juli 2010 nummer 5

INFORMATIEBEVEILIGING

Forensic Readiness

Internationale aanpak Cybercrime in Proces Control Systems

Mobile PKI

Bruce Schneier over privacy en meer

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Ik weet niet hoe het u eind juni verging, maar op dit moment is het warm. En op warme dagen is het best wel moeilijk werken. Concentratie te midden van de WK-koorts en de aanloop naar de Tour de France is maar moeilijk op te brengen. Gelukkig is het dan ook niet alleen gewoon werk wat de klok slaat, maar zijn er ook genoeg afleidende activiteiten. Zo mocht ik eind juni de Burton Catalyst-conferentie in Praag bijwonen. Niet alleen is Praag de moeite waard, maar ik heb ook Catalyst zeer op prijs gesteld. Interessante bespiegelingen van de diverse Burton-analisten over onderwerpen als Unified Communication, BPM, Cloud, Virtualisatie, Identity Management en BI. Niet alles had met informatiebeveiliging te maken, gelukkig niet, de wereld is groter dan IB. Toch wordt bij heel veel van deze onderwerpen security als belangrijk aandachtspunt aangehaald. Een aantal interessante analyses:

- Outsourcen van Identity Management (niet alleen Provisioning en Authenticatie, maar ook Autorisatie!) wordt steeds belangrijker. Het probleem is het ontbreken van een Trust Framework voor identity providers. Kijk, dat hadden we in Nederland gelukkig ook al vastgesteld (zie het OpenIDplus-artikel in nummer 3 van IB), maar uitbesteden van autorisatieservices op basis van bijvoorbeeld XACML is toch wel een intrigerende ontwikkeling;
- Risicomanagementtechnieken zijn er genoeg, maar adoptie van ISO27000 (mn 5) loopt niet soepel door onder andere problemen rond de auteurs- en licentierechten. Tja, waarom zou je die documenten ook eigenlijk moeten kopen? Ook moeten we het begrip 'waarschijnlijkheid' binnen risico-analysetechnieken maar loslaten en ook 'kwantitatieve analyses' maar laten voor wat ze zijn;
- Mobile security is niet meer heel spannend (de risico's worden eigenlijk alleen groter door de toename van het aantal gebruikers en devices). Wel weer leuk is de toepassing van VPN's om beheerde componenten toegang te geven tot de interne netwerken.

Misschien was niet alles tijdens de drie dagen even verrassend, maar ik was wel onder de indruk van de kwaliteit. Het is voor herhaling vatbaar.

Wat ook wel voor herhaling vatbaar is, is een privacy special. Het blad lijkt in goede aarde te zijn gevallen. Wat me erg is meegevallen is dat ik, ondanks een nogal specifiek artikel, niet vaker ben lastig gevallen dan voordat de special uitkwam. We hebben al wel een goed onderwerp voor een toekomstige uitgave omdat mevrouw Kroes in het kader van de nieuwe Digitale Agenda van de EU een nieuw privacykader wil laten opstellen. Daar willen wij ook vast wel een bijdrage aan leveren, toch?

Voor dit nummer hebben we weer een keur aan artikelen. Van zwaar technisch tot visionair, voor elk wat wils. We wensen u dan ook veel leesplezier, een prettige vakantie en mooi weer.

Groetjes,

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Borger (Domus Technica)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
Rachel Marbus (BetterID4all)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
De Drie Poorten, Nijkerk

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

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

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

ISSN 1569-1063

Inhoud





Herstel van de zwakste schakel

Sympathie

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

Dit is het vijfde artikel in een serie van acht waarin wordt ingegaan op de psychologische trucs die door Social Engineers worden gebruikt om slachtoffers te manipuleren. Waarom en hoe werken ze? Hoe zijn ze te herkenen en wat is de beste verdediging? In dit artikel komt het aspect Sympathie (de vriendelijke dief) aan de orde.

Social Engineering; een korte terugblik

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

Uit een onderzoek onder 250 CIO's en CISO's van bedrijven en overheden naar (informatie)beveiliging (CapGemini 2003-2008) is gebleken dat 60% GEEN aandacht schenkt aan het beveiligingsbewustzijn van de medewerkers. Een opmerkelijk hoog percentage aangezien 16% aangeeft dat er informatie is gestolen met behulp van SE en zelfs 23% 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 kan worden gemaakt door profiteurs, is bedoeld als bijdrage aan een reeds bestaand bewustwordingsprogramma van een organisatie. Maar het is ook als zelfstandig bewustwordingsprogramma prima inzetbaar voor een risicogroep zoals secretaresses of bewakingspersoneel. De artikelen behandelen de psychologische mechanismen die door SE's worden gebruikt om tegenstanders te manipuleren. Er wordt ingegaan op de achtergrond van de werking en er vindt een verduidelijking plaats aan de hand van voorbeelden uit de praktijk. Verder worden maatregelen aangedragen om een aanval te herkennen en af te slaan.

Sympathie, de vriendelijke dief

Naast wederkerigheid en verplichting (uitgave maart 2010 nummer 2) is er een nieuw maar zeer sterk en effectief beïnvloedingswapen; de sympathie. In een zakelijke of persoonlijke relatie waarin sympathie een grote rol speelt kan voldoen aan een verzoek of de beantwoording van een vraag een soort morele 'verplichting'

Sympathie: eigen ervaring

Ik voerde een Social Engineering Assessment uit bij een organisatie die opleidingen en trainingen verzorgde ten behoeve van openbare orde en veiligheid. Niet alleen het veiligheidsbewustzijn met betrekking tot informatie werd getest, maar ook het veiligheidsbewustzijn met betrekking tot het gebruik van wapens. Ik belde de beheerder van de wapenkamer vanuit mijn huisadres en vroeg hem om voor de volgende dag vijf pistolen, magazijnen en exercitiepatronen aan mij uit te geven voor een wapenles die ik als instructeur in opleiding zou moeten geven. Hij wees me erop dat de aanvraag via een bepaald bureau moest lopen en dat daar een speciaal formulier voor bestond. Ik werd een beetje boos op de organisatie omdat ze blijkbaar nieuwe instructeurs in opleiding geen informatie verstrekten zodat deze alle procedures maar zelfstandig moesten ontdekken. De beheerder van de wapenkamer beaamde dat dit wel vaker voorkwam. Met deze korte reactietijd van slechts een enkele dag zou het mij niet meer lukken de aanvraag op tijd in behandeling te laten nemen. Daarom gaf ik aan dat hij in deze situatie de enige was die mij zou kunnen helpen. Met een dergelijk bureaucratische organisatie moest hij zelf ook regelmatig tegen dit soort problemen aanlopen en het herkennen. Er ontstond een verbondenheid omdat we de zelfde soort problemen ondervonden. En natuurlijk zou ik bij hem aan het juiste adres zijn voor een praktische oplossing. Hij bleek gevoelig voor deze vleierij en zei dat de wapens op het genoemde tijdstip klaar zouden liggen. Toen ik aankwam om de wapens in ontvangst te nemen bleek er een grote poster van een muzikant in zijn werkplaats te hangen en al snel ging het over onze gemeenschappelijke interesse voor de muziek. Er bleef geen tijd meer over voor formaliteiten en de wapens werden zonder verdere plichtplegingen verstrekt.

Toen ik de man na mijn onderzoek sprak over het incident bleek dat het grenzeloze vertrouwen bij de uitgifte van wapens plaats had gemaakt voor een juiste invulling van de procedures. Hij had er een paar slapeloze nachten van gehad, maar was, zoals dat vooraf met de opdrachtgever overeengekomen was, niet gestraft voor zijn incorrecte handelswijze.

Het gemeenschappelijke probleem (de bureaucratie) en het opwekken van sympathie (gemeenschappelijke interesses en oplossingsgerichtheid van betrokkene benadrukken) resulteerde in het verstrekken van wapens.

worden. Binnen een kwalitatief goede relatie is het namelijk heel normaal dat je een verzoek van de ander inwilligt. De relatie oefent daarmee druk uit op het voldoen aan een verzoek. Het wordt een soort morele verplichting ook al voelen we dat niet zo. We willigen toch graag het verzoek van een vriend of naaste collega in?

Het niet voldoen aan een morele verplichting is onvriendelijk en onvriendelijkheid past niet in een goede relatie. Er wordt binnen deze relatie druk uitgeoefend door sympathie en verbondenheid. Het is moeilijk om een verzoek te weigeren als deze van een goede vriend of naaste collega afkomstig is. Maar het gaat nog verder. Ook

met de vriend van een vriend kunnen we ons verbonden voelen. Via de gemeenschappelijke vriend ervaren we een verbondenheid waarin we opnieuw merken dat het een morele verplichting is vriendelijk te zijn en verzoeken in te willigen.

Met behulp van sympathie kan misbruik worden gemaakt van een relatie. Indien een Social Engineer voor het eerst in contact komt met zijn potentiële slachtoffer zal hij proberen om in korte tijd een vriendschappelijke relatie op te bouwen. Complimentjes over kleding of gedag, grapjes en het noemen van een bekende naam zal snel leiden tot een luchtig gesprek. Als de tijd rijp is zal het gesprek worden omgebogen naar een onderwerp waarbij de eigenlijke vraag om informatie verpakt wordt in een vorm die past bij het gespreksonderwerp.
Bij een andere succesvolle methode wordt gerefereerd aan een zogenaamde wederzijdse vriend of kennis. Het verzoek kan nu eigenlijk niet meer worden geweigerd.

De strijd der sexen

Indien een SE binnen een korte periode een goede relatie wil opbouwen moet hij rekening houden met het geslacht van zijn slachtoffer. Mannen zijn minder snel geneigd om in een korte periode een goede onderlinge relatie op te bouwen. Dat geldt eveneens voor vrouwen onderling. Er bestaat tussen gelijke seksen een groter wantrouwen (concurrentie, haantjesgedrag) dan in een relatie tussen mannen en vrouwen. Mensen (van het andere geslacht) die ons loven vinden we meestal aardig, ook als ze het niet menen. We reageren vanzelf positief op vleierij en lof, en dit automatisme kan door profiteurs natuurlijk slim worden uitgebuit.

In de pogingen om vertrouwelijke informatie op te vragen is het daarom van belang om het 'andere' geslacht in te zetten. Mensen zijn namelijk zeer gevoelig voor complimentjes en vleierij van de andere sekse.

Het uiterlijk

Over het algemeen kan worden gesteld dat knappe en goed geklede mensen een voorsprong hebben. Zij wekken nagenoeg automatisch sympathie op; een reactie waarvan wij ons zelden bewust zijn. Knappe mensen worden als sympathieker beschouwd en lijken beter te kunnen overtuigen. Grote mannen stralen kracht en energie uit. Ze lijken slimmer en over meer positieve karaktereigenschappen te beschikken. Profiteurs of oplichters kleden zich daarom vaak goed en maken gebruik van accessoires om dat te ondersteunen zoals sieraden,gsm's en dure auto's.

Gelijksoortigheid en vertrouwdheid

Een andere factor die van belang is bij het opwekken van sympathie is de factor gelijksoortigheid. Iemand die op ons lijkt, dezelfde mening heeft, op dezelfde school heeft gezeten of bij dezelfde vorige werkgever heeft gewerkt, vinden we sympathiek en het wekt vertrouwen. Zie het voorbeeld in het tekstkader.

Een voorbeeld van de combinatie van gelijksoortigheid en vertrouwdheid is te vinden in de samenwerking tussen een slechte en een goede agent bij een ondervraging:

1. door het contrastprincipe lijkt de goede agent een stuk redelijker en sympathieker dan zijn zogenaamde kwade collega;
2. doordat de sympathieke agent het voor de verdachte lijkt op te nemen en hem ook een kopje koffie heeft gebracht, krijgt de ondervraagde het gevoel iets terug te moeten geven (de regel van wederkerigheid);

Sympathie: creëren van verbondenheid

Ik had een gesprek met een potentiële opdrachtgever om onze werkwijze te verduidelijken. Het gesprek verliep wat stroef en was uiterst 'zakelijk', totdat ik hem vroeg of hij misschien op het Jacobus College gezeten had. We waren ongeveer van dezelfde leeftijd en hij kwam me bekend voor, alleen wist ik niet waarvan. Hij had inderdaad op het betreffende college gezeten en vanaf dat moment verliep het gesprek op een veel vriendelijkere manier. Aan het einde van het gesprek heb ik hem verteld dat ik nooit op het Jacobus College heb gezeten maar dat ik de informatie van zijn Linkedin-pagina had misbruikt om sympathie op te wekken. Nou dat was gelukt zei hij!

3. doordat er iemand aan de kant lijkt te staan van de verdachte, maakt de aardige agent een heel goede indruk. Hij wordt voor de ondervraagde van een helper tot een redder (een biechtvader) waarbij hij zijn verhaal (dus de bekentenis) kan doen.

Slecht nieuws wordt in verband gebracht met de persoon die het moet brengen. Alleen al de relatie tussen slecht nieuws en de boodschapper ervan maakt de boodschapper in onze ogen minder sympathiek. Omgekeerd wordt de brenger van een goede boodschap als sympathiek beschouwd. Er is hier dus sprake van een associatieprincipe dat zowel negatief als positief kan zijn. Dit verklaart ook waarom mensen zichzelf in verband brengen met positieve gebeurtenissen en afstand nemen van negatieve dingen. Experts in de misleiding maken hier handig gebruik van door zichzelf alleen te associëren met goede berichten en positieve emoties.

Sympathie: de strijd der seksen

Mijn vrouwelijke collega en ik waren eerst meegelift via de leveranciersingang van de organisatie en later tot op de afdeling waar grote hoeveelheden apparatuur en datastromen bewaakt werden. Het was duidelijk dat de aandacht van de mannen meer gericht was op mijn vrouwelijke collega dan op de grote projectieschermen met statusinformatie. Zij maakte daar handig gebruik van door bij een jonge medewerker te vragen naar zijn werk. Die was kennelijk zo gebrand om een goede indruk op haar te maken dat hij alle vragen van haar beantwoordde en uiteindelijk zelfs een demonstratie gaf hoe je tijdens een storingsdienst vanaf huis kon inloggen. Ten tijde van het onderzoek ging dit alleen op basis van username/wachtwoord. Toen we later de video-opname terugkeken die we met de verborgen knoopcamera hadden gemaakt bleken zijn toetsaanslagen duidelijk herkenbaar.

Verdediging

We kunnen ons verdedigen tegen de eventuele gevaren van sympathie door de signalen te leren herkennen die ons duidelijk maken dat een persoon te sympathiek is voor een bepaalde situatie. Zodra we het gevoel krijgen dat iemand ineens heel aardig is, terwijl voor deze sympathie geen aanleiding lijkt te zijn, moeten we ervoor oppassen dat er plotseling een verzoek aan ons gericht kan worden. Als dit inderdaad het geval is, moeten de zogenaamde sympathieke persoon en het verzoek van elkaar worden gescheiden en moeten we ons alleen op de inhoud van het verzoek richten. Het zal echter niet eenvoudig zijn om een balans te vinden in een gezond portie wantrouwen en het opbouwen van een normale relatie met andere mensen.

Samenvatting

We staan van nature open in een nieuwe ontmoeting met een onbekende, zeker als dat in een vertrouwde omgeving, zoals op het werk, plaatsvindt. We laten ons daarbij beïnvloeden door uiterlijk, schijnbaar gemeenschappelijke vrienden of werkgevers en vriendelijk gedrag. We zullen daarbij bedacht moeten zijn op al te vriendelijk gedrag waardoor we kunnen vermoeden dat medewerking wordt gevraagd om vertrouwelijke informatie te verstrekken.

Forensic Readiness

Ofwel: hoe bereid je je voor op het onverwachte?

Auteur: Eward Driehuis CISSP > Eward Driehuis is manager van de business unit Works bij Fox-IT. Hij is bereikbaar via driehuis@fox-it.com

Een CEO zit in overleg met zijn COO. Ze spreken over een strategieverandering die invloed gaat hebben op de financiële prognoses. Dan vliegt ineens de deur open en de CIO komt met een rood hoofd binnen. "Kan ik jullie nu spreken? Onze prognose ligt op straat. De media zitten er bovenop en onze aandelenkoersen dalen!"

We kennen deze verhalen maar al te veel. Veel forensische onderzoeken hebben een dergelijke zakelijke context. Soms gaat het over industriële spionage, soms over fraude of diefstal. De organisaties die hier het slachtoffer van zijn krijgen twijfels over hun procedures, over hun mensen en over wie ze kunnen vertrouwen. Wie zit hier achter? Hoe kon dit gebeuren? Waarom waren we niet voorbereid? En de meest urgente vraag: is het nog steeds aan de gang?

Deze vragen beantwoord je met digitaal forensisch onderzoek. De antwoorden vinden we in telefoons, laptops, servers en TomToms. Elke e-mail, elk telefoontje en elk bezoek aan een website laat digitale sporen achter. Een digitaal forensisch onderzoeker gebruikt deze sporen om een profiel te maken van de verantwoordelijke en zijn acties. De sporen worden gecombineerd tot aanwijzingen, gekoppeld aan plaatsen en tijden, en uiteindelijk om de dader mee te ontdekken. Hier eindigt het forensische werk echter niet. Sommige organisaties hebben bewijsmateriaal nodig voor gerechtelijke stappen. Anderen hebben informatie nodig om aan de autoriteiten te presenteren. Alle organisaties delen echter een wens. Ze willen weten hoe ze dergelijke incidenten kunnen voorkomen. Daarom eindigen de meeste forensische onderzoeken met advies over hoe incidenten in de toekomst het hoofd te kunnen bieden. We moeten hierbij alert zijn op een paar dingen.

Tijd wordt te vaak gestoken in het zoeken naar data, in plaats van het onderzoeken van data

Bedreigingen uit onverwachte hoek

Criminelen (of nette mensen die minder net gedrag vertonen) worden steeds technischer. Iedereen jonger dan dertig is opgegroeid met een toetsenbord onder de vingers. Deze mensen weten hoe computers werken en hoe je ze kunt misbruiken. Detectie of authenticatie omzeilen is voor hen niet meer ingewikkeld. Organisaties moeten hun IT zo organiseren dat elk gebruik (en misbruik) te herleiden is tot plaatsen, tijden en personen. De 'audit trail' moet werken. Bij organisaties die dit niet doen, treedt willekeurigheid op in het vermogen om incidenten te onderzoeken. Ze laten zaken aan het toeval over.

Een minder voor de hand liggende bedreiging ligt in de ingewikkelde structuur van grote organisaties. Verschillende operationele units, IT-afdelingen, veel verschillende leveranciers, de risicomanagementafdeling, juridische zaken, informatiebeveiliging; ze grenzen aan elkaar of overlappen. Ondanks dat ze dezelfde doelstellingen hebben, moeten we begrijpen dat hun insteek hierin verschilt. Business managers willen risico's verkleinen en marges vergroten. Security managers willen adequaat en proportioneel reageren op een incident. De IT-afdeling wil zo min mogelijk tijd kwijt zijn met graven in logfiles zodat ze het netwerk sneller en stabieler kunnen maken.

Een typisch forensisch onderzoek

Wat zien we vaak gebeuren als een digitaal forensisch team start met een onderzoek? Ze wachten op data. Ze wachten. Ze praten. Ze wachten. Ze smeken. Ze krijgen wat data, vinden wat aanwijzingen, maar hebben er meer nodig. Ze worden naar de hosting provider gestuurd. De hosting provider laat een SLA zien in plaats van data. De situatie escaleert naar de business managers. Boze telefoontjes. Zakelijke relaties ontwrichten. De kosten stijgen. Tijd wordt te vaak gestoken in het zoeken naar data, in plaats van het onderzoeken van data. Uiteindelijk wordt er een dader gevonden, maar soms ook niet. Misschien zijn er aanwijzingen, maar geen solide bewijslast. Er zijn veel kosten gemaakt, de operatie is verstoord en zakelijke relaties zijn beschadigd geraakt.

