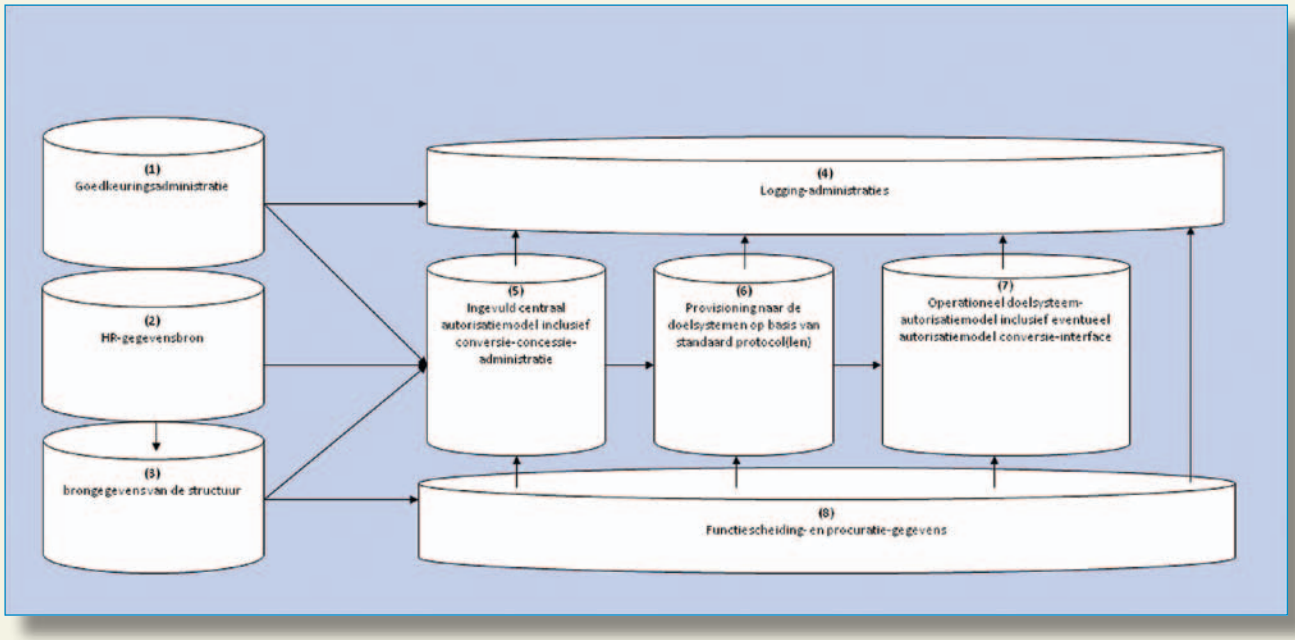
Het snel en efficiënt kunnen doorvoeren van mutaties van een volumineus, maar helder autorisatiemodel kost minder dan wanneer dit moet gebeuren in een complex en voor de business ondoorgrondelijk autorisatiemodel met een beperkt volume.

Toepassing in de praktijk

Bij een grote zorgverzekeraar wordt op dit moment identity en access management voor medewerkers conform de beschreven visie succesvol geïmplementeerd. Een belangrijke ervaring is dat de gekozen structuren in de praktijk niet altijd even goed worden toegepast als dat papier doet geloven. Een implementatieproject moet dan ook voorzien in ruimte om de structuren goed met de praktijk te laten aansluiten en hier eventueel verbeteringen in door te voeren. Een identity en access managementproject wordt daarmee een project van en voor de business. Dat verhoogt de acceptatiegraad van de introductie van het (business gerichte) autorisatiemodel.

De auteurs van dit artikel willen graag de visie verfijnen en uitbreiden. Ervaringen zijn derhalve welkom, aarzel niet om hen uw reactie per e-mail toe te sturen.

Figuur 3. Een voorbeeld van het koppelen van bron- en doelsystemen aan een centraal ingevuld autorisatiemodel.



Herstel van de zwakste schakel

De aspecten wederkerigheid en onmiddellijke invloed

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

Dit is het tweede artikel in een serie van acht waarin wordt ingegaan op de psychologische trucs die door Social Engineers (SE's) worden gebruikt om slachtoffers te manipuleren. Waarom en hoe werken ze? Hoe zijn ze te herkennen en wat is de beste verdediging? In dit artikel komen de aspecten Wederkerigheid (iemand iets verschuldigd zijn) en Onmiddellijke Invloed (besluitvorming onder druk) aan de orde.

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

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

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

Wederkerigheid: het aloude geven en nemen
De mens gedraagt zich soms naar de regel van wederkerigheid: de drang om te moeten compenseren wat andere mensen ons hebben gegeven. Door het gevoel te hebben iemand iets verschuldigd te zijn, wordt gemakkelijker aan een wederverzoek voldaan dan normaal. Deze regel is een zeer effectief en doeltreffend beïnvloedingswapen met een sterke werking. Het geeft ons namelijk de innerlijke opdracht om te compenseren wat andere mensen ons hebben gegeven.

De regel van wederkerigheid kan echter ook voor ongewenste wederzijdse verplichtingen zorgen. Dit betekent dat iemand iets voor jou gedaan kan hebben, hoewel je het niet wilde of er niet om gevraagd hebt, en je toch het gevoel van een wederzijdse verplichting hebt gekregen. We zijn in dat geval toch geneigd in te stemmen met het verzoek, terwijl we dat eigenlijk helemaal niet willen. Maar het kan nog erger: het simpele feit dat een profiteur zegt dat hij iets voor zijn slachtoffer heeft gedaan, kan het slachtoffer al verplichten om iets terug te doen (zie voorbeeld 1).

Concessie
Er bestaat nog een andere mogelijkheid om de regel van wederkerigheid te gebruiken, namelijk in de vorm van een concessie. Wanneer een partij een concessie heeft gedaan, wordt de regel van wederkerigheid van kracht. Eerst wordt er een verzoek gedaan waarvan de vrager bij voorbaat eigenlijk al weet dat dit geweigerd zal worden. Vervolgens wordt het eigenlijke verzoek gedaan. Deze wordt als een concessie ervaren en zal met een concessie van de andere partij beantwoord worden. Autoverkopers zijn meesters in het gebruik van deze techniek. Na het sluiten van de koop is de verkoper tevreden omdat hij meer heeft ontvangen dan zijn minimumprijs en u bent tevreden omdat u minder heeft betaald dan op het prijskaartje stond. De concessie is in dit geval een lagere prijs of een extra accessoire.
Uit onderzoek is gebleken dat een profiteur altijd voordeel heeft bij het principe van een concessie: het eerst doen van een extreem verzoek en daarna een kleiner verzoek doen, levert de vraagsteller namelijk het meeste op.

1. Het slachtoffer voelt zich meer verantwoordelijk voor het behaalde resultaat na het doen van een concessie en zal zich er dan ook vaker aan houden.
2. Het slachtoffer is meer tevreden wanneer hij een concessie heeft kunnen doen. Het geeft dus eigenlijk voldoening.

