iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#3

SECURITY BY DESIGN

INTERVIEW: Jaya Baloo (KPN)

Security met LiFi

Big Data herijking

Waar begint de cirkel?

Succesvol opereren

PROTACT
BY FOX IT

Hybrid SOC

ACCELERATING SECURITY OPERATIONS

Participation levels & tools for your SOC

Fox-IT introduces ProtACT Hybrid SOC. The foundation is a Shared SOC Service where experienced Security Analysts from Fox-IT deliver 24x7 incident handling capabilities.

With ProtACT Hybrid SOC you can participate anywhere in the process, depending on your ambition level, using tools we provide.

This paves the way for running your own SOC.

From full managed service to self-operated SOC

METRICS - REPORTS - ALERT & INCIDENT INVESTIGATION - SIEM-FEEDS - INCIDENT HANDLING - IOC-MANAGEMENT

MSSP — Fully managed service

LEVEL 1 — + real-time security metrics and reporting

LEVEL 2 — + basic investigation tooling, SIEM-feeds, full access to alerts and incidents

LEVEL 3 — + full detection and response tooling, incident handling capabilities & IoC-management

OWN SOC — All components implemented on-site to deliver a self-operated SOC

FOX IT

FOX-IT
Olof Palmestraat 6, Delft
PO BOX 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
E fox@fox-it.com

FOXPROTACT.COM

#SECURITY SPRINT

De Nucleair Security Summit (#NSS2014 op Twitter) was in Nederland. Dat is niet ongemerkt voorbij gegaan. Ik kan me niet herinneren dat er ooit zo veel omleidingen en afsluitingen ingesteld zijn en er zoveel militair vertoon rondom Schiphol en Den Haag was. Een grote verkeerschaos werd gevreesd, maar die bleef uit.
Waarom? De Nederlander bleef massaal thuis. Met thuiswerken of een dagje vrij werd de weg ontlast. We hadden als land voldoende veerkracht om dit op deze twee dagen te regelen.
Ik heb dit eens eerder meegemaakt. In 1984 woonde ik bij Los Angeles toen daar de Olympische Spelen georganiseerd werden. Het wielrennen werd bijna in mijn achtertuin georganiseerd. Ook toen werden vuile lucht en chaos op de weg verwacht, maar beiden bleven uit. De lokale bevolking ging een aantal weken massaal aan de carpool, een vierdaagse werkweek en reizen buiten de spits. Na de Spelen kwamen de smog en de gridlock terug.
Uit deze observaties concludeer ik dat we dus best gedurende een korte tijd flexibel kunnen zijn, maar niet altijd. De sprint van de NSS top of de Olympische Spelen zijn prima te lopen, maar maak er geen marathon van. Terwijl ik dat bedenk, denk ik aan de heren van de Secret Service. Zij lopen niet eens een marathon, het is meer een marathon van sprints. Eigenlijk is het dan geen wonder dat wij tegen hun maatregelen aankijken als zijnde extreem. Een eigen pantserlimousine meenemen, eigen helicopters, rijen containers, het is allemaal 'normaal' geworden voor deze agenten.
Zo kunnen we ook kijken tegen de beveiligingsmaatregelen uit onze eigen praktijk. Wij zijn dagelijks bezig met de details van maatregelen, maar de gebruikers die er 'last' van hebben niet. Voor hen zijn wij als informatiebeveiligers de extreem-denkende beveiligers die de marathon van sprints lopen. Voor hen is één sprint al veel, maar het is uit te leggen als je wel eens een keer 'extreme' maatregelen gebruikt, vooral als het voor een duidelijk doel is, zoals een migratie of een registratie. Maar daarna moet de beveiliging weer makkelijk en onzichtbaar zijn. Het moet vooral niet in de weg staan.
We kunnen dit als beveiligers vervelend vinden, we kunnen er tegen ten strijde trekken en campagnes over voeren. Uiteindelijk zul je moeten erkennen dat dit de aard van het beestje is: af en toe een beveiligingssprint mag, maar dan moet het weer even afgelopen zijn.

Lex Borger, hoofdredacteur

In dit nummer

SECURITY MET Li-Fi

COMMUNICATIE VIA LED LICHT

Het in Duitsland gevestigde Fraunhofer Instituut is één van Europa 's grootste toepassingsgerichte onderzoeks-organisaties. De onderzoeksinspanningen van Fraunhofer zijn volledig afgestemd op de behoeften van mensen: gezondheid, veiligheid, communicatie, energie en milieu. Binnen het Fraunhofer Instituut is professor Harald Haas actief. Onder zijn leiding is een technologie ontwikkeld waarmee een LED lichtbron geschikt gemaakt wordt om gegevens te verzenden. Deze techniek is bekend onder verschillende namen: Li-Fi (Light Fidelity), D-light of VLC (Visible Light Communications). Mondiaal zijn er naast het Fraunhofer Instituut verschillende onderzoeksinstituten en universiteiten bezig met onderzoek naar datacommunicatie via LED lichtbronnen. Deze partijen zijn verenigd in het Li-Fi Consortium waarin zij werken aan een standaard voor Li-Fi. In deze standaard zijn naast eigenschappen voor datacommunicatie ook een aantal zeer interessante functionaliteiten voor security toepassingen beschreven (hierover later meer).

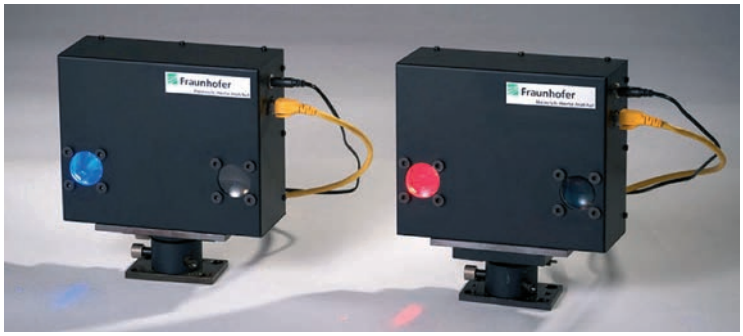
Li-Fi is een techniek om LED lichtbronnen te gebruiken voor dataoverdracht. Dit gebeurt met ultrakorte pulsen van licht die met het blote oog niet zijn te zien. Er hoeven maar een paar componenten van bestaande LED verlichting van gebouwen aangepast te worden om ze te laten functioneren als dataoverdragers. In principe kan elke gewone LED lamp met behulp van een Li-Fi microcontroller worden omgebouwd tot een Li-Fi transmitter. Het uitgezonden licht wordt vervolgens opgevangen door een optical receiver en omgezet in een digitaal signaal zodat een datacommunicatiestroom ontstaat.

De Li-Fi techniek kan worden gebruikt voor tweerichtingsverkeer. De uplink en downlink kunnen worden gescheiden op een aantal manieren. Hierbij kan worden gedacht aan scheiding op basis van; golflengte, tijdslot en/of type codering. Een andere mogelijkheid is ruimtelijke en/of optische scheiding. Bij bi-directionele datatransmissie dient de Li-Fi microcontroller -uitgerust met lichtbron als zender en een optical receiver als ontvanger- bij voorkeur ondergebracht te zijn in de behuizing van een lichtarmatuur. Onderzoekers van de Britse universiteiten van Oxford en Edinburgh hebben een techniek bedacht om de gegevens parallel te versturen met een rij LEDs waarin iedere lamp een andere datastroom verstuurt. Zij doen dit met een combinatie van rode, groene en blauwe LEDs. Hierdoor verandert de frequentie van het licht. Iedere lichtfrequentie verstuurt dan een andere gegevensstroom. Een team van wetenschappers aan de Chinese Fudan University, onder leiding van de professor Chi Nan, claimen met een 1 watt LED lamp de Li-Fi snelheid van 150 Mbit/s met succes in praktijksituaties te hebben getest. In deze praktijksituaties zijn normale, makkelijk verkrijgbare, onderdelen gebruikt.

Li-Fi vanuit informatiebeveiligingsoogpunt

Het gebruik van Li-Fi heeft vanuit informatiebeveiligingsoogpunt veel voordelen ten opzichte van wifi. Omdat muren een barrière voor licht vormen blijft Li-Fi binnen de ruimte waar het wordt uitgezonden. Mocht de ruimte voorzien van ramen, dan kan eenvoudig met doorzichtig filter folie een barrière worden gemaakt. Van ongewenste radiostraling buiten het gebouw heeft men bij Li-Fi geen last. Dit in tegenstelling tot wifi. Hierdoor is Li-Fi afluisterproof. Ook Interferentie tussen verschillende netwerken, wat vaak bij wifi voorkomt, is vrijwel afwezig omdat muren een barrière voor licht vormen. Het is relatief eenvoudig om de overgrote meerderheid van interferentie van natuurlijke bronnen, zoals zonlicht en kunstmatige bronnen (denk aan het in de optical receiver schijnen met een zaklamp) met behulp van optische filters (die verzadiging van de ontvanger voorkomen) te elimineren. De analoge en digitale filtering achter de optische

Ronald Eygendaal is werkzaam als senior security consultant bij KPN Consulting en heeft meer dan twintig jaar ervaring in bewaking & beveiliging, elektronische & technische beveiliging, fraude onderzoek en informatiebeveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsmanagers Nederland (VBN). Ronald is te bereiken via ronald.eygendaal@kpn.com.