Hoe moet het wel?

Organisaties die 'forensic ready' zijn, kunnen onverwachte incidenten managen. Ze weten dat incidenten nu eenmaal plaatsvinden en ze zijn er op voorbereid. Hun business doelstellingen zijn vertaald in risicomanagement. Ze hebben nagedacht over de eisen en wensen die ze stellen aan hun onderzoeksdata. Ze hebben hun IT-middelen hierop afgestemd. Forensic Readiness helpt om processen de baas te zijn, in plaats van dat incidenten de operatie verstoren. Als er een incident is treedt er een draaiboek in werking, parallel aan de dagelijkse operationele business.

Forensic Readiness

Organisaties zouden zichzelf de vraag moeten stellen: zijn wij klaar voor onverwachte incidenten? Om deze vraag te kunnen beantwoorden heb je een grondige kennis nodig van informatiebeveiliging, en je moet weten wat een forensisch onderzoek inhoudt. Ik zal enkele handvatten aanreiken. Om te beginnen is het belangrijk om niet afzonderlijk te kijken naar incidenten, management, de beveiliging, of de IT. Je moet ze gezamenlijk, holistisch, beschouwen als onderdeel van hetzelfde systeem. Ten tweede zijn de business doelstellingen het belangrijkst. Deze laten zich vertalen in de security architectuur, die op zijn beurt weer de basis is voor de procedurele en de logische oplossingen die Forensic Readiness vormen. Deze oplossingen bevatten onder meer: intelligente logging en monitoring systemen, en forensische incidentsimulaties. Traceer de oplossingen terug naar de business doelstellingen. "Waarom deden we dit ook al weer?" Ten slotte: ga niet zo maar willekeurig dingen loggen. Dit heeft averechtse effecten zoals een false sense of security. Om van de kosten maar te zwijgen.

In deze wereld, waar cybercrime snel groeit, zouden organisaties rekening moeten houden met het onverwachte. Laat zaken niet aan het toeval over, maar wees voorbereid. Wees Forensic Ready.

Bruce Schneier over privacy en meer

Auteur: Lex Borger > Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.

Bruce Schneier is 'the closest the security industry has to a rock star', volgens The Register. Dit staat vermeld op de omslag van 'Schneier on Security', niet eens meer het laatste boek van Bruce. Hij heeft verschillende boeken geschreven over security, zowel technisch diepgaand als over de sociale aspecten van security. Niet veel auteurs kunnen dat claimen. Voeg daarbij dat Bruce heel actief blogt en een elektronische nieuwsbrief publiceert, dan kom je tot de conclusie dat als je de kans krijgt om hem te interviewen, je dat met beide handen beetpakt. Ik heb een aantal jaren geleden in dit blad al geschreven dat 'Secrets and Lies' het beste security boek was wat ik tot die tijd gelezen had, en het staat nog steeds dik in mijn top tien. Bruce, die in het dagelijks leven Chief Security Technology Officer van BT is, was 27 mei in Nederland voor twee presentaties. Ik woonde zijn presentatie 'De psychologie van security' bij.

Lex Borger.

De presentatie van Bruce had als titel 'de psychologie van security'. Het uitgangspunt van Bruce hierbij is dat er een essentieel verschil is tussen je veilig voelen en veilig zijn. Hij stelt: "Je kunt je veilig voelen, ook als je dat niet bent en je kunt veilig zijn, zonder dat je dat zo voelt. In onze taal is er niet echt een verschil tussen deze twee begrippen."

"Economisch gezien is security altijd een afweging. Je geeft iets op om iets aan security te winnen. In een kogelvrij vest ben je veilig. Maar je geeft een stuk bewegingsvrijheid op en waarschijnlijk ook een stuk modebewustzijn. Dus de beslissing om er een te dragen is een persoonlijke afweging. Het is dus niet belangrijk om je af te vragen of een beveiligingsmaatregel werkt. Je hoort je af te vragen of een maatregel de moeite waard is. Daarom dragen mensen in Amsterdam over het algemeen geen kogelvrij vest."

"Deze afwegingen worden echter gemaakt op basis van een gevoel van veiligheid. Ik kan je een veilig gevoel geven, door je te beveiligen en te hopen dat je dat ook zo voelt. Of door je onterecht veilig te doen voelen en hopen dat je dat niet merkt. Beide methodes werken. Vroeger, toen we nog in het wild leefden, lagen gevoel en werkelijkheid dicht bij elkaar. Tegenwoordig kan daar een groot verschil in zitten." Een groot deel van zijn presentatie gebruikt Bruce om uit te leggen waar dat verschil dan in zit.

Foto: Peter Houlihan

Privacy en anonimiteit

Op het internet trekken we privacy en anonimiteit vaak gelijk. Het internet wordt steeds minder anoniem. Ik vraag Bruce naar zijn mening en hij is wat genuanceerder: "Sociale netwerken maken het internet zeker minder anoniem. Echter, anonimiteit op het internet bestaat nog steeds. Dit lijkt een paradox, maar het is echt waar. Als je dat wilt, kun je volledig anoniem zijn op het web. Kwaadwillende gebruikers passen dit toe, maar ook diegenen die verborgen willen blijven voor kwaadaardige entiteiten."

"Privacy is very much maintained by the fabric of inefficiency"

Dus anonimiteit is niet gelijk te stellen aan privacy. Wat is privacy dan wel? Bruce: "Privacy is een sociaal gegeven. Het gaat over relaties en vertrouwen. In het dagelijks leven is privacy in overvloed aanwezig. Het delen van informatie is binnen de fysieke context inefficiënt. Zelfs als je informatie deelt in een publieke setting, dan is de gedeelde informatie niet meteen publiek bekend. We zijn sociale wezens en hebben continu sociale interacties met elkaar, in verschillende contexten. Je kunt leraar zijn, vader, 's avonds uitgaan. Elke keer is de context anders en het is heel eenvoudig dat gescheiden te houden."

"Op het internet is dat net andersom. Publiekelijk delen van informatie is eenvoudig. Je hoeft maar een blog te beginnen of lid te worden van Facebook of Twitter en je gedeelde informatie is publiek bekend. Het is eenvoudig geworden om bekend of zelfs beroemd te worden op het internet. En alle context is weg. Je kunt niet langer informatie delen in de juiste context. Als je je hier niet van bewust bent, kun je van een koude kermis thuiskomen. Privacy is op het internet heel moeilijk te krijgen."

Ik haalde Ashton Kutcher aan, die zelf zegt zijn privacy te waarborgen door juist veel informatie over hemzelf en zijn vrouw Demi Moore publiekelijk te delen. Bruce vindt dit geen privacy. "Hij heeft zichzelf oninteressant gemaakt."

Maar wie is dan verantwoordelijk voor de afscherming van jouw informatie? Bruce: "Dat gaat over techniek, die taak kan niet bij jezelf liggen, het is de verantwoordelijkheid van het bedrijf wat jouw informatie verwerkt. Zo werkt het in de gewone wereld ook. Je sluit je hotelkamer af, en verwacht dat daardoor jouw spullen veilig zijn. Je controleert de kwaliteit van hun elektronische sleutelsystemen niet, daar heb je geen verstand van. Blijkt dat ontoereikend zijn, kijk je het hotel erop aan.

"All infrastructure is outsourced, always"

Bij de meeste instanties heb je geen keuze om hen jouw informatie te verstrekken, zoals overheden, banken en verzekeraars. Je hoopt

maar dat ze het goed beschermen. Bij sociale netwerken heb je wel de keuze. Naast te vertrouwen op hun technische verantwoordelijkheid hoor je zelf ook sociaal bewust te zijn over wat je deelt. Bedenk dat je eigen privacy-instellingen van Facebook niet te begrijpen zijn. Je wordt misleid. Jij bent ook niet de klant van Facebook, dat zijn de adverteerders. Facebook wil graag dat je informatie deelt en probeert delen aanlokkelijk te maken." Bruce trekt een vergelijking: "Jouw portemonnee bevat doorgaans informatie die te misbruiken is. Als ik jou kan verleiden tot het aan mij tonen van de inhoud van je portemonnee, is

"Single sign-on is hard, authentication is hard"

er nog niets aan de hand. Ik haal jou over dat te doen met een verhaal dat ik onderzoek doe, of ik kan je overtuigen dat iedereen het doet. Ik heb je alleen maar gemanipuleerd tot dat moment. Als ik die informatie daarna publiceer, heb ik jouw vertrouwen gebroken, maar nog steeds is jouw informatie niet misbruikt. Dat gebeurt pas als iemand die de informatie tot zich neemt er iets kwaads mee doet."
Deze vergelijking illustreert mijns inziens ook het verschil in privacybeleving tussen de VS en Europa. In Europa zien we de manipulatie al als misbruik.

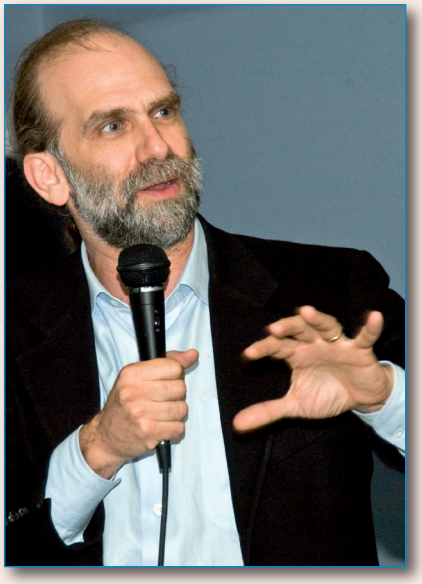


Foto: Bob Andrews

Ik begon over de generatie 'Y'-jongeren, de generatie die opgegroeid is met internet en sociale netwerken. Als iemand sociaal bewust kan zijn, zijn zij het wel. Delen zij hun informatie bewust? Bruce: "Nee, er is veel onderzoek naar gedaan en jongeren begrijpen niet hoe hun informatie gebruikt wordt." Na het doorprikken van dit ballonnetje verlaat ik dit onderwerp maar.

Outsourcing

Het sourcen van IT-beveiligingsdiensten is een discussiepunt in menig boardroom en managementteam van de IT-afdeling. Men vraagt zich

"You cannot understand your Facebook privacy settings"

af: wel/niet doen, en onder welke voorwaarden? Bruce heeft hier desgevraagd een duidelijke mening over.
"Alle diensten kunnen worden geoutsourced. Dus ook securitydiensten. Het maakt niet uit wat het specifiek is, als het een infrastructurele dienst is, kun je het outsourcen. Nu maakt iedereen zich hier nog druk over, maar dat zal veranderen. Outsourcing gaat aanslaan. CEO's zullen zich hier echt niet meer druk over maken, het wordt gewoon contractueel uitgevoerd. Er wordt alleen gekeken of de dienstverlener goed werk levert. De CEO gaat zich echt niet druk maken over details. Wereldwijd wordt van alles geoutsourced. Als

"You can feel secure, even if you are not"

het fout gaat, riskeert de CEO gevangenisstraf (SOX), maar uiteindelijk zal infrastructurele dienstverlening extern afgenomen worden."
Ik neem authenticatie als voorbeeld voor zo'n dienstverlening. In Nederland is men bezig aan een nationaal initiatief, OpenID plus. Is dit dan een handig alternatief voor de inrichting van een eigen (gesloten) authenticatiedienst? Bruce: "Dat hangt er helemaal vanaf. Wat omvat de dienst precies? Hoe wordt het toegepast? Waarvoor wordt het gebruikt? Of authenticatie nu open of gesloten is maakt niet uit. Het belangrijkste is om je te realiseren dat om het goed uit te voeren vooral de dienst in detail goed ingevuld moet zijn."

Friday Squid Blogging

Een opvallende blogactiviteit van Bruce is 'Friday Squid Blogging'. Iedere vrijdag blogt Bruce iets gerelateerd aan de pijlinktvis. Is dit de sociale netwerkversie van een vrijdagbeleving? Vergelijk het met de 'Follow Friday (#FF)' activiteit op Twitter. Ik vroeg Bruce over zijn squid blogging.
"De filosofie achter de squid blogentries is dat ik er elke vrijdagmiddag eentje maak. Soms sla ik een vrijdag over, soms zet ik er twee neer, wanneer ik wat meer materiaal heb." Maar ja, dit zegt nog niet waarom hij het doet. Dat geeft hij echter niet prijs, ook niet na verder aandringen. Wel wil hij nog kwijt: "Blogentries zijn geen eindige bron die geconserveerd moet worden. Als ik minder zou bloggen over pijlinktvissen maakt dat niet dat ik meer over security ga bloggen." Dit laatste is in ieder geval goed nieuws voor de critici die deze wisseling van onderwerp niet helemaal begrijpen en bang zijn iets te moeten missen van security door de squid entries.

Links
Blog: www.schneier.com
Boeken: www.schneier.com/books.html

Securitytrends 2010

Verslag PvIB bijeenkomst 16-3-2010

Auteurs: Stefan van der Wal en Jean-Paul van Haastert> Beiden zijn student aan De Haagse Hogeschool, opleiding Information Security Management

Op 16 maart 2010 vond het PvIB-event Security trends plaats. Dit keer in The Beach te Aalsmeer. De ontvangst was in een oude veilinghal waar iedereen welkom werd geheten door dagvoorzitter Jeroen Bierkart, daarna was het woord aan Jan Friso Groote die ons meenam in een verhandeling over 'software constructie ingebed in de maatschappij'.
Vervolgens stonden een aantal parallelsessies geprogrammeerd , ingedeeld in een technische en een organisatorische stroming. Daarna werd er weer plenair afgesloten met een verhandeling over 'security trends'. De paneldiscussie werd wegens tijdgebrek helaas afgeblazen.

Plenair: Softwareconstructie ingebed in de maatschappij, door Jan Friso Groote, TU Eindhoven
Aan het begin van zijn presentatie, legt Groote ons uit dat de informaticarevolutie nog lang niet voorbij is en hoe software daar een hele grote rol bij speelt. Als voorbeeld haalt hij Philips aan (80% systeemontwikkeling betreft software) daarnaast wordt aangegeven dat veel wetenschapsgebieden zeer sterk afhankelijk zijn geworden van de ICT.
Na de inleiding worden er vooral sterke vormen getoond van hoe programmeerfouten een sterk negatieve invloed hebben op de werking van geavanceerde apparatuur. Daarom zou er volgens de spreker meer kwaliteitscontrole moeten komen op programmacode.
Daarnaast haalt hij zeer uit naar de instituten die hij verantwoordelijk acht voor het gebrek aan controle op softwarekwaliteit en -opleiding. Toch komt hij ook met een aantal constructieve oplossingen:

- 'Rijksdatastaat' (keurt en controleert softwareprojecten, schrijft standaarden voor);
- 'Softwareongevallenraad';
- fatsoenlijk secundair onderwijs in de informatica;
- fatsoenlijke positionering informatica in wetenschappelijk Nederland;
- grote campagne om studenten IT te laten studeren (bètatechniekplatform en bèta- en informatietechniekplatform)[1]

1 Bron: Presentatie Jan Friso Groote Software constructie ingebed in de maatschappij

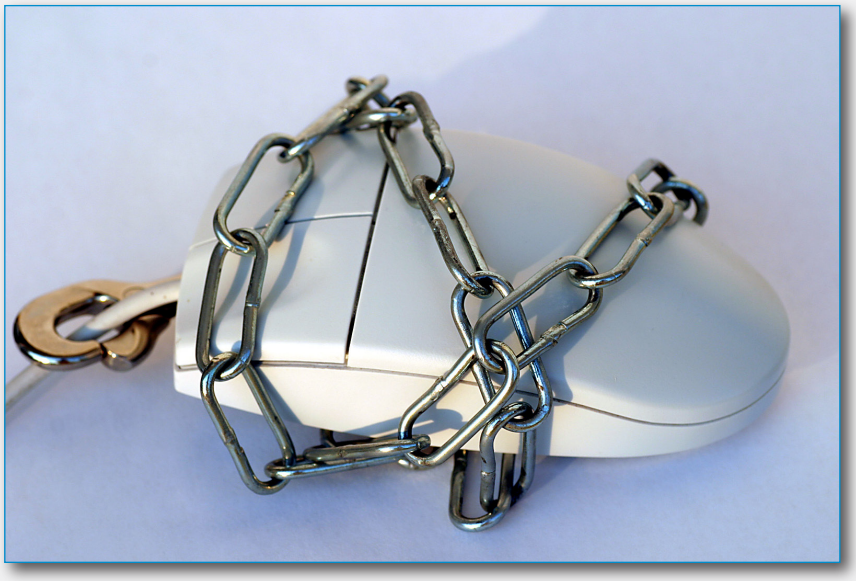
Hoewel deze presentatie in mijn ogen niet heel veel van doen had met informatiebeveiliging, was het zeer interessant en misschien ook een beetje schokkend om te horen hoe het zit met de manier waarop met software wordt omgegaan. Het was prettig om naar iemand te kijken die zo gepassioneerd daarover kan vertellen.

VMware Hacking
Technology College VMware hacking, door Djéan Iritié, Tshukudu
Toen de studenten van de HHS hoorden over de presentatie VMware hacking was de keuze snel gemaakt. Spijtig voor de andere spreker maar hier wilden zij allemaal bij zijn. Vooral omdat virtualisatie een interessante optie is nu machines steeds sterker worden, moet ook zeker niet uit het oog worden verloren dat het een bepaald veiligheidsrisico met zich meebrengt. Een hacker hoeft nu namelijk nog maar een fysieke machine aan te vallen om grip te krijgen op meerdere virtuele machines. Dit kwam uitgebreid naar voren in deze presentatie. Na een aantal voorbeelden gegeven te hebben over hoe het mogelijk is om een VMware apparaat met standaard instellingen aan te vallen en een mooi verhaal dat een weergave gaf hoe snel gebruikers geconditioneerd worden om risicovolle handelingen te nemen (het wegklikken van beveiligingswaarschuwingen, dit omdat we dat al zo vaak doen), werd er duidelijk uitgelegd dat het verstandig is wanneer men een virtueel apparaat draait dit zorgvuldig in te stellen en niet met de default instellingen. Het hanteren van veilige defaults blijft kennelijk nog steeds lastig! Ook bleek uit dit verhaal weer eens dat de menselijke factor nog steeds een zeer zwak punt is in de informatiebeveiliging.

Impact social media

De impact van social media in 2010 op uw security infrastructuur, door Peter Mesker, SecureLink en Marcel Derksen, Palo Alto Networks

De presentatie werd hoofdzakelijk gegeven door Florian. Hij opende met een overzichtsshot van enkele sites die ons dagelijks leven vullen in 2010: Hyves, Facebook, Myspace en Twitter. Hoewel al dit soort sites erg leuk en interessant zijn voor ons en onze vrienden, zijn ze dat ook voor inbrekers, hackers en concurrenten. Diverse bedrijven, waaronder Forbes en FBTO, berichtten over het uitlekken van informatie. Prototypes van motoren, Israëlische legerstrategieën tot aan locaties van maffiakopstukken, die door middel van IP-tracing gevonden zijn.