Verdediging
De regel van wederkerigheid kan worden vermeden door te voorkomen dat de andere partij een gunst kan verlenen. Het consequent afwijzen van gunsten kan echter beledigend of zelfs kwetsend werken en is dus af te raden. Beter is het om de gunsten van anderen te accepteren, maar dan alleen voor dat wat ze in hun kern zijn, en niet voor wat ze representeren. Als vermoed wordt dat de gulle gever een profiteur is, hoeven we alleen maar te onthouden dat de regel van wederkerigheid niet van toepassing is op mensen die van ons willen profiteren. Die hoeven we dus ook niet met een gunst te beantwoorden.

VOORBEELD 1

Wederkerigheid: eigen ervaring

Ik was binnengeslopen en belde de secretaresse van de directeur met de mededeling dat we over enkele minuten een deel van het netwerk zouden afsluiten in verband met een grote virusbesmetting. Ik gaf aan dat ik wist hoe belangrijk zij en haar chef voor de organisatie waren en dat ik daarom het netwerksegment waarop zij werkten als eerste zou controleren. Ze zou met tien minuten weer verder kunnen werken. Ze was erg blij met mijn aangeboden hulp en ze stelde graag het wachtwoord van zichzelf en haar chef ter beschikking om even de mailboxen te controleren op een besmetting.

Onmiddellijke invloed: primitieve volgzaamheid

Wanneer we een besluit nemen over iemand of iets, maken we vaak geen gebruik van alle aanwezige gegevens. In plaats daarvan gebruiken we maar een klein gedeelte van alle beschikbare informatie. Wanneer het ons aan tijd, energie, zin of de middelen ontbreekt om een situatie grondig te analyseren, nemen we besluiten op grond van soms slechts een enkel gegeven; hoe groter de tijdsdruk, hoe minder informatie we gebruiken.

Ook in het dagelijkse leven kunnen we steeds moeilijker een situatie weloverwogen onderzoeken voordat we tot een besluit komen; het ontbreekt ons aan tijd. Daarom vertrouwen we steeds meer op slechts één specifiek element van de situatie. Een profiteur kan ons in een situatie brengen waarin snel een besluit genomen moet worden. Hij weet dan dat we onze besluitvorming op slechts een enkel aspect zullen baseren. Indien hij dat aspect dan ook vervolgens nog zelf aandraagt, zijn we snel geneigd in zijn voordeel te beslissen (zie voorbeeld 2).

Verdediging

Realiseer je dat de tijdsdruk van een ander niet automatisch betekent dat je zelf ook onder tijdsdruk staat. Ken je de ander niet, hanteer dan het principe dat een gebrek aan planning van zijn kant niet hoeft te betekenen dat jezelf harder moet lopen.

Samenvatting

Mensen zijn zich doorgaans niet bewust van de manier waarop zij zich een mening vormen of soms automatisch reageren op een verzoek. Profiteurs kunnen je het gevoel geven dat je ze iets verschuldigd bent of ze proberen je onder tijdsdruk een besluit te laten nemen. Door hieraan aandacht te besteden in een bewustwordingsprogramma, gericht op Social Engineering, kan de weerbaarheid tegen dit soort manipulaties vergroot worden. In het volgende artikel zal nader worden ingegaan op de psychologische truc van consistentie: de neiging om in overeenstemming te handelen met eerder genomen besluiten en hoe een profiteur daar misbruik van kan maken.

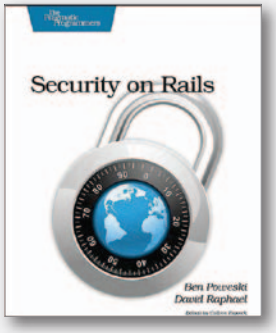
VOORBEELD 2

Onmiddellijke invloed: eigen ervaring

Ik was meegelift met de stroom mensen tijdens de ochtendspits (alle deuren stonden open) en ik was in een lege vergaderzaal gaan zitten. Met behulp van de interne telefoongids die daar lag, belde ik naar de secretaresse twee deuren verder en ik vroeg haar om die uiterst belangrijke medewerker van het hoofdkantoor, die in de vergaderzaal zat (ikzelf dus), te informeren dat de vergadering met twee uur was vertraagd. Blijkbaar stond zijn gsm uit. Ze werd dringend gevraagd deze belangrijke man te voorzien van tijdelijke werkruimte met toegang tot internet. De dame in kwestie gaf keurig de boodschap aan mij door en nodigde me uit om plaats te nemen in de kamer van haar afwezige chef. Ze logde onder haar naam in op het interne netwerk en gaf mij toegang tot het internet (en natuurlijk tot haar mail, die van haar chef, intranet en alle beschikbare informatie op de netwerkstations).
Het slachtoffer was door tijdsdruk niet in staat om de rechtmatigheid van het verzoek te verifiëren. Mede door de sociale afstand (belangrijke medewerker van het hoofdkantoor versus 'eenvoudige' secretaresse op een filiaal) durfde ze mijn identiteit niet rechtstreeks te verifiëren.

InZicht

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



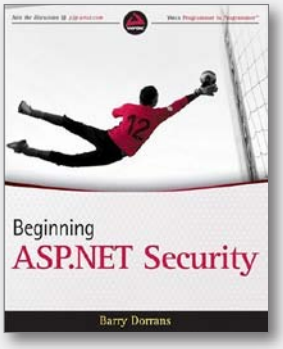
Security on Rails
Auteurs: Ben Poweski, David Raphael
ISBN: 978-1-934356-48-7
Uitgever: Pragmatic Bookshelf
Druk: 1e druk, december 2009
Vorm: Hardback, 304 blz, Engels

Security on Rails provides you with the tools and techniques to defend your Rails applications against attackers. Do you have a well-developed plan to test your application from a security perspective? Do you need more sophisticated access control? With Security on Rails, you can conquer the bad guys who are trying to exploit your application. You'll see the very techniques that hackers use, and then journey through this full-fledged guide for writing secure Rails applications.

The advantage of using Rails is its agility; it makes developing your web applications easy and fast. The disadvantage is that it can leave holes in your security if you are not aware of common vulnerabilities. It's a nerve-wracking and unfortunate fact that there are plenty of malicious people lurking on the Web. As a Rails developer, it is essential that you understand how to assess risk and protect your data and your users.

Security on Rails uses established security principles to teach you how to write more secure software, defend your applications from common threats, and encrypt your data. We'll give you an example of a hacking exploit, and explore how to fix the weaknesses in an application.
You'll learn the steps you need to take to control access to information and authenticate users, including cryptography concepts and authorization. In addition, you'll see how to integrate your applications with external management systems; in short, the crucial details you must consider to protect yourself and your data.

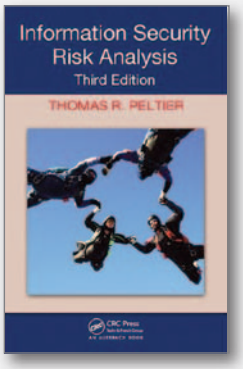
The most important element of security is to plan for it before it becomes an issue. Security on Rails helps beginner and intermediate developers to take control of their applications and guard against attacks.