Li-Fi apparaten van het Fraunhofer instituut

filters zorgen dat de resterende interferentie te verwaarlozen is. De kans op sabotage van de draadloze verbinding is daardoor minimaal. Dit in tegenstelling tot wifi waarbij het vrij eenvoudig is om met behulp van een radio de verbinding te verstoren. Het zal duidelijk zijn dat een line-of-sight tussen zender en ontvanger de voorkeur heeft. Echt noodzakelijk is dit niet, zolang de optical receiver maar fotonen kan verzamelen is er gegevenstransmissie mogelijk. Zij het in een lagere datasnelheid dan normaal. Het signaal heeft weinig last van reflectie van het licht tegen obstakels. Het volledig afplakken van de lichtbron zal leiden tot het wegvallen van het signaal, echter de gebruiker van de ruimte zal in het donker zitten waardoor deze vorm van sabotage gelijk opvalt.

Daarnaast werkt het Li-Fi Consortium aan een aantal security eigenschappen voor Li-Fi. Zo stelt het consortium dat er door de LED lichtbronnen zogenaamde Li-Fi cloud area's ontstaan die worden gemonitord door de optical receivers. Deze ontvangers hebben een ingebouwde chip met een bewegingsdetector. Hoewel deze functionaliteit bedoeld is om user mobility tussen Li-Fi cloud area's te ondersteunen, kan het ook worden gebruikt voor inbraakdetectie of zoals het consortium zelf aangeeft voor "Home or office security". Zoals eerder aangegeven zullen de optical receivers in de lichtarmatuur worden ondergebracht. Hierdoor ontstaat, ten opzicht van traditionele bewegingsdetectie, een ongekende projecteringsdichtheid van de detectie, die je normaal gesproken alleen in high security omgevingen ziet. Het beschikbaar komen van de functionaliteit bewegingsdetectie binnen de IT infrastructuren is de volgende stap in de convergentie tussen fysieke beveiliging en IT beveiliging.

Andere geluiden

De Vereniging voor Experimenteel Radio Onderzoek in Nederland (VERON) heeft onlangs een aantal zorgen over Li-FI geuit. Zo is, om de datastroom naar de LED-verlichting te brengen, bedrading nodig, waarover zeer snelle pulsvormige signalen worden getransporteerd. Een combinatie van kabel en pulsen zal zich als radio antenne gaan gedragen. Hierdoor kunnen storingen in het radiospectrum ontstaan. De VERON verwacht dat hun leden daarvan last zullen ondervinden. Een ander verschijnsel dat ontstaat, wanneer combinatie van kabel en pulsen als zendantenne gaan werken, is dat kwaadwillenden het radiosignaal kunnen aftappen. Hier ontstaat dus een veiligheidsrisico. Daarom is het van belang dat de bekabeling voorzien is van afscherming en dat deze afscherming verbonden is met een deugdelijk aarde. Dit ter voorkoming van het zogenaamde TEMPEST effect.

Conclusie

Markt onderzoeksbureau MarketsandMarkets verwacht dat de Li-Fi-industrie in minder dan vijf jaar vijf miljard euro zal zijn. Li-Fi is een snel ontwikkelende technologie waardoor nieuwe IT infrastructuren ontstaan en die op het punt staat commercieel beschikbaar te komen. Op de Consumer Electronics Show 2014 in Las Vegas hebben SunPartner Technologies en Oledcomm de eerste met Li-FI uitgeruste smartphone gepresenteerd. Ook zijn bij de Franse energie reus EDF de eerste pilots met Li-Fi netwerken gestart. Door de opkomst van Li-Fi ziet het er naar uit dat er een andere kijk op beveiliging van draadloze IT infrastructuren gaat ontstaan.

Links

http://visiblelightcomm.com/top-10-li-fi-myths/
http://www.lificonsortium.org/
http://alexwiddowson.co.uk/2014/01/08/lifi-wireless-communication/
http://purelifi.co.uk/news/
http://www.het-bar.net/modules.php?name=News&file=article&sid=3093
http://www.engineersonline.nl/nieuws/id21799-lifi-wifi-met-licht.html
http://www.international.to/index.php?option=com_content&view=article&id=13048:visible-light-communication-(vlc)-li-fi-technology-market-worth-$6-138-02-million-2018&catid=309:pitchengine&Itemid=446
http://www.digitalversus.com/mobile-phone/li-fi-smartphone-presented-at-ces-n32333.html

Auteursinformatie: interview door Chantal Craandijk, ZZP-er en bereikbaar via chantal@craandijk.com, met Jaya Baloo, CISO KPN.

KPN: 'DE HACK HEEFT ONS WAKKER GESCHUD'

De missie van Jaya Baloo is simpel. Zorgen dat KPN betrouwbaar, veilig en vertrouwd is voor klanten, partners en de maatschappij. Als Chief Information Security Officer geeft ze leiding aan KPN's security team.

Op de vraag wat de impact was van 'de' hack op KPN is ze duidelijk: 'Weet jij wat 'de' hack was? Dat was een jongen van 17 die is binnengekomen, heeft rondgeneusd en niets heeft buitgemaakt.' Daarna kregen we te maken met een ander probleem: iemand hackte Babydump.nl en maakte daarbij klantgegevens openbaar. Klanten van Babydump bleken hetzelfde wachtwoord voor hun Babydumpbestellingen als voor hun KPN-mail te gebruiken. 'Ons voornaamste probleem was dat onze monitoring niet op maat was waardoor we niet capabel konden reageren.'

Vliegensvlugge maatregelen

Daar is inmiddels verandering in gekomen. KPN nam vliegensvlug maatregelen om de IT-systemen veiliger te maken en heeft de besturing van de IT-organisatie verbeterd. Meteen na het constateren van de hack is informatiebeveiliging van de infrastructuur onder de loep genomen. Alle IT moet voldoen aan de modernste security-standaarden en het beleid is drastisch op de schop genomen. IT-processen zijn aangepakt, het CIO Office NL is opgericht -waar Jaya en haar team onder vallen- en de Portal Authority -het REDteam- werd gelanceerd, een securitytoets waaraan alle KPN-websites en programma's moeten voldoen voor zij live mogen. Er zijn stappen genomen om KPN'ers bewuster te maken van veiligheid en er is er een speciaal incidentproces ingericht voor security-problemen. Tot slot is het Security Operations Center opgericht, waarbij TNO en FOX-IT hebben geholpen.

Jaya Baloo is sinds oktober 2012 Chief Information Security Officer bij KPN. Ze geeft leiding aan KPN's securityteam.

Samenwerking belangrijk

In het vergroten van de digitale veiligheid van de organisatie werkt KPN veel samen met andere partijen, zowel met andere bedrijven als de overheid. KPN's CEO Eelco Blok is bijvoorbeeld

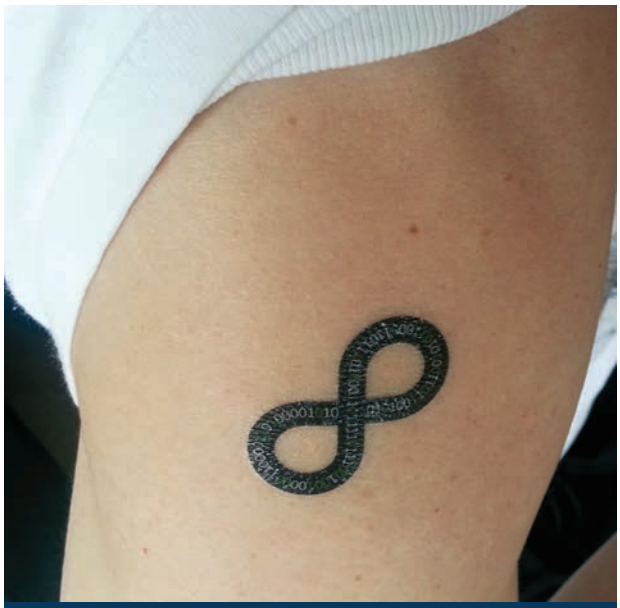
co-voorzitter van de Cyber Security raad. Het bedrijf heeft verder samen met Alliander, DNV KEMA, TNO en de Radboud Universiteit een nieuw Europees kenniscentrum voor cyber security opgericht -ENCS- dat zich bezighoudt met onderzoek, testen, kennisdelen en training in internetveiligheid voor vitale infrastructuren, zoals energie, water en telecom. Er is een goede samenwerking met het Nationaal Cyber Security Centrum van het ministerie van Justitie en Veiligheid. Beide organisaties schreven onlangs samen met de High-Tech Crime Unit van de landelijke politie en TNO de eerste editie van het jaarlijks te verschijnen rapport Cyber Security Perspectives met daarin een overzicht van alle cyber-gebeurtenissen van het afgelopen jaar. Eén van de trends die ze verwachten voor 2014: het plegen van cyberaanvallen wordt steeds gebruiksvriendelijker, met alle schade van dien.

Baloo: 'Niet alle hackers zijn natuurlijk gevaarlijke criminelen.' Daarom heeft KPN speciaal voor gewetensvolle hackers die een veiligheidsrisico of veiligheidslek vinden en willen helpen het probleem op te lossen zonder risico op vervolging -ook wel ethisch hacken genoemd- een Responsible Disclosure-procedure ingericht. 'Een laagdrempelig loket op kpn.com waar zij een beveiligingslek kunnen melden om gegevensmisbruik te voorkomen.'

