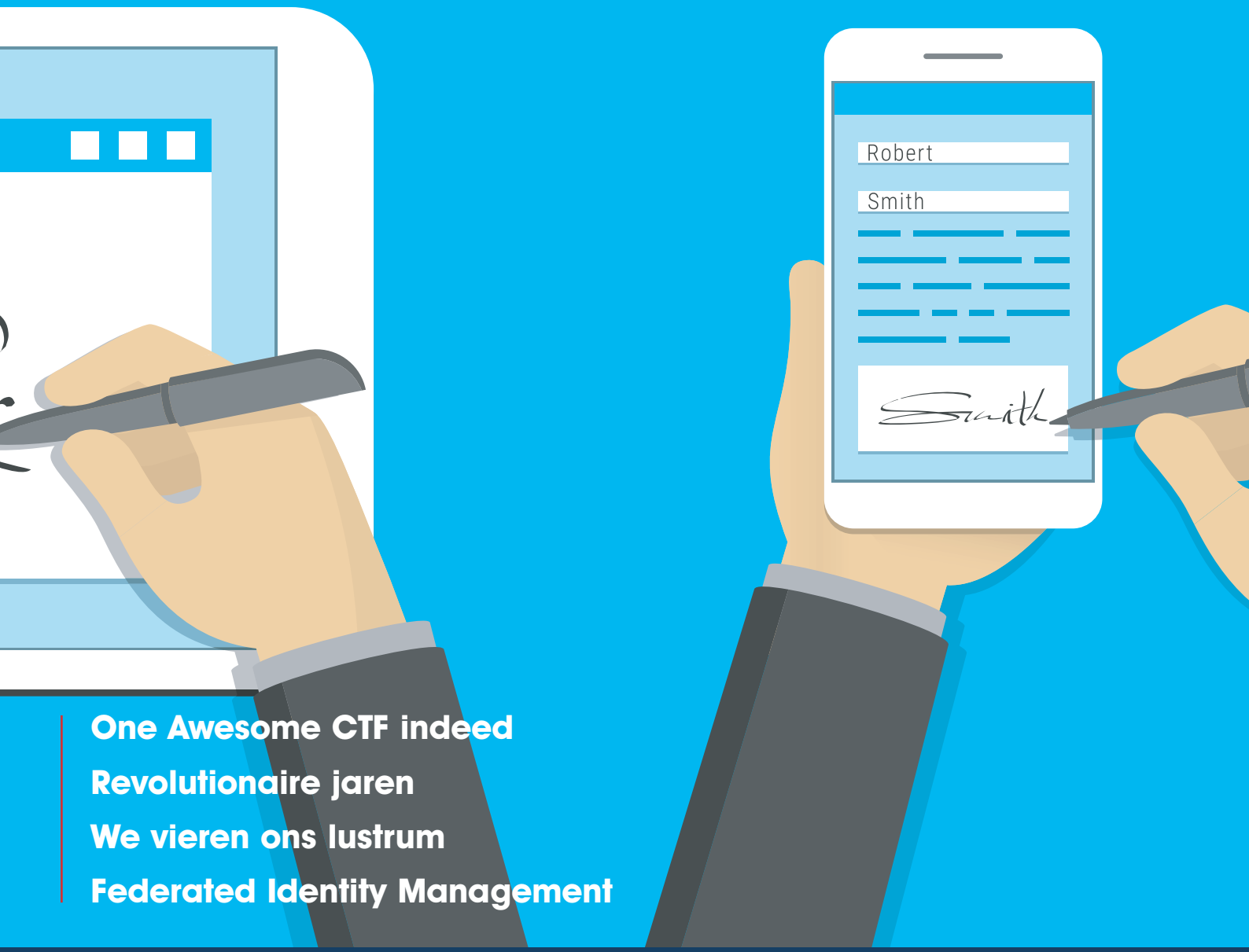
iB

INFORMATIEBEVEILIGING

10 JAAR
LUSTRUMEDITIE

jaargang 17 - 2017

#4



One Awesome CTF indeed

Revolutionaire jaren

We vieren ons lustrum

Federated Identity Management

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers

HET TWEEDE LUSTRUM VAN DE BELOFTE VAN DE ELEKTRONISCHE HANDTEKENING

Als je mij tien jaar geleden gevraagd zou hebben hoe lang het nog zou duren voordat de (geavanceerde) elektronische handtekening algemeen ingevoerd zou zijn, dan zou ik het misschien een jaar of drie gegeven hebben. We hadden de techniek én de organisatie geregeld, er was zelfs al vijf jaar een wet (WEH).

Maar het is er niet echt van gekomen. In plaats daarvan kregen we een crisis en lijken we door de komst van het touchscreen de digitale handtekening omarmd te hebben. Het is nu gewoon dat we met onze vinger of een plastic pennetje (ik ga het geen stylus noemen) over een scherm bewegen om te tekenen. Het lukt mij nauwelijks om een voor mijzelf herkenbare krabbel te zetten, laat staan dat mijn handtekening herkend of geverifieerd zou kunnen worden. "Dat geeft niet", is steevast de reactie van de medewerker of vertegenwoordiger. Verificatie later is kennelijk niet meer de reden dat we moeten tekenen.

Nee, alles moet 'frictieloos' gedaan worden. Het mag geen tijd kosten, het moet tijd besparen. Zo worden pakketbezorgers afgerekend op het aantal pakketten dat ze bezorgen. Verstuur je een pakket verzekerd mét handtekeningverplichting en is er niemand thuis om het pakket aan te nemen? Een weldenkende bezorger gaat niet het pakket terugnemen met als gevolg niet betaald te worden. Je tekent zelf gewoon voor ontvangst en je zet het pakket op de trap. Wat kan er nu mis gaan?

Het pakket wordt natuurlijk bij thuiskomst niet meer aangetroffen. Track&trace laat echter wél een bezorging zien. Een claim bij de post levert ook niets op, want er is getekend - met zo'n onduidelijke krabbel. Niet te herkennen, niet te verifiëren. En dit is nou juist waarom ik verwachtte dat de verifieerbare elektronische handtekening wel zijn intrede zou doen.

Dit is nu eindelijk aan het veranderen. Er is nu Europese wetgeving (eIDAS). Er komen zakelijke oplossingen in de markt waarmee hoogwaardige handtekeningen gezet kunnen worden. Gaat 2018 dan het jaar van de elektronische handtekening worden?

Lex Borger, hoofdredacteur

In dit nummer

ONE-AWESOME-CTF INDEED

In een donkere achterafzaal van het World Forum in Den Haag staan tachtig laptops klaar. Mannen in zwarte T-shirts lopen driftig rond met dozen en kabels. Nog een uur te gaan en dan start de One-CTF, oftewel de Capture the Flag tijdens de NCSC One-conferentie. Ik word hartelijk ontvangen door Kas Clark van het NCSC. Zijn collega's hebben de challenges en software ontwikkeld. Ik vraag hem hoe de teams worden gevormd. "We hebben twintig teams van elk vier deelnemers. Ze weten vooraf niet met wie ze gaan samenwerken. Wij delen ze in, zodat we een mooie mix van skill-levels hebben en iedereen van elkaar kan leren."

Voorin komen alle netwerkkabels samen in een soort regieruimte van schermen, stapels apparatuur en nog meer mannen in zwarte shirts. De mannen hebben op de rug een code van 32 tekens – net als de vlaggen die gevangen moeten worden. Vlak voor de grote tafel staat een klein mysterieus kastje, met een printplaatje erop en eronder een oude monitor met ruis.

Achter de regietafel staan medewerkers van het Security Operations Center van de Belastingdienst. Zij blijken de hardware te hebben geleverd, inclusief twintig laptops voor deelnemers die er geen bij zich hebben. Ik vraag wat voor laptops het zijn. "Niets bijzonders, buiten gebruik gestelde laptops, maar uiteraard wel met Kali Linux erop. Ze kunnen standaardtechnieken gebruiken als Strings, Wireshark en Grep, geen speciale tooling ofzo."

Dit evenement is voor deze ambtenaren een mooie gelegenheid om te laten zien dat zij security niet alleen serieus nemen, maar ook wel in zijn voor fun. En wie weet wil een van de deelnemers hierna wel bij hen komen werken.

Teams

De zaal stroomt vol. Ik tel 72 deelnemers: 64 mannen en 8 vrouwen. Ik zie ook bekenden voorbijkomen: van andere cyber securitycongressen, BNH-ers (Bekende Nederlandse Hackers van tv) en uit mijn boek Helpende Hackers. Aangekomen bij hun tafels, stellen de deelnemers zich aan elkaar voor. Eerste opdracht: bedenk een naam voor je team, beginnend met de letter van je tafel. Tafel A noemt zich 'ateam'. Ik zal de hackerscode respecteren en geen persoonlijke namen noemen, alleen de namen van hun team. Met uitzondering van een

Chris van 't Hof is internetsocioloog, schrijver en presentator van het praatprogramma over informatietechnologie Tek Tok. Hij is bereikbaar via vraag@tektok.nl.

Game rules and hints:

- If you solve a challenge, you earn points. Difficult challenges are worth more points
- Piece of advice: if you're not familiar with CTF challenges, start with the easy ones
- The flag is in the format OneCTF{example-flag}, once you find this flag you have solved that challenge
- Team with the most points wins. In case of a tie, the first team to score the most points wins
- Hints may be released during the game. If so, they will be announced
- No denial of service or performance-hogging attacks
- Do not attack other teams
- Do not change anything in the CTF infrastructure
- No brute force attacks necessary: you won't have to crack any passwords or brute force any directories
- No nMapping on the game servers, all the relevant ports are provided to you
- The RECON challenges involve external/public websites. Do NOT attack these sites!
- Violations are punished

deelnemer die toch wel te opmerkelijk is om niet te noemen: oud-politicus Ad Melkert.

Op het grote scherm verschijnen de 'Game rules and hints'. Dan volgt de opdracht: "We have received some intelligence reports regarding a hacktivist group called the Cyber resistance Liberation Front. They want to destroy the internet by hacking IoT-devices. You are a team of experts assembled from across the world to prevent them. The attack will happen in 2 hours and you have to stop them!" De teams krijgen een wachtwoord en een url. Onderaan de slide staat: "Yes, we know it is a self-signed certificate. We ran out of budget :(".

Aan de slag

We kunnen beginnen. De klok start: slechts twee uur te gaan. Iedereen duikt in zijn of haar laptop. Ik zie sommigen Googlen op "Admin" en "Log in". Anderen typen van alles achter url's, op zoek naar verborgen directories. Uit de speakers klinkt een happy hardcore versie van 'Knocking on Heavens door'. Sommigen spreken me aan: "Chris, heb je nog een verlengsnoer voor me? Of: "Is dit de directory?" Dan realiseer ik me dat ik ook een zwart T-shirt aanheb en ze blijkbaar denken dat ik van de organisatie ben. Ik neem daarom een stoel onder het grote scherm tussen team 'Sharp' en 'Teem teeeeet' aan de andere kant van de zaal en kijk wat in het rond. Eerlijk gezegd heb ik geen flauw idee wat ik hier kan verwachten.

Gelukkig word ik snel vergezeld door Pieter Jansen, een ervaren CTF-er die vandaag niet meespeelt en ook even komt kijken. "Ziet er goed uit", zegt hij. "Enkele van de grote jongens doen ook mee. Er zijn er zelfs een paar Eindbazen." Dit is de naam van het roemruchte team dat veel internationale CTF's won, zoals we volgens hem kunnen zien op ctftime.org. "We doen het goed he?", probeer ik. "De jaarlijkse Cyberlympics worden steevast gewonnen door Nederland, toch?" Hij antwoordt: "Ja: hack.ERS, al vijf jaar eerste, gevolgd door veelal andere Nederlandse teams."

Volgens hem is dat historisch zo is gegroeid: "In de jaren tachtig waren we al bezig met telefoon hacking. Vervolgens waren we het eerste land buiten de VS met internet. Het Amsterdamse internetcafe Freeworld was toen de plek van waaruit we de hele wereld hackten. Toen de Cyberlympics begonnen, waren wij er klaar voor. Maar ja, veel van die gasten van toen zijn nu vader geworden en zie je ze wat minder bij de internationale events. Nu is Polen heel erg in opkomst."

Je moet er maar op komen

Op het grote scherm begint het scorebord te ratelen. Team Quantum Crypto neemt al snel de leiding, nauw gevolgd door Teem Teeeeet. Het ateam met Ad Melkert staat verrassend derde. Ik zie de oude partijleider wat onwennig in zijn scherm staren en druk aantekeningen maken in een schriftje. Naast hem zit iemand onafgebroken in zijn oor te fluisteren. Hun derde plaats wordt echter al overgenomen door team Noname, waarvan ik er enkelen herken als winnaars van het hackevent Game of Toons. Zij hadden 'The Most Dangerous Hack'. Bij Teem Teeeet zitten er ook twee. Hun team had toen de prijs voor 'The

Weirdest Hack' gewonnen. Een van hen kijkt argwanend naar de overkant, waar de leden van team Quantum Crypto opvallend stil naar hun scherm zitten te staren. Hij zegt: "Die gasten houden iets achter, ik voel het."

Dat klopt. Een van de Quantumjongens gaat ineens rechtop zitten en smoort verkrampt zijn gejuich: "Yes!". Het is een van de Eindbazen. Op het scorebord schiet zijn team plots met 400 punten omhoog. Hij heeft de challenge 'Ancient Protocols' opgelost. Ik loop naar de regietafel om te informeren wat er is gebeurd. Karl Lovink, hoofd van het SOC, wijst me op het mysterieuze doosje vooraan. Een van de begeleiders fluistert samenzwerend: "Ze hadden het ook kunnen weten als ze deze aarddraad hadden aangesloten. Maar ja, wie komt nou op dat idee."