Beginning ASP.NET Security
Auteurs: Barry Dorrans
ISBN: 978-0-470-74365-2
Uitgever: Wiley
Druk: 1e druk, januari 2010
Vorm: Paperback, 436 blz, Engels

A practical guide to securing ASP.NET sites. Beginning ASP.NET Security is for novice to intermediate ASP.NET programmers and provides a step-by-step solution to securing each area of ASP.NET development. Rather than approaching security from a theoretical direction, MVP Barry Dorrans shows you examples of how everyday code can be attacked, and describes the steps necessary for defense. Inside, you'll learn how you can defend your ASP.NET applications using the .NET framework, industry patterns and best practices, code libraries and resources provided by Microsoft and others.

Beginning ASP.NET Security:
- Explores issues with user input including validation, cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Teaches how to securely access your database and defend against SQL injection attacks.
- Shares techniques for keeping secrets, including encryption, hashing and preventing information leaks.
- Examines methods for authenticating and authorizing users, including ASP.NET membership providers and preventing cookie theft.
- Shares tips for securing your web server, including how ASP.NET uses trust levels and locking down IIS.
- Unveils ways to securely use WCF web services.
- Presents security with the Microsoft ASP.NET Ajax framework and Silverlight.
- Includes an overview of security with the Microsoft MVC framework.



Information Security Risk Analysis, Third Edition
Auteur: Thomas R. Peltier
ISBN: 9781439839560
Uitgever: CRC Press
Druk: 1e druk, 12 maart 2010
Vorm: Hardback, 456 blz, Engels

Authored by renowned security expert and certification instructor, Thomas Peltier, this authoritative reference provides readers with the knowledge and the skill-set needed to achieve a highly effective risk analysis assessment in a matter of days. Peltier demonstrates how to identify threats and then determine if those threats pose a real risk. Supplemented with online access to user-friendly checklists, forms, questionnaires, sample assessments, and other documents, this work is truly a one-stop, how-to resource for industry and academia professionals.

Hans Alfons over generiek beveiligen en CRAMM

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

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

Ik sprak met Hans over zijn visie op en zijn ervaring met informatiebeveiliging. Wat mij opviel was de rust en eenvoud die Hans uitstraalt als hij over zijn passie spreekt. Ik heb in mijn optekening getracht die stijl vast te houden. Hans had zoveel te vertellen, dat we besloten het verslag van dit gesprek over twee nummers van Informatiebeveiliging te verdelen. In deze uitgave het eerste deel, waarin Hans spreekt over generiek beveiligen en CRAMM.

Hans: "Mijn carrière is kort gezegd binnen het legerkorps begonnen, heel specifiek op informatiebeveiliging van systemen. Uiteindelijk ben ik steeds generieker gaan beveiligen door risicomanagement toe te passen. Ik heb methodieken ontwikkeld en gebruikt, met name CRAMM - waar de hele wereld een mening over heeft, zonder er ooit mee gewerkt te hebben. Ik heb missies beveiligd, zoals in Afghanistan. Uiteindelijk denk ik dat mijn ervaring bij Defensie helemaal niet zo bijzonder is vergeleken met het bedrijfsleven. Ik wil ook antwoord geven op de vraag waarom ik bij Univé ben gaan werken, en niet achter de geraniums van mijn pensioen ben gaan genieten."

Specifiek of generiek?

"Ik ben door de jaren heen steeds generieker naar beveiliging gaan kijken. Hoe gaat dat proces in zijn werk? Je moet anders gaan denken, daar begint het mee. Het is heel gemakkelijk om in 2010 te zeggen dat je anders moet denken, maar ik ben wel in 1998 begonnen dit te ontwikkelen. Dus als ik terugkijk, heb ik een opgaande lijn aan kennis doorlopen. Ik heb al een heleboel dingen meegemaakt. Iemand die nu van school af komt, mist nog de ervaring en kan niet terugkijken. In hoeverre is er dan sprake van anders denken? Ik hoop door mijn verhaal te vertellen daar wat bewustzijn te creëren."

Wat merk je van dit andere denken?

"Je krijgt vandaag de dag als consultant een opdracht en je komt nooit tot de kern van de zaak, het beveiligen van het laagste niveau, de details. Dat is het probleem waarmee je kampt bij bedrijven. Het is geen verwijt richting consultant of bedrijf, het is gewoon ervaring. Je krijgt een opdracht: 'Mijn bedrijf moet beveiligd worden'. Je hebt dan een bedrijf met zeg vijftig informatiesystemen en dan ga je netjes op elk systeem een risicoanalyse doen. En dan zegt dat bedrijf 'hartstikke mooi'. Ga je naar een groot bedrijf, zoals in mijn geval Defensie met twaalfhonderd systemen, moet je eens kijken wat dat gaat kosten. Ik heb bij de beveiligingsautoriteit eens uitgerekend dat als we de risicoanalyse deden bij iedere implementatie, ik het hele Nederlandse volk vierentwintig uur per dag anderhalf jaar kon laten werken. Eigenlijk zag ik toen hoe absurd de aanpak was, aan het begin van mijn carrière. Ik mocht daar niet van afwijken, simpelweg om de reden dat het moest. Wat zie je dan? Het blijkt dat een heleboel systemen, bijvoorbeeld financiële systemen, ongeveer hetzelfde zijn, maar net even iets anders. We konden dus niet clusteren. Als je een analyse doet op beschikbaarheid, integriteit en vertrouwelijkheid, scoren ze net allemaal even anders. En zeker met die risicoanalyses van vroeger kon het zijn dat je op één bepaald risico beschikbaarheid een laag niveau als drie scoorde, en dat andere risico's op een vier of vijf uitkwamen. Zo krijg je op alle aspecten gelaagdheid en kon je uiteindelijk wel dertig verschillende configuraties in je beschikbaarheid hebben."

"Daarvan hebben een paar mensen gezegd: 'We willen naar alleen laag, midden of hoog als niveau, dat is al een stuk eenvoudiger'. Je krijg dan totaal negen mogelijke BIV-classificaties (drie waarden voor ieder van de drie aspecten), en als je die gaat uitwerken in verschillende combinaties, dan kom je tot 27 (3x3x3) mogelijkheden. En bij Defensie heb je ook nog een tweedeling tussen de operationele situatie, het werken

Cat	Beschikbaarheid	Integriteit	Vertrouwelijkheid
1	laag	laag	laag
2	laag	laag	midden
3	laag	laag	hoog
4	laag	midden	laag
5	laag	midden	midden
6	laag	midden	hoog
7	laag	hoog	laag
8	laag	hoog	midden
9	laag	hoog	hoog
10	midden	laag	laag
11	midden	laag	midden
12	midden	laag	hoog
13	midden	midden	laag
14	midden	midden	midden
15	midden	midden	hoog
16	midden	hoog	laag
17	midden	hoog	midden
18	midden	hoog	hoog
19	hoog	laag	laag
20	hoog	laag	midden
21	hoog	laag	hoog
22	hoog	midden	laag
23	hoog	midden	midden
24	hoog	midden	hoog
25	hoog	hoog	laag
26	hoog	hoog	midden
27	hoog	hoog	hoog

Cat	B	I	V
1	laag	hoog	laag
2	laag	hoog	midden
3	laag	hoog	hoog
4	hoog	hoog	laag
5	hoog	hoog	midden
6	hoog	hoog	hoog