Hoe geeft KPN de door hun REDteam gevonden kwetsbaarheden door aan bedrijven of het NCSC? Baloo geeft een voorbeeld. 'Een paar weken terug vond het team een nieuw soort botnet op het netwerk dat we nog niet eerder hadden gezien. De beheerders van het botnet waren binnengedrongen op de testomgeving van nieuwe programma's en websites. Deze omgeving bleek niet zo goed beveiligd als onze live omgeving. Het RED detecteerde het probleem en gaf het door aan het Computer Emergency Response Team, dat het oploste. Daarna hebben zij het doorgegeven aan het NCSC. We vinden het belangrijk om het NCSC zaken door te geven die ook van belang zijn voor andere bedrijven. In dit geval een nieuw soort botnet. Op die manier heeft iedereen iets aan de zaken waar we allemaal tegenaan lopen.' Na dit incident heeft KPN het securitybeleid voor de testomgevingen aangescherpt.

Superprivé bellen

Onlangs kondigde het bedrijf een strategische samenwerking aan met het encryptiebedrijf Silent Circle. Hierdoor kunnen mobiele telefoongebruikers wereldwijd beveiligde telefoon- en videogesprekken voeren en data versleuteld versturen. Baloo: 'Er is veel vraag naar veilige alternatieven voor 'gewone' telefoongesprekken en sms'jes.' Gesprekken via Silent Circle worden op de telefoon versleuteld en op de andere telefoon weer ontsleuteld. Het verkeer tussen de telefoons is zo niet te ontcijferen. KPN is de eerste telecomaanbieder ter wereld die



Een tattoo voor betere ICT security?

Uit psychologisch onderzoek is bewezen dat als je 20 minuten nadenkt over iets, het een levenslange herinnering wordt. Baloo: 'Daarom hebben we een speciale niet-permanente tattoo ontwikkeld, die de drager ervan moet herinneren hoe belangrijk ICT security is. Hij blijft twee weken plakken dus ergens in die twee weken moet ik toch die 20 minuten aandacht kunnen krijgen. Je moet op een drastisch andere manier dan de traditionele foldertjes of liftposters de aandacht zien te krijgen, anders is het zonde van het geld.'

de diensten van Silent Circle gaat doorverkopen. Op de Mobile World Congress in Barcelona werd verder bekend dat het bedrijf ook de BlackPhone van Silent Circle gaat verkopen, een telefoon die zich volledig richt op de security en privacy van de gebruiker.

Hoe is die samenwerking tussen de telecommer en het encryptiebedrijf tot stand gekomen? Baloo: 'Eind jaren negentig kreeg ik een encryptie-cursus van Phil Zimmerman, de maker van e-mail encryptiesoftware Pretty Good Privacy -PGP- in Utrecht. We klikten, we zijn beiden Amerikaans en hij moest naar het station in Amsterdam dus ik gaf hem een lift. Sindsdien hebben we altijd contact gehouden. Hij heeft ook VoIP encryptieprotocols gemaakt, zoals ZRTP en Zfone. Nu is hij directeur en mede-oprichter van Silent Circle. Onze samenwerking is een logisch gevolg van ons contact.'

Derde bij de Cyberlympics

KPN's ethische hackers volgen de laatste securityontwikkelingen op de voet en verbeteren hun vaardigheden doorlopend bijvoorbeeld via deelname aan internationale hackwedstrijden.

KPN's hackers team SectorC tijdens de finale in Atlanta.

Bij de door de EC-Council georganiseerde Global Cyberlympics van afgelopen jaar werd het team dat pas voor de eerste keer meedeed derde. Zij hadden zich geplaatst door eerst Europees kampioen te worden. In de finale in Atlanta streden de beste teams van zes continenten tegen elkaar in een 'Capture-The-Flag'-wedstrijd met disciplines als digitaal forensisch hackonderzoek, Computer Network Defense en penetratietests. Naast KPN's team waren er nog twee Nederlandse teams in de finale die streden tegen teams uit de Verenigde Staten, Australië en Mongolië. Baloo: 'Tot de laatste tien minuten waren we nog volop in de race, maar het eindresultaat was uiteindelijk een derde plaats.' Over haar team niets dan lof: 'Ik ben enorm trots op onze prestaties en de toewijding die wij tot in de laatste minuut hieraan hebben gegeven. Dit was een onvergetelijke ervaring.' Een prestatie van formaat. Toch? Baloo blijkt competitief: 'We zijn daar om te winnen. Dit was een goede reality check voor ons.'

Het lijkt een leuk spel, en dat moet ook wel om een team geïnteresseerd te houden dat als teamuitje voor de lol (met permissie) probeert in te breken in het netwerk van het Rijksmuseum. Maar het is zeker serieus bedoeld. Baloo: 'Met de hackwedstrijden toetsen we niet alleen onze kennis, maar ook of we binnen de vastgestelde tijd problemen kunnen aanpakken. We meten ons met de beste hackers van de wereld. Hier worden wij én daarmee ook onze klanten alleen maar beter van.'

Hoe gaat de CISO om met de commerciële druk? Security is immers één van de dingen die als eerste uit het budget geschrapt worden. En KPN heeft de laatste jaren te maken met zwaar weer. Baloo: 'We kunnen onze waarde -ook intern- alleen bewijzen door te laten zíen wat we bijdragen. Door te laten zien hoeveel geld we KPN besparen. Daarom ontwikkelen we op dit moment een app – de PHOSI -Possible Harm Of Security Incidents- app – waarin je dit onder andere kunt narekenen.' Met die app kun je beveiligingsincidenten 'scoren', uitrekenen hoe duur het incident is en dat dan koppelen aan het securitybeleid binnen het bedrijf. 'Daarmee zie je dus makkelijk hoeveel geld het een bedrijf oplevert. Je laat zien dat je niet alleen geld kost. De app komt ook in de appstores omdat andere bedrijven met precies dezelfde vraagstukken worstelen als wij.'

Hackers proberen KPN een paar miljard keer per jaar binnen te dringen.

'Momentum pakken'

Baloo is nog lang niet zover dat ze al wil terugblikken op de afgelopen tijd. 'Ik zit hier pas anderhalf jaar. We hebben al veel goede dingen gedaan maar we zijn nog lang niet klaar. Ik wil het momentum pakken dat we nu hebben.' De vraag of ze zaken ook anders had willen aanpakken, oogst een stellig 'Nee'. 'Ik ben ervan overtuigd dat we dingen goed doen en ik wil me niet blijven richten op dingen die ik nu nog niet heb. Detectie en response zijn voor ons het belangrijkste. KPN heeft te maken met een paar miljard hack-pogingen per jaar. Dus je kunt gehackt worden niet voorkomen. Maar je kunt door het nemen van de juiste maatregelen wel werken aan het minimaliseren van de impact. Het is belangrijk te weten wat je wilt beschermen en waarom, te monitoren welke risico's er op dit moment zijn en met die informatie met de juiste mensen te reageren.' De 17-jarige hacker kreeg uiteindelijk een taakstraf. 'Hij heeft ons wakker geschud. We willen hem er niet voor bedanken maar het is wél goed geweest voor KPN.'

Cybercrime treft ruim een op de acht Nederlanders

- 1 op de 8 Nederlanders wordt slachtoffer van cybercrime
- Bij jongeren is dat aantal hoger: daar is het 1 op de 5 jongeren
- Bij 25- tot 45-jarigen ligt het aantal ook hoger dan gemiddeld: 15 procent
- Helft cybercrimeslachtoffers werd gehackt
- Een kwart werd gepest via internet
- Een kwart had te maken met aan- of verkoopfraude
- Een klein deel was slachtoffer van identiteitsfraude

Bron: CBS

Mr. Rachel Marbus, @rachelmarbus op Twitter

ACHTER DE LINIES

Terwijl ik dit schrijf hoor ik al dagen lang helikopters vol continue boven mijn huis cirkelen. Het gebrom verdwijnt na een tijdje wel naar de achtergrond, de aanleiding ervoor is alomtegenwoordig. Ik woon vlakbij het World Forum in Den Haag, deze dagen het strijdtoneel van 13.000 politieagenten, 4.000 marechaussees en 3.000 militairen, twee F16's continu in de lucht en drie marineschepen in de zee. Ook hangen overal extra camera's en kunnen via Live View de camerabeelden van particuliere instanties tot het wapenarsenaal gerekend worden.

Ik probeer mijn dochtertje uit te leggen waarom al dat gedoe bij onze voordeur nodig is. "Er komen 53 bazen van landen naar onze woonwijk toe, die moeten beveiligd worden." Ze snapt het niet. "Maar mama, wat komen ze dan doen hier en waarom moeten die dan beveiligd worden?" Ik vertel haar dat ze komen praten met elkaar. Over belangrijke dingen. En dat ze beveiligd moeten worden omdat de kans bestaat dat stoute mensen hen willen doodmaken. Ze snapt het nog steeds niet. "Kunnen ze dat dan niet gewoon ergens anders gaan doen? Waarom moet dat nou hier?" Ik kan het haar niet uitleggen dat dit allemaal nodig is. Als we op de Top-dagen door de buurt wandelen vindt ze het uiteindelijk allemaal maar saai, het is zo uitgestorven hier, er gebeurt helemaal niets! Dat ze een heus politiepaard mocht aaien was voor haar het meest enerverende dezer dagen.