De verleiding is groot deze onthulling te delen, want als ik terugwandel tussen de laptops zie ik een bekende directeur van een cyber security bedrijf wanhopig om zich heen vragen: "Ik heb een enorme database gedownload en kan er niks mee!" Een van de BNH-ers zit met hangende schouders. Zijn team staat helemaal onderaan. Maar, ze krijgen hulp. Iemand van het NCSC gaat langs de laag-scorende teams met adviezen. "Het moet wel leuk blijven", verzekert hij me. Het scorebord meldt: 'Hints just been added'. Een vrouw van de politie zwaait vrolijk vanachter haar laptop naar me en roept: "Dit is echt heel leuk, ook al snap ik er niks van". Gelukkig, ik ben niet de enige…

Teem Teeeeet stoomt ondertussen door met het nodige kabaal naar een score van 1,286 punten. Nu staan zij op nummer 1. Met nog maar een kwartier te gaan! De spanning neemt toe en de dj blaast nog wat vette hiphop uit de speakers. Ook Team Quantum Crypto haalt de 1,286. Als we nog maar vijf minuten te gaan hebben, start een aftellende klok en klinkt het onheilspellende nummer 'Tubular Bells' van Mike Oldfield. De score blijft gelijk. Krijgen we een gelijkspel?

NCSC directeur Hans de Vries is inmiddels gearriveerd en gaat klaar staan met de prijzen: voor elk teamlid een NetAid Kit en uiteraard een lousy T-shirt. Ik vraag hem waarom NCSC dit organiseert. "Dit is een manier om van elkaar te leren. De ervaren hackers zetten de beginnelingen aan het werk om eenvoudige challenges van 50 punten op te lossen, terwijl ze zelf beziggaan met een challenge van een paar honderd." Maar wat nu als het gelijkspel blijft? Dan wint het team dat als eerste die score haalde. Hans informeert welk team dat is.

Teem Teeeet dus. Een van de leden vertelt me: "Leek ons zo gaaf om Hans heel hard 'tiet' te laten roepen, vandaar die naam." Nu moeten ze met hem op de foto, wat ze zichtbaar minder leuk vinden. De BNH-ers zouden daar minder moeite mee hebben gehad, maar lijken nu vooral het slagveld zo snel mogelijk te willen verlaten. Een van de tv-sterren, die zesde werd, vertelt teleurgesteld: "Ik was eerst vooral bezig mijn teamleden aan het werk te zetten. Op een gegeven moment ben ik maar voor mezelf begonnen, maar ja, toen was het alweer bijna voorbij."

Terwijl de zaal leegloopt, geeft de eigenaar van het doosje 'Ancient Protocols' nog een korte uitleg. Iets met voltageniveaus die je online kon manipuleren om code te injecteren. Hij raakt een van de contactpunten op het printplaatje aan met de aarddraad. Op de oude monitor verschijnt: "ONECTF {01101001}". Zo kan het dus ook. Je moet er maar net op komen.

PRIVACYVERLEIDERS

Ik las een artikel uit een Amerikaans blad waarboven de gillende kop prijkte "Students will betray their friends' online privacy for pizza". Onderzoekers hadden dat ontdekt. Het ging om onderzoek van toch behoorlijk gerenommeerde instituten MIT en Stanford. De volgende quote van de onderzoekers deed het hem wel voor mij: "Whereas people say they care about privacy, they are willing to relinquish private data quite easily when incentivized to do so". Dit slaat zo ongelooflijk de plank mis dat ik er misselijk van word. Ten eerste; waarom zou je niet én om privacy kunnen geven én indien gevraagd gegevens verstrekken? De twee sluiten elkaar niet uit. Ik ben een intens gepassioneerd voorstander van privacy maar ik zet ook foto's op Facebook waar mijn vrienden opstaan. Ik hou daarna echt niet ineens heel veel minder van privacy. Ik ben ook best bereid persoonsgegevens te geven als er een goede 'whats in it for me' aan vastzit. En als ik weet dat er dan ook goed met die gegevens omgegaan wordt. Het morele oordeel wat onder deze zinsnede van de onderzoekers ligt, stuit me echt tegen de borst. Zoiets past een onderzoeker niet, je hoort weg te blijven van waardeoordelen. Ten tweede; wat denk je nou zelf? Studenten hebben altijd honger en nooit geld. Die houd je een pizza voor en natuurlijk geven ze je dan persoonsgegevens. Sterker nog, toen ik 18 was en voor het eerst op kamers ging, had ik je nog het BSN van mijn moeder gegeven voor een goede maaltijd.

Ten derde, en dit is eigenlijk het allerbelangrijkste; we moeten het eens gaan hebben over het moraal van de partijen die dit soort dingen doen om mensen te verleiden hun eigen privacy en dat van anderen op te geven. Want dat is het echte probleem. Hier vindt gewoon ordinaire gaslighting plaats. Het is een Engelse term waarvoor ik nog geen goed Nederlands woord vond, maar de definitie is als volgt: Gaslighting is a form of manipulation that seeks to sow seeds of doubt in a targeted individual or members of a group, hoping to make targets question their own memory, perception, and sanity.

Groepen mensen worden verleid iets op te geven. De verleiders gebruiken daarbij verschillende technieken om een doel te bereiken, wat tegen het grondrecht op privacy indruist – namelijk het inbreuk maken op eens anders rechten of het opgeven van de eigen rechten. De verleiders zeggen daaropvolgend dat diegenen die ingaan op de verleiding het recht op privacy niet eens waardig zijn want ze zeggen wel dat ze privacy belangrijk vinden "maar kijk nou eens wat ze vervolgens doen!" en daarmee lukt het ze om de aandacht van het eigen onbehoorlijke gedrag af te leiden. En vergeten ze voor het gemak dat de waarden die het grondrecht op privacy ondersteunt, het recht op vrijheid en het recht op autonomie zijn. Mensen mogen zelf weten wat ze met hun persoonsgegevens doen.
Laten we dat onderzoek eens omdraaien. Ik denk dat het hoog tijd wordt om onderzoek te doen naar de intrinsieke waarden van de verleiders en dan ook graag aandacht voor de vraag hoe je de verleiders naar een beter ethisch perspectief zou kunnen verleiden.

Mr. Rachel Marbus
@rachelmarbus op Twitter

STOOM EN KOKEND WATER

Een goede vriend van me is gek op oude treinen. Regelmatige stoomtreinvakanties, verjaardagskalenders met treinfoto's, penningmeester van de stoomtreinvereniging. Ik dacht altijd dat de actieradius van een stoomtrein werd bepaald door de hoeveelheid kolen in het wagentje net achter de locomotief. Net zoals bij een IT-project het beschikbare budget ('Kohle' in plat Duits) bepaalt hoe snel het gaat en hoe ver het komt.

Hij vertelde me dat de actieradius van een stoomtrein echter wordt bepaald door de hoeveelheid water. Van het water wordt immers die stoom gemaakt en de trein in beweging gezet. Zoals ook de uitdrukking 'onder stoom en kokend water tot stand gekomen' aangeeft, die je weleens hoort in een IT-project.

Dit zette me aan het denken over IT-projecten. Ook daar is vaak de gedachte dat als er maar eenmaal budget (geld) is geregeld, dat dan alles wel goed komt. Business cases worden opgesteld, en project initiatieformulieren, hier en daar een aanvullende projectbrief, maar uiteindelijk wordt aan het begin van het project vooral het geld geregeld. De (human) resources die het project moeten gaan uitvoeren, worden daarna pas gezocht. En dan vaak niet, of pas te laat, gevonden. Ook zijn er organisaties die bij hun planning de 'named resources' toestaan; de aanstaande projectleiding vraagt dan niet zoals het eigenlijk hoort om een 'systeemontwerper met minstens drie jaar ervaring in webprojecten' maar om specifiek Jan Klaassen (of Katrijn). Die Jan voldoet op zich ook wel aan die functionele eis, maar de claim van een project op die ene persoon maakt hem tot een SPOF (single person of failure) wat de planning van andere projecten bemoeilijkt. Projecten kunnen dan zogenaamd niet starten 'omdat er geen resources zijn', of

Drs. Robert Metsemakers RA RE CISSP heeft een rijk arbeidsverleden bij Achmea en diens voorgangers in verschillende security en audit functies. Deze column is op persoonlijke titel geschreven. Robert is bereikbaar via metsemakers@live.com.

'omdat afdeling Planning te langzaam werkt'. Maar in feite komt het omdat Jan Klaassen ook maar op één plaats tegelijk kan werken.

Securitypersoneel

In het bijzonder geldt dit wanneer het over securitypersoneel gaat. Veel organisaties hebben er daar al niet veel van: soms is er één security officer voor het hele bedrijf. In een aantal business cases worden helemaal geen kosten voor security opgenomen, dus is er na goedkeuring van het budget ook geen financiële ruimte om een security deskundige in het project op te nemen. Meestal komt het aan het eind van het project toch nog een beetje goed. Veel organisaties beseffen gelukkig wel dat het een goed idee is om voorafgaand aan het in productie nemen van een nieuw systeem, toch een 'akkoord van afdeling security' te hebben. Ten onrechte bestaat weleens het idee dat dit een soort stempelzetters zijn. Maar zoals mijn eerste verzekeringscursus mij leerde: 'de afdeling Acceptatie keurt, ondanks haar naam, ook weleens een verzekeringsaanvraag af'. Het akkoord van security betekent in feite (u als lezer van dit magazine weet het, maar toch nog even expliciet) dat de risico's van deze nieuwe onderneming of activiteit zijn beoordeeld ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid, en dat in de voor de beoordeling beschikbare tijd en met behulp van de kennis en ervaring van de beoordelaar er geen onoverkomelijke bezwaren zijn gevonden. Zoveel schrijfruimte is er natuurlijk niet op dat beruchte ene toegestane A4-tje voor de risicoanalyse, maar daar gaat het wel om.

Mijn pleidooi is: neem in de budgetten niet alleen financiële ruimte (kolen) op voor uitgaven aan security, maar reserveer ook meteen een redelijke hoeveelheid tijd (water/stoom) voor deelname door 'een' security deskundige in het projectteam. En dan niet alleen voor de laatste twee dagen van het project... Door security-eisen vanaf het begin van een project mee te nemen, is minder kostbaar last minute herstelwerk nodig. Die extra security-uren maken het project natuurlijk wel iets duurder. Daardoor zal af en toe een business case in uw bedrijf omvallen, omdat een op het eerste oog lucratief innovatief idee niet voldoende beveiligd kan worden naar bijvoorbeeld wettelijke normen zoals de Nederlandse Wbp. Of de qua boetes strengere opvolger daarvan, de Europese GDPR. Dat is wat mij betreft mooi meegenomen. Dan kun je het uitgespaarde bedrag besteden aan projecten die wel voldoende beveiligd zijn. Want klanten van allerlei organisaties en bedrijven hebben steeds hogere verwachtingen van de informatiebeveiliging in de hen aangeboden producten en diensten. Zeker als je let op hoe fel er in zowel traditionele media als op social media wordt gereageerd op ontdekte beveiligingslekken.

REVOLUTIONAIRE JAREN

In dit lustrumjaar heeft de redactie teruggekeken naar de artikelen die gepubliceerd zijn in het beginjaar van het PvIB, 2007. In dat jaar was er nog geen iPhone hype, nog geen BYOD, nog geen Dropbox, nog geen massa-IoT. Social media kanalen Facebook en Twitter werden nauwelijks zakelijk gebruikt, LinkedIn was nog geen social media kanaal, maar een professioneel telefoonboek. Blogging kwam net op.

De werkdag van een professional voltrok zich op locatie, meestal ook op een PC. De luxepaardjes hadden een laptop. Consultants zeulden rond met meerdere laptops. Middels desktop virtualization kon je daaruit bevrijd worden, als je wilde. Patch management van werkstations werd door gebruikers zelf gedaan en had het risico dat het werkstation onbruikbaar werd. Het Jericho Forum moest nog actief waarschuwen dat de-perimetrisatie echt was. Als CISO kon je dat nog ontkennen.

De georganiseerde misdaad en overheden moesten de offensieve mogelijkheden in het cyberdomein nog ontdekken, hackers waren lastig, maar niet destructief. Malware had geen merknamen, AV-scanning werd nog geaccepteerd als strategie tegen malware.

Enkele artikelen kunnen gebruikt worden als reflectie van het tijdsbeeld. De redactie kiest ervoor om twee van deze artikelen te herplaatsen. Het eerste is 'Security Awareness bij outsourcing' door Frank Breedijk. De problematiek speelt tien jaar later nog steeds en afgezien van de gehanteerde standaarden is het zelfs actueel plaatsbaar.

Het tweede artikel is 'Het einde van de digitale sleutelbos' door Martijn Verbree en Emanuël van der Hulst. Een goed artikel over een belangrijk onderwerp, maar leest tien jaar later als achterhaald. Bedrijven zijn inmiddels wel klaar om over de bedrijfsgrenzen heen te kijken. Nieuwe ontwikkelingen maken dat het onderwerp veel verandering heeft doorgemaakt.

Tussendoor laten we het bestuur en de lustrumcommissie aan het woord. We hopen iedereen te zien op de komende lustrumviering in september.