Een deel van de risico's wordt veroorzaakt door, wat Florian omschrijft als, generatie Y, de millenniumgeneratie (mensen van na 1980). De reden hiervoor is dat deze generatie is opgegroeid in een tijd van technologische vooruitgang (internet, mobieltjes) en economische voorspoed. De generatie Y netwerkt, multitaskt en combineert werk en privé, zonder daarbij de risico's in te zien. Wanneer dit wordt vertaald naar bedrijfssystemen zien we nog een andere trend, namelijk het verzanden van applicaties en protocollen. Waar vroeger poort 25 gebruikt werd voor e-mail, en poort 80 voor webpagina's, is tegenwoordig 54% van al het http-verkeer voor client-server communicatie. Hierover verloopt streaming media, gaming, P2P en meer. HTTP lijkt hiermee het nieuwe TCP te zijn geworden. Het beheren van deze stroom aan informatie is zeer lastig. Gebruikers hebben tal van tactieken dit te omzeilen (Ultrasurf, TOR, socks2http, bypassthat, enz.), de firewallfilters die uitsluitend op poortniveau werken, proxy's die gelimiteerd zijn tot protocollen en URL's, met als gevolg dat beheerders het netwerk langzaam stil zien komen te staan. Verder is het koppelen van netwerkverkeer aan personen lastig. Door middel van DHCP worden IP's willekeurig uitgedeeld en als er vreemde laptops in het netwerk zijn is ook filteren op MAC geen optie.

Florian oppert daarom het gebruik van een Next generation security firewall. Deze kan applicaties identificeren, ongeacht de poort of het protocol (of gebruik van SSL!), gebruikers identificeren ongeacht hun IP-adres, beheerd worden door middel van policy's, realtime-beveiligingen en doen al dit werk zonder prestatieverlies. Technieken die gebruikt worden zijn App-ID, User-ID en Content-ID. Door gebruik te maken van sterke integratie in het bestaande netwerk (bijvoorbeeld Active Directory) is het mogelijk om gebruikers te volgen. App-ID maakt gebruik van een overzicht van meer dan 950 applicaties om het juiste verkeerd op te sporen en content-ID houdt rekening met creditcardnummers en virussen/spyware/enz.

Aan het einde van de presentatie wordt duidelijk dat deze 'next generation' firewall al bestaat, in de vorm van een apparaat aangeboden door Paloalto networks. Marcel Derksen beantwoordt hierna nog kort enkele vragen vanuit het publiek met betrekking tot het filteren van SSL-verkeer en de benodigde policy's die binnen een bedrijf nodig zijn om een dergelijk systeem te implementeren.

Lezing over de virtualisatie 'lifecycle' Waar te beginnen met betrekking tot informatiebeveiliging in jouw virtualisatie 'life-cycle'? door Alex Pelster, inVirtualize

Na een korte uitleg over wat Invirtualize eigenlijk is wat zij doen, krijgen we een overzicht van de voordelen van virtualisatie en in hoeverre dat nu gebruikt wordt door bedrijven. De cijfers liegen er niet om 100% van de Fortune-100 en 98% van Fortune-1000, wat neerkomt op zo'n 140.000 klanten[2]. Ook hier wordt wederom duidelijk dat beveiliging voor de business vaak een ondergeschoven kindje is. Immers, er moet eerst geld verdiend worden en daarna kunnen we altijd nog kijken of het wel veilig is, toch?

Er zijn bedrijven die zich dit beveiligingsaspect wel aantrekken (Cisco, Netapp, VMware) deze hebben de handen ineengeslagen om te komen met oplossingen voor de beveiliging van virtuele apparaten. Daarnaast worden er voorbeelden gegeven van het bedrijf Catbird security en hoe zij omgaan met auditing en beveiligen.

Conclusie:

Een voor IB'ers zeer interessante bijeenkomst, die met een wijd verbreide kennis van mensen uit verschillende disciplines een goed beeld geeft van de mogelijke trends in informatiebeveiliging.

2 Bron: Presentatie Alex Pelster Waar te beginnen m.b.t. informatiebeveiliging in jouw virtualisatie 'life-cycle'?

Nederlandse Staatsloterij verhoogt veiligheids-bewustzijn met e-learning

Wilbert Pijnenburg Marleen Kamminga

Auteurs: Wilbert Pijnenburg en Marleen Kamminga > Wilbert Pijnenburg is directeur Nederland bij InfoSecure en tevens gastdocent bij Cibit-DNV op het gebied van bewustwordingsprogramma's. Hij is bereikbaar via wilbert.pijnenburg@infosecuregroup.com.

Marleen Kamminga is freelance tekstschrijver met opdrachtgevers in bedrijfsleven en overheid. Het thema veiligheid is voor veel van haar opdrachtgevers van groot belang.

"Gefeliciteerd, maar nu begint het pas echt!" Met deze woorden overhandigde een assessor van de World Lottery Association in 2007 het ISO 27001 en het WLA-certificaat aan Yvonne van Oort, algemeen directeur van de Nederlandse Staatsloterij. Want hoe zorg je ervoor dat zo'n omvangrijk boekwerk over de hoogste standaards in informatiebeveiliging en procesmanagement z'n weerslag vindt in het dagelijks werk van alle medewerkers? De Nederlandse Staatsloterij zette e-learning in om informatiebeveiliging tussen de oren te krijgen én te houden.

Voor een kansspelorganisatie die is gelieerd aan de staat, is het vertrouwen van de consument het grootste goed. Daarin speelt het beveiligen van informatie een grote rol. Daarom ontwikkelde de World Lottery Association (WLA) een stevig boekwerk aan regels en richtlijnen voor hun leden overal ter wereld. Voor de Nederlandse Staatsloterij gingen er twee jaar voorbereidingen aan vooraf om de organisatieprocessen geheel in te richten conform de WLA-certificering. Dat vergde bovenal veel van de ICT. In samenhang met de overstap naar een nieuw loterijsysteem zijn de processen nog verder aangescherpt. In 2007 brak het uur van de waarheid aan. De WLA-assessor kwam vijf dagen over de vloer. Die stelde in alle geledingen van de organisatie vast dat aan alles was voldaan. "Het voelde als een overwinningsroes", blikken securitycoördinators Mike de Bruijn en Andrew Lomax terug. "De dag van de uitreiking kreeg dan ook een feestelijk tintje. Het voltallige personeel was in het atrium bijeengekomen om de uitreiking van het certificaat bij te wonen. En toen, om in de woorden van de WLA-assessor te blijven, 'begon het pas echt' voor ons…"

Hoe ervaren medewerkers de e-modules?

Kristel Tap, officer operatie: *"Toen ik hier vorig jaar werd aangenomen, werden de informatiebeveiligingsregels met me doorgenomen in een gesprek. Dat was nieuw voor me. In mijn vorige baan had ik daar niet zo nadrukkelijk mee te maken gehad. Door de e-learningmodules ben ik me bewuster geworden van bijvoorbeeld hoe gemakkelijk je een usb-stick kwijt kunt raken en hoe informatie op sociale netwerken op anderen over komen. Dat waren wel eye-openers."*

Elyan Zegers, manager financiën: *"Elke module begint met een filmpje waarin een situatie wordt geschetst en dat triggert je om de module te doen. Toch sla ik nu soms het filmpje over en begin ik direct met de test, gewoon om te zien of ik er dan ook uitkom. Informatiebeveiliging zit namelijk logisch in elkaar. Als ik even over een vraag nadenk weet ik meestal het goede antwoord wel. En als je eenmaal snapt waarom het nodig is, kun je het je eigen maken."*

Rob Willemsen, retail sales en product-trainer: *"Salesmensen zijn doeners. Die vinden informatiebeveiliging al gauw taaie kost. Ik zie dat sommige medewerkers er te snel doorheen willen en dan teleurgesteld zijn dat ze niet meteen slagen. Maar het brengt wel het gesprek over het onderwerp op gang. Een spiegelmoment. Waarom is het van belang en wat is jouw rol daarin?"*

Zo bevorder je het veiligheidsbewustzijn: Vier tips van Andrew Lomax en Mike de Bruijn (de Nederlandse Staatsloterij)

1. **Overtuig alle medewerkers van nut en noodzaak van informatiebeveiliging.** Overtuig alle medewerkers ervan dat hun rol daarin onmisbaar is.
2. **Maak de regels werkbaar en uitvoerbaar.** Andrew en Mike hebben bijvoorbeeld gezorgd voor sjablonen zodat elke medewerker de regels die gelden voor het opstellen van documenten gemakkelijk kan toepassen.
3. **Maak de drempel om (bijna)incidenten te melden niet te hoog en beloon goed gedrag.** Stel je als informatiebeveiliger niet op als een strenge politieagent.
4. **Houd de aandacht vast.** Breng informatiebeveiliging regelmatig opnieuw onder de aandacht van medewerkers.

Zo bevorder je het veiligheidsbewustzijn: Vijf tips van Wilbert Pijnenburg (Infosecure)

1. **Zorg voor managementcommittment:** laat medewerkers weten dat het management het belangrijk vindt dat ze hun verantwoordelijkheid (blijven) nemen in informatiebeveiliging.
2. **Maak het niet te vrijblijvend.** De Staatsloterij koos er bijvoorbeeld voor om het met goed gevolg doorlopen van de e-learning modules te koppelen aan het jaarlijkse beoordelingsgesprek.
3. **Maak het meetbaar.** Door voor en na het doorlopen van een module kennis, houding en gedrag te meten, weet je exact hoe effectief het programma is.
4. **Maak het leuk.** Met pakkende filmclips en interactieve oefeningen krijg je ook minder geïnteresseerde medewerkers over de drempel.
5. **Sluit aan bij actuele ontwikkelingen.** Zorg dat de informatiebeveiliging en het veiligheidsbewustzijn van medewerkers aan blijven sluiten op ontwikkelingen in en rond de organisatie.

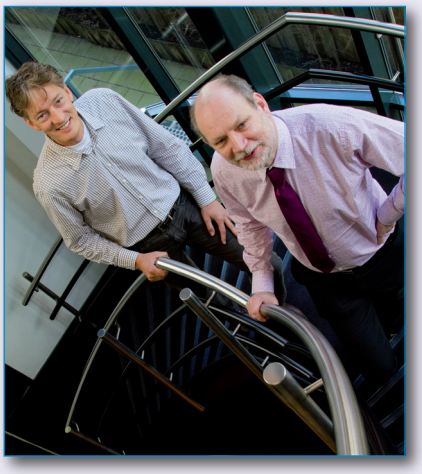
Over de Nederlandse Staatsloterij

Doelstelling/missie: de Staatsloterij is de loterij van Nederland met het grootste prijzenpakket, de grootste winkans, het hoogste uitkeringspercentage en de hoogste en meeste prijzen. Vanuit haar positie ziet de Nederlandse Staatsloterij het als haar opdracht een optimale balans te creëren tussen de geleverde kwaliteit van haar dienstverlening en een zo breed mogelijke maatschappelijke acceptatie.

Klanten: jaarlijks spelen zo'n acht miljoen mensen incidenteel of regelmatig mee.

Distributiekanalen: honderden verkooppunten in Nederland (tabaks- en gemakzaken, terminals bij supermarkten en benzinestations) en de eigen websites www.staatsloterij.nl en www.dayzers.nl.

Mike de Bruijn is Proces & Security Coördinator bij de Nederlandse Staatsloterij.
Andrew Lomax is Proces & Security Coördinator bij de Nederlandse Staatsloterij.



Veilige en zorgvuldige processen

'Proces- en securitycoördinator'. Dat is de titel die op de businesscards van Mike de Bruijn en Andrew Lomax prijkt. Logisch, want de Nederlandse Staatsloterij is een organisatie waarin alles draait om uiterst goed beveiligde en zorgvuldige processen. In 2009 was de omzet € 889,7 miljoen en het prijzengeld moet altijd weer zonder fouten of oponthoud bij de rechtmatige winnaars terechtkomen. Maar aan de basis van al die processen staan mensen. Hoe houd je hen scherp als het gaat om zorgvuldigheid en risicobewustzijn?

De hoge jaaromzetcijfers ten spijt is de Nederlandse Staatsloterij geen omvangrijke organisatie. Het personeelsbestand telt zo'n 120 medewerkers. Dat lijkt heel behapbaar maar, zo benadrukken Mike en Andrew, het brengt tevens een wat informele organisatiecultuur met zich mee. Andrew: "Iedereen kent elkaar immers. En dan is het toch lastiger om mensen te overtuigen van nut en noodzaak van bijvoorbeeld een clean desk policy of het strikt hanteren van het pasjessysteem."

De regels vormen uiteraard de basis

Nut en noodzaak

Nut en noodzaak. Die twee termen duiken steeds weer op in het relaas van de beide veiligheidscoördinatoren. Gedurende het certificeringsproces hielden ze de aandacht van de medewerkers erbij door onder meer een speciale 'examenkrant' uit te geven en bureauklappers met de regels over informatiebeveiliging uit te delen. Vervolgens gingen ze op zoek naar een middel dat niet alleen overtuigingskracht bezat, maar ook de aandacht voor informatiebeveiliging kon vasthouden.

Lastig om mensen te overtuigen van noodzaak clean desk policy

"Op een beurs zagen we een demo van de e-learningmodules van Infosecure en dat leek geheel aan onze eisen te voldoen", aldus Mike. "De methode sprak ons aan. E-learning sluit goed aan op ons overwegend jonge medewerkersbestand. Bovendien hoorden we van andere organisaties dat die er goede resultaten mee boekten." Maar waren de modules inhoudelijk ook voldoende toegespitst op hun organisatie? Ze besloten in gesprek te gaan met de aanbieder Infosecure, specialist en internationaal marktleider in het bevorderen van veiligheidsbewustzijn in organisaties. "In overleg met Wilbert Pijnenburg van Infosecure is een meerjarenplan opgesteld. Met als doel: het informatiebeveiligingsbewustzijn hoog houden onder alle medewerkers."

De aftrap, inmiddels twee jaar geleden, geschiedde volgens Mike op passende wijze. "Infosecure maakte een introductiefilmpje waarin algemeen directeur Yvonne van Oort het belang van ieders rol in informatiebeveiliging nog eens benadrukte." Wilbert Pijnenburg vult aan: "Op deze wijze maken we het committment van het management zichtbaar. We weten uit ervaring hoe belangrijk dat is voor het welslagen." De respons bevestigt het: zo'n 97 procent van de e-modules wordt tijdig afgelegd.

Onthouden en bewustmaken

Het eerste jaar zijn modules ingezet die de regels duidelijk maken en eraan bijdragen dat ze goed worden onthouden en nageleefd. "Een deur open laten die dicht zou moeten zijn, een collega even op jouw account laten werken, een zieke die vanuit huis zijn inlogwachtwoord doorgeeft, een bekende relatie tijdens de 'bezoekersspits' aan de receptiebalie zonder

Over Infosecure

Doelstelling/missie: bijdragen aan de veiligheid van organisaties en hun medewerkers, relaties en andere belanghebbenden, met name door het veiligheidsbewustzijn van management en medewerkers te vergroten en up-to-date te houden.

Kerncompetentie: het ontwikkelen van op de organisatie toegesneden bewustwordings- en trainingsprogramma's. Daarnaast levert Infosecure oplossingen voor risicoanalyse, compliance management en consultancydiensten op het gebied van informatiebeveiliging.
Klanten: nationale en internationale profit en non-profit organisaties.

Vestigingen: kantoren in Nederland, België, Duitsland, Engeland, Scandinavië en Canada en partners in Zwitserland, Kroatië, China en Japan.

Wilbert Pijnenburg is directeur Nederland bij InfoSecure en tevens gastdocent bij Cibit DNV op het gebied van bewustwordingsprogramma's. Hij is bereikbaar via wilbert.pijnenburg@infosecuregroup.com

officiële aanmelding binnenlaten. Zulke dingen gebeuren toch gemakkelijker in een relatief kleine organisatie waarin iedereen elkaar kent", aldus Mike. Strikte naleving van de regels staat echter los van het vertrouwen tussen collega's. Die boodschap moest ook overkomen om 'nut en noodzaak' te onderstrepen. "De regels zijn er niet alleen om incidenten te voorkomen, maar ook - als er onverhoopt toch iets gebeurt - om mogelijkheden uit te sluiten, zodat je snel en gericht op zoek kunt gaan naar oorzaken."
Het tweede jaar is de aandacht uitgegaan naar de sociale aspecten van informatiebeveiliging en zijn modules ingezet die de medewerkers informeren over de gevaren van sociale netwerken en wapenen tegen onder meer social engineering. In het derde jaar kiezen ze voor een serie korte modules waarin het werken met externe partijen centraal staat. Mike: "De informatiestromen zijn de afgelopen jaren sterk toegenomen nu de Nederlandse Staatsloterij steeds meer als regie-organisatie is gaan werken. Er zijn talloze externe partners. Van de drukkerij die de loten produceert tot de ruim 3.200 verkooppunten in het land. Er gaat dus een hoop informatie over en weer". Wilbert Pijnenburg vult aan: "We adviseren graag bij de keuzes van modules. Zo kunnen we aansluiten bij actuele ontwikkelingen in de organisatie. Daarnaast zorgen we voor een goede afstemming tussen algemene, en meer organisatiespecifieke, modules. Omdat we de afgelopen jaren in zoveel verschillende organisaties in binnen- en buitenland ervaring hebben opgedaan met bewustwordingsbevordering, hebben we een goed beeld van wat nodig is en wat wel en niet werkt." Mike: "Wilbert is altijd bereid met ons mee te denken en dat werkt erg prettig. Zo is gaandeweg een module aangepast toen bleek dat veel medewerkers moeite hadden met een vraagstelling."

Aandacht vasthouden

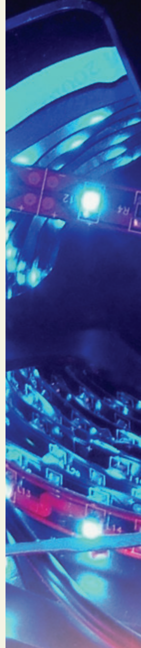
Om de aandacht van de medewerkers vast te houden, is e-learning een vast onderdeel van het werk geworden. "Goede informatiebeveiligingsregels vormen uiteraard de basis. Die worden met elke nieuwe medewerker doorgenomen en daar tekenen ze ook voor", vertelt Mike. "Vervolgens moet je ervoor zorgen dat die aandacht niet verslapt en dat je waar nodig actuele kennis aanvult." Het valt hem op dat de meeste mensen het leuk vinden om de modules te volgen. Bovendien, wie de modules met goed gevolg heeft afgelegd, ontvangt een certificaat. Dat wordt op prijs gesteld. Andrew: "Ze komen het persoonlijk bij ons afhalen op kantoor. Heb je meteen weer even een contactmoment." Mike: "Vaak horen we dan: 'en wanneer komt de volgende module'?"

Regelmatig lopen de securitycoördinators het gebouw door om te kijken of de regels worden nageleefd. Wat ligt er op de bureaus? Staan de schermbeveiligers aan? Zijn bureaulades afgesloten? Dat doen ze strikt, maar streng zijn ze alleen als het echt niet anders kan. "Met een kwinkslag bereik je meestal meer. Mensen moeten hun fouten toe durven geven." Laatst hebben Mike en Andrew alle medewerkers weer bijeengeroepen in het atrium. "Het aantal incidentmeldingen is flink gestegen", lieten ze toen weten. Om direct daarop te zeggen: "En daar willen we jullie voor bedanken." Mike: "Want dat betekent dat de boodschap is overgekomen. Mensen herkennen onveilige situaties. Zo kan bewustwording daadwerkelijk bijdragen aan de beveiliging van informatie."

Samenvatting

De Nederlandse Staatsloterij is in 2007 ISO-27001 gecertificeerd en voldoet daarmee aan de hoogste normen in procesbeveiliging zoals vastgesteld door de World Lottery Association. Maar aan de basis van die processen staan mensen. Om het informatieveiligheidsbewustzijn onder medewerkers te verhogen en op peil te houden, heeft de organisatie met succes e-learningmodules ingezet van Infosecure, wereldwijd marktleider in bewustwordings- en trainingsprogramma's.