Zelf fotografeer ik al weken lang de veranderingen in mijn wijk. De metershoge hekken die geplaatst worden, de metalen stootkussens voor de parken, de wegblokkades en het verschijnen van steeds meer politieagenten en militairen. Ik realiseer me dat ik in de dagen voor de Top steeds even goed om me heenkijk voordat ik mijn iPhone trek. Ik maak snel een foto en stop de telefoon direct weer weg. De afschrikwekkende werking van potentieel nadelige repercussies heeft zich in mij genesteld. Toch knap van ze, ik ben nou niet het type vrouw dat snel ergens van onder de indruk is.

Ik bespreek mijn NSS-zorgen met een lieve meneer die me verzekert dat – hoewel het vol 'over the top' is al het ingezette machtsvertoon – het straks allemaal heus weer voorbij is. "Maar die camera's, daar zullen er vast wel een paar van blijven hangen", verzucht ik. "Hier in de straat hangt er eentje extra en die ziet er echt heel erg permanent uit. Ik bedoel, die is er nu toch al en dan is het net zo makkelijk om hem te laten hangen." Hij bezweert me dat dit niet het geval zal zijn. Politieagenten hebben ook helemaal geen tijd of zin om die beelden telkens te bekijken zegt hij me. Hij kan het overigens weten want hij was ooit een van hen. Toch zit het me nog steeds niet lekker, want je hoeft helemaal niet live te kijken. Dat doe je dan gewoon achteraf, de beelden heb je immers toch al! De lieve meneer is niet te overtuigen, "die camera's zijn straks allemaal weg en ook die ene hier in de straat". Ik hoop oprecht dat hij gelijk heeft.

BIG DATA

herijking noodzakelijk!

Big data is een ontwikkeling die wereldwijde invloed heeft op de maatschappij van vandaag en de economie van morgen. Een uniforme definitie van big data ontbreekt echter nog. Dit maakt het onderwerp -waarin de komende jaren een miljardenomzet wordt verwacht- subjectief en onvoorspelbaar.

Er direct inspringen zonder duidelijk te weten waar te beginnen lijkt niet verstandig. De ontwikkeling negeren is net zomin een optie. Tegelijkertijd gaan steeds meer bedrijven sturen op basis van big data en conclusies hieruit direct omzetten in besluiten.

Hoog tijd voor een (her)ijking!

Een negental relevante ijkpunten worden benoemd in dit artikel, als eenduidig referentiekader bij het onderwerp big data. Het eerste ijkpunt is de gulden snede van big data eigenschappen volgens Gartner – volume, snelheid en diversiteit (Engels: volume, velocity and variety). In big data context vormt elk van deze eigenschappen al een technologische maar vooral ook een organisatorische uitdaging.

Business

Big data lijkt het moderne goud, nu wereldwijd grote hoeveelheden en soorten data beschikbaar komen. Maar net als bij het delven van waardevolle grondstoffen als goud en olie, vergt het succesvol 'ontginnen' van big data ook specialistische kennis, ervaring en focus. In dit stadium niet zozeer op het technologisch vlak, maar meer op het begrip van de mogelijke waarde en de impact ervan op de bedrijfsvoering.

Een onderzoek onder honderd van de Fortune top 1000 bedrijven, uitgevoerd in 2013 door New Vantage Partners, leert dat er verschillende big data gerelateerde initiatieven lopen. Diverse initiatieven staan gepland, maar slechts een beperkt aantal initiatieven is in productie. Kenmerkend hierbij is dat er vooralsnog wordt gesproken over een verwachte investering bij big data maar nauwelijks over de verwachte baten voor de organisatie.

Dat brengt ons bij de belangrijkste vragen waar veel organisaties mee stoeien. Wat betekent big data, wat is de toegevoegde waarde en wat zijn de risico's ervan voor de eigen organisatie, klanten en branche? De concrete business case moet hierover uitsluitsel geven.

Door Wouter Verburg en Paul van Orsouw. Wouter en Paul zijn consultants in dienst van i-to-i. Zij zijn te bereiken op wouter.verburg@i-to-i.nl en paul.van.orsouw@i-to-i.nl.

Big data lijkt het moderne goud nu grote hoeveelheden en soorten data beschikbaar komen

De andere kant van deze business case is niets doen met big data, terwijl branchegenoten dat wel doen. Mis je hierdoor de boot of behoud je juist waardevolle financiële en organisatorische reserves voor andere ontwikkelingen die wellicht meer waarde toevoegen? Essentieel is de kernvraag: ***"Wat is de toegevoegde waarde van een correcte en tijdige integratie van big data binnen mijn bedrijf?"***

Om een goede invulling te kunnen geven aan deze business case, moet er gericht gekeken worden naar de business van vandaag en welke data er voor nodig is om succesvol te zijn. Deze 'IST' situatie als tweede ijkpunt is te bepalen met vragen als:

- **Aan welk business model wordt bestaansrecht ontleend?**
- **Wat is onze organisatorische volwassenheid ten opzichte van branchegenoten?**
- **Hoe flexibel zijn onze bedrijfsprocessen ingericht, zodat we mee kunnen bewegen met ontwikkelingen in de markt?**
- **Welke data is essentieel voor de gezondheid van onze bedrijfsvoering?**

Dit zijn slechts een paar potentiële vragen bij het bepalen van de impact van big data. Hierbij geldt het volgende principe: bedenk niet óf big data impact heeft maar leg de focus op het achterhalen waar en wanneer wordt verwacht dat big data impact heeft.
Onderstaande vragen helpen invulling te geven aan het derde ijkpunt: de ´SOLL´ situatie van de organisatie. Ze zijn essentieel om de risico's van de marktontwikkeling rondom big data helder te kunnen krijgen en de invloed ervan op de eigen organisatie.

- **Hoe ziet onze bedrijfstak er over drie tot vijf jaar uit door de invloed van big data?**
- **Wat is onze positie over drie tot vijf jaar in deze bedrijfstak als we niets doen met big data?**
- **Wat is de invloed van big data op onze organisatie?**
- **Welke positie willen wij innemen over drie tot vijf jaar?**
- **Welke data is dus essentieel voor de gezondheid van onze bedrijfsvoering over drie tot vijf jaar?**

Gezien de hoge snelheid van de huidige mondiale technologische ontwikkelingen is een horizon van drie jaar al zeer ambitieus. Tegelijkertijd is het binnen vijf jaar succesvol en duurzaam inrichten en optimaliseren van de bedrijfsprocessen voor sommige organisaties ook praktisch onmogelijk.

Risk

Het begrijpen van potentiële risico's met big data in een vroeg stadium, maakt dat een organisatie uiteindelijk sterker kan sturen en meer focus kan leggen op het ontdekken en realiseren van mogelijkheden ervan. Gartner beschrijft hiervoor een aantal relevante aandachtspunten. Met de term 'big data' is al snel de relatie gelegd met de technologieën om ons heen. Om big data goed te begrijpen, is het zaak verder te kijken dan alleen betrokken technologieën. Waar welke impact ligt – zowel met baten als met kosten - heeft niet alleen invloed op techniek, maar ook op organisatie, financiën, imago, security en zeer waarschijnlijk zelfs juridische gevolgen. Omdat big data grote invloed heeft op de maatschappij en de bedrijfsvoering, is het verstandig geplande investeringen te toetsen aan de big data context. Aanscherping van de bedrijfsstrategie op voorziene marktveranderingen door big data, zorgt ervoor dat de onderneming een mogelijk slechte investering bespaard blijft. Investeringen in de onderneming zullen dus een duidelijke relatie moeten krijgen met big data, zelfs al is dit niet de oorspronkelijke drijfveer van deze verandering. Gartner's 'Hype Curve' geeft een projectie van nieuwe ontwikkelingen die steeds meer data genereren. In deze 'data generating society' speelt data bij elke evolutie of revolutie een steeds belangrijker rol. Dit leidt tot het risico, dat door gebrek aan inzicht en overzicht, teveel data te breed beschikbaar gemaakt wordt. Privacygevoelige of strategisch belangrijke informatie kan hierdoor onbedoeld op straat komen te liggen.
Het classificeren van deze strategische en privacy gevoelige informatie is het vierde ijkpunt.
In de toekomst zal er alleen maar meer data bijkomen. Deze zal echter niet direct te combineren zijn met bedrijfseigen data. Standaardisatie van specifieke technieken, functionaliteiten en processen vereenvoudigt integratie en beheer en vergroot de kans op succes. In de kern zullen er altijd unieke aspecten blijven bestaan die simpelweg niet inwisselbaar zijn, omdat ze ten grondslag liggen aan de bedrijfsvoering. Maar verreweg de belangrijkste van allemaal is het omzetten van data naar

Beschikbaarheid van data	Bruikbaarheid	Betrouwbaarheid
-kunnen we bij de data-	-kunnen we de data gebruiken-	-kunnen we de data vertrouwen-
Toegankelijkheid	Definitie/Documentatie	Consistentie
Autorisatie	Herkenbaarheid	Integriteit
Exclusiviteit	Oriëntatie	Nauwkeurigheid
Tijdigheid	Structuur	Compleetheid
Prestatie	Effectiviteit	Actualiteit
Efficiëntie		Auditeerbaarheid (toetsbaar)
		Verantwoordelijkheid

Tabel 1: Criteria voor data kwaliteit

Het begrijpen van risico's van big data maakt dat een organisatie sterker kan sturen op de mogelijkheden

informatie. En naarmate de bedragen waarover besloten wordt groter zijn, is de noodzaak voor een goed begrip van de data, haar oorsprong en daarmee de waarde van de informatie essentieel. Dit bewustzijn is het vijfde ijkpunt.