De redactie

Opmerkelijke artikelen uit 2007

- Federated Identity Management
- De Sinistere Site
- Effectiviteitverhoging in bewustwordingsprogramma's
- Security Awareness bij outsourcing
- Extended Validation SSL Certificates
- Gevraagd Particulier Digitaal Onderzoekers
- Security update management in complexe organisaties
- Tweesporenbeleid op weg naar een betere bescherming persoonsgegevens
- Veilig internetbankieren

WAAROM IK VEREERD EN TROTS BEN OM VOORZITTER TE MOGEN ZIJN VAN HET PVIB

Toen ik meer dan vijftien jaar geleden in aanraking kwam met de vakverenigingen GvIB en PI, viel het me meteen op dat het hier om een groep zeer enthousiaste vaklieden ging. De leden bezaten een bepaalde vorm van leergierigheid die sfeerbepalend was voor de bijeenkomsten. Tijdens de lezingen werd er aandachtig geluisterd en vragen werden met de nodige voorzichtigheid en precisie geformuleerd. Tijdens de pauzes zocht men elkaar bewust op, onderlinge afspraken werden gemaakt ('netwerken') en er werd altijd gretig aangevallen op de borrelhapjes. Het kennisniveau was toen al hoog en is in de afgelopen jaren alleen nog maar meer gegroeid. Deze groei is mede veroorzaakt door het fanatisme van onze leden en de ambitie om kennis te delen.

Iets anders ging het bij de IBO (Informatiebeveiliging Overleg). Daar was het juist de bedoeling dat er stevig gediscussieerd werd. Allemaal geleid door Bart van Staveren. Tijdens deze discussies bleef het ook weer heel serieus. Wat vaak naar voren kwam, was de rol die informatiebeveiliging speelt in de hedendaagse maatschappij. Keer op keer kwam het tijdens de IBO-bijeenkomsten weer aan de orde dat het zaak is dat wij, informatiebeveiligingsdeskundigen, het bedrijfsleven en de samenleving bijbrengen waarom het belangrijk is dat de informatie van de burger beveiligd of - beter gezegd - beschermd wordt. Wij zijn een groep met een eerlijke missie dat het maatschappelijk belang dient.

Wat ook direct opvalt, is dat we een groep zijn die voornamelijk uit mannen bestaat. Ik, als een van de weinige vrouwen vanaf het eerste uur, moet zeggen dat vrouwen bij het PvIB dezelfde rol toebedeeld krijgen als mannen. Dit heeft mij als vrouw altijd een enorme kick gegeven en ik ben er trots op dat wij zo'n vereniging zijn.

Vereniging in beweging

We zijn ook een vereniging in beweging. Met trots kijk ik terug op een van onze laatste initiatieven; Young Professionals opnemen in ons midden. Toen ik werd aangesteld als voorzitter, heb ik alle commissievoorzitters gesproken. Lodewiek Jansen van YP vertelde mij hoe moeilijk het soms is om de groep bij elkaar te houden. Want dan ging de een op stage, de ander samenwonen en weer een ander in het buitenland studeren. Allemaal hele normale gebeurtenissen die wél impact hebben op het succes van te plannen en geplande activiteiten. Het is geweldig dat deze groep jonge vakgenoten zich niet laat ontmoedigen en keihard doorgaat met het ontsluiten van kennis. Ondertussen is het een groep die niet weg te denken is uit ons midden.

Een constante factor binnen het PvIB is onze secretariële ondersteuning, MOS bv en 'Debbie'. Debbie is onze vaste gastvrouw bij bijeenkomsten en organisatieheldin. MOS en Debbie zijn onderdeel van ons fundament en ook al is het 'just another job', de wijze waarop beiden zich gecommitteerd hebben aan onze vereniging is geweldig.

Drive

Vraag een willekeurige vakexpert naar het PvIB en er wordt direct een relatie gelegd met onze bijeenkomsten, IB-Magazine en het Security Congres. Het PvIB bestaat niet alleen uit vaklieden die hun vak verstaan, het PvIB wordt door het bedrijfsleven en de overheid serieus genomen. Onze commissie- en bestuursleden zijn allemaal dagelijks in het bedrijfsleven op het vakgebied actief, en stuk voor stuk zetten zij zich vrijwillig in om kennis te delen en meer kennis op te doen. De 'drive' waarmee onze vrijwilligers hun taken verrichten, geeft energie, is aanstekelijk en maakt dat ik geloof in een geweldig succesvolle komende vijf jaar.

De afgelopen jaren zagen we een toename aan bezoekers op onze bijeenkomsten en het Security Congres was nog nooit eerder zo goed bezocht. Er wordt hard gewerkt aan de implementatie van een kwalificatiestelsel voor ons vakgebied waarbij het PvIB een belangrijke rol speelt. Juristen, Risico Managers, Auditors, IT-architecten en systeemontwikkelaars willen allemaal met ons samenwerken. Ons vakgebied groeit en wordt steeds belangrijker. Wij gaan als vereniging een geweldige tijd tegemoet en ik ben trots dat ik mijn bijdrage kan leveren.

Samen met alle bestuursleden wens ik de leden van het PvIB een fantastisch Lustrumfeest.

Jessica Conquet is voorzitter van PvIB. Zij is te bereiken via jessicaconquet@pvib.nl.

Security Awareness bij outsourcing

Ing. Frank Breedijk > Frank Breedijk werkt op dit moment as Security Engineer bij Schuberg Philis, een organisatie die zich richt op de outsourcing van complexe bedrijfskritische applicatie infrastructuren met hoge beschikbaarheidseisen. In het verleden was hij manager van het EMEA Security Operations Center voor managed security services van Unisys en werkte hij als security officer voor Interxion.

Security awareness is onmisbaar voor iedere organisatie, ook bij outsourcing. Echter bij outsourcing heeft security awareness een aantal extra dimensies. Zo moet de klant zich bij het aangaan van een overeenkomst, naast een groot aantal andere security gerelateerde zaken, in korte tijd op de hoogte stellen van de security awareness bij de dienstverlener (de outsourcer). Omdat er sprake is van twee verschillende organisaties kan er sprake zijn van een verschil in kennis en inzicht tussen de twee organisaties. In dit artikel probeer ik een aantal min of meer outsourcing specifieke kanten van security awareness te belichten.

Dat het voor organisaties van levensbelang is security awareness onder haar medewerkers te borgen, behoeft geen discussie, maar hoe zit dat wanneer (een deel van) de IT activiteiten buitenshuis uitgevoerd gaan worden? Hoe kun je als outsourcingsklant de security awareness van een outsourcer beoordelen?

Een aantal professionele outsourcingspartijen is in het bezit van een BS7799 dan wel een ISO27001:2005 certificaat. Kun je als klant er vanuit gaan dat een gecertificeerde partij ook een partij is waar de security awareness goed geregeld is? In de basis is dit het geval. Dit internationale normenkader omschrijft de eisen waaraan een Information Security Management System (ISMS) zou moeten voldoen en security awareness maakt hier deel vanuit. De eisen voor certificering stellen dat het ISMS regelmatig door een onafhankelijke partij tegen de norm getoetst moet worden. Security Awareness zal hier in de praktijk, in het geval van een goed werkend ISMS, altijd aanwezig zijn. Toch is een certificaat op zichzelf niet altijd zaligmakend, omdat het bijvoorbeeld mogelijk is te certificeren met een zeer beperkte scope. Ik heb in het verleden marketing materiaal gezien waarbij een bedrijf aangaf in het bezit te zijn van een BS7799 certificaat. Bij verdere navraag bleek dit echter alleen te gaan om de operations van één specifiek datacenter. Een kritische klant doet er dus goed aan om te onderzoeken in hoeverre de scope van het certificaat ook de outsourcingsactiviteiten en bij voorkeur ook de specifieke klantsystemen omvat.

Een andere manier om bij het aangaan van een contractrelatie onder andere de security awareness van een outsourcingspartij te testen, is het vragen van een 'Comply or Explain' statement met betrekking tot de security policy van de klant. Hierbij is het aan de outsourcer om aan te geven in welke mate hij aan de security policy van de klant kan voldoen en uitleg te geven wanneer hij hiervan wil afwijken. Hoewel het verleidelijk is om de kwaliteit van een outsourcer aan de hoeveelheid groene vlakjes ('Comply') te verbinden is het eigenlijk veel interessanter om te kijken naar de antwoorden die bij non-compliance ('Explain') gegeven worden, zeker als het om het vaststellen van de security awareness van een organisatie gaat. Omdat we, per definitie, te maken hebben met twee verschillende organisaties is een '100% Comply' statement praktisch onmogelijk en zullen er dus altijd 'Explain' statements zijn. Deze statements zullen een inzicht geven in hoe professioneel de outsourcer met beveiliging omgaat.

Een voorbeeld uit de praktijk: Een klant, die een outsourcingsovereenkomst voor een bedrijfkritische applicatie op een Unix platform aan wil gaan, heeft in de security policy staan dat door middel van een password cracker iedere maand de kwaliteit van de gebruikerswachtwoorden moet worden vastgesteld en dat gebruikers met een zwak wachtwoord hierop moeten worden aangesproken. De outsourcer stelt voor van deze policy af te wijken en geeft middels een 'Explain' statement de volgende verklaring: "Wij werken niet met wachtwoorden, alle logins worden geauthenticeerd via public/private key authenticatie. Er zijn op de systemen geen wachtwoorden aanwezig en het uitvoeren van een dergelijke audit is dus ook niet zinnig."

Aan de uitleg van de outsourcer, die een preventieve maatregel neemt in plaats van een achteraf controlerende maatregel, kan worden afgelezen hoe security aware deze organisatie is.

Security awareness, een integrale benadering

Zodra de outsourcingsovereenkomst is aangegaan, verandert security awareness van eenrichtingsverkeer (heeft mijn outsourcer wel voldoende security awareness?) naar een bidirectioneel mechanisme. Immers nu beide partijen een relatie zijn aangegaan, zullen zij beiden verwachtingen hebben met betrekking tot elkaars security awareness.

Security awareness en business awareness liggen hier zeer dicht bij elkaar, immers het accepteren van bepaalde risico's is te allen tijde een business decision waarbij de techniek slechts de input kan geven. Outsourcer en klant zullen elkaars business moeten begrij-

pen om tot een optimale wederzijdse security awareness te komen. Immers de business van de klant bepaalt in zeer hoge mate hoe er in bepaalde situaties gereageerd moet worden. Een voorbeeld hiervan is de prioriteiten bij het herstellen van incidenten. Bij de ene klant, bijvoorbeeld bij een online shop, zal de prioriteit liggen op beschikbaarheid, terwijl bij een andere klant, bijvoorbeeld een online bank, de data integriteit en vertrouwelijkheid een veel hogere prioriteit zullen hebben. Een outsourcer die ervoor kiest zich rond de klant te organiseren en daardoor een beter begrip van de klant krijgt, zal ook beter in staat zijn risico's op waarde te schatten.

Risicomanagement en daarmee ook securitymanagement zullen op een geïntegreerde wijze en met een nadrukkelijk afgestemde governance tussen partijen en binnen de afzonderlijk partijen moeten plaatsvinden om helder en eenduidig richting te geven aan de gewenste doelstellingen, maatregelen en (onafhankelijke) controle van die maatregelen. Met name de wederzijdse governance zal er voor zorgen dat er een gezonde balans ontstaat tussen de security belangen van de klant en van de outsourcer, zonder dat dit de, voor de klant zo noodzakelijke, flexibiliteit in de weg staat. In deze wederzijds governance structuur is het belangrijk de verantwoordelijkheden en bevoegdheden van zowel security organisaties van de klant en outsourcer afzonderlijk als die van de gezamenlijke security organisatie vast te leggen. Daarnaast is het belangrijk vast te leggen hoe security beslissingen in noodsituaties en onder tijdsdruk genomen worden.

Reverse awareness

Er zullen zich situaties voordoen waarbij de outsourcer security risico's anders ziet dan de klant. Dit kan komen door een verschil in de mate van inzicht en ervaring of omdat de outsourcer vanuit zijn werkzaamheden een beter inzicht heeft in wat er in de omgeving gebeurt en welke mogelijke risico's dit met zich mee brengt. Een goede manier om de klant van de risico's bewust te maken is hem meer inzicht te geven. Een voorbeeld kan dit beter illustreren.

Bij een outsourcer komt een verzoek binnen tot het opstellen van Internet toegang via TCP port 6667 zodat gebruikgemaakt kan worden van een 'online collaboration tool'. Een kort onderzoek van de outsourcer leert dat de zogenaamde 'online collaboration tool' waarschijnlijk IRC is, het grootste online chat netwerk op het Internet. Hoewel zakelijk gebruik van IRC niet ondenkbaar is, weet de outsourcer dat het gebruik van chat boxen in de security policy van de klant nadrukkelijk verboden is. Door het wijzigingsverzoek van de klant middels een impact analyse met mogelijke risico's toe te lichten, kan de klant het verzoek in de juiste context beoordelen en een onderbouwde business decision nemen.