Bedankt, het aantal incidentmeldingen is flink gestegen



Internationale aanpak Cybercrime in Proces Control Systems

Auteur: Hans Baars > Hans Baars is beleidsmedewerker bij Enexis en hij is per e-mail bereikbaar via j.h.baars@blixt.nl

ACTUEEL / MARKTMONITOR

BEVEILIGING Verschillen belemmeren samenwerking tussen lan

Cybercrime vraagt om internationale aanpak

■ Beveiligingsbedrijven missen aanspreekpunt

Computercriminaliteit kan alleen goed bestreden worden als er internationaal samengewerkt wordt tussen overheidsopsporingsdiensten en met de IT-beveiligingsindustrie. Daarover was iedereen het wel eens tijdens de RSA-conferentie vorige week in Londen. Maar hoe, wanneer en wie, is niet duidelijk.

Misdrijven van computercriminelen blijven zelden binnen de grenzen van één land. De criminele organisaties gebruiken servers en botnets die verspreid zijn over de hele wereld, vestigen zich officieel in landen die weinig samenwerken met andere landen en de geldstromen voeren ook over vele grenzen heen. Lokale bestrijders van computercriminaliteit kunnen de strijd met de steeds beter georganiseerde criminelen niet aan. "Dit zijn internationale problemen. Daarop past alleen maar een internationaal antwoord", aldus Keith Mularski van de FBI. Hij noemt daarbij als voorbeeld het Russian Business Network uit Sint Petersburg, dat zeker drie jaar probleemloos zijn gang kon gaan met de distributie van kinderporno, phishing, spam en malware. De organisatie was lange tijd ongrijpbaar, maar kon volgens

Ouzounis van ENISA ziet dat ook binnen de EU-lidstaten: "Iedereen heeft dezelfde problemen, maar elke lidstaat ontwikkelt er zijn eigen visie op, heeft zijn eigen wetten en cultuur. Het is heel goed dat men de eigen capaciteiten ontwikkelt, maar de problemen zijn wereldwijd. Er moet informatie gedeeld worden over bedreigingen, over hoe men zich voorbereidt op aanvallen. Er zou samengewerkt moeten worden om dit te testen. Er zijn wel een paar landen die met elkaar praten, maar dat gebeurt meer uit traditie. Er is geen significante pan-Europese strategie."

ENISA is een voorstander van een platform voor het delen en analyseren van informatie. "Daarbij gaat het om een publiek-private samenwerking. Al kom je maar vijf of zes keer per jaar bij elkaar in een ontspannen, neutrale omgeving om informatie uit te wisselen."

ENISA start daarom binnenkort samen met het Nederlandse NICC het project 'Information Sharing in a Box'. Dat is een promotiepakket voor het delen van informatie over computercriminaliteit, dat over alle EU-lidstaten verspreid zal worden. Daarnaast zullen diverse EU-landen in de loop van volgend jaar zogeheten National Exercises uitvoeren. Hierbij worden rampen als gevolg van computercriminaliteit gesimuleerd. Ouzounis: "EU-

voor hen moeilijk zijn in verband m onderlinge concurrentie, maar he noodzakelijk."

"Wij zouden zeker bereid zijn m formatie uit te wisselen met de p maar dat stuit wel op enkele probleme zegt Corne de Rooij, directeur B van RSA. RSA richt zich met zijn be ligingsonderzoeken op de 'undergr community'. Daarvoor infiltreert he drijf en legt het contacten met de bouw van malware en distributietools daar Dat bouwen is niet verboden, zolan niets met de software wordt gedaan. D die contacten haalt het bedrijf zoveel m gelijk informatie over nieuwe malw "We kennen de botnets en kijken o naar de command control centers e Gaan ze bijvoorbeeld met nieuwe Tro aan de slag, dan snijden we commu catielijnen door van die centers. Ook dropzones, waar de gestolen gegeven gestald worden, kunnen we uit de lucht halen. Dan volgt de credentials recove waarbij aan de banken wordt doorgege ven welke informatie is gestolen. M daar stopt eigenlijk ons werk."

RSA wil de informatie die het he gevonden in die 'underground commu nity' best uitwisselen met de overh

'Cybercrime vraagt om internationale aanpak', kopte de automatiseringsgids op 30 oktober 2009. "Verschillen belemmeren de samenwerking tussen de verschillende landen….."

Is dat wel zo? Proces Control Systems zijn systemen die binnen een, in verhouding met de 'gewone automatisering', beperkt deel van de (wereld)markt gebruikt worden.

Dit artikel gaat in op het fenomeen SCADA of Proces Control Systemen, de risico's die de gebruikers of de samenleving al dan niet lopen en hoe er in (inter)nationaal verband mee moet worden omgegaan.

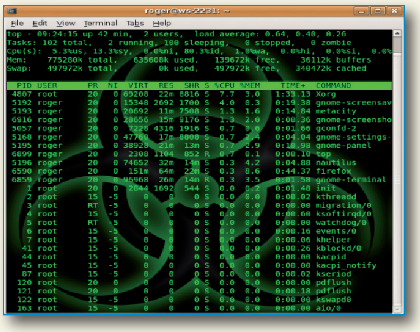
SCADA, afkorting van Supervisory Control And Data Acquisition, is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen. Een SCADA-systeem bestaat uit een computer met daarop de SCADA-software. Een SCADA-systeem vergemakkelijkt het uitwisselen van meetgegevens, het zichtbaar maken van gegevens voor de menselijke operator (visualisatie), het beïnvloeden van deze systemen (sturing), en het verwerken van de meetgegevens tot rapporten (gegevensverwerking) of alarmering.

Vertalen we dit naar de praktijk dan moet je bijvoorbeeld denken aan het omzetten van wissels in een spoorwegtraject, het op afstand mengen van chemicaliën in een chemische fabriek of het op afstand schakelen van transformatoren in een elektriciteitsnetwerk.

PCS zorgt er bijvoorbeeld voor dat (even op het voorbeeld elektriciteitssector inzoomend) bij storing in een transformatorstation het mogelijk is op afstand een transformator uit te schakelen en de stroomkring zodanig te schakelen dat het mogelijk is om zo dicht mogelijk bij het beschadigde punt toch de stroomvoorziening te hervatten. Hierdoor kan de 'downtijd' tot een zo kort mogelijke periode worden beperkt. Na het op grote schaal uitvallen van elektriciteitssystemen in de Verenigde Staten van Amerika en Brazilië is de aandacht voor de beveiliging van dit soort systemen de laatste tijd sterk toegenomen.

Onderscheid tussen 'gewone' ICT-omgeving en de PCS-omgeving

In de, wat hier genoemd wordt 'gewone ICT-omgeving' wordt gebruikgemaakt van veelal standaard applicaties in een vaak op Microsoft gebaseerde werkomgeving, SAP of Oracle-programmatuur, om er maar enkele te noemen. De lijst leveranciers is enorm en de lijst met applicaties nog veel groter. Vrijwel iedere organisatie



heeft een directe internetkoppeling liggen waarmee de medewerkers van het internet gebruik kunnen maken en klanten de bedrijfsinformatie (publieksinformatie) vanaf iedere werkplek ter wereld kunnen benaderen. De gemiddelde doorlooptijd van de gebruikte systemen is slechts enkele jaren. Weinig organisaties maken nog gebruik van Windows 98 en 2000. Office 2003 sterft uit. Vaak is het gebruik de nieuwste versie min 1 te gebruiken. Daar zijn de kinderziektes uit en de beveiligingsgaten gevonden en gedicht. Voor de meeste organisaties geldt dat er tegenwoordig een redelijk groot besef van risico's is en veel beveiligingsmaatregelen worden getroffen.

De PCS-omgeving daarentegen is gemaakt om constant in de gebruik te zijn. Machines worden via dit systeem aangestuurd en die machines moeten productie draaien. In het verleden zijn de PCS-systemen als stand-alone-systemen of in dedicated netwerken geplaatst waarbij er werkelijk geen enkele koppeling met communicatienetwerken of andere systemen bestond. Dit was een situatie die ervoor zorgde dat je ook nu nog MS-Dos, Windows NT en Windows 2000-systemen tegenkomt en sterk verouderde Linux- en Unix-varianten. Servicepacks, security updates, patches enz. werden nooit geïnstalleerd. Dit maakt de systemen over het algemeen zeer zwak en kwetsbaar voor aanvallen.

De gebruikte systemen zijn aangesloten op een lokaal netwerk zonder enige koppeling met kantoorautomatisering of internet. De gebruikte hard- en software is afkomstig van een beperkt aantal bedrijven dat wereldwijd in dit segment opereert. Dit heeft voor- en nadelen. Enerzijds maakt dit het mogelijk internationaal samen te werken aan de bestrijding van cyber crime, anderzijds zijn alle systeemspecifieke protocollen die gebruikt worden uitgebreid gedocumenteerd en op internet te vinden. Daarmee zijn ook de zwakheden te vinden om aan te vallen als er internet of interne netwerkkoppelingen aanwezig zijn.

Koppeling tussen bedrijfsapplicaties en PCS

Voor het koppelen van PCS met kantoorautomatisering zijn veel valide en minder valide gronden te vinden. Het is een onlosmakelijk feit dat de automatisering steeds verder gaat. Iedereen wil 24 uur per dag, 7 dagen in de week en 365 (366) dagen per jaar stroom, water en/of gas in huis hebben en we worden boos als het een paar minuten uitvalt. De leverancier kan

Originele door kernenergie aangedreven vliegtuigmotoren. Nu nog een vliegtuig bedenken dat je hiermee kan aandrijven.

tegenwoordig gekozen worden. Nou ja, degene die de goedkoopste rekening biedt, want de leverancier is nog steeds dezelfde. We gaan gelukkig nog niet zover dat we twintig kabels naar de woning trekken en twintig meters plaatsen, voor het geval de klant van leverancier wil wisselen.
Anno 2010 wil het management maand-, kwartaal- en nog meer rapportages het liefst online meekijken. Meekijken vanuit het bedrijfsvoeringcentrum is ook handig. Als we een koppeling maken met de kantoorautomatisering dan kunnen we het zwarte scherm met gekleurde lijntjes ombouwen naar een Geografisch Informatie Systeem dat exact laat zien waar leidingen lopen en geschakeld kan worden. Een internetkoppeling zou ook wel handig zijn. Plotseling is dat o zo veilige systeem veranderd in een doos van Pandora. Dat alles vraagt om koppelingen met managementinformatiesystemen, geografische informatiesystemen, asset management enz.

Internationale samenwerking

Hoewel de indruk gewekt is dat internationale samenwerking mogelijk een probleem zou zijn is niets minder waar. In 2009 zijn op uitnodiging van het Amerikaanse US Department of Homeland Security (DHS) diverse internationale groepen naar Idaho afgereisd voor een training van een week waarin de basis wordt gelegd voor het herkennen en onderscheppen van cyber attacks.
De groepen bestonden uit afgevaardigden uit Australië en Nieuw Zeeland en medewerkers van internationale Govcert[1] organisaties. Het Nederlandse NICC[2] zorgde voor de door haar georganiseerde Energy-ISAC[3] een training voor medewerkers in de energie- en watersector, consultancybedrijven en bedrijven die materialen aan deze beide sectoren leveren. Het Programma NICC is een publiek-private samenwerking bedoeld om de bestrijding van cybercrime te verbeteren. Het NICC brengt partijen bij elkaar in de 'Nationale Infrastructuur ter bestrijding van Cybercrime'. Het Informatieknooppunt Cybercrime is het kloppende hart van deze Nationale Infra¬structuur. Hier wisselen overheid en bedrijfsleven informatie uit en delen kennis en good practices. De informatie-uitwisseling vindt binnen een sector of sectoroverstijgend plaats. Onder het motto 'verbinden en versterken' bouwt het NICC aan die infrastructuur. Binnen en buiten de overheid werkt een groot aantal partijen aan die bestrijding. Dankzij deze samenwerking krijgen zowel de leverancier die meestal sterk gericht is op functionaliteit en minder op security, de consultant en de beveiligingsverantwoordelijken binnen deze bedrijven een beter inzicht in de risico's en de beveiligingsmaatregelen die minimaal genomen moeten worden.

1 Computer Emergency Response Team
2 National Infrastructuur CyberCrime
3 Information Sharing and Analysis Center

De training

De Amerikaanse overheid staat niet echt bekend om haar bereidheid tot het delen van (cybercrime)informatie. In het nabije verleden hebben er echter incidenten in de energiesector plaatsgevonden waarbij gerede vermoedens zijn gerezen dat cybercriminaliteit (mede) de oorzaak was van kleinschalige en grootschalige uitval van elektriciteitsnetten.

Wie kent niet de TV-reclame van een verzekeringsmaatschappij waarbij een paar jongens een stad, met uitzondering van de eigen woonkamer, stroomloos leggen. Een prachtig gezicht, die ene verlichte flat, in een verder volkomen donkere omgeving. Dit is het schrikbeeld dat de Amerikaanse overheid heeft getriggered om de samenwerking te zoeken met bevriende internationale overheidsinstanties om te zoeken naar samenwerking met als doel de vitale infrastructuren te beschermen.
Op 7 november 2009 startte een training op het gebied van cybersecurity in Proces Control Systems in Idaho Falls, USA.
De reden dat dit onderzoekscentrum is gevestigd in Idaho Falls, in het verre Midden-Westen van de Verenigde Staten ligt in het feit dat er in de directe omgeving meerdere kernenergiecentrales staan waar op experimentele wijze elektriciteit wordt opgewekt. Deze kerncentrales zijn zuiver experimenteel en genereren net voldoende energie om in de eigen energiebehoefte van de 'plant' te voorzien. Dit levert echter ook een 'speeltuin' op waar met energie en communicatievoorzieningen kan worden geëxperimenteerd. Dat laatste brengt ons dan bij communicatielijnen, internet en dus, helaas… cybercrime.

De training

In de locatie te Idaho was een compleet bedrijf in het klein gebouwd. Dat betekent dat er in het gebouw meerdere PCS-systemen stonden opgesteld. Een chemisch apparaat, watersystemen en nog wat testapparatuur waar wij verder niet bij betrokken waren.
Er was een PCS-netwerk, via een DMZ gekoppeld aan een corporate netwerk. Het corporate netwerk werd zowel bedraad als draadloos ontsloten.
De eerste dag stond in het teken van bewustwording. Hoe zitten PCS in elkaar en wat zijn de beveiligingsrisico's? Een eerste stap op het gebied van hacking hoorde er ook bij. Je moet leren denken als een hacker om te bedenken wat hij zou doen om binnen te komen. Heb je dat door dan kan je serieus aan de slag met het verdedigen van je systemen. In de loop van de middag was het moment dan ook gekomen dat de instructeur zijn Powerpoint-presentatie spontaan vervangen zag worden door de mededeling dat de 'dader' toch wel graag een ritje in zijn Shelby wilde maken.
De volgende dag werd gevuld met hands-on-trainingen gevolgd door het uitreiken van de instructie voor de voor donderdag gepland staande red team/blue team-training, waarover verderop meer.
Het laatste deel van dag twee en de hele derde dag werden gevuld met een keuzeprogramma. Er waren sessies over Network discovery en Mapping, Basic Intrusion Detection, Advanced Metasploit Features, Linux administration, Windows Administration, network exploitation. Allerlei wetenswaardigheden op het gebied van hacking en verdediging kwamen voorbij. Zeer

intensieve maar ook zeer interessante sessies. Alle lessen werden ondersteund door een Linux Live CD boordevol hacking tools. Zo boordevol dat het dringende advies luidt het alleen maar in een live netwerk te gebruiken in overleg met de netwerk- en systeembeheerders en alleen als je goed weet wat je doet.

Dag vier, de donderdag werd van de vroege ochtend tot begin van de avond een rollenspel gespeeld. Het was de red team/blue team-training waarbij de blauwe partij een bedrijf vormde dat tot doel had de bedrijfsdoelstellingen te waarborgen. Dat betekent het produceren van het chemische product. Daartoe had men het bedrijfsnetwerk binnen het pand beschikbaar.

Het chemische proces bestond uit twee tanks met 'zuren' die gemengd moesten worden volgens strikte mengverhoudingen. De blauwe partij had bovendien te maken met het bestuur van het bedrijf dat er alles aan gelegen was productie te draaien. Dus beleid werd uitgestippeld. Change- en configurationmanagement werden ingericht en gelukkig ook security- en incidentmanagement. Het formeel regelen van compliancy (SOx) was voor een Amerikaans bedrijf van belang en leverde punten op.

De blauwe partij werd bovendien voorzien van een netwerkplaatje met de mededeling 'het is net als in het echt, dus vertrouw niet volledig op je netwerktekening'. Inderdaad er waren meer componenten aanwezig dan getekend, zoals twee draadloze accespoints en drie extra IP-camera's, waarvan de toegang via gebruikers-

Het rode team in actie met informatievergaring. In vuilnisbakken kan je soms verrassende informatie vinden…

naam en wachtwoord admin je toeliet op het netwerk.

De rode partij kreeg niets anders dan de gelegenheid te gaan onderzoeken of ze toegang konden forceren en het ultieme doel was het stopzetten van het productieproces van het PCS.

Bij elkaar leverde dit een lange dag hard weken van beide partijen op, waarbij de 'onafhankelijke' Amerikaanse cursusleiding enerzijds niet zo onafhankelijk en anderzijds ook niet zo onpartijdig bleek te zijn als zij zich deed voor-

komen. Het voordeel voor het blauwe team was dat wij Nederlanders onderling 'Crypto' spreken. Wat wil je als Amerikaan, wanneer Engels de enige taal is die je beheerst.

Bijzonder was te constateren dat de aanvallende pc's op het netwerk sporen achterlieten met ip-ranges die waren te herleiden naar Nigeriaanse providers. Vreemd, ze zaten twee kamers verderop… Een klein kunstje bleek, voor de Amerikanen, om willekeurige IP-adressen te gebruiken…. Dat kan bij een echte aanval dus ook gebeuren.

Op het einde van de dag, de roden waren binnen, maar hadden de PCS-omgeving nog niet onder controle weten te krijgen, viel de stroom 'virtueel' uit. De reden, de alom aanwezige eekhoorns hadden geprobeerd van stroomkabels wintervoorraad te maken. Daar kon de stroomvoorziening niet tegen, de eekhoorns overigens ook niet.

De lessons learned

Wanneer we een en ander kort samenvatten kunnen we de conclusie trekken dat voor er ook maar gedacht wordt aan het koppelen van PCS- (SCADA)systemen met kantoorautomatisering, de OS'en en onderliggende serversystemen zoals webservers, ftp-servers, Sql-servers enz. volledig up-to-date moeten zijn en alle security patches gehad moeten hebben.

Alle hacking tools zijn vrij downloadbaar van het internet. Het is zelfs als compleet pakket in een Linux Live-distributie te downloaden. De door ons gebruikte versie was door de cursusleiding alleen nog iets verbeterd.

De gebruikte PCS-systemen zijn internationaal overal hetzelfde. Er zijn slechts een beperkt aantal fabrikanten op deze markt. De systeeminformatie is voor de liefhebber via het internet te downloaden en daardoor zijn de gaten ook eenvoudig te vinden. Alle handleidingen zijn te verkrijgen, de besturingssystemen, protocollen en hun kwetsbaarheden zijn bekend. Dit betekent, dat wanneer de systemen van buitenaf of binnenuit bereikbaar zijn, ze ook heel kwetsbaar zijn.

Permanent monitoren van het netwerk is van levensbelang. Zorg eerst dat het normale verkeer bekend is en stel dan alarmen in op abnormale handelingen.

Zorg dat inkomende IP-adressen bekend zijn zodat vreemde IP-adressen gemakkelijk herkend worden. Internationale samenwerking, maar ook nationale samenwerking tussen de verschillende partijen in deze sectoren is van groot belang. Het NICC heeft hier grote stappen mee weten te zetten.