Figuur 1: Reductie van aantal beveiligingsniveaus

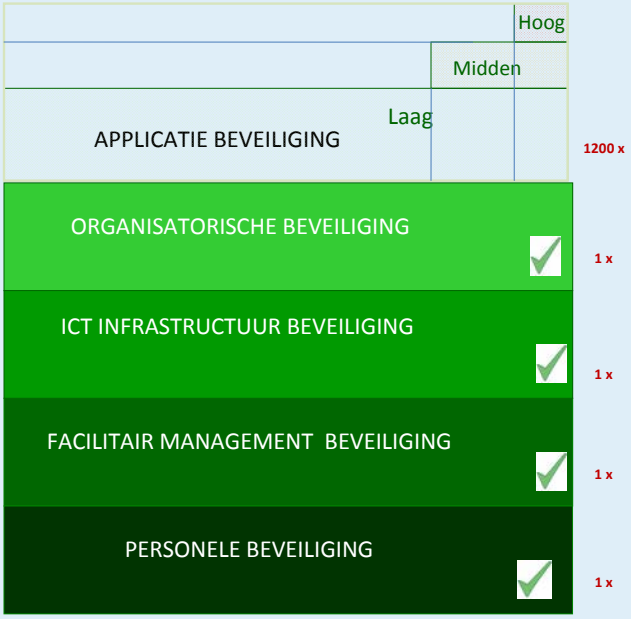
in het veld, en de situatie op de kazernes. We hadden vierenvijftig niveaus en dat is niet te doen. Dus ga je denken: hoe kan ik dat verder vereenvoudigen? Bijvoorbeeld door ervan uit te gaan dat in het veld de beschikbaarheid altijd hoog is en dat op een locatie de beschikbaarheid altijd laag of midden is. De generieke basisstandaard voor het netwerk, in het licht van de ISO-normering bekeken, zit tussen laag en midden in. Het hoogste niveau - midden - is dan het basisniveau en daar moet je niet één of twee aspecten uit halen; daar moet je kritisch naar kijken en je afvragen of je het hele netwerk op dat niveau moet brengen of dat je dat in je systemen doet. Tegen al dat soort dingen ben ik bij Defensie aangelopen."

"Op een bepaald moment zei ik: 'Waarom doen we al die risicoanalyses? Kunnen we er niet slechts één doen?' Dan zwem je tegen de stroom in, daarom dat ik net al zei dat je moet anders moet kunnen denken. Want dan zeg je: 'Wat beveilig ik nou eigenlijk?' Ik beveilig alleen maar data, ik ga dus niet naar processen of informatiesystemen kijken, ik pik de data er tussenuit. We zijn op het hoogste niveau primaire proces gaan zitten, want daar wordt eigenlijk bepaald hoe zwaar data beveiligd wordt. Dan kom je tot de conclusie dat je bijvoorbeeld op exclusiviteit wel drie niveaus overhoudt, qua integriteit kwamen we bij Defensie op één niveau uit: hoog."

"Bij Univé roepen ze: 'Ja maar, in de verzekeringsbranche is het wel handig dat je daar twee niveaus in hanteert'. Nou, daar heb ik begrip voor, omdat daar financiële consequenties aan kunnen vastzitten. Bij beschikbaarheid, als je er even logisch over nadenkt, ga je geen 27 niveaus netwerk aanbieden. Binnen een IT-organisatie kan dat gewoon niet. Je hebt gewoon een standaardnetwerk met een bepaalde beschikbaarheid, bijvoorbeeld je mag één dag uitval hebben. Dat bied je aan en dan kan ik me voorstellen dat je, als je een hogere beschikbaarheid nodig hebt, dat type netwerk apart gaat aanbieden. Het verschil zit vooral in de continuïteit, in de uitwijk in dat geval. Daar laat je gewoon andere maatregelen op los."

"Eén van de andere dingen die wij toen ook bedacht hebben, in de implementatiesfeer, is dat we bouwstenen hebben gemaakt. Informatiebeveiliging is heel erg breed. Je kunt dat in vier standaardbouwstenen onderscheiden als je dat wil: één is persoonele veiligheid, de andere zijn fysieke beveiliging, netwerkbeveiliging en organisatorische beveiliging. Dan houd je één setje met maatregelen over en dat is specifiek gericht op de applicatie. De hele handel bij elkaar vormt een informatiesysteem."

"Stel dat in een gebouw honderd informatiesystemen draaien. Van die honderd systemen bepaal je wat de grootste gemene deler is, wat de basisbeveiliging van het gebouw moet zijn, en dat regel je. Dat doe je geen honderd keer, dat doe je één keer en dat leg je vast in die bouwsteen. Hetzelfde met IT; daar moet je bepalen wat het



Figuur 2: Bouwstenen van beveiliging

basisniveau van het netwerk en de infrastructuur is. Uiteindelijk moet je dáárvoor betalen. Als je dat zo doet, is het voor iedereen te behappen. Je kunt een onafhankelijke deskundige laten controleren of het aan het niveau voldoet. Je hoeft niet al die systeemeigenaren, die in het gebouw rondlopen, te laten vragen of je het voor hun eisen wel op orde hebt. Dat wil je niet. Je zegt tegen de IAD: 'Jij legt elk jaar vast dat wij aan onze eisen voldoen'. Die eisen worden dus opgesteld vanuit het beveiligingsplan, daar moet de business het mee eens zijn. De laatste set aan maatregelen zijn niet standaard. Deze zijn specifiek voor de applicatie, vooral gericht op exclusiviteit (of vertrouwelijkheid, afhankelijk van waar je werkt). Daar zeg je: 'Het moet een geheim systeem zijn, een confidentieel systeem of een ongerubriceerd systeem'. Of je dan laag, midden of hoog gebruikt, ligt aan het bedrijf waar je werkt. Het voordeel hiervan is dat op het moment dat iemand een applicatie bouwt, je al weet waar de data aan moeten voldoen. Je weet wat de eisen zijn, de fysieke beveiliging is al gedaan, de organisatorische beveiliging is al gedaan, dus je kunt het systeem zo de organisatie binnenschuiven. Als je meerdere niveaus van integriteit onderscheidt, dan moet je ook daar rekening mee houden. Bij een verzekeringsbedrijf is het handig om meerdere niveaus van integriteit te onderscheiden. Het eerste integriteitsniveau geldt voor het gros van de informatie en we kijken speciaal nog naar de integriteit van financiële systemen, waar je een heleboel schade kan oplopen bij problemen. Het is maar de keuze die je maakt."

"Een niet te onderschatten aspect van organisatorische beveiliging is monitoring. Operationeel zie je bij Defensie dat je mensen hebt die werken en mensen die monitoren. Ik zat bij de verbindingsdienst, dan moet je een verbindingsstelsel over een deel van Nederland uitleggen. Daar wordt continu gemonitord of de verbinding er nog is. Vroeger moest je dan doorbellen om de zoveel tijd, later werd dat gewoon elektronisch gedaan en nu zijn het computers die dat doen. Dat zit er gewoon ingebakken. Als je niet weet hoe de zaken werken, heb je geen zekerheid. Neem bijvoorbeeld je auto. Daar zitten ook allerlei controlelampjes in en dat vinden we allemaal normaal."