Informatie

Zelf data genereren of big data inkopen is vaak het minst lastige deel. Het beoordelen van de bruikbaarheid ervan is veel intensiever. Het moet namelijk leiden tot zinnige informatie, kennis, begrip en voorspelbaarheid voor verantwoorde besluitvorming, Voordat hiermee begonnen kan worden, is het verstandig een aantal fundamentele vragen te beantwoorden, zoals:

- **Hoe wordt de data verkregen en onder welke condities?**
- **Wat voor soort(-en) data worden wel of niet gebruikt en weten we waarom?**
- **Wat is de huidige definitie rond betrouwbaarheid van onze eigen data?**
- **Is en blijft de data die we gebruiken actueel en hoe stellen we dit zeker?**
- **Wat is de impact van big data op onze historische data (analyses en conclusies)?**
- **Kunnen we onze eigen interne data zonder meer functioneel combineren met externe data?**

Veel van de bovenstaande vragen hebben een directe samenhang met criteria voor data kwaliteit.
Huidige criteria en definities van beschikbaarheid, bruikbaarheid en betrouwbaarheid van data zijn wellicht verouderd binnen de eigen organisatie. Het actualiseren van deze criteria kan leiden tot aanpassingen op bestaande systemen, betrokken infrastructuren, gerelateerde bedrijfsprocessen en zelfs denkwijzen rondom data. Dit zesde ijkpunt kost daarmee tijd en geld maar kan los van toekomstige ontwikkelingen, vrijwel altijd direct opgestart worden.

Nieuwe toekomstige databronnen genereren waarschijnlijk meer data en mogelijk andere datatypen dan dat waar de organisatie momenteel op is ingericht. Het is dan ook te verwachten dat in de nabije toekomst de organisatie te maken krijgt met nog meer diversiteit aan data. Daarom is het belangrijk te zorgen voor een uniforme enterprise- en proces architectuur als zevende ijkpunt. Door definities te standaardiseren en uniformeren, wordt het makkelijker om nieuwe data en informatie 'op hun waarde te schatten' en een juiste plek te geven. Door het modelleren van de bedrijfsvoering in procesmodellen en datamodellen -zowel logisch als technisch- ontstaat er overzicht en inzicht in de (on)mogelijkheden van verschillende datasets. Tevens biedt dit weer een natuurlijk moment om de betrouwbaarheid van de verschillende datasets te valideren en, indien nodig, te verbeteren. De geüniformeerde, geschoonde en gevalideerde datasets vormen het achtste ijkpunt.
Omdat technologische ontwikkelingen snel gaan en de impact van big data mondiaal is, staat er ook volop druk op internationale wet- en regelgeving. Waar financiële en publieke instellingen al onder toezicht staan, zal een verscherpte wet- en

regelgeving ook andere bedrijfstakken beïnvloeden. Een doordacht ingerichte beveiligingsorganisatie gaat hierbij helpen.

Security

Belangrijk voor een doordachte beveiligingsorganisatie is balans tussen business en security. Het is goed mogelijk dat business wensen in conflict zijn met het beveiligingsbeleid. Een conflict kan vermeden worden door vroegtijdige afstemming en heldere procesgang. Dit negende ijkpunt is van groot belang voor een duurzame inrichting van de beveiligingsorganisatie. Het correct definiëren, toekennen en beheren van de rollen en verantwoordelijkheden en een passende inrichting van identity & access management vormen hierin cruciale schakels. Dit zal tot op strategisch en tactisch niveau afgestemd moeten worden, aangezien het beveiligingsbeleid bepalend is voor de continuïteit van een moderne bedrijfsvoering die sterk afhankelijk is van data. De huidige enterprise- en procesarchitectuur maakt duidelijk welke rollen & verantwoordelijkheden benoemd en belegd moeten zijn voor een goede bedrijfsvoering. Hieruit volgt logischerwijs welke data wanneer en voor welke rol toegankelijk zou moeten zijn. Het onvoldoende beschrijven en beleggen van rollen en verantwoordelijkheden vergroot het risico op operationele verwarring en de kans op bedreigingen. Vanuit het applicatie- en systeemlandschap zal inzicht verkregen worden, wie waar vanuit welke processen binnenkomt en toegang heeft tot welke data/informatie. Op basis van eerdere uitgewerkte ijkpunten kan vervolgens inzichtelijk gemaakt worden:

- **Wie heeft,**
- **op welke manier,**
- **toegang tot welke data?**

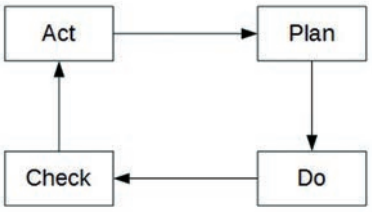
Conclusie

Big data is niet meer weg te denken en is overal om ons heen. Het succesvol gebruiken ervan vereist een stapsgewijze (her)ijking van de eigen bedrijfsvoering op deze ontwikkeling. Het opstellen van een actuele businesscase, het uniformeren en opschonen van de eigen informatie huishouding en het actief beveiligingsbeleid levert toegevoegde waarde.

(advertentie)

WAAR BEGINT EEN CIRKEL?

Je kent ze wel, die presentaties waarin de visie van een bedrijf op het het security managementproces of beheerprocessen wordt gevisualiseerd in de vorm van een Deming cirkel. Je wordt door een presentator door zo'n plaatje geleid waarmee het duidelijk wordt dat er sprake is van een zichzelf herhalend proces en waarbij je steeds dichter bij het procesnirvana geraakt: het gaat steeds beter, de kwaliteit van de beheerde omgeving gaat vooruit, we zijn in control. En ja, dat is nu precies de doelstelling van de Deming werkwijze: kwaliteitsverbetering door permanente sturing: toetsing aan de planning en bijsturen bij afwijkingen: Je begint met het definiëren van een plan, vervolgens ga je het uitvoeren, toetsen en verbeteren. Daarna ga je opnieuw aan de slag met het maken van een plan, waardoor het hele proces wordt herhaald.



Figuur 1 - Basismodel

Dat zijn in het kort ook de stappen in het kwaliteits verbeteringsproces zoals die door Deming zijn verwoord en zoals die binnen heel veel procesmanagementprojecten worden uitgevoerd.

Nu heeft Deming dat natuurlijk niet voor niets opgeschreven. Hij heeft deze aanpak opgedaan door zijn betrokkenheid bij het opzetten van de kwaliteitssystemen die in Japan in de jaren '70 en '80 van de vorige eeuw werden opgezet om de industriële revolutie vlot te helpen; Japan wilde goede kwaliteit tegen een knappe prijs leveren. Begrippen als TQM, EFQM, INK etc. begonnen opgeld te doen en de hele wereld veranderde in een kwaliteitsbewuste hemel op aarde. En iedereen bouwt nu voort op de Deming Circle.

Het leuke van het model is dat het zo logisch is, het is een regelkring, net als bijvoorbeeld een thermostaat. En dat is een helder concept: Je stelt de temperatuur in. De thermostaat geeft dat signaal door naar de CV-installatie. De thermostaat

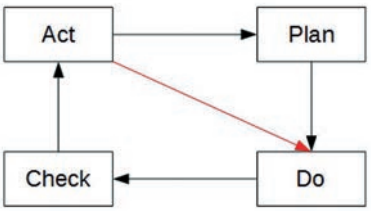
André Koot is security en IAM consultant bij Strict Consultancy in Vianen en redacteur van dit vakblad. Hij is per e-mail bereikbaar via a.koot@strict.nl.

meet constant of de temperatuur in de ruit overeenkomt met de ingestelde waarde en als de temperatuur te laag wordt, geeft de thermostaat een bijstuursignaal naar de CV. Simpel, je stelt de norm en kijkt of die n bij.
Maar het bijzondere fenomeen doet zich voor dat de Deming Circle in de praktijk heel anders werkt dan zoals in deze theorie wordt beoogd. De cirkel is eigenlijk helemaal niet compleet en bovendien, waar begint dat proces nu eigenlijk? Waar begint de cirkel?

Die vraag is eigenlijk zo gek nog niet. Ik kan me namelijk al heel lang niet echt vinden in het hanteren van het model. Laat ik voorop stellen dat het concept prima is en dat Deming de wereld wel degelijk heeft verbeterd. Maar het is helemaal niet zo simpel om het model te projecteren op de werkelijkheid, of om de werkelijkheid te modelleren naar het model. Daar zijn verschillende redenen voor. De belangrijkste is dat een model niet meer is dan een versimpelde visuele weergave van een idee. En ideeën moet je niet letterlijk interpreteren. Daar moet je over nadenken en nagaan wat de implicaties voor jou zijn. Je moet zo'n idee niet in praktijk brengen. De praktijk is weerbarstig.