Wissel informatie over incidenten met elkaar uit. Schaam je niet voor incidenten, ze worden vertrouwelijk behandeld maar helpen uiteindelijk de gemeenschap met het in een (nog) vroegtijdig(er) stadium herkennen van incidenten.

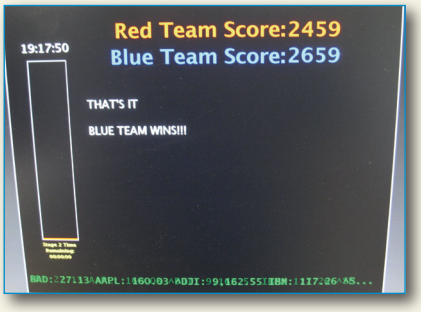
Tot slot de vraag of dit nu in Amerika had moeten gebeuren

Deze is op dit moment volmondig met `ja` te beantwoorden. Ten eerste zijn de Amerikanen zonder voorbehoud bereid om de kennis die zij hebben op het gebied van cybersecurity te delen met de bevriende staten. DHS hebben een faciliteit beschikbaar die in ons land niet beschikbaar is.

DHS hebben de kennis om zich heen verzameld die nodig is om grootschalig onderzoek te doen. De trainingen is maar een facet uit hun werkzaamheden.

Toch zou het ook in Europa van de grond getrokken moeten worden. Kijk je naar wat er nu precies staat, dan moet het haalbaar zijn om in Nederland een soortgelijke faciliteit in te richten. Beter zou zijn wanneer een organisatie als ENISA vanuit haar EU-context iets dergelijks opzet.

Een dergelijk trainingcentrum kan veel breder getrokken worden dan de huidige opzet, PCS/SCADA. Daarnaast zou er een studiecentrum voor (informatie)beveiliging in het algemeen en samenwerking tussen diverse landen binnen en buiten de EU opgezet kunnen worden.



Column

Ik vriend, jij vriend, wij vrienden

Ik heb veel vrienden. Op Hyves althans. Wel 123. Op Linkedin heb ik ook veel vrienden, al noemen ze het daar dan weer 'contacten', 181 om precies te zijn. Op Twitter heten ze 'volgers' en daar zijn het er 170. Er zit enige overlap in, maar niet zo heel veel. Als je de cijfers bekijkt, dan zou je kunnen zeggen dat ik een gezegend mens ben met zo'n groot sociaal leven met al die vrienden. Maar schijn bedriegt. Met het risico dat ik nu een aantal vrienden verlies: online vrienden zijn geen vrienden. Althans, niet in de conventionele zin van het woord. In het offline-leven hebben wij niet zoveel vrienden, sterker nog, wij vinden dat helemaal niet nodig. Uit recent Brits onderzoekt blijkt zelfs dat vrouwen niet meer dan vier 'echte' vrienden om zich heen willen hebben. In het offline-leven gaan wij liever voor kwaliteit dan voor kwantiteit, aldus het onderzoek.

Hyves

Vrienden laat je toe in jouw privéleven. Zij komen in die private sfeer waar het 'de rest van de wereld' niet toegestaan is te kijken. Uit onderzoek van socioloog Gerard Mollenhorst naar de ontwikkeling van vriendschappen blijkt dat de gemiddelde Nederlander 2,5 vriend heeft met wie hij persoonlijke kwesties bespreekt. Een belangrijke opmerking die Mollenhorst daarbij maakt is dat wij veel meer mensen kennen dan we vrienden hebben. Aha! In de online-wereld zijn het dus kennissen of bekenden en geen vrienden.

Eigenlijk worden we dus op het verkeerde been gezet door de Hyves, Facebooks en Twitters van de wereld. Iedereen waarmee we daar contact leggen wordt een vriend genoemd. En op die manier gaan we ook met hen om. Wij hebben bepaalde ideeën over wat het betekent een vriend te zijn. Die aannames nemen wij mee in de online-wereld. Een collega op de Universiteit van Tilburg maakte een tijdje geleden een fictief Hyvesprofiel aan. Zonder ook maar enige vorm van informatie op dat profiel te zetten, is hij lukraak honderden mensen gaan uitnodigen om zijn vriend te worden. Het merendeel van de verzoeken werd zonder navraag geaccepteerd. Onderzoekster Danah Boyd heeft het al eens eerder gezegd. Er lijkt wat vreemds aan de hand te zijn met die vriendschapverzoeken. Vooral jongeren durven een dergelijk verzoek niet te weigeren omdat dat 'not done' is en je daardoor in een sociaal isolement terecht zou kunnen komen. Ook is het cool om veel vrienden te hebben wat het lukraak uitnodigen en accepteren verder in de hand

LinkedIn®

werkt.
Clay Shirky wijst op de gevaren die kleven aan dat online-begrip van vriendschap in combinatie met de hoeveelheid die we ervan hebben. Hij zegt: "a friend of a friend of a friend is pronounced a stranger". Als ik honderd vrienden heb en al die vrienden hebben ook weer honderd vrienden en de vrienden van die vrienden ook, dan bevind ik me al snel in een enorm netwerk van mensen die alles over mij te weten kan komen. Dit wordt ook wel het 'onzichtbare' publiek genoemd. Ik kan dan wel denken dat ik zelf met wijsheid en voorzichtigheid mijn vrienden heb uitgekozen, maar de vrienden van mijn vrienden ken ik (meestal) niet.

Ik moest laatst weer aan de opmerking van Shirky denken toen ik in de pauze op een congres zat te 'krabbelbrowsen' (het lezen van de krabbels op andermans Hyves-pagina's). Ik zag bij een vriendin een hele rij krabbels staan van iemand die daarin extreem klaagde over haar baas. En met extreem bedoel ik dan ook het aanduiden van deze baas als 'kutwijf'. De krabbelaar was zo slim om de naam van het bedrijf en de baas niet te noemen. Althans, niet in díe krabbels. Al doorbladerend kwam ik bij krabbels uit van een maand ouder. En uiteraard. Daar vond ik diezelfde persoon weer. Het bedrijf en de naam van de baas werd meerdere malen genoemd. Voor de krabbelaar ben ik een 'vriend van een vriend'. Zij heeft mij nog nooit ontmoet. Ik ken haar niet en zij mij niet. Voor haar ben ik onderdeel van het onzichtbare publiek. En deze onzichtbare dame moest vervolgens meteen weer denken aan Google en mijnheer Schmidt die op veel commentaar - ook van ondergetekende - kon rekenen toen hij zei: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place". Zit er dan toch een kleine kern van waarheid in zijn woorden? Een kleine dan. Ik denk ook dat ik hem verkeerd verstaan heb, volgens mij zei hij namelijk: *"If you have something you don't want everyone to know, maybe you should think twice where you're going to be writing it in the first place".*

mr. Rachel Marbus
(@RachelMarbus op Twitter)

Interview met Omar Hussain, CEO Imprivata

Auteur: Hans Gründemann > Hans Gründemann, CISSP werkt bij ID & IT Consultancy.
Hij is te bereiken via hans.grundemann@idenit.nl

Omar Hussain

Hans Gründemann

Hans Gründemann was in de gelegenheid om met Omar Hussain te spreken over de karakteristieken van en beveiligingstrends binnen de zorgsector. Omar Hussain is CEO van Imprivata, een Amerikaans IT-bedrijf, dat bekendstaat om single sign-on en strong authentication-oplossingen dat het onder de naam OneSign verkoopt. Recentelijk richtte het bedrijf een speciale divisie op voor de gezondheidszorg.

Hussain verklaart de focus van Imprivata op de zorgsector: “De gezondheidszorg is een unieke sector omdat elke dag van een arts of verzorger er compleet anders uitziet, terwijl anderzijds ziekenhuizen over de hele wereld gelijkaardige processen hebben. In de gezondheidszorg kan snelle toegang tot informatie een kwestie van leven of dood zijn, terwijl er wel de eis is dat deze, persoonlijke, gegevens goed beschermd worden tegen ongeautoriseerde toegang. De prioriteit ligt echter altijd bij het welzijn van de patiënt. Dat wordt niet alleen gedreven vanuit de organisatie en door de overheid, maar is voor veel artsen en verzorgend personeel niet gewoon werk, maar een hoger doel.”

“De uitdaging voor de zorgsector wordt deels veroorzaakt door de steeds grotere invloed van IT-middelen, die veel opleveren maar ook nieuwe obstakels opwerpen. “Het grootste probleem is dat de informatie waarmee ziekenhuizen werken, zeer gevoelig is, en steeds vaker digitaal beschikbaar. Hierdoor zou de informatie in potentie beter beveiligd moeten zijn, omdat statusrapporten niet meer ‘hard copy’ aan het voeteneind van een bed liggen maar juist vanuit vele plaatsen beschikbaar zijn. In de praktijk blijkt echter dat computers met patiëntgevoelige data regelmatig ‘open’ blijven staan of dat gegevens gedeeld worden met ongeautoriseerde personen. Dit gedrag wordt niet ingegeven door kwade wil. Het is puur gebaseerd op het feit dat het volgen van alle procedures ten aanzien van inloggen en uitloggen zeer tijdrovend en dus productiviteitsverlagend is. De grote uitdaging voor computertoegang binnen zorginstellingen is, dat deze eenvoudig én veilig moet zijn. Het compleet toegang geven tot applicaties is een sinecure. Net zo relatief eenvoudig is het om alles helemaal ‘dicht’ te zetten. De kunst is het vinden van de juiste balans tussen veiligheid en productiviteit”, aldus Hussain. “Vrijwel alle landen met een volwaardig zorgstelsel kennen wet- en regelgeving op het gebied van privacyborging voor de patiënten. In Nederland is er de NEN 7510-norm. Die zegt over de toegangsbeveiliging van IT-systemen het volgende: *‘Toegangsbeveiliging heeft tot doel dat het raadplegen, veranderen, toevoegen en wijzigen van gegevens alleen gecontroleerd kan gebeuren.’* Hoe dit precies ingericht moet worden, blijft in het midden. Hiervoor zou gekeken kunnen worden naar de standaard die voor de credit card-industrie al in 2005 in gebruik is genomen, PCI-DSS. Deze schrijft specifieke maatregelen voor, zoals de encryptie van gebruikersdata, periodieke scans van het netwerk, logische en fysieke toegangscontrole, het monitoren van activiteiten en het vastleggen hiervan. Wie doet wat? De gevolgen van onvoldoende beveiliging van patiëntendata laten zich voelen in mogelijke schade en in sancties in de vorm van boetes of anderszins. Zo hebben recentelijk Californische wetgevers het Kaiser Permanente’s Bellflower-ziekenhuis een boete gegeven van 250.000 dollar, omdat zij niet konden voorkomen dat werknemers rondneusden in het medische dossier van Nadya Suleman, de moeder die een mediastorm veroorzaakte, nadat zij beviel van een achtling. Deze boete was de eerste geldelijke straf die werd opgelegd, en was de hoogst toegestane boete onder een nieuwe staatswetgeving in de Verenigde Staten, die is aangenomen nadat de privacy in het UCLA Medisch centrum van onder andere Farrah Fawcett, Britney Spears, de First Lady van Maria Shriver en andere beroemdheden was geschonden.”

Zorg voor sterke authenticatie

Binnen de zorgsector volstaan de traditionele wachtwoorden steeds minder om de informatieveiligheid te waarborgen. Ziekenhuizen beschikken over tussen de tien en de twintig applicaties, die elk met een complex wachtwoord beveiligd dienen te worden vanwege wet- en regelgeving.

Hussain stelt dat dit een barrière vormt, met name om de productiviteit te verbeteren. “De praktijk wijst uit dat werknemers gemiddeld één moeilijk wachtwoord kunnen onthouden, terwijl ze misschien wel tien wachtwoorden nodig hebben om toegang te krijgen tot al hun applicaties. Het gevolg is dat ze eenvoudige wachtwoorden kiezen of, wanneer ertoe gedwongen door de werkgever, moeilijke wachtwoorden die ze opschrijven. Beide sorteren niet het gewenste resultaat. Ik vergelijk het altijd met een luchthaven, waar je liever de
beveiliging concentreert rond een punt dan dat je de aandacht moet verdelen over zestig gates. Door te starten met single sign-on faciliteer je dat mensen vanuit één complex wachtwoord kunnen werken en plavei je de weg voor de introductie van sterke authenticatie.”

Imprivata richtte recentelijk de Healthcare Division op voor de gezondheidszorg. Hussain verklaart de keuze voor een separate divisie als een logisch gevolg van de behoefte in deze markt in combinatie met de track record die het bedrijf heeft binnen het segment. “We hebben een substantiële focus op de gezondheidssector die is
geworteld in de wereldwijd vijfhonderd ziekenhuizen en in totaal meer dan een miljoen gebruikers die we bedienen met onze

producten. Vanuit onze ervaring met klanten in de Verenigde Staten en in Nederland kunnen we stellen dat de uitdagingen rondom gegevenstoegang en -beveiliging identiek zijn voor beide regio's."

Hoewel de werkprocessen en de houding in zorginstellingen in de Verenigde Staten en in Nederland grotendeels overeenstemmen, zijn er organisatorisch en qua budgettering wel enkele fundamentele verschillen waar te nemen, vertelt Hussain. "Het grootste verschil tussen de Verenigde Staten en Nederland zit in het beslissingstraject van de zorginstellingen zelf, vanwege de herkomst van de budgetten. Waar in Nederland overheid indirect en de maatschappen binnen het ziekenhuis medebepalend zijn in de keuze voor een investering, ligt de verantwoordelijkheid daarvoor in de VS toch voornamelijk bij de Chief Medical Information Officer, die verantwoordelijk is voor de inkoop van faciliteiten die ter beschikking van het eigen en ingehuurde medisch personeel worden gesteld. Doordat ziekenhuizen in de VS private organisaties zijn met hun eigen kosten en inkomsten, is IT er meer centraal geregeld. De kosten komen voor rekening van de zorginstelling, die het gebruik van diensten verdisconteert met de externe partijen die er gebruik van maken. In Nederland is het belangrijk om een 'buy-in' te hebben van de maatschappen, waardoor beslissingen iets meer tijd in beslag nemen."

Virtuele zorgdesktops

Gedreven door beveiligingseisen en patiëntenprivacy is binnen ziekenhuizen wereldwijd, naast de inzet van sterke authenticatie en single sign-on, ook een andere technologische trend waarneembaar, namelijk die van de inzet van virtuele desktops oftewel Virtual Desktop Infrastructure (VDI). Vanuit het productiviteits- en kostenbeginsel investeren veel ziekenhuizen momenteel in een grote 'update' van hun werkplekken, waarbij de tendens naar virtuele desktops neigt. Er zijn minder werkplekken nodig, omdat de virtuele desktops toegang bieden tot alle applicaties ongeacht de locatie van het werkstation. Spreekkamers hoeven niet meer doktergebonden te zijn. Ook kun je lichtere werkstations (thin clients) gebruiken, die minder energie verbruiken. Dit alles resulteert in een kostenbesparing op hardware, op spreekkamers en op energie. Die kunnen met VDI immers gedeeld worden door verschillende specialisten met elk desnoods hun eigen applicaties. Vanuit beheerperspectief kan een groot deel van het beheer en de uitrol gecentraliseerd worden.

Hussain zegt hierover: "Deze architectuur heeft een behoorlijke impact op het beveiligen van informatie op de werkplekken. Vooral de coördinatie en het afdwingen van datatoegangsbeleid wordt een stuk complexer, omdat een identiteit relevant is binnen meerdere lagen die de virtuele desktop raken."

De volgende lagen kunnen worden onderscheiden:

- Het fysieke werkstation en diens eigen OS: wordt deze gedeeld met verschillende personen of toegewezen aan een persoon? In welk deel van het gebouw bevindt het werkstation zich of staat het op locatie? Is het een vaste of mobiele werkplek?;
- Het besturingssysteem van de virtuele desktop, over het algemeen betreft dit een Windows OS;
- De (HIS-)applicatie met daarin het patiëntendossier.

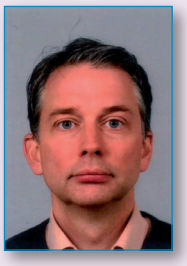
De complexiteit van de omgeving kan worden geschetst met het volgende werkproces. Een assistent maakt het patiëntendossier aan in de HIS-applicatie. Daarna moet de arts het dossier aftekenen. De gemakkelijkste en snelste manier om dit te doen is zonder volledig uit te moeten loggen en de rol binnen de ZIS-applicatie te veranderen van assistent naar arts (en weer terug). Op dat vlak kan Imprivata een belangrijke rol spelen.

Binnen de context van de VDI-omgeving dient de IT-afdeling goed na te denken over de manier waarop het gebruikersidentiteiten beheert en systemen authenticeert alsmede toegangsbeleid afdwingt binnen het bedrijfsnetwerk. De 'connection broker', die controleert hoe gebruikers, IT-beleidslijnen en wachtwoordrechten beheerd worden, houdt namelijk een beveiligingsrisico in. Ze dient als enkelvoudig toegangspunt voor de complete virtuele infrastructuur. Wanneer de connection broker wordt gecompromitteerd, staat de hele VDI potentieel bloot aan beveiligingsrisico's. Omdat VDI in veel gevallen applicaties 'hot' houdt via snapshots van alle gebruikerssessies, kan het kopiëren van een draaiende virtuele machine resulteren in het opnieuw creëren van dezelfde virtuele sessie op een andere machine, die gehackt kan worden om toegang te krijgen. Dit maakt auditing en rapportage tot kardinale punten, met als uitdaging dat rapportages en audits van de connection broker niet mogelijk zijn op het detailniveau dat vereist is om forensisch onderzoek te faciliteren. De IT-afdeling heeft vaak slechts zicht op de gebruikers wanneer die toegang zoeken tot de virtuele machines op het toegangspunt in de serverruimte. Vereist is echter dat ze op lokaal niveau inzicht hebben in waarvandaan precies de virtuele desktop geopend wordt, hetgeen mogelijk is via een IP-adres of een andere 'identifier'. Organisaties moeten kunnen zien wie toegang heeft gehad tot welke applicaties en vanaf welke locatie."

Door een single sign-on-systeem te introduceren, kunnen zorginstellingen auditen welke persoon toegang heeft gehad tot welke applicatie en virtuele desktop, door het oorspronkelijke IP-adres, de datum, tijd en de authenticatiemiddelen op te slaan. De logs waarin applicatiegebruik wordt geaudit, worden beveiligd en real-time verstuurd, opgeslagen en beschermd in separate servers, afgescheiden van de VDI-omgeving. Deze kunnen worden gebruikt in rapportages over de compliancy van het systeem.

De opkomst van virtuele desktops in zorginstellingen vereist een groot inzicht in de implicaties, aldus de topman. "Gebruikers alleen toegang bieden tot aangepaste desktops met gedefinieerde toegangsrechten kan zeer waardevol zijn om gegevens en computers te beveiligen. Het gebruik van een centraal punt om virtuele middelen te authenticeren, toegangsrechten tot werkplekken vast te leggen en te verkrijgen, en sessiegerelateerde informatie te auditen is binnen VDI nog belangrijker dan bij een conventionele desktopomgeving. Wanneer de beveiliging op deze manier wordt ingericht, zullen zorginstellingen kunnen profiteren van de voordelen op het gebied van flexibiliteit en productiviteit. Die worden bevorderd doordat binnen VDI 'follow me'-desktops geen utopie meer zijn. Tegelijk zullen ze een belangrijke stap maken om de lokale wetten en regels te volgen."

Awareness Campagne maakt beveiliger ook meer bewust



Auteur: Joe Stijnen > ir. J.P. (Joe) Stijnen CISA is projectleider binnen de gemeente Eindhoven. Hij is in de afgelopen tien jaar binnen de verschillende sectoren werkzaam geweest en heeft diverse functies vervuld. Sinds 2005 voert hij opdrachten uit op het gebied van informatiebeveiliging.