"ICT-ers hebben meer de neiging om alleen maar preventief te denken. Ze hebben ervoor gezorgd dat het niet kan plaatsvinden, alleen weet je het nooit zeker... Een mooi voorbeeld daarin vind ik de firewall. Je hebt een firewall ingericht, dus we weten wat we tegenhouden. Maar wat we niet weten, is wat we doorlaten. Dat is het nadeel van een firewall. Dus met een firewall alleen ben je niet klaar. Het is helemaal niet interessant om te weten hoeveel aanvallen je hebt tegengehouden, er hoeft er maar eentje door te glippen en je bedrijf plat te leggen. Voor een bank kan dat betekenen dat je failliet gaat als het rekencentrum meer dan vierentwintig uur onderuit gaat. Zo denken, vergt een andere mindset. Van de fysieke beveiliging kun je leren hoe je gaat monitoren: je mag veel investeren, als je het goed wilt doen. De monitoring technieken leveren financiële winst op doordat je minder mensen nodig hebt. Dat zijn allemaal ervaringen die je opdoet, waar je over nadenkt en waardoor je er uiteindelijk achterkomt dat het anders moet. Dan krijg je een bepaalde kentering bij het expertisecentrum informatiebeveiliging van de landmacht. Ik heb ongeveer honderdvijftig medewerkers, EDP-auditors en IT-personeel, gehad. Die hebben dus allemaal meegewerkt aan de ideevorming die hier uit tot stand is gekomen, die je daarna continu aan het verbeteren bent."

"We kregen de mensen buiten ons centrum niet mee en toen heb ik op een bepaald moment de beslissing genomen: ik ga het gewoon doen. Met alle risico's van dien, want ik moest een operationeel domein gaan beveiligen. Dus ik heb een eenheid gepakt en ik heb ze laten toepassen wat wij uitgedacht hadden. We hebben één beveiligingsplan geschreven voor die eenheid en we hebben alle informatiesystemen meegenomen. We hebben een risicoanalyse gedaan voor een bevelsgebied en daaruit hebben we afgeleid hoeveel niveaus we nodig hebben. We kwamen uit op zes niveaus. Die hebben we toegepast en we zijn naar de informatiesystemen gaan kijken door middel van een vragenlijst. Met die vragenlijst hebben we gecontroleerd op welk niveau het systeem past. Vervolgens was je binnen een halve dag klaar met het in kaart brengen van een informatiesysteem. Dat is de tijdswinst. Daarna hebben we het wel helemaal bij de operatie domeinen toegepast. Als je dan kijkt wat het verschil in kosten was, is een besparing van dertig op één gehaald door het verschil in aanpak. Dus deze aanpak levert tijdwinst en een forse besparing op."

Hoe kom ik nou van een specifiek naar een generiek beveiligingsplan?
"Je moet het juiste onderscheid maken. De code voor Informatiebeveiliging is in hoofdstukken opgedeeld en je ziet allemaal maatregelen staan op een hoog niveau, maar niet in detail. Die consultancybedrijven, waar ik het in het begin over had, leveren ook op dat abstracte niveau. Maatregelen worden bij de organisatie neergelegd en die moeten er wat mee gaan doen. Maar zij hebben de kennis niet in huis om die op hoog niveau beschreven maatregelen te vertalen naar effectieve maatregelen in detail. Wat je dan eigenlijk zou willen hebben, is een tool die dat wel aangeeft. De consultants zetten jou aan de slag om de maatregelen te bedenken om het werkend te maken. Dát is het probleem bij alle bedrijven. Dát is het probleem dat ik bij Defensie had en dát is ook het probleem dat ik bij Univé zie. En als je dan links en rechts met je collega's praat, dan hoor je dat ook: 'We gaan nu aan de bak, want we krijgen een set met maatregelen'. Maar het zijn geen maatregelen, het zijn doelstellingen die je moet bereiken."

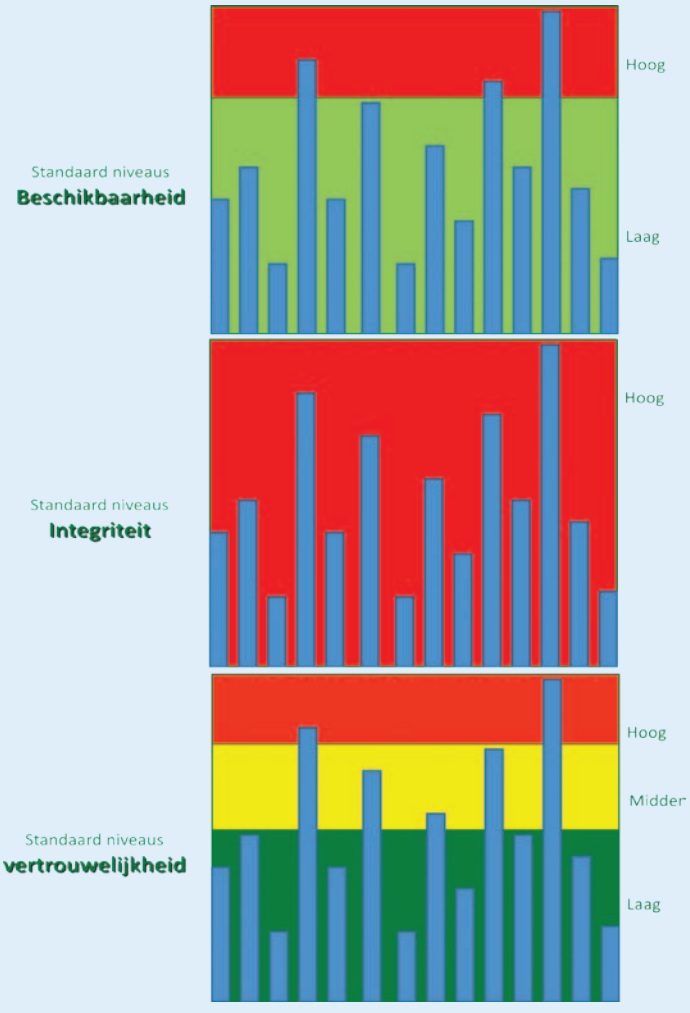
"Dan naar dat geautomatiseerde middel, ik neem weer het gebouw als voorbeeld. We hebben een gebouw, daar zitten honderd informatiesystemen in. Nu moet je als beveiligers al die systemen gaan onderzoeken om te bepalen welke maatregelen je moet nemen. En uiteindelijk zullen alle systemen in een serverruimte staan, je hebt maar één serverruimte, je hebt maar één set aan maatregelen nodig, je hebt maar één manier van toegangscontrole nodig. Als je nu CRAMM neemt, zie ik een aantal voordelen om in ieder geval op gestructureerde wijze en controleerbare wijze te komen tot bruto maatregelen, het vastleggen van geaccepteerd risico en je netto maatregelen.