Anders wordt het wanneer de outsourcer en de klant na het delen van de informatie nog steeds een verschil van inzicht hebben. Ik heb mij hier altijd op het standpunt gesteld dat de beheerde infrastructuur eigendom is van de klant en dat de oud-Hollandse stelregel 'Wie betaalt die bepaalt' dus van toepassing is. Met andere woorden, de klant bepaalt waar hij met zijn infrastructuur heen wil. Dit wil echter niet zeggen dat veranderingen waar de outsourcer het niet mee eens is, zonder meer uitgevoerd moeten worden. Ik heb in het verleden, en ook in mijn huidige functie, hiervoor meerdere malen gebruikgemaakt van een zogenaamd risk statement. Een risk statement bevat een omschrijving van de ontstane situatie of de voorgestelde verandering, de gevolgen en risico's die hiermee genomen (zouden) worden en de verklaring dat de klant zich bewust is van deze risico's en deze bewust neemt. Een dergelijk risk statement heeft twee functies: ten eerste legt het document vast dat de outsourcer aan zijn (morele) zorgplicht heeft voldaan en beschermt daarmee de outsourcer indien het mis gaat en ten tweede laat het de klant nogmaals goed nadenken over de te nemen risico's en heeft een dergelijk statement soms tot gevolg dat een klant tot een ander inzicht komt. Of de klant de verandering nu afblaast of juist bereid is het in kaart gebrachte risico bewust te nemen, het risico statement zorgt dat de verantwoordelijkheid uiteindelijk daar ligt waar die hoort, namelijk bij de business. De ervaring leert dat indien dit risicomanagement-proces zorgvuldig en adequaat wordt uitgevoerd klanten zeer goed in staat zijn juiste afwegingen te maken, redenerend vanuit de risico's en kansen voor hun dagelijkse business.

Periodieke risicoanalyse

Er zijn maar zeer weinig outsourcers die ervoor kiezen om samen met de klant periodiek via een gestructureerde methode, bijvoorbeeld CRAMM, een risicoanalyse te maken van de uitbestede applicatie infrastructuur. Doordat klant en outsourcer in een gezamenlijke sessie nadenken over het belang van de applicatie infrastructuur voor de klant, de mogelijke risico's en de eventuele gevolgen als er iets misgaat, ontstaat in beide organisaties een verhoogd (security) bewustzijn. Aan de hand van het resultaat van de risicoanalyse kan worden vastgesteld of genomen maatregelen nog steeds passen bij het risicoprofiel. Een periodieke risicoanalyse voorkomt ook dat verzuimd wordt na te denken over de gevolgen van een geleidelijke verandering van het belang van de applicatie infrastructuur. Iets dat bij de meeste bedrijven door de drukte van de dagelijkse praktijk gemakkelijk over het hoofd wordt gezien. Het is, zeker bij outsourcing van belang dat een applicatie infrastructuur na de implementatie niet bevroren wordt, maar met organisatie die ze ondersteunt mee verandert. Een klassiek voorbeeld hiervan zijn bijvoorbeeld reisorganisaties die de afgelopen jaren de verkoop via het Internet hebben zien stijgen, veelal ten koste van de verkoop via het callcenter. Doordat de bezoekersaantallen en de omzet van de webshops soms gestaag en, op basis van marketing acties, soms zeer sterk veranderen, realiseert men zich vaak pas te laat dat de maatregelen ter bescherming van bijvoorbeeld de privacy, beschikbaarheid, performance en schaalbaarheid niet meer in verhouding staan tot het belang van de, steeds meer kritische, applicatie infrastructuur voor de continuïteit van de organisatie. De periodieke strategische risicoanalyse creëert en onderhoudt de security awareness bij beide partijen op het noodzakelijke hoogste niveau.

One size fits all?

Uit het voorgaande mag worden afgeleid dat security awareness specifiek op de doelgroep en de situatie afgestemd moet worden. Hoewel er zoiets is als een basis awareness, waaronder zaken als omgaan met wachtwoorden vallen, is het een illusie te denken dat er zoiets

als een generiek security awareness programma bestaat. Het door de klant eenzijdig opleggen van maatregelen met betrekking tot awareness aan de outsourcer is weinig effectief. In het geval van een outsourcingsrelatie is security awareness een co-productie van betrokken partijen, waarbij de risicoanalyse en het constateren van (mogelijke) security violations ingebed dient te zijn in de dagelijkse operatie en waarbij de outsourcer in alle lagen van het bedrijf zicht moet hebben op de business van de klant. Op basis van adequate analyse waarin de outsourcer op basis van haar expertise dient te voorzien, zal binnen de afgesproken governance de risico-afweging vervolgens door de klant moeten worden gemaakt. Juist deze keuzes moeten worden vastgelegd, zodat een auditor kan constateren dat er op een gecontroleerde wijze wordt omgegaan met risico's en dat er sprake is van een integrale security awareness.

Link die aangeeft waarom awareness op alle lagen van de organisatie belangrijk is: *http://worsethanfailure.com/Articles/The_Direct_Approach.aspx*

De Sinistere Site – Suske & Wiske kweken awareness

De Stichting Kennisnet ICT op School heeft een Belgisch awareness initiatief overgenomen en zal dit najaar het speciale Suske en Wiske album 'De sinistere site' verspreiden op basisscholen en op aanvraag onder overige belangstellenden. Het is een uitgave van de Studio Vandersteen, geschreven door Erik Meynen.

Het is een bijzonder album, waarin vooral Wiske last zal krijgen van de duistere kanten van het internet. Zij wordt tijdens een internetsessie naar de betoverde site van professor Zwanzerik gelokt. Haar vrienden moeten haar natuurlijk redden uit handen van de boosaard.

Door het verhaal heen worden de gevaren van het internet uitgelegd en ook wordt erop gewezen op welke manieren deze gevaren vermeden kunnen worden. De laatste vier pagina's van het album bestaan uit tips voor het veilig gebruik van internet, zoals e-mail en chatten. Volgens lezertjes is de kwaliteit van de illustraties wat mager, maar is het wel een grappig verhaal en komt de boodschap wel over.

In België werd het album in 2006 uitgereikt, waarbij de kinderen ook een digitaal identiteitsbewijs (het Belgische e-ID) met een gratis kaartlezer ontvingen. In Nederland zullen de albums worden uitgereikt in het kader van het lespakket Veilig Internetten. Er zijn aparte lesbrieven beschikbaar voor onderwijs aan kinderen vanaf groep 5 en kinderen van groep 8.

Ook ouders en andere belangstellenden kunnen het boekje bestellen op de site: *http://www.desinisteresite.nl*

De lesbrieven zijn hier te vinden:
http://www.schoolpost.nl/desinisteresite/library/documents/lesbrief_a.pdf
http://www.schoolpost.nl/desinisteresite/library/documents/lesbrief_b.pdf

WE VIEREN ONS LUSTRUM!

Dit jaar is ons tweede lustrumjaar en dat vieren we groots op 28 september in Fort Voordorp. Een evenement waarbij de leden verwend worden met uiteenlopende activiteiten waarbij vooral plezier en vermaak centraal staan. Het lustrum is opgezet als festival waarbij er voor iedereen iets leerzaams, nuttigs en leuks te vinden zal zijn. En vergeet niet je stempelkaart vol te krijgen, want anders mis je je draaibeurt aan het Rad van Fortuin…

Het programma is eenvoudig; Naast de drie plenaire sessies van grote namen, vul jij je programma verder zelf in, geheel passend naar jouw stemming en interesse uit de vele korte activiteiten. Neem ook een introducé mee die nog geen lid is van het PvIB, maar eigenlijk wel zou moeten zijn. We laten ze wel even zien dat informatiebeveiliging ook heel veel fun en gezelligheid is!

De programmacommissie promoot persoonlijk diverse activiteiten:

Walter Leemhuis

"Het bestuur stelde een mooi budget beschikbaar om iets speciaals te doen bij dit tweede lustrum. De plannen werden echter per meeting steeds ambitieuzer voor dit event. Het was duidelijk dat we ook echt sponsors nodig hadden om het ook nog allemaal te kunnen betalen. Gelukkig werden er snel creatieve sponsorpakketten bedacht en waren er in ruime mate sponsors die het PvIB een warm hart toedragen en tegelijkertijd hun naamsbekendheid binnen de vereniging kunnen vergroten. Samen maken we er een onvergetelijke avond van!"

Bas Houtepen

"Ga de uitdaging aan en kom in record-tempo uit de ballenbak-bingo escaperoom. Laat je verrassen door de security awareness game Alpha op een arcadekast. Let's have fun!"

Erwin Bosma

"Wil jij weten wat het bestuur doet? Wil jij het bestuur helpen om het PvIB verder te laten groeien en nog meer te laten betekenen voor haar leden? Heb je suggesties, complimenten, klachten of wil je wat anders kwijt? Het PvIB-bestuur staat voor je klaar tijdens de break-outs. En we willen natuurlijk ook in contact komen met enthousiaste leden die willen meehelpen het PvIB nog succesvoller te maken.
Tot ziens bij de PvIB-stand!"

Andre Beerten

"Als een waardig opvolger van Hans van der Togt zal ik het Rad van Fortuin bedienen, echter wel zonder hulp van enige charmante assistentie. Op het rad bevinden zich fantastische prijzen (Pierre, wat hebben we vandaag voor onze prijswinnaars in petto?) gedoneerd door onze sponsors. Voor wie in zijn Lustrumpaspoort voldoende stempels heeft verzameld, geef ik er een slinger aan."

Ronald van Erven

"Hacken-hacken-hacken, tuurlijk gaan we dat ook doen op ons lustrum!"

Ali Agzanay:

"Pas op voor de lustrum-gek die iedereen doet verbazen met zijn prettig gestoorde vermaak!"

Debbie Reinders

"Tijdens een proeverij nemen de brouwers je mee op een ontdekkingstocht in de wereld van bier en jenever. Ontdek hoe ingrediënten worden gebruikt en welke stappen er genomen worden voordat je smaakvol kunt genieten!"

Hans Baars

"Ieder bedrijf dient zijn Business Continuity goed ingeregeld te hebben om bij calamiteiten te kunnen overleven. Onderdeel van Business Continuity is een goede zorg voor de mens die het bedrijfsproces draaiende moet houden. In Nederland betekent dat vooral dat medewerkers op tijd van een goede kop koffie worden voorzien. Een barista geeft een kijkje in de keuken van het maken koffie. Kom proeven hoe hoogwaardig kwalitatief koffie smaakt!"

Kelvin Rorive

"Een mooie bloem meenemen naar huis als aandenken van het Lustrum. Ook daar zorgen we voor! Maar dan moet je hem wel eerst zelf vouwen in de workshop ballonvouwen! Dikke lol en gekheid wat je allemaal kan doen met ballonnen. Kom het ervaren…..!"

Evert van Zanten

"Leren met een innovatieve app terwijl je fysiek wordt uitgedaagd? Hoe 'cool' is dat? Doe mee aan de 'Knowingo Cool Experience'. Maar je kan ook een virtuele ervaring krijgen die tot nu toe alleen voor generaals is weggelegd. Stap in deze bijzondere virtuele wereld en verken de legerbasis van de toekomst. Wauw… ook PvIB!"

Lodewiek Jansen

"De Young Professionals van het PvIB dagen je tijdens het IB-festival uit. Ben jij een teamspeler met torenhoge ambities? Ga dan de uitdagingen van de YP-commissie aan tijdens het lustrum!"

Erwin Kooi

Erwin Kooi en Stefan Veenendaal

"Niets is wat het lijkt tijdens het lustrum, Fort Voordorp zit vol geheimen. Weet jij alle verborgen elementen te vinden tijdens de zoektocht naar de verborgen schat?
Mocht je daarbij voor gesloten deuren komen te staan, dan kun je proberen deze te openen met de kennis die je in de lockpick village kunt opdoen. Een hands-on uitleg van sloten, hoe je ze opent en hoe je ze beveiligt. Alles onder de bezielende leiding van competitieve lockpickers."

Stefan Veenendaal

"Het lustrum is ook een moment van reflectie en eens terugkijken. Wat kan daar beter bij helpen dan een expositie van het Cryptomuseum, dat ons meeneemt in een boeiende reis door de tijd op het gebied van exotische vercijferingsmachines en andere bijzondere cryptodoosjes."

Lex Borger

"Kom tijdens het evenement groepsgewijs een (of twee) artikel(en) schrijven. We bieden de gelegenheid om ideeën op te doen en van elkaar leren voor toekomstige artikelen. Stapsgewijs en in vaste tijdblokken gaan we van context tot artikel, met de gelegenheid jouw bijdrage te leveren tijdens een of meer van die stappen. De redactie verzorgt de coaching."

Federated Identity Management

Het einde van de digitale sleutelbos?

Auteurs: Drs. Martijn Verbree en Emanuël van der Hulst > Martijn Verbree is consultant bij KPMG Information Risk Management, Emanuël van der Hulst is junior consultant bij KPMG Information Risk Management.

"Who am I?' In the context of the online world, the answer to this perennial question would be something like 'I am a collection of disconnected islands of identity information...which I have to maintain." [1]

Een belangrijke maatregel in het palet van informatiebeveiliging is het implementeren van logische toegangsbeveiliging. In de praktijk betekent dit dat gebruikers worden voorzien van een unieke gebruikersID, een authenticatiemiddel waarmee hun identiteit kan worden geverifieerd (zoals een wachtwoord of beveiligingscalculator) en rechten (autorisaties) om informatie in te zien, te wijzigen of transacties te verrichten. Als een gebruiker elektronische diensten afneemt van verschillende organisaties, wordt deze gebruiker voorzien van evenzoveel verschillende gebruikerID's en authenticatiemiddelen. Ga maar eens na over hoeveel gebruikersnamen, wachtwoorden, pincodes en tokens u momenteel beschikt. En vergeet vooral niet die van uw webmail, internetwinkels, nieuwsgroepen, bankpassen en uw werk mee te tellen. Zo is op basis van een onderzoek door KPMG [2] naar voren gekomen dat tachtig procent van de ondervraagden *op het werk* over meer dan twee en veertig procent over meer dan drie authenticatiemiddelen beschikt. Juist om deze digitale sleutelbos terug te dringen, is er de laatste jaren een nieuwe trend ontstaan. Deze trend wordt 'Federated identity management' genoemd en heeft als doel het terugdringen van het grote aantal gebruikersID's en authenticatiemiddelen, de beheerslast ervan te verminderen en het algehele beveiligingsniveau te verbeteren.