Een model is ook niet compleet. Het is een vereenvoudigde weergave van een werkelijkheid of van een gedachte.
Dat zie je in het model van Deming ook. Bijvoorbeeld: De laatste fase van Plan-Do-Check-Act is een vreemde. Je zou verwachten dat in de Act-fase op grond van het resultaat van de toets in de voorgaande fase besloten wordt om al dan niet een aanpassing door te voeren. Maar wat dat feitelijk zou betekenen is dat je ofwel besluit om de Norm aan te passen (een wijziging van het Plan) of dat je de operatie aanpast (een wijziging van de Do). Die laatste actie zie je niet in het model. Als je de pijltjes letterlijk volgt, betekent een kwaliteitsfalen dat in de Check-fase wordt geconstateerd, dat je op grond van de Act-analyse besluit dat je het plan moet bijstellen, ofwel de norm moet aanpassen. Dat is mooi: als je niet aan de norm voldoet, verlaag je de norm. Wat dat betekent is misschien wel leuk voor compliance, maar niet voor meneer Deming. Zo werkt dat dus niet en zo heeft hij dat ook niet bedoeld. Ik zal het Act-Do pijltje dan ook maar toevoegen aan het model:

Ik heb ook regelmatig presentaties gezien waarbij Plan wordt verwoord door de term Beleid, of 'Wet- en regelgeving'. In dat geval betekent de pijl vanaf de Act dat je bij afwijking de wet maar moet wijzigen. Zo kan dat niet bedoeld zijn. Zo zit



Figuur 2 - De regelkring

volgordelijkheid in het model niet in elkaar. En is dat model wel bedoeld voor dergelijke gedachtegangen?

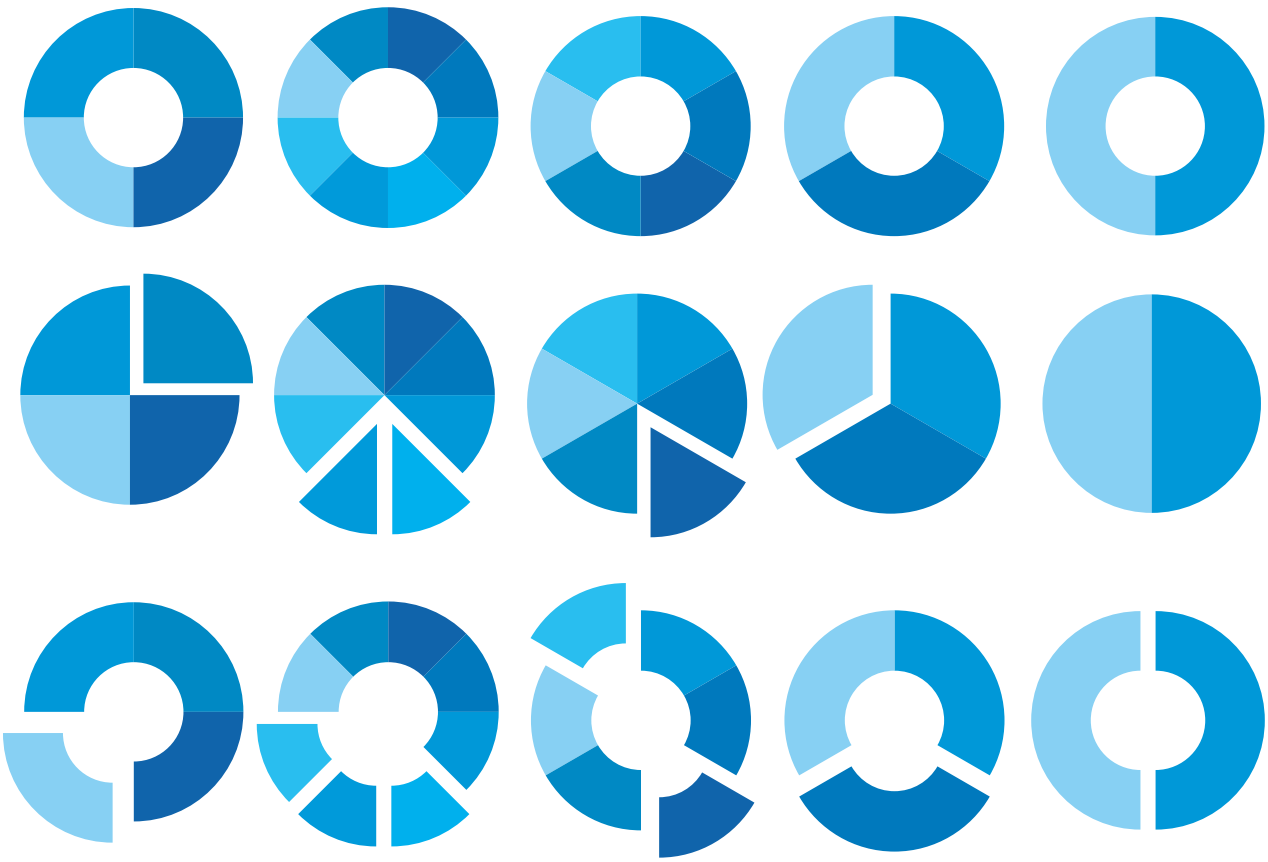
En wat doe je in een cirkelmodel als er eens geen afwijking wordt geconstateerd? Stopt alles dan? Op grond waarvan ga je dan Act'en of zelfs maar Plan'nen? Wat zou er gebeuren als er geen pijltje stond tussen Act en Plan? Is er dan niet gewoon sprake van een regulier sequentieel project? Waarom we altijd proberen de cirkel te sluiten is mij niet duidelijk, met name dat waar het op aankomt bij lange termijn programma's, zoals het uitleggen van een visie op bijvoorbeeld het security management proces.

Laten we liever een gebeurtenis definiëren op grond waarvan we het proces gaan starten, bijvoorbeeld de start van een jaarcyclus. Dat maakt het opeens veel interessanter, want dan wordt het herijken van security management onderdeel van de reguliere bedrijfsvoering.

Ik constateer twee knelpunten:

- **het model kun je niet hanteren om jouw visie op bijv. het security management proces te presenteren;**
- **het model is niet bedoeld als visualisatie van een lange termijn proces.**

En wanneer begint de cirkel? Kun je pas Act'en als je eerst de hele Plan-Do-Check fase achter de rug hebt en kun je pas nieuwe plannen maken als de oude zijn bijgesteld? De vraag stellen is hem beantwoorden. Je stuurt niet één keer, je stuurt permanent. Het is dan ook niet zo dat je in het proces één keer de norm stelt en vervolgens één keer stuurt en controleert. Er is sprake van een opeenvolging van gebeurtenissen die ieder voor zich maken dat je, voordat de cyclus helemaal is doorlopen, meteen een nieuwe procescyclus moet starten. Als je uitgaat van dat uitgangspunt, dan is er geen sprake van een



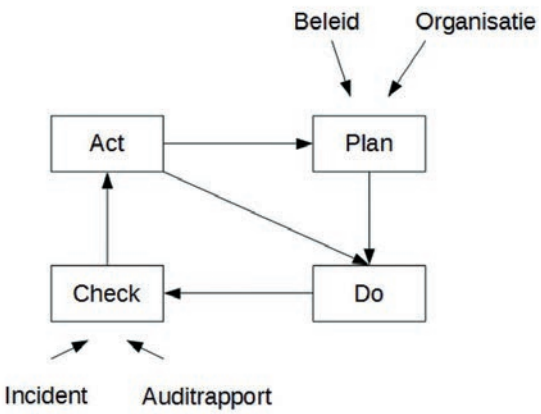
iteratief proces, maar van een flow, een voorgedefinieerde, voorgeprogrammeerde werkwijze, waardoor op een gestructureerde manier gestuurd wordt. Er is eigenlijk helemaal geen sprake van volgordelijkheid. Er is geen begin van een cyclus. Niet dat zo'n cyclus nooit begint, sterker nog, deze cyclus begint constant. En dat lijkt dan verdraaid veel op Case Management... Maar het begint niet uitsluitend daar waar je denkt dat het op grond van PDCA begint.

Laten we dit eens verder exploreren. Waar begint deze cirkel, of beter, waar kan dit proces starten? Zoals het er nu bij staat, is het een erg intern gericht proces. De triggers die we vinden zijn de pijlen vanuit de PDCA-fasen zelf. En dat betekent dat als er geen output vanuit de ene fase is, er ook geen trigger is om de vervolgfase te beginnen. Dat kan niet de bedoeling zijn. Er moet ook een externe trigger zijn. Laten we per fase eens onderzoeken of er naast de interne trigger ook een externe trigger kan worden onderkend.