- Locaties koppelen
  Je kunt met CRAMM op locatie de maatregelen er uithalen, als je weet welke systemen er op locatie zitten, want dat kun je koppelen in CRAMM.
- Impact, kosten en quick-wins
  CRAMM geeft ook aan wat de impact van die maatregelen is, afgezet tegen de kosten ervan: hoog, midden en laag. Dus de maatregelen die een hoge impact hebben en die lage kosten met zich meebrengen, zijn de eerste maatregelen die je wilt uitvoeren. Dit is precies wat de business wil zien: quick-wins. Ze willen zien waar ze hun geld aan uitgeven. Het nadeel van beveiligen is dat je eerst een hoop papierwerk hebt en dan pas tot resultaat komt. Met die quick-wins behaal je die acceptatie.
- Backtrack
  Een laatste voordeel vind ik dat als je een maatregel niet neemt, omdat het niet kan, je door middel van een backtrack kunt terugkomen bij de risico's, bij de bedreigingen. Van daaruit kun je dan een vergelijking maken en beslissen dat als je deze maatregel niet neemt, welke alternatieve maatregelen je dan kunt nemen, vanuit de hele set van maatregelen die er achter ligt.

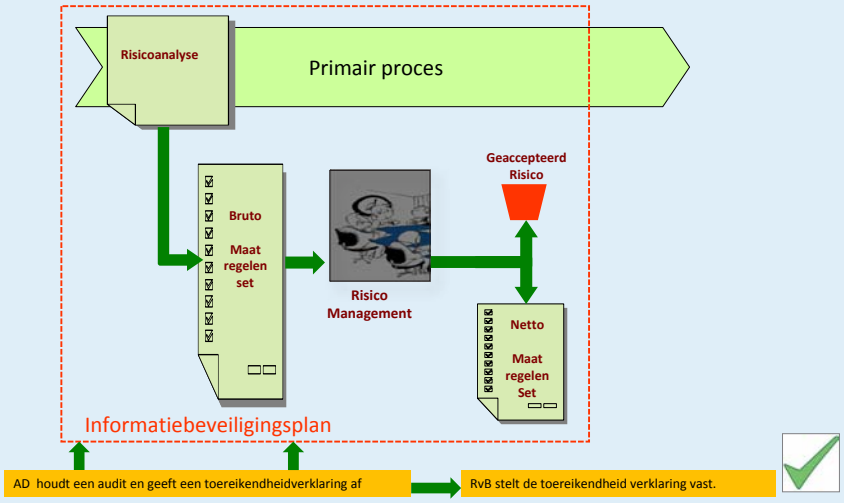
"Veel mensen met een mening over CRAMM hebben er nooit mee gewerkt. Ze hebben het CRAMM van vroeger in gedachten. Zo werkten we vroeger ook: er rollen een heleboel mappen papier uit en dan moet je maar zien dat het voor elkaar komt. Maar juist het werken met bouwstenen houdt in dat, als je organisatorische maatregelen krijgt, je maar zes velletjes papier krijgt, zoals:

- Ik moet een test doen;
- Ik moet mijn spullen in de juiste kasten opruimen;
- …

Maar ik krijg geen maatregelen van IT te zien, ik krijg geen fysieke maatregelen te



Figuur 3: Vaststellen van beveiligingsniveaus



Figuur 4: Het komen tot één beveiligingsplan

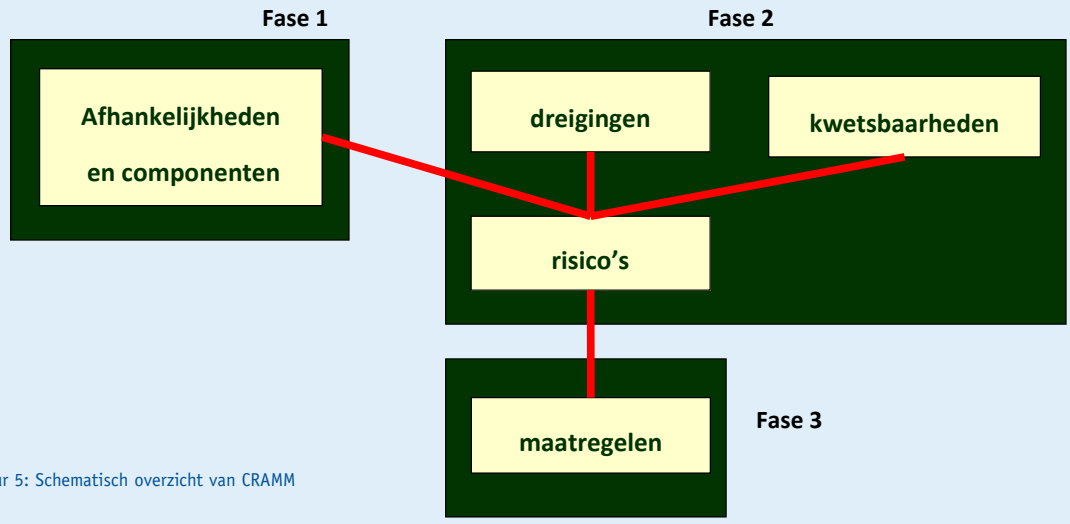
zien. Die kreeg je vroeger allemaal wel voorgeschoteld. Dus die uitsplitsing maakt het voor iemand die het moet doen overzichtelijker. Wat je in dit soort systemen ook wel ziet, is dat je een set aan maatregelen krijgt en die je zelf aan componenten mag hangen. Dan kom je op vragen als 'welke maatregel moet ik nu op een router nemen?' Daar denken mensen helemaal niet over na: dat je op een bepaald beveiligingsniveau een wachtwoord moet invullen op een router. De compleetheid van maatregelen in CRAMM is ook het gemak dat je weet dat je dingen niet over het hoofd ziet."

"Bij een beoordeling van CRAMM halen mensen altijd de extremen er uit. Bijvoorbeeld: gebouwen moeten wit geschilderd worden. Dat is een maatregel. En wat bedoelen ze ermee? Voordat ik de ICT in ging, heb ik ook vijf jaar fysieke beveiliging gedaan. Wij bewaakten MOP-complexen, dat zijn complexen waar alleen materiaal ligt, en dat werd beveiligd door onder andere bewakers met honden. Wanneer val je beter op? Als je een lichte achtergrond hebt, of een donkere? Als je hier niet bij stilstaat, kan het zijn dat je de oorsprong van de maatregel niet begrijpt. Als je de oorsprong begrijpt, kun je beslissen of je de maatregel wel of niet toepast. Begrijp je hem niet, kun je ook niet beslissen. Er is ook een maatregel dat er bij de deur van een donker object moet een lamp hangen. Die lamp hangt er zodat het bewakingspersoneel kan zien of er iemand bij de deur is. Dat wordt niet uitgelegd. Maar als jij een zaag koopt, wordt je ook niet verteld hoe je moet zagen. Er wordt van je verwacht dat je weet hoe je met de maatregelen omgaat. Men probeert met aandacht voor dit soort extreme maatregelen aan te geven dat CRAMM niet werkt. Dan zeg ik: 'Leg mij dan maar uit wat jij denkt dat er bedoeld wordt met die maatregel'. Mensen hebben onvoldoende kennis van het pakket aan maatregelen en oordelen op hun eigen gebrek. CRAMM levert geen uitleg bij de maatregelen, maar eigenlijk zou het wel goed zijn als CRAMM aangaf waarom ze tot die maatregel gekomen zijn."