Identificatie, authenticatie en autorisatie uiteengezet

Identificatie, authenticatie en autorisatie zijn in het kader van informatiebeveiliging veel voorkomende termen. Deze concepten worden vaak in één adem genoemd, maar wat is nu precies het verschil?
In de context van logische toegangsbeveiliging wordt *identificatie* omschreven als het proces inzake het vaststellen van de identiteit van een communicatiepartner, zoals een website, machine of persoon. De gebruikersID is het meest voorkomende gegeven dat wordt gehanteerd om een identiteit van een gebruiker uniek vast te stellen. Daarnaast kan ten behoeve van het identificatieproces van machines het IP-adres van het systeem of MAC-adres van een netwerkkaart worden toegepast. Vanzelfsprekend is louter een identificatie niet voldoende om met zekerheid vast te kunnen stellen met welke gebruiker precies wordt gecommuniceerd. In een elektronische omgeving is het immers voor een kwaadwillende partij vrij eenvoudig zichzelf voor te doen als een andere identiteit (spoofing). Authenticatie biedt hiervoor een oplossing en staat voor het verifiëren van de identiteit waarvoor een bepaalde partij zich uitgeeft. Een in praktijk veel voorkomend authenticatiemiddel is het wachtwoord dat behoort bij een specifieke gebruiker. Door de combinatie van een gebruikersID en wachtwoord te controleren, kan de door de gebruiker geclaimde identiteit met grotere zekerheid worden vastgesteld. Andere voorbeelden van authenticatiemiddelen zijn digitale certificaten (PKI) en challenge/response-tokens. Nadat een gebruiker succesvol is geauthenticeerd, dient een organisatie te bepalen welke rechten en permissies deze geauthenticeerde gebruiker heeft. Het bepalen en verlenen van rechten en permissies aan een bepaalde identiteit wordt *autorisatie* genoemd. Nadat autorisatie is verleend, kan de gebruiker gebruikmaken van de elektronische dienstverlening, zoals het inzien van informatie of het verrichten van transacties.

Wat is Federated identity management?

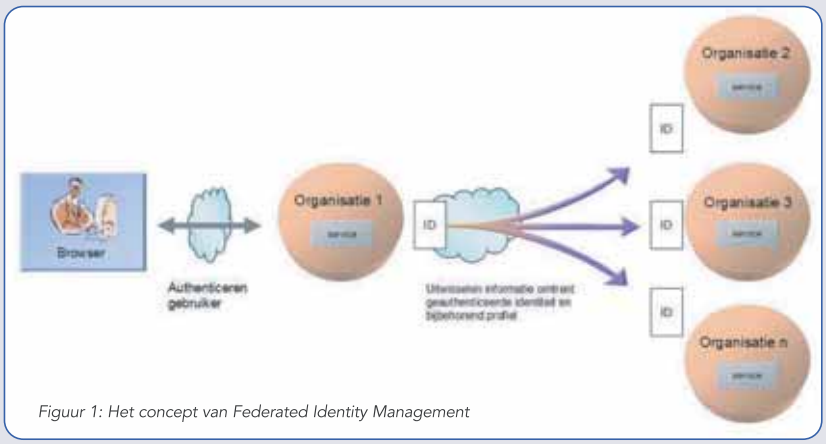
Om de totale kosten met betrekking tot uitgifte en beheer van authenticatiemiddelen te beperken en het gebruikersgemak te bevorderen, is de laatste jaren een trend waarneembaar genaamd Federated identity management (vanaf nu: FIM). Het woord 'Federated' stamt af van 'Federatie - een verbond van samenwerkende lichamen of staten die hun zelfstandigheid behouden [3]' en 'Identity management' stamt af van 'het beheer van (gebruikers)identiteiten en attributen'. FIM kan dan ook het best worden omschreven als *"een stelsel van afspraken, standaarden en technologieën die het mogelijk maken om elektronische identiteiten en bijbehorende profielen overdraagbaar en uitwisselbaar te maken tussen diverse autonome domeinen, zowel binnen één organisatie als tussen organisaties onderling"*.
Dit betekent concreet dat een authenticatie-oplossing, zoals geïmplementeerd door een bepaalde organisatie of organisatieonderdeel, door een andere organisatie of organisatieonderdeel kan worden hergebruikt. FIM stelt gebruikers hierdoor in staat om:

- Eén gebruikersaccount te verkrijgen om toegang te krijgen tot verschillende (organisatieoverschrijdende) netwerken en systemen (domeinen);
- Hun gebruikersaccounts over verschillende (organisatieoverschrijdende) domeinen met elkaar te verbinden, zonder dat hierbij één centrale database met accountgegevens ontstaat;
- Aan te loggen op hun account door gebruik te maken van het authenticatiemiddel van hun keuze;
- Toegang te krijgen tot verschillende applicaties binnen deze (informatieoverschrijdende) domeinen door slechts één keer aan te loggen (reduced/single sign-on).

In Figuur 1 is het concept van FIM op hoofdlijnen weergegeven. In de figuur wordt een gebruiker door een bepaalde organisatie geauthenticeerd met behulp van een gebruikersID en een authenticatiemiddel, waarna de identificatiegege-

[1] Roger Sullivan et al, OASIS Workshop, Gartner, Wednesday 20 april 2005
[2] KPMG National Identity Management Survey 2003
[3] www.woordenboek.nl

vens van deze geauthenticeerde gebruiker worden uitgewisseld met andere organisaties. Op basis van deze ontvangen identificatiegegevens en het bijbehorende profiel kunnen deze andere organisaties steunen op de door de eerste organisatie verrichte authenticatie, de gebruiker uniek herleiden in de eigen administratie en bepalen of deze al dan niet toegang mag worden verleend tot een elektronische dienst. Behalve identiteitsinformatie kunnen in het profiel van de gebruiker aanvullende gebruikersattributen, zoals zijn leeftijd staan vermeld. Op basis van de vermelde leeftijd kan dan bijvoorbeeld eenvoudig worden bepaald of de van toepassing zijnde gebruiker al dan niet (wettelijk) bevoegd is om een bestelling te plaatsen.



Figuur 1: Het concept van Federated Identity Management

Hoe werkt Federated identity management?

Functionele werking Federated Identity Management

In de onderstaande figuur wordt aangegeven op welke wijze een FIM-oplossing qua functionaliteit werkt. In deze beschrijving gaan we uit van John, die op basis van zijn werkaccount tevens toegang krijgt tot informatie in systemen bij zijn relaties. Op hoofdlijnen kunnen twee primaire processen worden onderkend, te weten het initiële registratieproces (1 en 2) en het gebruikproces (3, 4, 5 en 6).

Initiële registratieproces

Alvorens John gebruik kan maken van elektronische diensten, dient hij te zijn geregistreerd bij een authenticatiedienst en in het bezit te zijn van een authenticatiemiddel. In dit voorbeeld is de werkgever van John de organisatie die optreedt als authenticatiedienst en John bij zijn indiensttreding voorziet van een unieke gebruikersID en authenticatiemiddel (1). Nu kan John gebruikmaken van de elektronische voorzieningen van zijn werkgever, zoals inloggen op het bedrijfsnetwerk en het openen van zijn e-mailaccount via internet.

Omdat John en zijn collega's vanuit hun functie vaak toegang dienen te verkrijgen tot de informatiesystemen van relaties, zoals klanten of leveranciers, heeft hun werkgever besloten een directe beveiligde verbinding aan te leggen tussen de eigen systemen en die van haar relaties. Bij het aangaan van deze vertrouwensrelaties (2) worden afspraken gemaakt over onder meer het beheer van gebruikers, beveiligingseisen, het te hanteren authenticatiemiddel, het gebruik van unieke gebruikersID's, technische protocollen en juridische zaken zoals aansprakelijkheid.

Gebruiksproces

Voordat John toegang wordt verleend tot het systeem van zijn werkgever, dient hij zichzelf te authenticeren met behulp van zijn authenticatiemiddel (3). Op basis van de gecontroleerde identiteit bepaalt zijn werkgever vervolgens welke rechten John binnen het bedrijfsnetwerk heeft en wordt hem autorisatie verleend (4). Wanneer John voor het verrichten van zijn werkzaamheden toegang nodig heeft tot het bedrijfsnetwerk van een relatie, draagt het informatiesysteem van John's werkgever John's identiteitsgegevens en eventueel aanvullende informatie over aan de relatie (5). Na ontvangst van deze identiteitsgegevens bepaalt de klant of de in het bericht vermelde identiteit (John) toegang mag worden verleend tot de gevraagde diensten. Indien John voldoende rechten heeft, kan John direct autorisatie worden verleend (6). Een extra authenticatie is in dit geval overbodig aangezien de relatie weet dat John reeds door zijn werkgever succesvol is geauthenticeerd.

Voornaamste componenten binnen een FIM-oplossing

De afgelopen jaren zijn binnen organisaties diverse systemen ontwikkeld die interne federatie van identiteitsinformatie mogelijk maken. Een bekend voorbeeld is Kerberos. Wat nieuw is, is dat deze technieken nu ook buiten het eigen domein kunnen worden gebruikt en dat hierdoor aanzienlijk meer voordelen kunnen worden behaald. Dit maakt de problematiek echter ook aanzienlijk complexer, omdat nu allerlei additionele afspraken moeten worden gemaakt. De voornaamste aandachtspunten zijn hieronder weergegeven.

Technisch

- FIM-*systeem* - Dit is de voorziening die ervoor zorg draagt dat identiteiten aan elkaar kunnen worden gerelateerd, policies kunnen worden gedefinieerd en gebruikers- en authenticatie-informatie kunnen worden uitgewisseld tussen verschillende partijen en domeinen. Voorbeelden van dergelijke systemen zijn de FIM pakketten van RSA en IBM (Tivoli) en het open source product A-Select.
- *Directories* - Dit zijn databases waarin informatie is opgeslagen over gebruikers zoals gebruikersID's, verstrekte authenticatiemiddelen, gebruikersattributen en rollen.
- *Interfaces* - Het FIM-systeem zal diverse technische interfaces hebben met verschillende applicaties, webdiensten,

Figuur 2: Functionele werking van Federated identity management

domeinen, directories en authenticatieservers.
• *Authenticatiemiddelen* - Bij een FIM-oplossing zal minimaal één authenticatiemiddel moeten worden uitgegeven aan gebruikers.

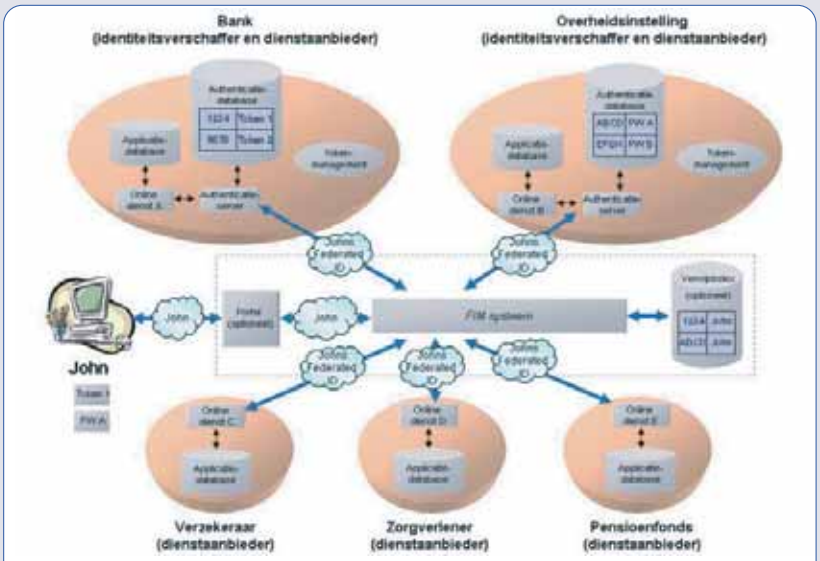
Functioneel
• *Gebruikersbeheer* - Het proces met betrekking tot gebruikersbeheer regelt de uitgifte en intrekking van gebruikersID's, attributen en, indien van toepassing, authenticatiemiddelen.
• *Authenticatiedienst* - Dit is een partij die gebruikers identificeert en de gebruikers voorziet van een gebruikersID en authenticatiemiddel. De authenticatiedienst verricht tevens de authenticatie van gebruikers voor dienstaanbieders en gebruikt hiervoor doorgaans een authenticatieserver en een gebruikers- en authenticatiedatabase.
• *Dienstaanbieder* - Dit is een partij die één of meerdere online-diensten aanbiedt en voor de authenticatie van haar gebruikers gebruikmaakt van de authenticatiediensten van één of meerdere authenticatiediensten.

Organisatorisch
• *Mapping van identiteiten* - GebruikersID's worden in de praktijk veelal niet consistent toegepast. Zo kan het voorkomen dat een gebruiker bij een bepaalde toepassing bekend staat onder gebruikersID 'JJansen' en bij andere toepassingen als '12345' of 'JanJansen21'. Omdat het in al deze gevallen om dezelfde gebruiker gaat, zullen deze gebruikersID's binnen een FIM-oplossing aan elkaar moeten worden gerelateerd. De mapping van identiteiten wordt vastgelegd in bijvoorbeeld een verwijsindex. Een alternatief voor de mapping van identiteiten is (organisatieoverschrijdende) afspraken te maken over het gebruik van één uniek gebruikersID voor alle gebruikers. De authenticatiedienst en dienstaanbieder zijn gezamenlijk verantwoordelijk voor de mapping van gebruikersID's.
• *Afspraken* - Alle bij een FIM-oplossing betrokken partijen (authenticatiediensten en dienstaanbieders) zullen afspraken moeten maken met elkaar over het gebruik van elkaars authenticatiemiddelen, gebruikersinformatie, te hanteren technische protocollen, vereiste betrouwbaarheidsniveau en juridische aansprakelijkheid.