Binnen de gemeentelijke organisatie staat dienstverlening aan burger, bedrijf of instelling centraal. De soort dienstverlening is divers. Zo kan het gaan over de uitgifte van reisdocumenten, over wijkvernieuwing en alles wat er tussenin zit. Burger, bedrijf of instelling moeten erop kunnen vertrouwen dat de informatie die de gemeente gebruikt klopt, compleet en actueel is. Tot op zekere hoogte is er weinig verschil tussen een gemeentelijke organisatie en het bedrijfsleven. Of je nou vrachtauto's produceert of verzekeraar bent, de bedreiging door te weinig awareness is hetzelfde. Er kan schade ontstaan als iemand misbruik maakt van te weinig awareness en zichzelf toegang tot het bedrijf verschaft. De doelstelling van alle organisaties is hetzelfde, namelijk het vergroten van awareness. Ook de mechanismen en het instrumentarium die de beveiliger tot zijn beschikking heeft om die awareness te verbeteren, zijn dezelfde. Beveiligingsbewustzijn is voor elke organisatie noodzakelijk, ongeacht de aard van de organisatie.

Informatiebeveiliging binnen de gemeente is niet nieuw. Zo kennen we van oudsher het domein van publiekszaken en de beveiligingseisen die uit de GBA[1]-wetgeving volgen. Ook stelt het BKWI[2] beveiligingseisen om op het SUWINET[3] aangesloten te zijn. In het verleden heeft de gemeente Eindhoven ervoor gekozen om elk specifiek domein hun eigen beveiligingsmaatregelen te laten uitwerken. Het gevolg hiervan is nu dat sommige sectoren hun eigen beveiligingsorganisatie hebben ingericht en opgezet. Omdat de gemeente Eindhoven toentertijd een Facilitair Bedrijf had, kon er altijd worden vertrouwd op centrale, technische beveiligingsmaatregelen. Dat betekent dat er een technische baseline is, die in principe voor de gehele gemeentelijke organisatie voldoet. Eenduidige, samenhangende, organisatorische beveiligingsmaatregelen berusten in de praktijk min of meer op toeval. Met andere woorden, er komen verschillen voor in de manier waarop sectoren hun beveiligingsorganisatie hebben ingericht.

De mystery guest kan zo bij persoonlijke bezittingen.

Het beveiligingsproject dat door de sector Informatisering & Beheer is gestart, heeft dan ook als uitgangspunt dat een technisch goed beveiligd systeem effect zal hebben met een goede implementatie en bij een organisatorische inbedding. We wisten bij aanvang dat we in technisch opzicht de zaken redelijk op orde hadden, maar dat de lijnorganisatie hier geen zicht op had. Als we dit wel konden laten zien, dan waren we ervan overtuigd dat de lijnorganisatie meer begrip zou tonen voor de geldende regels en procedures. Bovendien wilden we vanuit de sector Informatisering & Beheer de discussie aangaan over wie nou het risico draagt van het gebrek aan beveiligingsmaatregelen.

Niets menselijks is ons vreemd

Onderzoeken en studies tonen geregeld aan dat de medewerker zelf de zwakste beveiligingsschakel is. In beveiligingstermen vormt de medewerker een bedreiging door bewust of onbewust misbruik te maken van gegevens en systemen. Awareness of beveiligingsbewustzijn is dan ook de belangrijkste tegenmaatregel. Onze prioriteit lag uiteindelijk bij het voeren van een awarenesscampagne gericht op zowel medewerkers als ook management. Weten zij welke risico's er met informatiesystemen samenhangen? En weten zij welke rol zij hierin spelen? Weten zij dat zij door hun houding en gedrag de effectiviteit van die maatregelen enorm vergroten?

1 GBA: Gemeentelijke Basis Administratie
2 BKWI: Bureau Keteninformatiserig Werk & Inkomen
3 SUWINET: Elektronische infrastrcutuur gebruikt door de CWI, UWV en gemeenten om bij de uitvoering van de taken die bij of krachtens de wet SUWI of enige andere wet aan de CWI, UWV en bij of krachtens de ABW, IOAW en IOAZ aan gemeenten is opgedragen.

Awareness Campagne maakt beveiliger ook meer bewust

Awarenesscampagne

Het zwaartepunt van de campagne lag met name bij de bezoeken die een mystery guest aan onze organisatie zou afleggen. Een mystery guest is een indringer op bestelling. Omdat je daarmee beveiligingsincidenten creëert, is goedkeuring van het hoger management noodzakelijk. Een duidelijke afbakening van de uit te lokken incidenten is ook nodig. Sommige onderdelen zijn gewoonweg 'off limits' en in ons geval hebben we er voor gekozen om niet aan persoonlijke bezittingen te komen. Voor de mystery guest blijft er genoeg over, zoals zich voordoen als een ander, dossiers meenemen of applicaties gebruiken. Iemand die echt kwaad wil, zal zich ook niet aan regels houden.

Het bezoek van een mystery guest kan echter niet op zichzelf staan. Om ervan te kunnen leren is het noodzakelijk terugkoppeling te geven aan de medewerkers. De awarenesscampagne zag er als volgt uit:

- Online-peiling: Hoe groot is de interesse voor het onderwerp? En waar denkt men dan aan? Deze online-peiling vond in ons geval vlak voor de zomerperiode plaats. Ondanks deze ongelukkige timing kwam er toch veel respons. Ruim 40 procent van de medewerkers heeft gereageerd. Dat was een mooie start voor de awarenesscampagne;
- Interviews: In ieder bedrijf zijn er sleutelfiguren. Dit zijn medewerkers, die invloed kunnen uitoefenen. Wat weten sleutelfiguren al? Ook nu weer een behoorlijke deelname. De resultaten uit de online-peiling werden bevestigd. Bovendien kwamen er al concrete tips en hints naar boven;
- Eerste Mystery Guest-actie: De eerste actie was een soort vingeroefening met de vraagstelling: hoe weerbaar is de organisatie? Na deze eerste actie werd de medewerkers de gelegenheid geboden om tussentijds de stand van zaken te horen. Wij konden de organisatie vervolgens waarschuwen voor het volgende bezoek, waarbij we meteen concrete beveiligingstips mee konden geven. De term 'Mystery Guest' ging een eigen leven leiden en was bij verschillende informele bijeenkomsten al een geliefd gespreksonderwerp;

Toegangspasjes liggen verlaten op het bureau.

- Tweede Mystery Guest-actie: De tweede Mystery Guest-actie had als titel 'tegen de lamp lopen' meegekregen: hoe ver kan je gaan? Al gauw bleek, dat er geen verbetering in de weerbaarheid van de medewerkers zat. De Mystery Guest kon ongestoord zijn gang gaan, wat in sommige gevallen heel erg ver ging. Zo kwam hij op een afdeling waar een jarige medewerker trakteerde. Nadat de Mystery Guest zijn gebak had genomen en de jarige gefeliciteerd had, kon hij ongehinderd meerdere toegangspassen weghalen van verschillende bureaus. Het verdwijnen van meerdere toegangspassen maakte behoorlijk wat los: "wat we wel niet in ons hoofd haalden door zo'n actie uit te voeren?". Een beter voorbeeld om aan te tonen, hoe vervelend het is als je toegangspas verdwijnt, kun je je niet wensen;
- Terugkoppeling: Hebben we de interesse weten vast te houden? Wat hebben we met z'n allen ervan opgestoken? Helaas was de opkomst hierbij laag. Daar stond tegenover dat de aanwezige medewerkers erg betrokken waren en als ambassadeur voor awareness zouden gaan optreden binnen de organisatie.

Resultaten

Als de mystery guest eenmaal binnen is, dan ...
De grootste bescherming is de toegang tot het gebouw. Als de Mystery Guest eenmaal binnen is, dan kan hij overal bij. Bijzonder confronterend, maar wel realiteit.

Medewerker is al redelijk aware maar onzeker
De medewerker weet in principe waar het om gaat bij informatiebeveiliging. Hij is bereid een vreemdeling in de gebouwen aan te spreken. Hij moet alleen weten hoe hij moet ingrijpen en wat hij nog meer kan doen. Hoe concreter het beveiligingsbeleid is, des te eerder de medewerker ze ook zal opvolgen.

Men veronderstelt, dat het wel geregeld zal zijn
De medewerker vertrouwt er in veel gevallen op, dat beveiliging geregeld is. De medewerker gaat er gewoonweg van uit, dat niemand bij zijn gegevens kan of dat de bewaking ongewenste gasten tegenhoudt. Helaas gaan die veronderstellingen in werkelijkheid niet altijd op. Aan de andere kant doet de beveiliger ook veronderstellingen over de medewerker die niet altijd kloppen. Zo kan de beveiliger bijvoorbeeld aannemen, dat de medewerker exact kan aangeven wat gevoelige informatie is. Dat blijkt niet altijd het geval te zijn.

Er zijn (nog) geen harde kengetallen beschikbaar, waaraan we kunnen afmeten of de medewerker meer awareness toont. Het effect van de awarenesscampagne zien we terug aan de grotere naamsbekendheid van de eigen beveiligingsorganisatie. Meer medewerkers en managers melden incidenten en komen voor security adviezen. We zien ook een lichte toename in gerichte risico-analyses.

Eindhoven

De stad Eindhoven is met haar ruim 210.000 inwoners de vijfde stad van Nederland. Bij de gemeente werken ruim 2000 medewerkers. De gemeente kent naast het bestuur, dat bestaat uit de gemeenteraad, het college van burgemeester en wethouders en de burgemeester, een ambtelijke organisatie bestaande uit 24 sectoren. De Directieraad stuurt die 24 sectoren aan via sectorhoofden. De gemeente streeft continu naar het verbeteren van haar dienstverlening en bedrijfsvoering. De leden van directieraad en de sectorhoofden zijn verantwoordelijk voor de bedrijfsvoering, de beleidsontwikkeling en de uitvoering van beleid van de eigen dienst.

Een van die sectoren is Informatisering & Beheer. Zij is als sector verantwoordelijk voor alles wat met informatiemanagement te maken heeft. Zo voert deze sector niet alleen het functioneel en technisch beheer van ruim 1700 werkplekken verspreid over 24 locaties, maar realiseert ook I&A-projecten. Het opzetten van een gemeentebrede beveiligingsorganisatie is zo'n project, dat de naam IB-Cirkel (InformatieBeveiligingsCirkel) heeft meegekregen. De projectleider van de IB-Cirkel is ir. J.P. (Joe) Stijnen CISA. Hij is in de afgelopen tien jaar binnen de verschillende sectoren werkzaam geweest en heeft diverse functies vervuld. Sinds 2005 voert hij opdrachten uit op het gebied van informatiebeveiliging.

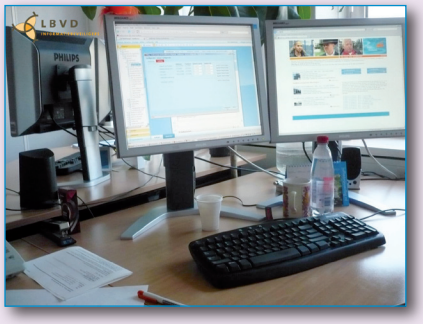
De leverancier
LBVD Informatiebeveiligers is de leverancier van de bovengenoemde diensten Online IB-peiling en Mystery-Guest.
LBVD biedt haar diensten op het gebied van informatiebeveiliging aan langs drie lijnen:
- organisatie-onderzoek;
- communicatie en awareness;
- ICT-security.

Uiteindelijk steekt de beveiliger er ook veel van op
Ook al is een awarenesscampagne en het bezoek van een mystery guest gericht op de gebruikersorganisatie, de beveiliger steekt er zelf het meeste van op.

Allereerst verwerft de beveiliger direct inzicht in het beveiligingsbewustzijn van de medewerkers. Hoe goed kennen zij de risico's van het digitale werken? In hoeverre weten zij wat zij moeten doen als het misgaat? Hoe groot is de weerbaarheid tegen ongewenste indringers?

Verder verwerft de beveiliger ook inzicht in welke beveiligingsonderwerpen de medewerkers het meeste bezighouden. Hij ziet onmiddellijk waar behoefte is aan zijn deskundigheid. Als medewerkers bijvoorbeeld de regels voor veilig telewerken onduidelijk vinden, kan de beveiliger deze verhelderen.

Maar bovenal ontdekt de beveiliger waar zijn blinde vlekken zitten. Dat zijn de onderwerpen waarvan de medewerker zegt: "maar dat is



De mystery guest kan zo aan het werk.

toch allang geregeld?". Zo leeft bijvoorbeeld de beveiliger in de veronderstelling dat de manager duidelijk aangeeft welke autorisaties gewijzigd moeten worden als de medewerker van functie verandert. De manager daarentegen gaat ervan uit dat dit een standaard onderdeel is van de organisatiewijziging en kijkt er verder niet naar om. Op het moment dat hij erop aangesproken wordt, is zijn (begrijpelijke) reactie: "maar dat hebben jullie toch allang geregeld?". De beveiliger kan er dus niet vanuit gaan dat de lijnorganisatie net zoveel met informatiebeveiliging bezig is als hijzelf. Hij zal voortdurend initiatieven moeten nemen om risico's en beveiligingsmaatregelen onder de aandacht te brengen bij diegenen die daarvoor verantwoordelijk zijn.

Samenvatting
Je wilt als beveiliger dat awareness in de organisatie ingebakken zit. Je wilt dat medewerkers informatie als hun belangrijkste bezit behandelen. Als er zich een beveiligingsincident voordoet, wil je dat zij automatisch kunnen handelen, omdat zij weten wat er van hen verwacht wordt. Een goed georganiseerde campagne blijkt niet alleen een goeie stap in de juiste awarenessrichting te zijn, de beveiliger kan er zelf ook iets van opsteken.

Boekbespreking

Reviewer: Ronald van Erven > Ronald van Erven MSc. RE CISSP is information risk officer bij de Grafische Bedrijfsfondsen (www.gbf.nl). Hij is sinds 2002 actief betrokken bij de PvIB. U kunt hem benaderen via ronald.vanerven@pvib.nl

Foundations of Information Security (Based on ISO27001 and ISO27002)
Auteurs: Julie Hintzbergen, Kees Hintzbergen, Andre Smulders, Hans Baars
Uitgeverij: Van Haren Publishing (www.vanharen.net)
ISBN: 978-908753-568-1
Vorm: Engels, 150 pagina's

Uit de serie 'best practice' brengt uitgeverij Van Haren Publishing het boekje 'Foundations of Information Security' uit.

De eerste vijf hoofdstukken geven een uigebreide introductie over definities, architectuur denken, security management, het doen van risicoanalyses en ten slotte het selecteren van maatregelen. In de introductie wordt ook het bedrijf 'Springbooks - an international bookstore' geïntroduceerd. Dit bedrijf wordt door het hele boek heen gebruikt als casus.
Het bedrijfje begint klein als een eenvoudige boekhandel en groeit uit naar een bedrijf met 129 vestigingen en een webshop. Het boek gaat in op de risico's en bedreigingen die op dit bedrijf van toepassing zijn.

Vanaf hoofdstuk zes volgt het boek duidelijk de ISO27001 en de toepassing op de casus:

6. bedrijfsgoederen en informatiebeveiligingsincidenten;
7. fysieke maatregelen;
8. technische (ICT) maatregelen;
9. organisatorische maatregelen;
10. beheer van ICT-processen;
11. naleving en juridische eisen.

Het boek sluit af met examenvragen, en antwoorden (met uitleg) voor het information security foundationsexamen.

Het boek is erg duidelijk geschreven en is goed als begeleiding om de ISO27001 en ISO27002 standaarden te leren begrijpen en te implementeren.

Inloggen en ondertekenen met je mobiel

Mobile PKI

Martijn Oostdijk Maarten Wegdam Roland van Rijswijk Joost van Dijk

Auteurs: Martijn Oostdijk > Martijn Oostdijk is onderzoeker in de Human Centric Services afdeling van Novay. Zijn werk richt zich op Identity & Trust. Martijn combineert een achtergrond in harde security met een brede interesse in beveiligings- en digitale identiteitsvraagstukken. Hij werkte eerder in de security groep aan de Radboud Universiteit Nijmegen en bij smart card security lab Riscure. Martijn is bereikbaar via martijn.oostdijk@novay.nl

Maarten Wegdam > Maarten Wegdam is een onderzoeker, ICT architect, consultant en project manager voor innovatieve ICT projecten. Sinds 2008 werkt Maarten voor Novay (voorheen Telematica Instituut), in the Human Centric Services afdeling. Hij is ook Operations Manager van deze afdeling. Voordat hij bij Novay ging werken, werkte Maarten in industrie R&D afdelingen (KPN Research, Bell Labs). Maarten is verbonden aan de Informatica afdeling van de Universiteit Twente (Information Systems group). Bij Novay coördineert Maarten de activiteiten op het gebied van identity, privacy en trust (online vertrouwen). Maarten is bereikbaar via maarten.wegdam@novay.nl

Roland van Rijswijk > Roland van Rijswijk werkt sinds 2008 als technisch product manager bij SURFnet. Hier houdt hij zich bezig met ontwikkeling van innovatieve diensten op het gebied van security, netwerk middleware en identity management. Hij heeft een achtergrond in high-end security en werkte eerder voor InTraffic, AET Europe en Philips. Roland is bereikbaar via roland.vanrijswijk@surfnet.nl

Joost van Dijk > Joost van Dijk werkt als technisch product manager bij de afdeling Middleware Services van SURFnet aan innovatie van diensten op het gebied van federatief identity management en PKI. Voorheen werkte hij bij TUNIX, als consultant voor diverse organisaties, het SERC, en de vakgroep Informatica van de Universiteit Utrecht. Joost is bereikbaar via joost.vandijk@surfnet.nl

Elke mobiele telefoon bevat een simkaart. Op deze sim kunnen veilige toepassingen worden geïnstalleerd die helpen bij inloggen op websites en bij het ondertekenen van documenten. De onderliggende technologie hiervoor heet Mobile PKI. Gecombineerd met het feit dat 'iedereen' een mobiel heeft en die vrijwel altijd bij zich heeft, maakt Mobile PKI een interessante kandidaat voor veilige authenticatie en digitale ondertekening. Novay heeft in samenwerking met SURFnet een studie gedaan naar Mobile PKI . Is Mobile PKI inderdaad de 'killer' applicatie die van de mobiele telefoon een zogenaamd Secure Signature Creation Device maakt dat geschikt is om door grote groepen mensen gebruikt te worden? En zo ja, waarom gebruiken we dit anno 2010 in het hoger onderwijs nog niet?

Traditionele PKI (Public Key Infrastructure) bestaat al geruime tijd en is met behulp van smart tokens of smart cards behoorlijk veilig te maken. Toch wordt PKI maar zeer beperkt ingezet, namelijk alleen in zakelijke omgevingen en voornamelijk voor diensten binnen de eigen organisatie. Voor consumenten van e-diensten is PKI al snel te ingewikkeld (certificaten installeren, hardware, drivers). En gebruikersnaam en wachtwoord waren voor veel toepassingen eigenlijk ook wel goed genoeg.

Mobile PKI

Een simkaart wordt door de mobiele operator primair gebruikt om de gebruiker te identificeren en te authenticeren op het mobiele netwerk. De simkaart biedt echter meer mogelijkheden. Zo kunnen op de nieuwste generatie sims op een veilige manier door de mobiele operator applicaties worden geïnstalleerd. Deze kunnen vervolgens worden gebruikt voor online authenticatie en digitale handtekeningen. Gebruikte termen hiervoor zijn Mobile PKI of Wireless PKI.