"Eén van de belangrijkste dingen van CRAMM is dat je het moet zien als het mes van de slager: het is slechts een hulpmiddel. Je moet er je gezond verstand bij blijven gebruiken. Vaak denken mensen dat een tool heilig is en dat je de gegeven maatregelen moet nemen. Dat is onzin. CRAMM geeft een aantal oplossingen voor een probleem. Je bekijkt zelf welke oplossing bij jou past. Het enige dat je moet doen, maar dat geldt voor elke methodiek die je gebruikt, is dat je iets beveiligt of dat je accepteert dat je risico loopt. Dat doe je ergens in het risicomanagement proces."

Tot zover het eerste deel van de weergave van dit gesprek. Volgende uitgave gaat Hans verder in op zijn ervaringen met CRAMM, de beveiliging in Afghanistan en zijn werkzaamheden bij Univé.

CRAMM Schematisch:



Figuur 5: Schematisch overzicht van CRAMM

Social Networks: getting your act together

Auteur: Rob Greuter > Rob is security consultant bij Secode en redacteur van dit blad. Hij is per email bereikbaar via r.greuter@upcmail.nl

LinkedIn, Plaxo, Xing, Hyves, Facebook, Ning, Twitter... Het gebruik van zakelijke en sociale netwerken door particulieren, organisaties en bedrijven is niet meer weg te denken. De voordelen zijn enorm, mits er verstandig mee wordt omgegaan. 'Always in touch with your friends'.

Echter; er zijn ook uitdagingen die stof tot nadenken en organiseren geven. Wat nu als een enthousiaste medewerker op eigen initiatief een Hyve of LinkedIn groep voor zijn bedrijf of afdeling opzet, compleet met het gebruik van logo en company pitch? Vaak worden dergelijke acties spontaan uitgevoerd, bestuursleden en managers komen er (als ze geluk hebben) per toeval achter. Voor je het weet vormen zich via berichten, krabbels en dergelijke allerlei discussies en reacties die niet in lijn zijn met corporate identity, visie gewenste PR, et cetera.

Dergelijke netwerkgroepen kunnen in korte tijd heel groot worden, des te groter is dus een eventueel negatieve impact. En het probleem kan nog groter worden. Per definitie is de oprichter tevens hoofdbeheerder. Deze heeft alle rechten, hij kan medebeheerders aanwijzen (en verwijderen), hij kan groepsberichten rondsturen en ga zo maar door. Stel nu eens dat zo'n medewerker of verenigingslid zich om wat voor reden dan ook tegen zijn werkgever of vereniging keert? Denk hier vooral niet te licht over. Met een social network zoals Hyves valt op geen enkele wijze te communiceren en de regeltjes bieden geen enkele bescherming.

Kan het nog erger? Jazeker, helaas wel. De oprichter kan iemand van de concurrentie zijn, die zich initieel voordoet als medewerker of verenigingslid. Het bewust aan te richten kwaad zal zo nog veel sneller rondzingen.

Okay, een aantal lezers zal nu wakker geschrokken zijn. Welke maatregelen kunnen helpen enigszins in controle te komen? Een eerste handreiking, deels gestoeld op eigen ervaring...

1) **Registreer naam en beeldmerk. Vooral verenigingen vergeten dat. Zou het PvIB dit al geregeld hebben...?**

2) **Verbied bij voorbaat het gebruik van company artwork door medewerkers en leden buiten de taakomschrijvingen.**

3) **Schrijf een Social Network gebruiksvoorschrift of een gedragscode en leg daarin tenminste vast dat altijd een door het bestuur of een door hun aangewezen persoon de hoofdbeheerder is.**

4) **Betrek de marketingafdeling bij dergelijke initiatieven ter bewaking van het corporate image.**

5) **Huur een bedrijf in dat het internet monitort op gebruik en misbruik.**

Spionage 2.0: de digitale dreiging

Digitale spionage meenemen in de risicoanalyse

Auteur: ir. Paul Bakker > Paul Bakker is manager van de Business Unit Crypto bij Fox-IT en dagelijks bezig met het fenomeen spionage en vertrouwen. Hij is te bereiken via bakker@fox-it.com.

Spionage lijkt een achterhaald fenomeen. Leuke inspiratie voor een spannend boek, maar niet meer van deze tijd. En al helemaal niet in Nederland. Wat heeft een spion bij ons nog te zoeken? De waarheid is anders. Al jaren waarschuwt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) voor inlichtingenactiviteiten van onder andere China en Rusland. Nederland is wel degelijk doelwit. En niet alleen de overheid, ook ons bedrijfsleven geldt als target.

Spionage... Zoals in een boek of film gaat het er niet meer aan toe. Voor de meeste informatie hoeven spionnen de deur niet meer uit, spioneren kan tegenwoordig ook digitaal. Via de digitale snelweg is elke organisatie te bereiken. Als er dan een achterdeur in de beveiliging van de internetkoppeling zit, kan een handige informant veel, zo niet alle begeerde informatie onopgemerkt verkrijgen. Kunnen we ons daar tegen wapenen? Ja zeker wel. Het is alleen wel zaak de juiste risicoafwegingen te maken en goed na te denken over de in te zetten security oplossingen.

Goede mix

De kracht ligt in het vinden van een goede mix van regelgeving, gebruiksvriendelijkheid en het gebruik van vertrouwde beveiligingsoplossingen. Regelgeving voor een situatie staat vanaf het begin vast, gebruiksvriendelijkheid is meetbaar en merkbaar en op basis van commerciële informatie zijn er beveiligingsproducten te vinden die aan de behoefte van zowel functionaliteit, als gebruiksvriendelijkheid voldoen. Maar er staat niet voor niets 'vertrouwde' beveiligingsoplossingen.

Afhankelijk van het dreigingsprofiel van een organisatie spelen meer aspecten dan alleen functionaliteit en gebruiksvriendelijkheid een rol. Vertrouwen in de oplossing én de producent, zijn minstens zo belangrijk. In het geval van de bescherming van bedrijfs- of staatsgeheimen mogen we bovendien ook het vertrouwen in 'de oorsprong' van de oplossing niet uit het oog verliezen. Internationaal wordt er nu eenmaal volop gespioneerd. In het verleden zijn er door landen regelmatig achterdeurtjes in beveiligingsproducten ingebouwd om zo later mee te kunnen kijken. Om deze reden doet een Nederlandse organisatie, met bijvoorbeeld veel concurrentie uit China, er verstandig aan haar IT-security niet op Chinese veiligheidsoplossingen te baseren. Maar dit geldt ook voor andere landen!

Vertrouwen versus controle

Maar daar zijn toch beveiligingsstempels zoals de Common Criteria of FIPS 140-2 voor bedoeld? Tja... De evaluatie van een product geeft aan dat het in de basis goed is bevonden. Het is echter niet mogelijk om producten echt te controleren. In versies die niet langs de controlerende instantie gaan, kunnen toch achterdeurtjes ingebouwd zijn. De binnenkant van een chip is al helemaal heel moeilijk te doorgronden. Op basis van een specifiek netwerkpakket van buitenaf kan de chip zomaar een achterdeur laten opengaan. Dat is ook de reden dat veel landen hun eigen nationale 'crypto' industrie hebben voor het maken van echt veilige producten.