FIM-architectuur
In de figuur hiernaast is een overzicht weergegeven van een wat complexere FIM-architectuur. De architectuur beschrijft een hypothetische oplossing waarbij een bank, een overheidsinstelling, een verzekeraar, een zorgverlener en een pensioenfonds afspraken hebben gemaakt over het onderling gebruik van de identiteitsinformatie van de banken en de overheidsinstelling.
Wanneer John op het portaal inlogt om vervolgens toegang te krijgen tot één van de achterliggende diensten, krijgt hij een keuzescherm te zien met welk authenticatiemiddel hij zich wenst te authenticeren. Hij kan hierbij kiezen of hij gebruik wenst te maken van het token (token 1) dat hij van zijn bank heeft verkregen of van een wachtwoord (PWA) dat hij van de overheidsinstelling heeft gekregen.
Afhankelijk van zijn keuze, wordt John door het FIM-systeem gerouteerd naar de betreffende identiteitsaanbieder om het authenticatieproces te doorlopen. Na succesvolle authenticatie zal de authenticatiedienst de identiteitsinformatie over John aan het FIM-systeem terugkoppelen. Afhankelijk van de door John gekozen dienst, zal het FIM-systeem in de verwijsindex de juiste gebruikersID van John opzoeken en deze aan de dienstaanbieder doorgeven. De reden hiervoor is dat een dienstaanbieder bijvoorbeeld niets kan met het bankID (1234) omdat John bij hen geregistreerd staat onder een ander gebruikersID (ABCD).
Binnen de bovenstaande architectuur zullen onder meer afspraken moeten worden gemaakt over de aan te sluiten diensten, de aan te sluiten authenticatiediensten, het beheer en de vulling van de verwijsindex (mapping van identiteiten), het beheer van het FIM-systeem, de betrouwbaarheidsniveaus van uitgegeven authenticatiemiddelen, de technische interfaces, aansprakelijkheid en de doorrekening van kosten (voor authenticaties en aanschaf en beheer van het FIM-systeem).

Voordelen van Federated Identity Management
Hieronder zijn de voornaamste voordelen weergegeven.

Verlaging van operationele kosten
FIM draagt eraan bij om een deel van de identity and access management-processen te stroomlijnen, harmoniseren en te consolideren. Hierdoor hoeft het beheer van gebruikers en hun authenticatiemiddelen slechts éénmaal te worden belegd bij de verantwoordelijken en niet voor elke applicatie opnieuw te worden ingericht. Daarnaast hoeft niet voor elke nieuwe gebruiker van een applicatie een nieuw en kostbaar authenticatiemiddel te worden verstrekt. Tenslotte zullen gebruikers, door de reductie van het aantal verschillende authenticatiemiddelen, minder snel hun authenticatiemiddel vergeten of kwijtraken, wat een significante verlaging in helpdeskkosten en overhead teweegbrengt.
Gebruikersvriendelijkheid
Een andere reden om een FIM-aanpak te hanteren, is het bevorderen van het gebruikersgemak. Een gebruiker behoeft zich slechts eenmaal bij de door hem gewenste authenticatiedienst te registreren en kan zich vervolgens op basis van hetzelfde authenticatiemiddel bij diverse andere organisaties authenticeren. Hiermee wordt voorkomen dat de gebruiker wordt voorzien van een digitale sleu-



Figuur 3: Voorbeeld van een FIM-architectuur

telbos. Daarnaast is binnen een FIM-omgeving het "single sign on"-principe van toepassing. Dit houdt in dat de gebruiker zich maar eenmaal behoeft te authenticeren en, indien deze voldoende autorisaties bezit, vervolgens direct toegang heeft tot andere elektronische diensten.

Risicobeheersing

Doordat de gebruiker niet wordt voorzien van een diversiteit aan authenticatiemiddelen en zich meer bewust is van het feit dat het middel voor diverse toepassingen kan worden toegepast, zal de gebruiker geneigd zijn het authenticatiemiddel met de nodige voorzichtigheid te behandelen. Daarnaast wordt de verantwoordelijkheid van het beheer van gebruikersID's en authenticatiemiddelen belegd bij de juiste stakeholders. Hierdoor zal de toepassing van FIM bijdragen aan het kunnen voldoen aan wet- en regelgeving, zoals de Wet bescherming persoonsgegevens en Corporate Governance richtlijnen zoals Sarbanes Oxley en Basel II.

Innovatie

Door het slim inrichten van FIM kunnen tenslotte nieuwe (organisatieoverschrijdende) toepassingen efficiënt en op een veilige wijze naar uw klanten, partners en leveranciers worden ontsloten, zonder dat hiervoor het gehele beheer van gebruikers en authenticatiemiddelen opnieuw behoeft te worden ingericht.

Standaarden en specificaties

Op dit ogenblik is een groot aantal verschillende initiatieven gaande die de uitdagingen met betrekking tot FIM, zoals standaarden, oppakken. De volgende vier initiatieven zijn het meest zichtbaar.

The Organization for the Advancement of Structured Information Standards (OASIS)

OASIS is een wereldwijde non-profitorganisatie die zich richt op standaardisatie van het XML-berichtenverkeer. OASIS heeft aan de basis gestaan van onder meer de volgende standaarden:

- Security Assertions Markup Language (SAML) - een XML-formaat voor het uitwisselen van authenticatie- en autorisatiegegevens (bijvoorbeeld:'heeft Persoon X recht op toegang tot dienst Y?'). Deze standaard is de basis voor veel FIM-oplossingen.
- eXtensible Access Control Markup Language (XACML) - een XML-formaat voor het definiëren van regels voor toegangscontrole. Om te bepalen of een gebruiker toegang krijgt tot een bepaald systeem, kunnen Policy Decision Points (PDP's) binnen SAML autorisatie-informatie consulteren die is opgemaakt in XACML.
- Directory Services Markup Language (DSML) - een XML-formaat voor het uitwisselen van directory gegevens over HTTP, in plaats van LDAP.
- Service Provisioning Markup Language (SPML) - een XML-formaat voor het automatisch aanmaken, wijzigen en verwijderen van gebruikersaccounts.

The Liberty Alliance Project

The Liberty Alliance Project is een alliantie van meer dan 150 bedrijven (waaronder RSA, SUN en HP), diverse non-profitorganisaties en overheidsinstellingen. The Liberty Alliance heeft een standaard gedefinieerd voor organisatieoverschrijdend (federatief) identiteitsbeheer. De standaard is voornamelijk in gebruik ten bate van federatieve single sign on oplossingen voor toegang tot de diensten over meerdere organisaties heen. The Liberty Alliance maakt hiervoor onder meer gebruik van SAML.

Web Services Security (WSS)

WSS, een initiatief van Microsoft en IBM, definieert een familie van standaarden voor de beveiliging van XML-berichtenverkeer over het Simple Object Access Protocol (SOAP). De WS-specificaties zijn ontwikkeld met als uitgangspunt dat deze interoperabel zijn met reeds bestaande beveiligingsmodellen zoals wachtwoorden, SAML en PKI.

Shibboleth

Shibboleth is een project van Internet2. Een belangrijk doel binnen Shibboleth is het waarborgen van de privacy van gebruikers. Shibboleth is afkomstig uit de onderwijssector en is gebaseerd op SAML.

Convergentie van standaarden

Ofschoon deze organisaties in eerste instantie veelal afzonderlijk bezig waren met het ontwikkelen van eigen FIM-standaarden, lijken deze initiatieven zich nu toch meer en meer te richten op één gezamenlijke standaard welke onlangs is vastgesteld, namelijk SAML 2.0.

Praktijkvoorbeelden van FIM

In de praktijk zijn diverse voorbeelden van FIM-implementaties terug te vinden. Bekende en zichtbare implementaties zijn onder meer de Passportdienst van Microsoft en de initiatieven binnen de Nederlandse en Amerikaanse overheid.

Microsoft Passport

De .NET-passport-dienst van Microsoft. Passport stelt gebruikers in staat zich bij diverse online-diensten aan te melden door gebruik te maken van één gebruikersnaam (e-mailadres) en een wachtwoord. Voorbeelden van door Passport ondersteunde diensten zijn Hotmail, MSN, Nasdaq, Starbucks en tot voor kort eBay.

Overheidsinitiatieven

Daarnaast zijn vooral in de overheidssector veel zichtbare FIM-initiatieven gaande. Onder de noemer DigiD heeft de Nederlandse overheid een start gemaakt met een overheidsbrede FIM-implementatie.

Conclusie

FIM biedt organisaties in potentie substantiële kostenvoordelen en biedt gebruikers het aantrekkelijke vooruitzicht om niet al die wachtwoorden te hoeven onthouden. Hoewel FIM in de praktijk steeds vaker succesvol wordt toegepast, is echter nog niet geheel duidelijk in welke richting FIM zich zal gaan bewegen. Dit komt enerzijds doordat veel partijen simpelweg nog niet klaar zijn voor een implementatie over de organisatiegrenzen heen omdat het eerst de eigen processen op orde zal moeten hebben en anderzijds doordat veel producten nog niet aan uitgekristalliseerde standaarden voldoen.

Om te voorkomen dat FIM nu onterecht naar het rijk der fabelen wordt verwezen of juist als de heilige graal wordt gezien binnen Identity Management, willen de auteurs de lezer graag de volgende slotoverwegingen meegegeven:

-Utopische dromen over 'één authenticatiemiddel voor alles' hebben plaatsgemaakt voor meer pragmatische benaderingen om het aantal authenticatiemiddelen te reduceren.

- Elektronische sleutelbossen zijn onvermijdelijk, maar kunnen substantieel worden verkleind door het toepassen van FIM.
- De acceptatiegraad bij eindgebruikers voor de uitgifte van nieuwe, geïsoleerde authenticatiemiddelen neemt steeds verder af.
- Standaarden met betrekking tot FIM beginnen nu te convergeren en zouden nu al moeten worden ingebed binnen beveiligingsarchitecturen.
- FIM gaat niet alleen over het realiseren van technische interoperabiliteit. Het gaat ook over het opbouwen van vertrouwensrelaties tussen partijen, het aangaan van juridische contracten, het omarmen van gezamenlijke beleidsuitgangspunten, authenticatiemiddelen en verklaringen.
- FIM maakt de bescherming van privacy de van gebruikers een noodzaak.
- Tenslotte zegt de Burton Group nog het volgende over FIM: "Issues will remain, but necessity is the mother of invention" [4]

Dit artikel is een aangepaste versie van het artikel dat eerder verschenen is in Compact

[4] Burton Group - Federation makes waves as standards and trust models emerge

TSTC

ICT en Security Trainingen

TSTC is een gerenommeerd IT opleidings-instituut en erkend specialist in informatie-beveiliging- en cybersecurity trainingen.

Security professionals kunnen bij TSTC terecht voor bijna vijftig security trainingen op zowel technisch als tactisch- strategisch gebied. Naast alle bekende internationaal erkende titels is het ook mogelijk diepgang te zoeken in actuele security thema's.

Top 10 Security trainingen

CEH • OSCP • CCSP • CCFP • CISSP • CJCISO • CRISC
Privacy CIPP/E-CIPM • CISM • ISO 27001/27005/3100

Recognition for Best ATC's and CEI's

TSTC Accredited Training Center of the Year 2016

Circle of Excellence Instructor 2016

www.tstc.nl

Want security start bij mensen!!

TEARS-FREE

You wanna cry? Been staring at a ransomware screen? The Attributer hopes not, but we all know it happened to a lot of people. So, what can we learn from this global incident and what should we do about protecting ourselves in the future? Three years ago The Attributer wrote an article named 'Patched'. We shall re-examine some of the principles mentioned then in the light of recent experiences with malicious software attack vectors.

Software patching is a standard security measure for maintaining the integrity of IT systems, and hence the business functionality that they perform and the business goals and success factors that they support. It is a conventional 'control strategy'. We should keep our systems patching up to date. Simple! Or is it? In the case of Wanna-Cry, it is clear that many systems at risk had not been patched, so why not?

The primary concern of patching is that there are vulnerabilities in complex software systems that become known as exploits for hacking and malware attacks. Software vendors issue patches and system managers apply the patches. However, there are many more aspects of patch management that bring more complex, unintended, incidental threats and vulnerabilities and therefore put the business at risk. If you want to know why the vendors can't supply bug-free software, it's because highly complex systems exhibit what are known as 'emergent properties'. These are unexpected and usually unwanted system behaviours that are the result of intense complexity. It is beyond human capability (at least for the time being) to predict all these behaviours and so we must live with the real world fact that software bugs exist and that malicious code can exploit them.

The standard approach is based up on the assumption that the patches will work perfectly. This is known from experience not to be the case. A patch is a software modification to fix an original flaw in a program, and so it is just another piece of code to be deployed and 'inserted' into the software. It will often delete previous code and previous parameter settings, over-writing them with new stuff. In a complex operating system environment such a change will often touch many parts of the system, parts that are shared with other applications that have a dependency on OS functionality. How will these other applications be affected? Whoops! Emergent properties showing up again. Hmmm, now we see that there are potential uncertainties here that may have been overlooked. Well that's risk for you: uncertainty of outcomes.