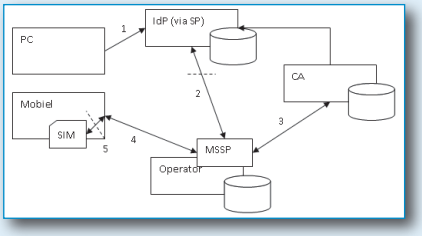


Fig. 1. Technisch architectuuroverzicht van Mobile PKI. Centraal staat de Mobile Signature Service Provider (MSSP), het back-end systeem bij de mobiele operator. Andere mogelijke rollen worden gespeeld door de Identity Provider (IdP), de Service Provider (SP) en een externe Certificate Authority (CA).

Mobile PKI werkt op basis van versleutelde smsjes, waarbij de gebruiker toestemming geeft voor authenticatie of digitale handtekening via de mobiele telefoon, beveiligd door een pincode die, typisch, per transactie opnieuw moet worden ingetoetst. De gebruikte standaarden op de mobiele telefoon bestaan al vrij lang (al sinds 2001), en werken op alle telefoons. Voordelen ten opzichte van sommige andere veilige authenticatiemiddelen zijn dat er geen aparte authenticatiedevice nodig is, en dat er bij de eindgebruiker geen installatie van software nodig is. Niet op de telefoon en niet op andere client devices zoals een pc. Ook hoeven er tijdens een transactie geen codes overgetikt te worden, zoals bijvoorbeeld bij sms one-time-passwords, wat de gebruiksvriendelijkheid ten goede komt. Eventueel op de pc draaiende malware zoals virussen of keyloggers hebben geen invloed op Mobile PKI.

Inloggen met mobile PKI

In een typisch gebruiksscenario doet de gebruiker vanachter de pc een poging om in te loggen bij een onlinedienst.

1. De gebruiker meldt zich via de pc met een gebruikersnaam bij de dienst.

2. De dienst verstuurt via sms een bericht met transactiedetails naar de mobiele telefoon. Dit bericht wordt afgevangen door de sim. De gebruiker merkt hier niets van.
3. De sim toont het bericht op het scherm van de mobiele telefoon. Er hoeven geen menu's doorlopen te worden om een berichtenbox te openen. De gebruiker bevestigt dit bericht door op 'oké' te drukken.
4. Hierna moet de gebruiker een pin invoeren, deze is gebonden aan de sim. De pin wordt lokaal door de sim gecontroleerd.
5. De sim stuurt nu een aantal sms-berichten, wederom zonder dat de gebruiker hier iets van merkt.
6. De gebruiker heeft zich nu succesvol geauthenticeerd en ontvangt ter informatie nog een bevestigingsbericht per sms in zijn berichtenbox.

Vanuit het gezichtspunt van een gebruiker is de interactie minimaal. De mobiele telefoon laat, schijnbaar uit zichzelf, de transactiedetails zien en vraagt om een pincode die door de gebruiker zelf is ingesteld.

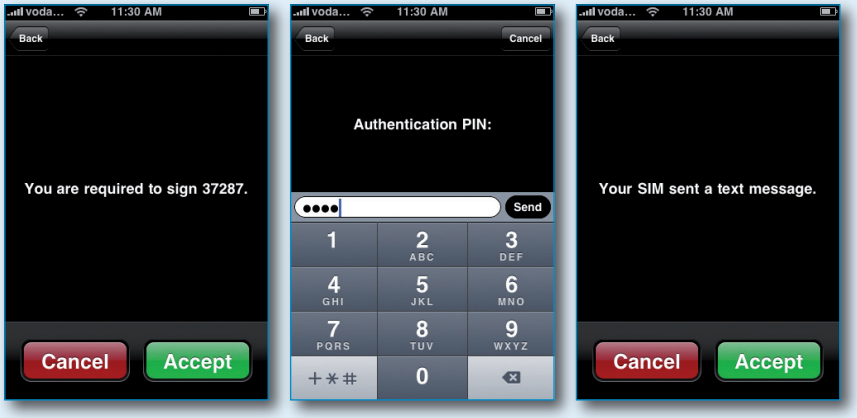


Fig. 2. Screenshots van een voorbeeld authenticatietransactie. De transactiedetails, hier vrij summier, kunnen bij een ondertekentransactie veel uitgebreider zijn. De te gebruiken pin is steeds dezelfde, door de gebruiker ingestelde, code.

Ondertekenen met mobile PKI

Ondertekenen van documenten geschiedt op vergelijkbare wijze.

1. De gebruiker, reeds aangemeld bij de dienst, geeft aan een document te willen ondertekenen.
2. De dienst verstuurt via sms een bericht met documentdetails naar de mobiele telefoon. Dit bericht wordt afgevangen door de sim. De gebruiker merkt hier niets van.
3. De sim toont een fragment van het document op het scherm van de mobiele telefoon, ongeacht wat de gebruiker op dat moment aan het doen is. Er hoeven geen menu's doorlopen te worden om een berichtenbox te openen. De gebruiker bevestigt dit bericht door op 'oké' te drukken.
4. Hierna moet de gebruiker een pin invoeren, deze is gebonden aan de sim. De pin wordt lokaal door de sim gecontroleerd.
5. De sim stuurt nu een aantal sms-berichten, wederom zonder dat de gebruiker hier iets van merkt.
6. De gebruiker heeft zich nu succesvol geauthenticeerd en ontvangt, ter informatie, nog een bevestigingsbericht per sms in zijn berichtenbox.

De gelijkenis met het authenticatiescenario is geen toeval. Authenticatie ten behoeve van inloggen bij een dienst is namelijk een bijzonder geval van ondertekening. Ondertekenen van documenten op de lokale pc van de gebruiker kan ook, maar dan moet er wel speciale software op de pc worden geïnstalleerd.

Hoe veilig is mobile PKI?

Mobile PKI is aan een scala van gestandaardiseerde veiligheidscontroles onderworpen. Verschillende implementaties zijn Common Criteria geëvalueerd op EAL4+ niveau. Daarnaast bevat de ETSI-standaard een uitgebreide checklist waaraan implementaties moeten voldoen.

Op de nieuwste generatie sims kan op een veilige manier applicaties worden geïnstalleerd

In de security-analyse die Novay voor SURFnet uitvoerde, kwamen als belangrijkste dreiging 'Man-in-the-Middle'- attacks naar voren. Deze zouden door (kwaadwillende insiders bij) dienstverleners of door geïnstalleerde malware op de pc van de gebruiker kunnen worden uitgevoerd. Deze aanvallen zijn echter door een goed oplettende gebruiker te herkennen, maar dan moeten de getoonde authentieke transactieberichten goed herkenbaar zijn en daadwerkelijk gelezen worden door de gebruiker. Voor het inloggen bij een dienst biedt de grafische gebruikersinterface van een mobiele telefoon hiertoe voldoende mogelijkheden. Voor het ondertekenen van documenten heeft ook Mobile PKI last van het klassieke what-you-see-is-what-you-sign-dilemma. Het kleine scherm van een mobiele telefoon kan niet het hele te ondertekenen document weergeven.

In vergelijking met andere authenticatiemiddelen is Mobile PKI zeer veilig te noemen (zie ook de 'vergelijking met andere oplossingen' iets verderop in dit artikel).

Waarom is mobile PKI nog niet overal ingevoerd?

De standaarden die Mobile PKI mogelijk maken bestaan al sinds 2001, en in ICT-tijd is dat een eeuwigheid. Toch worden voor de meeste toepassingen andere authenticatie- of ondertekenmiddelen gebruikt.

De laatste jaren (2007 - 2009) is er wel wat beweging geconstateerd. Veel pilots zijn uitgevoerd of aangekondigd. Mobile PKI is ook reeds in gebruik genomen voor diensten voor banken, bijvoorbeeld in Turkije, Scandinavië en de Baltische staten. De voornaamste leveranciers van Mobile PKI hebben partnerships met alle grote simkaartfabrikanten en veel Europese mobiele operators.

Aan de simkaart worden wel wat eisen gesteld (qua geheugen en cryptografische rekenkracht) en mobiele operators zullen pas beginnen met het uitgeven van Mobile PKI - ready simkaarten als daar voldoende (markt)vraag naar is. De belangrijkste redenen voor langzame adaptatie van Mobile PKI-technologie lijken echter niet van technologische of veiligheidsaard, maar gaan meer over de kosten en het businessmodel. Mobile PKI-technologie wordt op dit moment alleen nog voor beperkte pilots ingezet in Nederland, dus de kosten zijn nog moeilijk in te schatten. Maar deze zouden, zolang er geen andere grootschalige

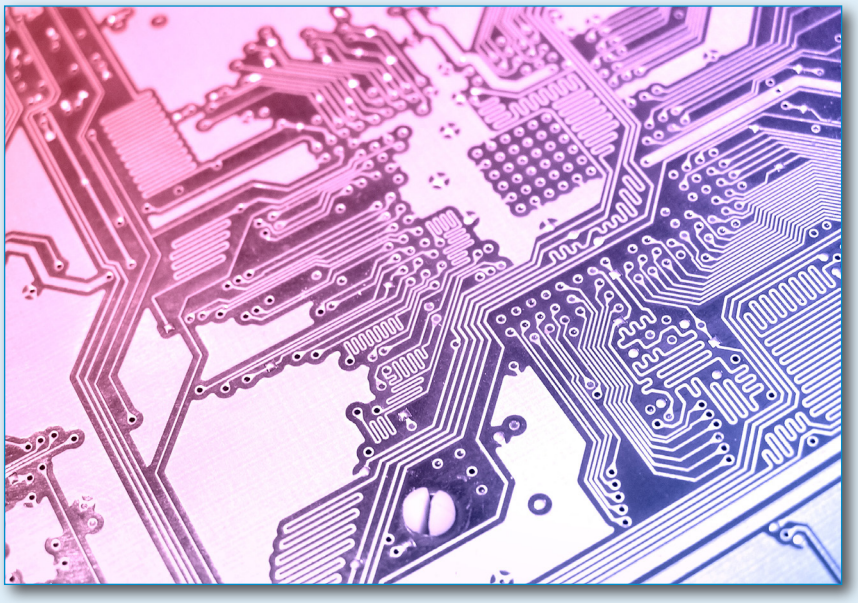
toepassing voor Mobile PKI is, voor veel toepassingen wel eens te hoog kunnen liggen. Gerelateerd hieraan is het businessmodel voor de mobiele operators. Aangezien de simkaart eigendom is van de mobiele operator, kan deze technologie alleen worden gebruikt met medewerking van de operator. Bij grootschalig gebruik betekent dit ook dat alle operators moeten meewerken. Daarbovenop komt nog dat het op grote schaal vervangen van de huidige generatie eenvoudige simkaarten door een nieuwe generatie simkaarten (een zogenaamde sim swap) een kostbare operatie is waaraan een mobiele operator niet zomaar begint als het verdienmodel niet helder is.

In vergelijking met andere authenticatiemiddelen is Mobile PKI zeer veilig te noemen

Vergelijking met andere oplossingen

De vraag dient zich aan hoe Mobile PKI zich laat vergelijken met andere oplossingen. Wat zijn de Unique Selling Points van Mobile PKI? In deze vergelijking wordt aangenomen dat Mobile PKI wordt ingezet als authenticatiemiddel voor het inloggen via een pc bij een dienstverlener.

- Mobile PKI gebruikt een 'something you have'-token, namelijk de simkaart in de mobiele telefoon. Daardoor sluit de oplossing vele problemen uit die bijvoorbeeld eenvoudige *gebruikersnaam/wachtwoord*-authenticatie wel heeft. Phishingaanvallen behoren bijvoorbeeld tot het verleden.
- Een *TAN-lijst* (TAN = Transaction Number) vormt ook een 'something you have'-token. Mobile PKI heeft op het vlak van gebruiksgemak voordelen omdat de mobiele telefoon door veel gebruikers vaker wordt meegedragen dan een lijst met TAN-codes. Bovendien kunnen TAN-codes niet gebruikt worden om berichten te ondertekenen.
- Een *SMS-OTP* (OTP = One Time Password) oplossing vormt ook een 'something you have'-token. Mobile PKI heeft als voordeel dat geen code overgetypt hoeft te worden op de pc. De pincode is steeds dezelfde. Bovendien kan SMS-OTP niet worden gebruikt om berichten te ondertekenen.
- Een niet-aangesloten *'OTP token met display'* (of vergelijkbaar een bankcalculator) vereist ook dat een code wordt overgetypt. En de gebruiker kan zo'n token vergeten terwijl hij zijn mobiele telefoon doorgaans wel altijd bij zich draagt. Bovendien kan een OTP-token niet worden gebruikt om berichten te ondertekenen.
- Ook een USB-PKI-token of PKI-smartcard zal door de gebruiker vaker vergeten worden dan een mobiele telefoon. Bovendien vereist deze soms pincode-invoer via een onvertrouwd pc-toetsenbord (denk aan keyloggers en andere malware), en vereist deze geïnstalleerde hardware (een kaartlezer) en/of software (drivers, middleware).
- Een voordeel van Mobile PKI boven andere oplossingen is dat moderne sims zogenaamde 'over-the-air'-updates ondersteunen. Dit maakt allerlei flexibele migratiepaden mogelijk, bijvoorbeeld van niet-gekwalificeerde certificaten naar gekwalificeerde certificaten.
- Een nadeel van Mobile PKI (gedeeld met sms-OTP) is de afhankelijkheid van het mobiele netwerk. Als sms-berichten vertraagd, of helemaal niet aankomen kan opeens niet meer worden ingelogd of ondertekend.



Conclusie

Mobile PKI heeft een aantal indrukwekkende voordelen op het gebied van beveiliging en gebruiksvriendelijkheid ten opzichte van andere oplossingen. Mobile PKI combineert de veiligheid van de sim met de relatief vriendelijke gebruikersinterface van de mobiele telefoon. Een apparaat dat door de meeste gebruikers gekoesterd en altijd bij hen wordt gedragen.

De afhankelijkheid van de mobiele operator is echter een zwakte van Mobile PKI. Invoeren van Mobile PKI voor een dienst kan alleen als wordt samengewerkt met een mobiele operator. Een heterogene groep gebruikers (met abonnementen bij verschillende mobiele operators) kan dus alleen gebruik gaan maken van Mobile PKI als alle mobiele operators meedoen. Voor de mobiele operators is nog niet helemaal duidelijk of er genoeg diensten zijn om de voordelen van Mobile PKI op te laten wegen tegen de hoge kosten van nieuwe simkaarten.

We verwachten echter dat Mobile PKI als veilig authenticatiemiddel op den duur breed gebruikt kan worden. Voor de kortere termijn zal Mobile PKI alleen worden ingezet voor diensten die door beperkte groepen werknemers worden gebruikt en bovendien hoge veiligheidseisen hebben.

Het rapport dat Novay voor SURFnet schreef ging over de toepassing van Mobile PKI in de SURFfederatie. Voor uitrol naar studenten en algemene authenticatie voor de SURFfederatie lijkt de tijd nog wat vroeg. In de tussentijd kan wel overwogen worden sms-OTP meer te gaan gebruiken voor step-up-authenticatie of password reset via sms omdat dit goedkoper is en gebruikers klaarstoomt voor Mobile PKI. Dit geldt niet alleen voor studenten en medewerkers in het hoger onderwijs (de doelgroep van SURFnet), maar ook voor alle toepassingen waarbij de gebruikers consumenten zijn.

Verslag ISACA's EuroCACS Conference

Auteur: Tom Bakker > Tom Bakker is lid van de redactieraad van Informatiebeveiliging en te bereiken via tom_bakker@deltalloyd.nl

De jaarlijkse EuroCACS van ISACA werd van 22 tot en met 24 maart 2010 gehouden in het mooie Boedapest. Het was prachtig lenteweer. Er waren ongeveer 275 deelnemers uit 47 landen. Nederland was met 23 deelnemers redelijk vertegenwoordigd.

Op de zaterdag en zondag voorafgaand aan de conferentie en de donderdag en vrijdag na de conferentie kon men eventueel deelnemen aan een flink aantal workshops. Het

'Special Evening Event' in de vorm van een dinerbuffet werd gehouden in het Hungarian Railway Museum. Aparte ambiance zo tussen de klassieke wagons en een bijpassend Hongaars orkestje.

De conferentie zelf bestond uit vier streams met break-out presentaties over:

1. IT governance;
2. IT audit and assurance;
3. Information security management;
4. Compliance and IT risk management.

De conferentie werd geopend door de international vice president van ISACA, Rolf von Roessing. Daar werden ondermeer mensen naar voren gehaald die wereldwijd de hoogste scores hebben behaald voor de CISA-, CISM- en CGEIT-examens.
De conferentie had een key-note spreker als eerste spreker van de conferentie. Deze spreker was minder van belang voor informatiebeveiliging.
Een paar impressies en samenvattingen van presentaties die betrekking hadden op informatiebeveiliging:

Security in the Cloud - Mike Small, UK
'Security in the cloud' is een populair onderwerp. De zaal was aardig vol. De spreker ging eerst in op wat algemene zaken rond clouds. Ook het ENISA-rapport werd aanbevolen. Uiteindelijk kwam er een lijst met tien security gerelateerde vragen die je zou moeten stellen aan je (beoogde) cloudprovider.

Compliance Means Never Having to Say You're Sorry - Marne Gordan (IBM Tivoli, USA)
Spreekster gaf een overzicht met praktijkvoorbeelden van reputatieschade (brand damage) en wat de rol van het compliant zijn daarin betekend heeft. Compliant zijn wil niet zeggen dat security-incidenten niet meer zullen voorkomen maar wel hoe effectief men die incidenten aanpakt en wat men er van leert.

Scenario-based IT Risk Assessment and Management - Peter R. Bitterli (Bitterli consulting, Zwitserland)
De spreker begon met de stelling dat de vele regelgevingen met operational riskeisen hebben geleid tot een 'explosie' van tools en methodieken die een effectief risk management zouden moeten garanderen. Met als gevolg dat de kennis en ervaring van getrainde mensen zijn vervangen door het volgen van een mechanische aanpak afgedwongen door een onpersoonlijk en inflexibele tool die nauwelijks geschikt is voor de specifieke IT-(security)issues. Daarom hield de spreker een pleidooi voor een andere aanpak van risk assessments, namelijk Scenario Based Risk Assessment. Deze aanpak maakt het mogelijk dat een team van (IT)professionals een consistente behandeling van risico's kan uitvoeren. Daarbij gebruikmakend van de ervaring van interne resources die verzameld zijn door middel van gestructureerde maar ook creatieve workshops met een aantoonbaar volwassen risk managementproces. Daarna kwam een vrij lange uitleg over de basisprincipes van riskmanagement, wat al die

methodieken gemeen hebben. Zowel een bottum-up- als topdownaanpak hebben voor- en nadelen. Vervolgens de stap naar scenario based risk assessments. De methode volgt een topdownbenadering om te komen tot een high level-overzicht van de risicosituatie zonder een compleet gedetailleerde studie. Je komt dan op twintig top risico's. De methode maakt gebruik van reeds beschikbare gegevens van onderkende zwakheden, incidenten, bevindingen van audits en reviews en ook de kennis en verbeeldingskracht van ervaren (IT)security-specialisten. Binnen het Scenario Based Risk Assessment worden alleen toegesneden en redelijke risico´s geëvalueerd waarbij de reeds genomen maatregelen meegenomen worden. Hoe weet je of je volledig bent met je scenario´s? Allereerst komen de realistische scenario's uit de workshops, specifiek voor het bedrijf. Daarna kunnen externe bronnen geraadpleegd worden, zoals de BSI Grundschutzhandbuch Threat list, CobIT, ISO 27001/2 enz. Maar ook regionale bronnen (gemeentes) voor overstromingen, aardbevingen, transportroutes (trein, vliegtuig) enz. De spreker ging daarna uitvoerig in hoe je zoiets moet aanpakken (er waren totaal 96 slides!). Ook rollen en verantwoordelijkheden binnen scenario based risk management kwamen uitvoerig aan de orde, Van essentieel belang is nog dat men niet de aansluiting moet vergeten met de reeds bestaande operational risk managementactiviteiten binnen een organisatie.