Is dan niets meer te vertrouwen en moeten we alles zelf maken? Natuurlijk niet. Dat is het mooie van vertrouwen. Dat kun je krijgen. Het heeft bovendien ook alles te maken met uw situatie, de risico's, de dreigingen en de organisatie zelf. Anders gesteld: het draait om het gebruik van vertrouwde oplossingen die aansluiten bij uw specifieke situatie. De Nederlandse overheid gebruikt bijvoorbeeld veelvuldig producten uit landen waarmee openheid en een vertrouwensband is, zoals Duitsland en Zweden.

Fox-IT is dagelijks actief op het terrein van beveiliging van organisatie- en staatsgeheimen en maakt in dat kader ook bij voorkeur zelf haar eigen apparatuur voor de beveiliging van staatsgeheimen.

Links

- Jaarverslag AIVD over heimelijke activiteiten van buitenlandse mogendheden: *http://www.jaarverslag.aivd.nl/jaarverslag/Jaargang.2008/Aandachtsgebieden.Spionage/Regio.China/aDU1092_default.aspx)*
- Historisch voorbeeld: Crypto AG: The NSA's Trojan Whore: *http://mediafilter.org/caq/cryptogate/* (Historisch voorbeeld van achterdeurtjes in beveiligingsapparatuur door de Amerikanen)
- Toenemende dreiging Chinese activiteiten: *http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece*

Verkniezingsdag

Kortgeleden mochten we ons recht weer gebruiken door een nieuwe gemeenteraad te kiezen. Ik zal in mijn beschouwingen geen mening geven over het nut of het onnut hiervan en ook zal ik geen oordeel geven over de inmiddels bekende uitslag, hoewel ik daar wel een hele uitgesproken mening over heb. Nee, vandaag wil ik mijn column laten gaan over het proces. Dat begon ergens in februari, toen ik van de gemeente een stempas kreeg toegezonden, die ik kan gebruiken in combinatie met een geldig identiteitsbewijs. Dat laatste is nieuw en het wordt niet door iedereen met gejuich ontvangen, want u wilt niet weten hoeveel Nederlanders geen geldig identiteitsbewijs hebben. Denk hierbij aan bejaarden die hun paspoort niet meer verlengen en het rijbewijs ook al hebben ingeleverd.

Met enige weerzin begeef ik me naar het stemlokaal en daar word ik begroet door maar liefst drie gewichtig kijkende mensen, die ik regelmatig tegenkom als ik met mijn hond een rondje maak. Ze hebben grote lijsten voor zich waar de nodige streepjes op gezet worden. Mijn stempas wordt bestudeerd, het inmiddels uitgevouwen rijbewijs wordt vergeleken met mijn gezicht en ik groet Gretha, die mij mijn rijbewijs weer teruggeeft met daarbij een groot vel papier waarop alle namen van de te verkiezen politici staan. Bij mijn vrouw wordt hetzelfde ritueel herhaald en ook zij groet Gretha, die onverstoorbaar het rijbewijs van mijn vrouw vergelijkt met het gezicht dat voor haar staat. Ook mijn vrouw krijgt een groot stembiljet, waarop we zorgvuldig het rondje rood maken van onze grote favoriet.
De ingevulde biljetten worden in de grote stembus gegooid en we spoeden ons naar buiten.

Mijn verwachting komt uit; we hebben het stemlokaal nog niet verlaten of mijn vrouw vraagt me of deze poppenkast anno 2010 niet een beetje achterhaald is. Ik leg mijn vrouw uit dat stemcomputers te kraken zijn en dat de software in de computer vervangen kan worden door software waarmee is geknoeid. Ze kijkt me ongelovig aan en ik vertel haar dat in er Rotterdam een opslagplaats is waar vierhonderd van die machines bij elkaar staan. Er is geen bewaking, er zijn geen camera's en om het helemaal gemakkelijk te maken, hebben alle stemcomputers dezelfde sleutel. Die zo eenvoudig na te maken is, dat je het niet eens als slot op je fiets wilt hebben. In totaal zijn er achtduizend stemcomputers in Nederland en u raadt het al: die hebben inderdaad allemaal dezelfde sleutel. In Amerika is bewezen dat een stemcomputer binnen zeven minuten van een nieuwe codering is te voorzien.

We kijken die avond nog even naar de uitslagen die binnendruppelen en we verbazen ons over het amateuristische niveau van deze verkiezingen. De dagen daarop blijken er fouten gemaakt te zijn bij de tellingen in Maastricht, de Rotterdamse uitslag is op dat moment nog omstreden en ook een Amsterdams district wordt besproken, omdat het protocol daar niet goed opgevolgd zou zijn. En mijn moeder heeft haar stem niet kunnen uitbrengen omdat zij haar originele paspoort aan mijn zuster heeft mee gegeven en dat kan natuurlijk niet de bedoeling zijn, volgens de ernstig kijkende mensen in haar kiesdistrict. Nee, het origineel is geen geldige legitimatie voor een machtiging, dat mag alleen met een kopie. Mijn zuster kijkt om zich heen of er niet ergens een kopieermachine staat, maar helaas, dat mag niet baten. Onverbiddelijk wordt zij weggestuurd wegens het doorbreken van het protocul.

In juni gaan we het allemaal nog eens dunnetjes overdoen en het aantal stemmers zal dan waarschijnlijk een stuk hoger zijn dan bij de gemeenteraadsverkiezingen. Ook het aantal hertellingen zal ongetwijfeld hoger zijn, want in het kader van 'niet geschoten, is altijd mis', zullen er twijfels over de uitslag geuit worden, wanneer deze niet naar tevredenheid is. Of zullen we dan weer met de stemcomputer gaan werken? Nee, die garantie durf ik wel te geven, want voordat die stemcomputer goed is getest, zijn we maanden verder. En alles wat te kraken is, zal ooit gekraakt worden en voor zover ik kan nagaan is alles kraakbaar.

Misschien dat we dan bij stemlokalen komen waar vier mensen achter de tafel zitten, omdat we bedacht hebben dat daarmee nog een turfstreepje gezet kan worden, waarmee we nog beter 'in control' zijn. Ik hoop dat Gretha tegen die tijd ook weer achter de tafel zit, dan wordt de verkiezing toch wat knusser.

Groet,
Berry

BLENDED THREATS?

Hiding. Waiting. Patient. Deadly.

You can't stop what you can't see.
What does a blended threat look like?

A blended threat can look like just about anything.

- A credit card alert.
- An online shopping confirmation email.
- A prize notification.
- Even a customer service survey from a well known retail store.

Blended threats are spam stealth attacks; perfectly camouflaged to look like something else — something familiar — until they strike. And when they do, the damage can range from compromised personal or corporate data, to the "recruitment" of computers into a network of bots, to keystroke recording that collects passwords and other information.

See through the camouflage — protect your network and data from ambush.
What you can't see can hurt you.

For more information or free product evaluation visit our website:
www.crypsys.nl/m86 or call +31(0) 183 62 44 44

CRYPSYS
data security
www.crypsys.nl

M86™
SECURITY