This means that patch management is not just a simple exercise in applying the patches. It requires a careful risk management approach. It needs an end-to-end process that takes account of the other incidental risks. Typically there will be hundreds, even tens of thousands of platforms to be patched, and this can take a long time to roll out the patch. Another issue is: which systems should be patched first and what is the priority order?

The patch management process should begin with creating a state of 'patch-readiness', meaning having the process in place and tested for it's own suitability. Some of the key steps to be incorporated into the process should include:

1. Make the patch management process an integral sub-process of business continuity management.
2. Ensure that patch management will enable business and not hinder it.
3. Assess the business criticality of IT systems so that priority in patching can be decided based on critical need.
4. Ensure good vulnerability intelligence from CERT bulletins and the like, so that zero-day attacks can be identified and likely consequences assessed. This is an essential aspect of patch prioritisation – which ones should be applied first and what sequence of patches is the best. Some at least will be recursive patches – patches on patches.
5. Test each patch on a test platform to assess its effects on overall system performance. Assess the risks of patch failure.
6. Always develop a regression plan before applying any patch in a live production environment. This may require having a disk image of the unpatched state, because many patches are irreversible once applied.
7. The regression plan should also be tested thoroughly to ensure that it would work if needed.
8. Roll out the patches in a systematic way according to the priorities identified and monitor the impacts on live production systems in case the patch testing has failed to identify problems.

The SABSA approach requires us to consider all aspects of risk from a business perspective, not just applying controls in a blind, uninformed fashion. Far too often the application of security controls is done without this type of holistic consideration.

The Attributer

INZICHT IN MOBIELE APPARATEN: DE SLEUTEL TOT BEVEILIGING

In deze steeds snellere wereld zijn mobiele telefoons van onschatbare waarde. Medewerkers kunnen werken waar ze willen en wanneer ze willen – alles wat nodig is, is een internetverbinding. Dat zorgt ook voor risico's: de meeste apparaten werken via een eigen mobiele verbinding, maar maken van tijd tot tijd ook verbinding met het bedrijfsnetwerk voor toegang tot gevoelige bedrijfsdata als e-mail en presentaties.

Nu zou dat geen probleem zijn als deze apparaten adequaat beveiligd waren, maar dat is vaak juist niet het geval. Bovendien richten cybercriminelen en hackers hun pijlen steeds vaker specifiek op mobiele apparaten, omdat ze weten dat deze relatief eenvoudig toegang tot waardevolle bestanden bieden. Het goede nieuws is dat, zoals bij elk beveiligingsrisico, er wel degelijk maatregelen kunnen worden getroffen.

Weten wat de risico's zijn, is het halve werk

Onlangs publiceerde Lookout de zogenoemde mobile risk matrix, waarmee bedrijven heel duidelijk kunnen zien welke mobiele dreigingen er zijn en daar gericht actie tegen ondernemen. Naast app-gebaseerde dreigingen en verouderde besturingssystemen, is app-gedrag een groot probleem: voor gebruikers is vaak niet inzichtelijk welke toegang apps hebben. Voor hun werkgevers kan dat tot compliance- of beveiligingsproblemen leiden.

Neem een kaartenapp: natuurlijk moet die toegang tot GPS-sensoren krijgen om goed te kunnen werken. Toegang tot contactgegevens of de microfoon is dan weer een stuk minder logisch. Maar hackers investeren veel geld om zich dit soort toegang stiekem te kunnen verschaffen: als het lukt, kan met doorverkoop van deze gegevens veel geld worden verdiend. Helaas beheert de meerderheid van de bedrijven hun mobiele apparaten niet goed, of zelfs niet. Software-updates worden vaak niet uitgevoerd, beleid over bepaalde problematische applicaties ontbreekt. Soms is dat een gevolg van een gebrek aan juiste technologie, maar vaak weten bedrijven ook gewoon niet waar ze moeten beginnen.

Waar moet je beginnen?

Allereerst is het belangrijk dat een bedrijf de risico's inzichtelijk maakt door ze onder te verdelen. Voor mobiele apparaten zijn er drie kerncategorieën: interne & externe bedreigingen, softwarekwetsbaarheden en gedrag & instellingen. Nagenoeg elk mobiel risico is in één van deze categorieën onder te brengen, of het nou gaat om hackers die een gerichte aanval uitvoeren of de CEO die zonder het te weten een verdachte app downloadt. Vervolgens moet bij elk risico bedacht worden wat de meest gevoelige plekken zijn. Voor mobiel zijn dat applicaties, apparaat-type, netwerken en web & content. Het is inmiddels net zo belangrijk om te weten wat er op mobiele apparaten gebeurt, als wat er in de datacentra plaatsvindt.

Minstens net zo belangrijk is om uit te zoeken welke invloed apps uitoefenen. Zonder professionele oplossing kan dat lastig zijn: per apparaat gedetailleerd uitzoeken welke apps erop staan, welke versie van een besturingssysteem gebruikt wordt, en welke beveiligingspatches zijn geïnstalleerd is een tijdrovende klus. Maar bedenk ook dat kwaadwillende apps en geïnfecteerde devices uiteindelijk voor nog veel meer ellende kunnen zorgen.

Tref de juiste maatregelen

Toch is weten welke risico's er zijn maar het halve gevecht. IT-beveiligingsprofessionals moeten onderkennen dat mobiele dreigingen bij elk bedrijf voor andere risico's zorgen. Er is niet één medicijn: elk bedrijf moet investeren in een op maat gemaakte oplossing. Dat is een flinke opgave, maar geen onmogelijke: voor bedrijven die mobiele risico's serieus nemen, zijn er genoeg hulpmiddelen. Organisaties die de juiste maatregelen treffen, zullen zonder zorgen kunnen blijven profiteren van de grote voordelen die mobiele apparaten bieden.

Lookout

Jeroen Wijdogen is mobile security consultant bij Lookout.

HARDWARE.IO
KLEINSCHALIG EN INTERESSANT

Van 19 tot en met 22 september vindt de derde editie van Hardwear.io plaats. Deze kleinschalige vierdaagse training en conferentie, waar de veiligheid van hardware centraal staat, zal wederom in Den Haag worden gehouden.

De bijeenkomst telde vorig jaar circa 200 deelnemers. De verwachting is dat dit jaar het aantal deelnemers zal toenemen, zonder dat daarbij de informele sfeer die kenmerkend is voor dit kleinschalige event zal verdwijnen. In vier dagen zullen de deelnemers getraind en bijgepraat worden over tal van onderwerpen. Het definitieve programma wordt eind juli bekend gemaakt. Bekend is al dat Dr. Sergei Skorobogatov, Senior Research Associate aan de universiteit van Cambridge, een van de keynotes zal verzorgen. Trainers en sprekers zijn vanzelfsprekend professionals. Om een indruk van de opzet en het programma te krijgen, zijn op de website van Hardwear.io links naar de YouTube-opnames van de 2016 talks geplaatst.

Voor wie is Hardwear.io interessant?

De twee voorgaande edities van Hardwear.io zijn bezocht door onderzoekers, security professionals en vertegenwoordigers van

verschillende (semi-) overheidsinstellingen. Deze groepen zullen ook dit jaar weer aanwezig zijn. Daarnaast verwacht de organisatie bezoekers die specifiek afkomen op de trainingen en talks die betrekking hebben op IoT, betalingsverkeer en crypto currencies.

VERSLAG CISO 17 - ESMERALDA-LEZING

CYBERSECURITY OP DE BESTUURLIJKE AGENDA

In de Esmeralda-lezing, die dit jaar plaatsvond op 7 juni in het Koetshuis van Kasteel de Haar, keek Aart Jochem terug op zijn ervaringen als CISO bij Capgemini, GovCert en PGGM.

Bart van Staveren opende de bijeenkomst in de fraaie ambiance met een korte toelichting op de naam Esmeralda-lezing. Die is afgeleid van het sprookje van Jaap Fischer waarin Hans eist dat zijn vrouw een meisje moet zijn met prachtige kleren en goudblonde lokken, met ogen als meren die niet kunnen jokken, een mond als van honing en dan weer scherp als een mes, en hopelijk is haar vader koning en zij dan prinses. Maar… ze moet Liesje heten! En toen keek de prinses hem aan en zei: "Ik heet Esmeralda, maar zeg maar Liesje". Deze versie van toe-eigening van identiteit was aanleiding tot de naamgeving van de Esmeralda-lezingen, waarin bijzondere buitenstaanders hun visie op ons werkveld geven.

Deze keer had de organisatie het idee aangepast en iemand uit eigen gelederen gevonden om zijn ervaring en visie met ons te delen. Aart Jochem is Corporate Information Security Officer bij PGGM, de pensioenuitvoerder voor onder meer het pensioenfonds voor Zorg en Welzijn. Hij heeft een achtergrond in elektrotechniek en computerarchitectuur en heeft voor zowel publieke als private organisaties gewerkt voordat hij in december 2016 de overstap maakte naar PGGM. Als een van de grondleggers van het Nationaal Cyber Security Centrum in Nederland en daar verantwoordelijk voor monitoring en respons heeft hij bijgedragen aan de ontwikkeling van cyber security in Nederland en Europa en van dichtbij ervaren hoe incidenten impact hebben op organisaties. Aart is sinds 2006 actief lid van het GvIB/PvIB.

Aart Jochem behandelde de trendrapportage en factsheets van GovCert en stond uitgebreid stil bij de case Diginotar, medio 2011, die voor alle aanwezigen nog een bekend fenomeen was. Aart kon een mooi 'inside' beeld schetsen van de ontwikkelingen die in de eerste dagen van de Diginotar-crisis plaatsvonden en welke acties er waren ondernomen. Aart benadrukte dat het succes van de afhandeling lag en ligt in herkenbaarheid en bereikbaarheid. Door het goed opgebouwde netwerk kon er snel geschakeld worden en door het snel inrichten van een centraal centrum is in de bereikbaarheid voor alle relevante actiehouders voorzien.

Aart vond het teleurstellend dat bij de overgang van GovCert (Computer Emergency Response Team voor de Rijksoverheid) tot Nationaal Cyber Security Centrum (NCSC) in 2012 geen Nationaal Centrum is ingericht, maar dat NCSC nog steeds beperkt blijft tot de Rijksoverheid en 'vitale functies'.

Verder besprak Aart dat cases als de aanval op KPN en de DDos-aanvallen op de banken in 2013 alsmede de actie van Brenno de Winter om een tijd lang iedere dag een lek te bespreken ertoe hebben bijgedragen dat een aantal bedrijven nu over CERT/CISO-teams beschikken.

Ontwikkelingen

Vanuit zijn ervaring ziet Aart belangrijke ontwikkelingen:

- Samenwerking. Aart benadrukte vooral de rol van samenwerking. Er zijn nu veel CERT's. Het gebruik van dezelfde tools stelt organisaties in staat snel met elkaar te schakelen en gezamenlijke acties op te pakken. Bij PGGM heeft Aart een CERT ingericht en daarmee verbinding gelegd met de ketenpartners. Bij PGGM zitten de CERT en kwaliteitsmanagement met succes bij elkaar, dit levert een

goede kruisbestuiving. Het treft hem dat bij veel besturen/organisaties er slechts een paar personen zijn, die beseffen dat een kleine fout op beveiligingsgebied kritiek kan uitpakken voor de organisatie.

- Professionalisering. Criminelen worden steeds professioneler. Dat brengt de noodzaak mee dat ook van onze kant continu aan de professionaliteit gewerkt moet worden. Een van die aspecten is dat criminelen meer tijd nemen om rustig kennis van de business op te doen om daarna heel gericht toe te slaan. De tijd van 'hit & run' is voorbij. Dat brengt de noodzaak mee om vroegtijdig aanvallen te detecteren. Continue monitoring/logging en opmerken van abnormaal gedrag. Van belang is het inrichten van eigen CERT die niet alleen moet focussen op de eigen organisatie, maar breed moet kijken naar ontwikkelingen en ook de omgeving erbij moet betrekken, met name de ketenpartners. Tot slot is het belangrijk te kijken naar de nieuwe instroom van problemen, die de noodzaak meebrengt medewerkers met een frisse kijk, kennis en ervaring aan te trekken: nerds en hackers.
- Veilige producten. Volgens Aart is er een grote urgentie om te kijken naar en het ontwikkelen van veilige producten. Hij besprak onder andere IP-scans, MongoDb en Agile-werken. Je hebt geen tijd meer om in alle rust een watervaltraject te doorlopen. Het wordt ook steeds moeilijker alle in en outs te kennen. De inrichting van zogenoemde devil teams is dan ook een goede richting.
- Raad van Bestuur. Aart komt tot de conclusie dat van de RvB een andere kijk, een ander geluid vereist wordt. De rol van een bestuurder zal in Belbin-termen van vormer/voorzitter naar zorgdrager moeten verschuiven. Besturen hebben ook zelf geleerd: door zelfassessments, incidenten en wetgeving. De samenleving verwacht tegenwoordig veel van bedrijven. Daardoor komt het besef dat de data het kapitaal van de organisatie vormt en continue innovatie in ICT essentieel is. Vanwege de samenhang wordt de rol van ketens steeds belangrijker, maar ook moeilijker. De RvB moet dus weten wie de strategische partners zijn en die beoordelen op hun interne beheersing, met name de leveranciers (zowel nieuwe als de bestaande). Daarbij is de CISO adviserend, onafhankelijk, en dient een directe lijn naar RvB te hebben.