- **Plan:** kan er een externe reden bestaan om een plan te maken of aan te passen? Ja. Wijzigingen van of binnen de externe omgeving kunnen leiden tot plannenmakerij. Denk aan een beleidswijziging, een reorganisatie of een wijziging van externe wetten en regels. Dergelijke wijzigingen zullen moeten leiden tot het maken of bijstellen van plannen.
- **Do:** kan er buiten de Plan-trigger een andere reden bestaan om de operatie te starten of bij te stellen? Ja, maar die staat al eerder vermeld: als een norm niet gehaald wordt, kan dat de aanleiding zijn om de operatie bij te sturen, zonder het plan zelf te raken. Andere triggers zouden feitelijk ongewenst zijn, aangezien die buiten het kwaliteitsmodel vallen om in zouden grijpen. Mijn premisse is dat externe triggers om een operatie te starten/wijzigen ongewenst zijn, die verhinderen ook de kwaliteitsborging die je juist met procesinrichting beoogt.
- **Check:** De output van de Do-fase zal beoordeeld moeten worden ten opzichte van de norm. Die beoordeling vindt niet plaats binnen het PDCA-proces zelf, maar die vloeit voort uit de operatie, waarin (als het goed is) toetsing plaatsvindt. Maar er kunnen ook andere redenen zijn om te controleren of de operatie wel werkt volgens plan. Denk aan een gesignaleerd incident, of een andere auditrapportage die leidt tot de constatering dat er iets aan de hand kan zijn.
- **Act:** Je gaat niet zomaar een besluit nemen, dat kan alleen op grond van de juiste inputs. De Check-fase levert die input. Het ligt niet voor de hand dat we een besluit nemen zonder afdoende waarborg omtrent de informatievoorziening die binnen dit model gerealiseerd

wordt. Bijstuuracties mogen in een kwaliteitssysteem niet spontaan elders plaatsvinden, dus externe triggers voor de ACT-fase zijn niet wenselijk.

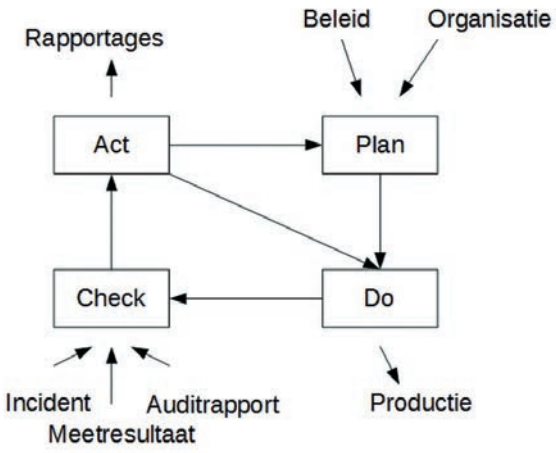
Op grond van deze analyse kan de cirkel dus op twee plaatsen beginnen: namelijk in de Plan-fase en in de Check-fase.



Figuur 3 - Het begin van de cirkel

De vervolgvraag kan dan zijn of de cirkel wel eens eindigt? Dat ligt eigenlijk niet voor de hand, we streven immers naar permanente verbetering van kwaliteit?

Je kunt wel zien dat er resultaten naar buiten komen. En het ligt voor de hand dat die in de beide overgebleven fase tot output leiden: De Do-fase is eigenlijk helemaal geen feitelijke operatie. Als dat zo is, dan is er in beginsel helemaal geen sprake meer van functiescheiding: de uitvoerende (Do) kan immers zijn eigen plan trekken, uitvoeren, meten en zal constateren dat alles goed gaat. Dat kan niet echt de bedoeling van het model en concept daarachter zijn. Nee, de Do-fase is het initiëren van de operationele uitvoering van activiteiten en het initiëren van wijzigingen van de operatie. De output is dus feitelijk de planning, de instructies gericht op de daadwerkelijke productie. De Act-fase levert de dashboards en rapportages: de resultaten van de Check-fase en de op grond hiervan genomen besluiten. Verschillende modellen van de PDCA-cyclus bezitten ook een 'Control' fase. Dat is het proces waarbinnen de



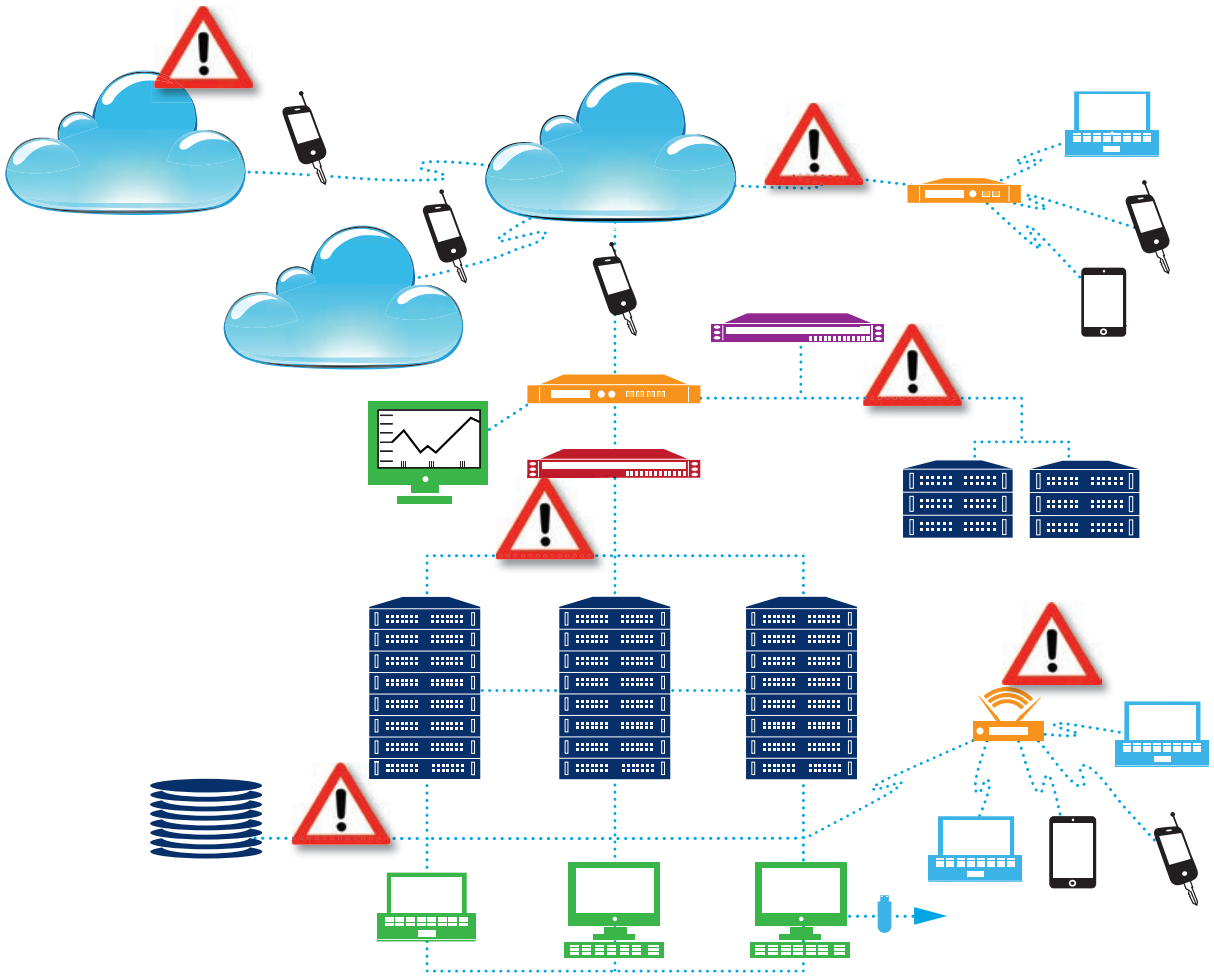
Figuur 4 - Ja, volmaakt…

procesbeheersing plaatsvindt. En dat is dan weer een bijzondere aanvulling op het model. Het PDCA model is een kwaliteits beheersingsmodel in zichzelf. Control op dat vlak is bijzonder. Eigenlijk willen we dat niet, want het loopt dwars door het proces heen. En heeft daarmee een verstorende invloed op het besturingsmodel.

De PDCA-cyclus is feitelijk een besturingsmodel. En het interessante fenomeen doet zich voor dat het eigenlijk ook niet tot zijn eigen dimensies beperkt hoeft te worden. Onbevredigend in het model is namelijk de modellering van de daadwerkelijk operatie, de echte Do. Vindt de Do nu plaats binnen het model zelf, of is de Do de sturing van de operationele uitvoering. Als we een verdiepingsslag uitvoeren, dan kunnen we daar echter wel mee uit de voeten.

Dit gezegd hebbende, moeten we dan de Deming Circle maar overboord zetten, of actualiseren? Nee, het zij verre van mij om hierop aan te sturen. Ik pleit alleen voor relativeringsvermogen als het gaat om het gebruik van dit model. Het model is een idee om kwaliteit gestructureerd te kunnen verbeteren. Het is nooit bedoeld geweest als model voor procesinrichting of procesmanagement. Het is al helemaal niet bedoeld om een visie uit te dragen. Doe dat dan ook niet.

Risico's van computer-bestuurd ICT-landschap?



Waar zitten uw risico's in het ICT-landschap? Adequate beveiliging door een ervaren, betrouwbare en loyale partner is meer dan ooit noodzaak. Crypsys is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

CRYPSYS secure computing 25 years

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos, SMS Passcode, Norman, Adyton, Lumension en Nessus

RISK MANAGED

Ever since the very first version of the SABSA Business Attributes taxonomy developed in early 2000, one of those attributes has been 'risk managed'. Fourteen years later one might ask the question: "What does that mean? Surely SABSA is all about risk management. One might as well say SABSAised." Yes, that would be a fair comment, because the evolution of SABSA has indeed led to that concept; that the entire framework and method is all about being business risk driven in the architecting and operation of business capabilities. So what exactly does 'risk managed' mean?