Establishing the Information Security Culture - Vernon Poole (Sapphire,UK)

De spreker begon met een uitleg over het BMIS-model. Business Model for Information Security. BMIS is bedoeld om de complexiteit van Information Security in kaart te brengen en om te zorgen voor een balans tussen business en beveiliging. Elementen uit het model zijn: organisatieontwerp en strategie, mensen, processen en technologie. Tussen deze statische elementen bestaan dynamische relaties. Tussen de elementen 'organisatie en mensen' heet dit cultuur. Wat zijn de uitdagingen? Ondanks de security awarenessprogramma's neemt het aantal incidenten toe waarbij menselijk falen de oorzaak is. Mensen ontwijken controls, verliezen mobiele data zoals USB-sticks, zijn niet bewust hoe om te gaan met belangrijke informatieassets. Er zijn vele definities voor cultuur maar BMIS houdt het op gedragspatronen, geloof, houding, veronderstellingen en normen. Na een uitgebreid betoog hoe belangrijk (bedrijfs)cultuur is kwam de spreker met zes aspecten van cultuur die van belang zijn voor information security. Regels en normen, tolerantie voor regels (niet te rigide), machtsafstand, beleefdheidsfactor, context en collectiviteit versus individu. Aan het eind gaf de spreker aan hoe je een security-cultuur creëert in acht stappen waarbij een pleidooi werd gehouden voor het gebruik van een Personal Information Security Policy wat een beetje neerkomt op bedrijfsgedragsregels (bijvoorbeeld e-mail- en internetgebruik, gebruik van social media).

The Compliant Cloud - Marne Gordan (IBM Tivoli, USA)

Net als eerder Mike Small ging de spreekster ook in op de algemene definities, principes en risico's van clouds. Zij refereerde aan een IBM-enquête onder 1090 IT- en linemanagers over cloudadoptie (IBM Market Insights, Cloud Computing Research, July 2009). Zorgen om security en privacy zijn de grootste drempels voor de adoptie van public clouds. De spreekster introduceert het begrip Cloud Compliance. Dat wil zeggen compliant met een aantal factoren zoals Data Protection, Identity and access maar ook Cross Border Protection en Intellectual Property and Export Laws. Er werd nader ingegaan op elk van die factoren waarbij ook voorbeelden werden getoond waar het mis ging. Ook hier ten slotte de factoren samengevat in een top 10 voor een secure en compliant cloud infrastructuur.

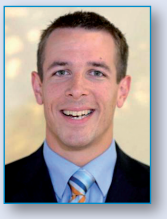
Fridges to the Eskimo's: Selling Information Security to Your Marketing Department - Wendy Goucher (Idrach, UK)

De inhoud van deze presentatie kunt u uitgebreid vinden in een apart artikel in nummer 3, 2010 van dit blad onder de titel: In Marketing Shoes. Waar het op neer komt is dat wanneer je marketingmensen aan je zijde krijgt, het leven als security professional een stuk gemakkelijker wordt. Communicatie is hierbij essentieel.

Het was weer een leerzame en goed verzorgde conferentie. Er werd mij ingefluisterd dat men alleen sprekers had geselecteerd en uitgenodigd die in voorgaande conferenties een hoge score hadden behaald. Het zou best waar kunnen zijn want de kwaliteit was hoog hoewel er natuurlijk toch ook uitzonderingen waren.

De volgende EuroCACS staat gepland voor 20-23 maart 2011 in Manchester, UK. Voor de liefhebbers is er in november weer de ISACA Information Security and Risk Management Conference. Vorig jaar in Amsterdam, nu in Wenen.

Expertbriefsessie Access Management



Auteur: Jan-Roel Löwenthal CISSP > Drs.ing. Jan-Roel Löwenthal CISSP is managing consultant IT governance strategy en thoughtleader identity & access management binnen Capgemini Nederland B.V. Zijn speerpunten zijn informatiebeveiliging, informatie(voorziening)management en enterprise architectuur. Binnen de PvIB-expertgroep access management is hij twee keer co-facilitator geweest en de afgelopen bijeenkomst in de rol van facilitator. Jan-Roel is bereikbaar via janroel.lowenthal@capgemini.com.

Access management is complex. Het raakt immers alle medewerkers in de hele organisatie op het gebied van logische toegangsbeveiliging. Steeds meer bedrijven buigen zich over identity en access managementvraagstukken. Deze vraagstukken zijn in essentie vaak dezelfde, alleen verschillen de bedrijfssituaties en daardoor de oplossingsrichtingen. Er zijn in de afgelopen jaren al heel wat goede artikelen verschenen over Access Management in bijvoorbeeld dit blad. Je kunt daaruit ook zien dat het vakgebied volwassen wordt en dat niet meer alleen wordt gekeken naar role based access control.

De scope van deze expertbrieven richt zich op access management. Identity management is buiten scope. Beiden kunnen echter niet zonder elkaar, waardoor het maken van scheiding lastig is. We besteden dus geen aandacht aan identificatie- en authenticatie-oplossingen, beheer en controle op smart-card-oplossingen, SSO-oplossingen en mechanismes om te controleren of 'je bent wie je zegt dat je bent'.

Access management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van systemen en informatie te faciliteren, beheren en controleren. Access management betreft het regelen van de toegang van een subject (bijvoorbeeld een medewerker, systeem, service, enz.) tot data of het mogen gebruiken van een service. In beide gevallen moet worden vastgesteld of de betreffende subject het recht heeft om bij de databron te komen (de resource mag de data inzien of muteren) of de service te gebruiken (bijvoorbeeld: licentie is voor de resource beschikbaar). In een enterprise-omgeving gaat het hierbij om veel rechtenverstrekkingen en de controle daarop (schaalgrote). Daarom loont het om de uitvoering ervan efficiënt in te richten door middel van helder beleid, strakke processen, juiste bemensing, correcte administraties en goede hulpmiddelen.

De expertbrief heeft tot doel een hulpmiddel te zijn bij het implementeren of verbeteren van een access management organisatiestructuur en beheeromgeving. De expertbrief formuleert per onderwerp aandachtspunten waarvan de lezer zelf kan beoordelen of deze in zijn situatie van toepassing zijn en hoe deze in zijn situatie kunnen worden toegepast.

18 mei 2010 heeft de derde expertbriefsessie Access Management plaatsgevonden

Om van het hele vakgebied toch een beeld te kunnen weergeven in expertbrieven, is het onderwerp door een kernteam in vier hoofdgebieden opgesplitst die ieder worden uitgewerkt in een expertbrief. De vier hoofdgebieden behelzen het navolgende.

1. Visie: het eerste onderdeel betreft het vormen van een visie over het daadwerkelijk bestaan van één ideaal access managementconcept. Start een ideaal concept met het hebben van concreet beleid en wat die moet die beschrijven? Het realiseren/implementeren van een compleet access managementconcept zal, als gevolg van kosten (businesscase) of complexiteit, niet altijd volledig of in een keer haalbaar zijn. Welke risico's worden onderkend die het succes van een implementatieproject kunnen tegenwerken?
2. Architectuur: in het tweede onderdeel wordt access management vanuit architectuur beschreven. Zowel contextueel, als de aspecten omtrent organisatie- en procesinrichting, autorisatiemodellering en techniek.
3. Projectmanagement: in het derde onderdeel zal worden beschreven hoe de implementatie kan worden gerealiseerd en welke werkwijzen en projectinrichtingen daarbij kunnen worden toegepast.
4. Beheer en gebruik: het vierde onderdeel richt zich op de operationele situatie. Het beantwoordt de vraag hoe een beheerorganisatie er concreet uit kan zien, welke ervaringen zijn opgedaan met beschikbare hulpmiddelen, enz. Ook kan, als gevolg van de activiteiten van de expertgroepen, de visie op access management zodanig zijn ontwikkeld dat de 'oude' PI-studie RBAC nader kan worden aangepast.

Via diverse media rondom het PvIB is aandacht gevraagd voor de aankomende expertbrieven en potentiële deelnemers konden zich laten registreren via de co-facilitator. Vanuit het kernteam werd bepaald dat er geen deelnemers vanuit leveranciers werden toegelaten om het beeld niet te kleuren (ondanks dat leveranciers vaak veel verstand hebben van het vakgebied en weten waar tegenaan gelopen wordt). Misschien zou het interessant kunnen zijn om leveranciers een expertbrief te laten opstellen, maar daar heeft het kernteam indertijd niet voor gekozen.

18 mei 2010 heeft de derde expertbrief-sessie Access Management plaatsgevonden op een satellietlocatie van Capgemini in Amsterdam. Vanuit mijn huidige rol als facilitator van de expertbrief wil ik u graag een keer meenemen in zo'n bijeenkomst. Het was geen typische bijeenkomst, maar wel leerzaam.

Het eerste gedeelte van de sessie hebben we als kernteam (Danny Mol als co-facilitator, Jean-Pierre Vincent als ghostwriter, Karin van de Kerkhof als probleemeigenaar en ikzelf als facilitator) gebruikt om met de aanwezige deelnemers terug te kijken en vooruit te kijken. Terug te kijken of de eerste twee Access Management-expertbriefsessies voldoende diepgang boden, de eindresultaten een representatie was van de sessies en of er een relatie/afhankelijkheid gewenst is tussen de expertbrieven. Vooruit te kijken in de zin of de avond wel besteed moet worden aan het onderwerp projecten, of dat de eerdere sessies meer diepgang moesten krijgen en of de vierde en eventueel vijfde bijeenkomst (toekomstige ontwikkelingen) gewenst waren.

Conclusie, zonder alle details, was dat de meerderheid vond dat de afgelopen sessies - gezien de tijd - voldoende diepgang hadden, het resultaat van de eerste twee expertbrieven gedragen wordt door de experts en dat de relatie/afhankelijkheid tussen de expertbrieven juist laat zien dat het een complex en breed onderwerp is. De eerste twee expertbrieven (visie en architectuur) waren wellicht iets te academisch geschreven, maar de algemene opvatting was dat dat ook te wijten is aan de aard van de onderwerpen. De volgende twee onderwerpen (project en beheer) kunnen en moeten iets meer prikkelend geschreven worden ten bate van de doelgroep. Ook werden er vraagtekens gezet bij de representatie van de sessie. De gele post-its die het resultaat waren van de sessie bevatten alleen steekwoorden maar de ghostwriter moest er een coherent verhaal van maken en had vanuit het kernteam 'kwaliteit' als criterium meegekregen. Op zich hoort een expertbrief een verslag te zijn van wat er in de sessie is besproken. De kwaliteit vond en vind iedereen echter ook een belangrijke issue en die werd als belangrijker gezien dan snelheid. Maar de snelheid mocht iets meer omhoog om onder andere de samenhang van de groep te borgen. Bij de eerste expertbrief werd teveel basismateriaal meegenomen die niet gefilterd was (complete ISO-normen en presentaties van meer dan honderd slides), bij de tweede was er geen materiaal meegenomen en voor deze derde sessie was de vraag vanuit het kernteam niet helder genoeg gesteld om 1 á 2 A4-tjes mee te nemen. Dus we begonnen de derde sessie ook weer zonder uitgangsmateriaal.

Nieuwe invulling van de expertbrieven

Ten bate van de vierde sessie (en vervolgsessies) is er zijdeling nagedacht over een nieuwe invulling van de expertbrieven. Dit is in het algemeen een zaak voor de professionaliseringscommissie, maar voor sessie vier gaan we de nieuwe opzet uitproberen. Het is een andere invulling van de, nog steeds dezelfde, fundamentele basis. Alleen willen we met moderne hulpmiddelen als collaboration tooling, het voorwerk wat meer aandacht geven, waardoor de discussies in de bijeenkomst extra aandacht hebben en we dieper in kunnen gaan op de verschillende meningen. Het kapstokdocument als entiteit gezien kan daarbij als een goede start dienen. Belangrijk uitgangspunt bij de discussie was dat voorkomen moet worden dat de meningen van de verschillende experts genivelleerd/afgevlakt worden tot een democratisch compromis. Juist de pieken/afwijkingen zijn interessant voor lezers van een expertbrief. Daarbij wel de argumentatie aangevend waarom er afwijkende meningen bestaan. De input van een sessie is dus een ruwe expertbrief met de input van de verschillende experts, eventueel met een eerste schifting van het kernteam. Het resultaat van de sessie is voor de ghostwriter eenvoudiger en sneller te verwerken, en hij hoeft minder zelf te 'verzinnen'. Daarnaast moet het kernteam (via de co-facilitator) strakker sturen op deadlines.
De vierde expertbrief wordt op deze nieuwe manier opgesteld. Als dit goed bevalt kunnen op dezelfde manier een eventuele vijfde en zo nodig een vernieuwing van de eerste twee brieven plaatsvinden. Er is vertrouwen in het nieuwe proces, maar de probleemeigenaar geeft (ik vind terecht) aan dat ze een actieve deelname verwacht bij de voorbereiding, anders heeft deelnemen geen zin. Het gaat er tenslotte om de verschillende meningen te bediscussiëren. Natuurlijk kan een ieder input leveren zonder deel te nemen aan de sessie. Daarvoor is het een openbare samenwerkingsomgeving en dat willen we ook stimuleren.

Uiteindelijk is ervoor gekozen om de derde expertsessie uit te voeren zonder geeltjes maar wel plenair. Daar leende de grootte van de groep zich ook voor (tien personen). Het kapstokdocument was een goede voorzet, maar het was te inconsistent. Na de aanpak voor het avondgedeelte te hebben besproken waren er wat problemen met de broodjes die door de catering vakkundig omgezet werden in een heerlijke warme maaltijd. Bij de maaltijd zelf werd er alvast druk doorgepraat over het onderwerp. In de sessie erna werd diep ingegaan op de vragen die de probleemeigenaar had geformuleerd. Daardoor werden niet alle vragen beantwoord, maar de plenaire aanpak werd zeer goed beoordeeld, ondanks dat het door het eerste gedeelte minder productief was. Het was volgens de deelnemers leuker en interactiever. En belangrijk vond ik ook dat er unaniem werd gesteld dat het interessanter was vanwege de nieuwe aanpak.

Niet alleen brengen, maar ook halen

En dat is ook belangrijk. Niet alleen brengen, maar ook halen. Voor de deelnemers van de derde expertbriefsessie wordt naar aanleiding van hun inzendingen nog bekeken of er een noodzaak is voor een 3b-sessie. Ik verwacht echter een goed resultaat. Temeer omdat er in de sessie een deelnemer zich opwierp als tweede ghostwriter om de snelheid van het schrijfproces te verhogen.

Ik hoop u met bovenstaande iets meer inzicht te hebben gegeven in het enthousiasme wat er toch nog altijd is binnen de groep van access managementexperts. Waarvoor mijn waardering.

Een uniek ID voor iedereen

Kortgeleden de tuin eens even flink gesnoeid. De berg met takken en struiken was zo hoog dat ik het moest afvoeren naar de gemeentelijke vuilstort. Trekhaak achter mijn auto gezet en naar onze plaatselijke verhuurder van aanhangers gegaan. Deze had gelukkig nog een aanhanger staan en ik pakte mijn rijbewijs om mij te legitimeren. Geduldig wachtte ik op het moment dat hij een kopietje zou maken van mijn rijbewijs. Maar helaas, ik had naast mijn rijbewijs ook een ander legitimatiebewijs

nodig omdat de verzekeraar van de aanhanger een dubbele legitimatie wenste. In de jaren dat mijn haar grijzer en grijzer werd heb ik geleerd mij niet af te reageren op de brenger van het slechte nieuws, en ben mijn paspoort gaan halen. Wonderlijk is het wel dat een normale transactie van nog geen 25 euro een dubbele legitimatie vereist. Daarover nadenkend vroeg ik mij af hoe ik mijn eigen auto had verzekerd. Op internet even naar independer.nl en daar mijn keuze gemaakt. Naam en adres ingeven, leeftijd, schadevrije jaren en het kenteken van mijn nieuwe auto ingegeven en hopla, verzekerd met een onmiddellijke dekking. Vreemd, ik hoef niet aan te geven dat de auto van mij is en ik hoef ook niet te bewijzen wie ik ben. Als ik naar het ziekenhuis ga dan moet ik een kaartje laten maken zodat mijn adresgegevens op verwijsbriefjes, recepten en de rekening komen te staan, ook daar heb ik nooit een rijbewijs laten zien. Mijn elektronische belastingaangifte doe ik met DiGiD als legitimatie en dat gaat goed. Ja een aantal jaren geleden kon je ook aangifte doen als je maar een DiGiD-code had, of die van jou of de buurvrouw was maakte niet uit. De maatschappij wordt steeds argwanender.
Bij het stemmen voor de Tweede Kamerverkiezingen hebben we een variant uitgevonden. Als je zelf stemt is een rijbewijs voldoende en als je gemachtigd bent om voor iemand te stemmen dan mag er alleen een kopie van een ID worden gebruikt. Bij sommige webwinkels hoef ik me helemaal niet te legitimeren. Dat is handig als je voor een van je vijanden een grootbeeld televisie wilt bestellen. En doe er ook nog maar een videocamera bij. Ik begrijp best dat het als leverancier van spullen of diensten handig is om te weten of je de juiste persoon voor je hebt maar ik begrijp de enorme grote verschillen in handelswijze niet helemaal goed.
Wat zou het toch handig zijn als we in de virtuele wereld allemaal een eigen en uniek ID hebben waarop iedereen kan vertrouwen. Ondanks het feit dat er veel initiatieven zijn geweest en ook nu nog lopen (ook in Nederland) lijkt het allemaal erg moeizaam van de grond te komen. Het stempel van de burgemeester van mijn gemeente is goed genoeg om iedereen ter wereld te laten geloven dat ik echt Berry ben, zelfs op plekken waar mijn gemeente niet bekend is, laat staan de burgemeester van mijn gemeente. Op internet zijn veel nationale of internationale initiatieven gestart maar een goede oplossing is nog niet gekomen. Het eerder genoemde DiGiD is een methodiek die mij niet zo aanstaat omdat ik niet wil dat DiGiD van mij weet waar ik mij overal heb aangemeld. Daarbij is het initiatief ook discriminerend want alleen non-profit-organisaties en overheidsinstanties mogen van DiGiD gebruikmaken. Succesvol is het wel want als je elektronisch belastingaangifte wil doen dan moet je dit met behulp van een DiGiD doen. En dan is het niet opmerkelijk dat er zoveel DiGiD's zijn uitgegeven.
Toch lijkt het allemaal niet zo lastig voor iedereen een uniek ID te maken. Je zet een aantal grote bedrijven bij elkaar dat ook zaken op internet doet en laat ze iemand authenticeren, laat rijbewijs of paspoort zien en je krijgt een ID voor alle aangesloten bedrijven. Iedereen die een user aanbrengt krijgt een kleine vergoeding als de door hen aangebrachte persoon een transactie doet met het ID. De vergoeding wordt betaald door het bedrijf die zaken doet met het ID. Uiteraard kan het ook minder ingewikkeld door alles gewoon met gesloten beurs te doen maar dit zal allemaal wel te eenvoudig gedacht zijn. Zorg dat er een paar multinationals bijzitten en de Europese uitrol is begonnen. En voor je het weet zal het ID zich als een olievlek over de hele wereld kunnen verspreiden. Misschien zou het wel handig zijn als BP deel uitmaakt van de groep initiatiefnemers. Dat bedrijf heeft inmiddels ervaring genoeg met olievlekken.

Groeten Berry

Discover the next best thing since the introduction of FTP!

BEFINE cryptshare®

- Easily send large files up to 2GB
- Confirmation of file download
- Simple and secure file transfer

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