Afsluitend ziet Aart de noodzaak dat bestuurders hetzelfde traject doorlopen als het PvIB de afgelopen tien jaar heeft doorgemaakt. En bestuurders moeten beseffen dat een substantieel deel van de innovaties aan IT-security nodig is; bijvoorbeeld tien procent, maar dat is geen hard getal. Dit dient vanaf het begin meegenomen te worden. Security by Design begint bij het bestuur. Het wordt essentieel dat besturen een intuïtie ontwikkelen voor (de risico's van) nieuwe ontwikkelingen.

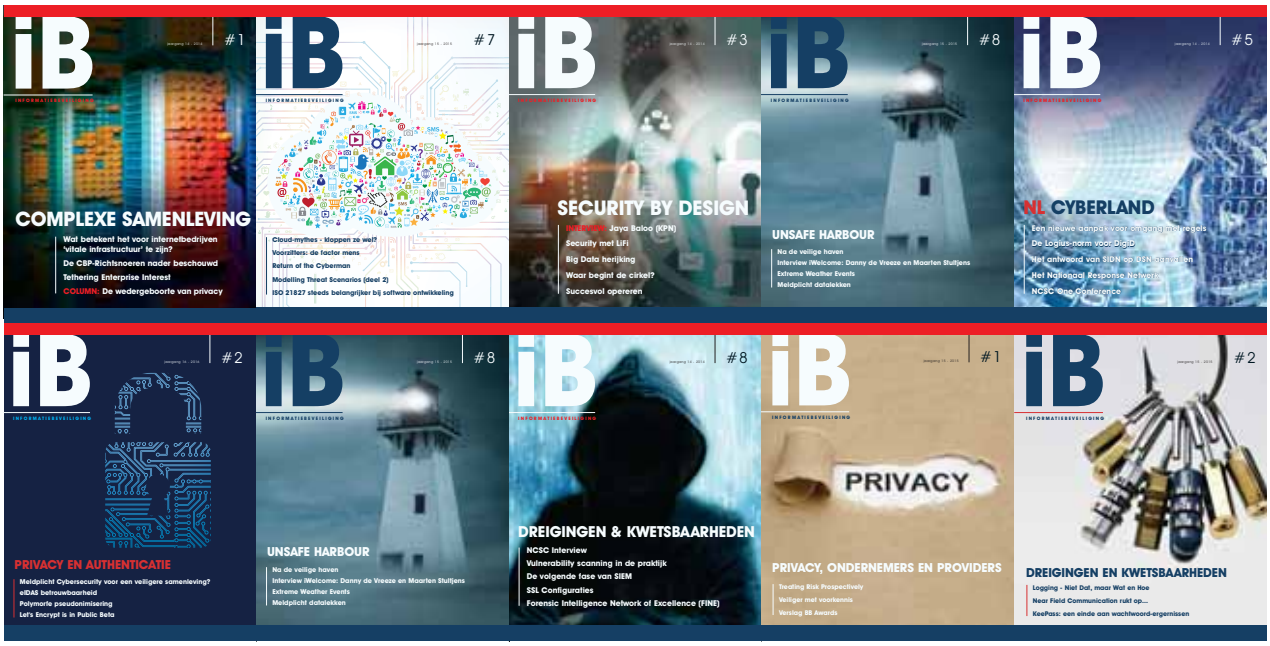
Tips

De laatste vraag van Bart was wat Aart afgelopen tien jaar aan NOREA heeft gehad. Aart gaf aan dat hij veel gehad heeft aan (de regelmatige ontmoetingen met) collega's en ook van de vertegenwoordiging door NOREA/PvIB van het vakgebied in de media. Tot slot adviseerde Aart om zelf (alsnog) een programmeertaal te leren, bijvoorbeeld C, Java, Jason of iets over API's om beter te begrijpen hoe bedreigingen kunnen ontstaan.

Geert Martens was senior ICT/OA auditor en senior proces en financieel controller bij UWV. Sinds februari 2017 is hij met pensioen, maar hij is nog steeds geïnteresseerd in issues ten aanzien van Governance, (risico)beheersing en kwaliteitszorg. Hij is bereikbaar via gjm.martens@hccnet.nl en via LinkedIn.

Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.



PVIB JUBILEERT

Het is nu tien jaar geleden dat PI en GvIB fuseerden tot PvIB. Hiermee ontstond een vereniging met zo'n 1200 leden. Allen professionals op het gebied van informatiebeveiliging. De vereniging moest hét kennisplatform zijn voor alle leden en op die wijze ondersteuning bieden voor de beroepsuitoefening in de praktijk. Het delen van kennis werd georganiseerd door het inrichten van commissies om kennis te verzamelen (K&I) en te delen (activiteiten, redactie en IBO -nu CISO-) aangevuld door ondersteunende commissies. Nu PvIB tien jaar bestaat, is dat ook voor de redactie een goed moment om terug te kijken of de vereniging de status heeft bereikt die ze beoogde bij de fusie en zo niet, wat er zou moeten veranderen om die status van hét kennisplatform voor de informatiebeveiligingsprofessional in Nederland te bereiken.

Lex Dunn

In de afgelopen tien jaar is het PvIB als vereniging behoorlijk gegroeid. Er zijn diverse initiatieven ontplooid vanuit PvIB, waarbij diverse leden (en ook niet-leden) hun steentje(s) hebben bijgedragen. Denk aan de expertbrieven, deelname aan Security Congressen en natuurlijk de artikelen in het blad. De themasessies worden steeds beter bezocht (in mijn begintijd bij de Activiteitencommissie waren we al blij als we eens dertig bezoekers hadden!)

Alles dus goed en wel? Nou nee. Ik zie telkens dezelfde gezichten als er iets georganiseerd moet worden. En alhoewel er in de diverse commissies de afgelopen jaren wel nieuw bloed is binnen gestroomd, komt het uiteindelijk toch vaak op dezelfde vrijwilligers neer. Ook blijkt het vaak een uitdaging om voldoende artikelen te krijgen voor het blad, het moeten doorschuiven van een artikel vanwege ruimtegebrek is een weinig voorkomend fenomeen. Bij deze dus een oproep aan al die leden, die wel eens overwogen hebben zich als vrijwilliger of


Lex Dunn


Lex Borger

auteur te melden, maar het om wat voor redenen dan ook nog niet gedaan hebben. Tot slot nog even over hét kennisplatform: vandaag de dag zijn er vele gremia die zich opwerpen als de vertegenwoordigers van cyber-Nederland. Tot op heden is het niet gelukt het PvIB dé partij te laten zijn die door BNR, NOS, Een Vandaag, en alle praatprogramma's gevraagd wordt om een toelichting te geven op ontwikkelingen of gebeurtenissen in het cyberwerkveld. We hebben ruimschoots specialisten voorhanden, maar het wil maar niet lukken de juiste specialist op het juiste moment aan het juiste (praat)programma te koppelen. Hoe kunnen we dat voor elkaar krijgen?

Lex Borger

Dit vraagt een kritische blik naar jezelf. We ontleden de stelling in delen. Wanneer ben je 'hét kennisplatform'? Ik zou denken: wanneer je bovenaan staat bij Google/Bing resultaten; wanneer professionals eerst op jouw website kijken als ze een vraag hebben; wanneer er over jouw vereniging geschreven wordt. Hoe doen we het op dit punt? Bij vlagen goed. Zeker voor Nederlandstalige termen scoort het PvIB vaak goed, maar niet per se. Over het PvIB wordt in andere vakpers niet veel geschreven. Toch ben ik hier wellicht te kritisch. Vaak word ik verrast door de plekken waar bijvoorbeeld een expertbrief opduikt als informatiebron. En dat het dan juist expertbrieven zijn die zo'n lange adem hebben, zegt wel wat over de collectieve expertise van het PvIB. Want hier hebben we het juist over het creëren van kennis. Doorgaan hiermee! En publiceer ze ook in het Engels.

Wanneer ben je 'voor de informatiebeveiligingsprofessional in Nederland' hét kennisplatform? Wanneer elke professional lid wil zijn; wanneer lidmaatschap vanzelfsprekend lijkt. Hier doet de vereniging het veel beter. We hebben een groot ledenaantal en ik merk dat wie zich in Nederland als IB-professional bekend maakt, het PvIB kent, en meestal om de activiteiten of het blad. Een kritische noot die ik hierbij heb, is dat we ook aandacht moeten blijven hebben voor de jongere professional.
Al met al: Het PvIB mag er zijn, maar het kan nog beter.

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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 2017
De abonnementsprijs in 2017 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

WAT GAAT DE TIJD TOCH SNEL!

Tien jaar geleden ontstond het PvIB uit een fusie van PI en het GvIB, met het doel de informatiebeveiliging op een hoger niveau te brengen en om een platform te bieden om kennis te kunnen delen. Dat is geweldig gelukt en één van de bewijzen hebt u momenteel in de hand. In de afgelopen tien jaar is informatiebeveiliging gegroeid tot een noodzaak om de sterk groeiende bedreigingen te kunnen pareren. Mijn overtuiging is dat de groei van het PvIB gelijke tred zal houden met de groei van het aantal bedreigingen. Het besef dat informatiebeveiliging noodzakelijk is, leeft bij het PvIB sterk. Jammer genoeg is dat besef niet overal aanwezig.

Terwijl ik deze column schrijf,denk ik terug aan 2007; het jaar van de oprichting van het PvIB. In dat jaar werd ook op een meesterlijke wijze de iPhone geïntroduceerd door Steve Jobs [1]. Met deze iPhone zette Apple de wereld op de kop. Door sommige analisten wordt de introductie van de iPhone gezien als één van de belangrijkste ontwikkelingen op het gebied van techniek. De start van de iPhone was het begin van het einde voor compact camera's, navigatiekastjes, discmans enzovoort. Door de enorme verkoopcijfers werden veel fabrikanten wakker geschud. Men had door dat er een nieuw tijdperk begonnen was en overhaast ontwikkelden ze hun eigen versie van de iPhone, veelal op het Android platform. De telefoonmarkt werd op de kop gezet.

Liet je vroeger trots je Nokia zien, nu hield je hem angstvallig in de zak en hoopte dat je niet gebeld zou worden. En Blackberry's? De introductie van de iPhone zorgde ervoor dat binnen tien jaar meer dan negentig procent(!) van de Nederlandse bevolking een smartphone had. Iedere medaille heeft een keerzijde, dus ook deze trend. De ontwikkelingen gaan snel en eenieder probeert de veranderingen bij te houden. En zo nu en dan gaat dat weleens ten koste van de beveiliging. Trouwe lezers van dit blad weten dat ik een sterke voorkeur heb voor iOS (de uiteindelijke naam voor iPhone OS), omdat Apple erop gebrand is deze gewoon veilig te laten zijn en te houden. Soms lukt dit niet, meestal wel. Op dit moment draait meer dan tachtig percent van de iPhones en iPads op de laatste versie van iOS. Het is volstrekt onbekend hoeveel Android-phones de laatste, meest veilige updates hebben. Schattingen van experts zijn slechts percentages gebaseerd op één cijfer.

U zult denken: "Waarom maakt Berry zich altijd zoveel zorgen over de veiligheid van telefoontjes?" De ontwikkelingen gaan snel en je nieuwe auto betalen met een vingerafdruk is prachtig, maar toch ook een beetje eng. Dat mijn telefoon op verzoek alle inlogcodes onthoudt is ideaal, maar toch ook wel een beetje eng. Het is en zal een wedloop blijven tussen nieuwe ontwikkelingen en veiligheid. Tussen hackers en ontwikkelaars, een wedloop waarbij af en toe de een of de ander voor ligt, zonder dat er een duidelijke winnaar is. Is alles dan verloren? Nee. Omarm de nieuwe ontwikkelingen, maar blijf nadenken over de mogelijke risico's van het gebruik.

Berry

Referentie

[1] iPhone introductie: https://www.youtube.com/watch?v=uD0UlkreOhc

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

INFORMATION SECURITY *CERTIFICATION TRACK*

- S-ISF®: Information Security Foundation opleiding
- S-ISP®: Information Security Practitioner opleiding
- S-ISME®: Information Security Management Expert opleiding

IT-SECURITY *CERTIFICATION TRACK*

- S-ITSF®: IT-Security Foundation opleiding
- S-ITSP®: IT-Security Practitioner opleiding
- S-ITSE®: IT-Security Expert opleiding

PRIVACY & DATA PROTECTION *CERTIFICATION TRACK*

- S-DPF®: Privacy & Data Protection Foundation opleiding
- S-DPP®: Privacy & Data Protection Practitioner opleiding

ETHICAL HACKING *CERTIFICATION TRACK*

- S-EHF®: Ethical Hacking Foundation opleiding
- S-EHP®: Ethical Hacking Practitioner opleiding
- S-EHE®: Ethical Hacking Expert opleiding

BUSINESS CONTINUITY *CERTIFICATION TRACK*

- S-BCF®: Business Continuity Foundation opleiding
- S-BCP®: Business Continuity Practitioner opleiding
- S-BCME®: Business Continuity Management Expert opleiding

Preparation courses

- CISSP® Preparation Course
- CCSP® Preparation Course
- CISM® Preparation Course
- CRISC® Preparation Course
- CISA® Preparation Course

Hierboven ziet u een greep uit ons portfolio. Bij de Security Academy kunt u terecht voor het behalen van verschillende internationale titels van SECO-Institute®, ISC²® en ISACA®. Daarnaast biedt de Security Academy een aantal opleidingen aan op specialistische onderwerpen binnen Security. Denk hierbij aan opleidingen als Internet of Things Security, Encryptie of Social Engineering.

Voor het complete overzicht, meer informatie en cursusdata kunt u terecht op onze website.

www.securityacademy.nl info@securityacademy.nl +31(0)348-40 80 61