One rather good answer is that SABSA follows completely the philosophy and principles of ISO 31000: Risk Management. This is the international gold standard of risk management as a business discipline. It makes clear that risk is concerned with the uncertainty of outcome and is thus neutral. There are both opportunities for gain and improvement, and threats of loss or damage. Good risk management is all about creating a balance in which the gains outweigh the losses, and in which business performance is optimised.

ISO 31000 also makes it clear that risk management as an activity is not something separate, but something to be embedded in every aspect of business decision making and business management. You cannot put 'risk management' on the side and attend to it some of the time. It is by definition something intrinsic in doing business. Without risk there would be no business. Business is built on seeing opportunities and exploiting them for business advantage. The threats are a necessary part of the whole picture and come with the territory. In this context 'business' is any type of human corporate activity – whether for profit or for public service, government, military, charity, anything.

Arguably risk management is part of everyday life for every human being. From the moment of conception in the womb to the moment of death, life is a string of opportunities and threats. Living a successful life means managing these risks at all times of life, and creating a balance, whether it be an individual life, a family life or a corporate life. Every decision is a risk decision – shall I do this thing or not? Or should I do something else? Doing nothing also has risks, so risk is unavoidable in life. Consider what life would be like if there were no risks – it would not be life. Life means you have to face risk and manage it all the time. Otherwise why would you get out of bed and do stuff? What drives life and living is the inherent risk that it implies. 'Risk' and 'life' are closely coupled concepts. Without risk there could be no such thing as 'life', and the struggle that is implicit in staying alive and competing with other life forms for survival of both the individuals and the species as a whole.

Risk is experienced on several levels: strategic risk (long-term effects such as what career shall I choose? Shall I get married to this person?); tactical risks (medium term projects and programmes, such as where should we go on holiday this year? Should I apply for new job to enhance my career?); and operational risks (immediate and short term – such as is it safe to cross the road now? Is this food good to eat?).

Now we begin to see the granularity of risk, how it is both pervasive and at different levels of significance in life. Almost paradoxically it is the operational risk that is the most dangerous to handle. Strategy and tactics can be changed and recovery is possible after poor decisions, but a poor operational decision can kill you dead long before the strategy and tactics have time to take effect. That is why operational risk management is so important in business management and life management. SABSA mostly concerns itself with all aspects of operational risk management, providing operational performance targets and monitoring of performance against those targets on a regular basis. That is why SABSA is such an important framework to be applied in a modern business environment.

The Attributer

Dick Brandt (voormalig CISO PostNL) en Johan Bakker (voormalig CISO KPN) hebben beiden meer dan 25 jaar ervaring in het bedrijfsleven, volop opererend op het grensvlak van techniek en business. Beiden zijn vanuit een technische achtergrond meer dan 10 jaar geleden in het information security werkveld begonnen om vervolgens door te groeien tot CISO van een multinational. Dick en Johan zijn nu beiden actief als zelfstandig ondernemer (advies en consultancy) en hebben tevens samen de CISO Masterclass BV opgericht, waar ze als docenten hun opgedane kennis en ervaring overdragen aan toekomstige en zittende CISO's. Zij zijn te bereiken via dick.brandt@cisomasterclass.nl en johan.bakker@cisomasterclass.nl.

SUCCESVOL OPEREREN OP HET GRENSVLAK VAN TECHNIEK EN BUSINESS

Succesvol Information Security Management staat of valt bij de mate van aansluiting en draagvlak die de "information security verantwoordelijke" weet te vinden bij "de business." De Chief Information Security Officer (CISO) opereert op het grensvlak van techniek en business en dat is in de praktijk niet altijd eenvoudig. CISO's met een technische achtergrond hanteren doorgaans een analytische insteek, communiceren probleem- en oplossingsgericht en hebben een andere risicobeleving dan de business.

De business wil niet van de CISO horen hoe iets werkt, maar wil begrijpen wat het hen oplevert!

Binnen een technische (ICT) omgeving is dit de norm en werkt dit constructief. Echter, om succesvol te zijn binnen zijn of haar organisatie, moet de CISO zich ook soepel kunnen bewegen in de wereld van de business; de business begrijpen, de taal spreken en security kunnen verkopen. Van hem of haar wordt dus veelzijdigheid verwacht.

Alleen wanneer information security zichtbaar de organisatiedoelstellingen ondersteunt en de business daadwerkelijk helpt haar strategie te realiseren, zal er draagvlak binnen de organisatie ontstaan en wordt security niet ervaren als last maar als 'enabler'.

De samenhang doorgronden

De CISO zal dus de samenhang van die twee werelden moeten doorgronden en die kennis moeten gebruiken om een win-win situatie voor beide werelden te creëren. Hiermee voegt de CISO waarde toe aan het bedrijf of de organisatie en groeit het draagvlak voor information security als geheel en voor zijn of haar positie in het bijzonder.

Hoe dit het beste gedaan wordt, verschilt per sector, organisatie en organisatiecultuur. Het is doorgaans een proces van vallen en opstaan, waarbij er voortdurend lessen geleerd kunnen worden uit de opgedane ervaringen en opnieuw richting kan worden gekozen.

De eigen business begrijpen

Eén uitgangspunt is echter voor alle sectoren, organisaties en organisatieculturen hetzelfde; om effectief met managers en bestuurders te communiceren, en daarmee invloed uit te kunnen oefenen, zal de security professional de wereld van de business moeten doorgronden, hun management cultuur en drives moeten begrijpen en hun taal moeten spreken. De CISO moet zich als één van hen onder hen kunnen bewegen.

Om de business van binnen uit te kunnen ondersteunen, moeten zaken als de marktbenadering, businessdoelen, de waardeketen, het verdienmodel, de jaarrekening en de businessuitdagingen bekend terrein zijn.

Een schaap met vijf poten

Verder zal hij om invloed uit te kunnen oefenen, zich, naast de voor de hand liggende soft skills, moeten verdiepen en bekwamen in zaken als organisatiekunde en managementvaardigheden en daarnaast een zekere organisatiesensitiviteit moeten ontwikkelen om binnen de heersende organisatiecultuur te kunnen opereren.

Een CISO moet in staat zijn de information security strategie over de business strategie heen te kunnen leggen en zo te formuleren dat de bijdrage van information security aan het realiseren van de business strategie voor iedereen binnen de organisatie helder is.

Herkenbare business doelen

De securitydoelen en het beleid kunnen zodoende herkenbaar voor de organisatie worden geformuleerd, dat de discussie over nut en noodzaak grotendeels vermeden wordt en het draagvlak toeneemt. Voor de business herkenbare doelen zijn zaken als:

- **strategische waarde**
- **bijdrage aan de business doelen**
- **reputatie, merkwaarde of concurrentiekracht**
- **kostenverlaging of omzetverhoging**

Let op: De business wil niet van de CISO horen hoe iets werkt, maar wil begrijpen wat het hen oplevert! En als de CISO de bijdrage van het security beleid en de implementatie ervan niet in bovengenoemde termen kan uitdrukken, dan is er iets mis met of de inhoud of zijn of haar wijze van communiceren.

Wat te doen als CISO?

Het voorgaande suggereert bijna dat iedere CISO een volledige MBA opleiding zou moeten volgen; bij een aantal grote multinationals is dit overigens al de norm. In de praktijk is binnen de meeste organisaties MBA-niveau nog niet nodig of niet haalbaar. Wel moet iedere CISO zich verdiepen en bekwamen in de hier besproken kennis en vaardigheden, om hem of haar in staat te stellen als een volwaardige partner van de business te opereren.

Verantwoorde onthullingen #6

DISMANTLING MEGAMOS

Hoe Volkwagen de Radboud publicatie over 'gekraakte' autosleutels tegenhield.

Toen de Radboud universiteit in 2008 de Mifare Classic RFID chip kraakte, spande chipfabrikant NXP een rechtszaak aan om publicatie tegen te gaan. Radboud won: een triomf voor academische vrijheid en responsible disclosure. Hoe anders verging het de academische security onderzoekers in 2013 in Engeland. Daar werd hun publicatie over een gekraakte elektronisch autosleutel door de rechter tegengehouden. Aanklager was niet de maker van de chip of het algoritme, maar een gebruiker: Volkswagen. Hoe was dit mogelijk?

Chris van 't Hof (www.cvth.nl)

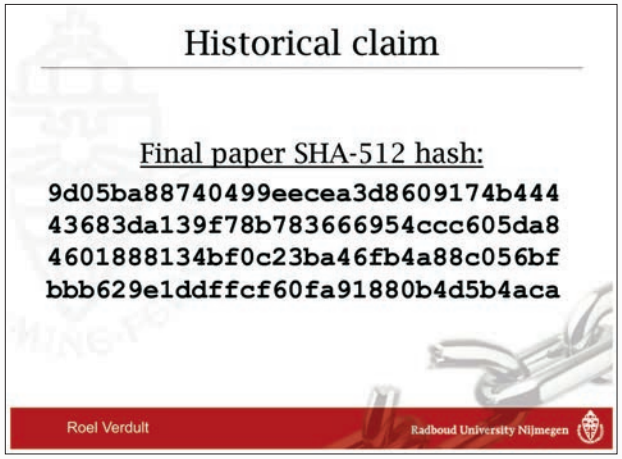
Al meer dan tien jaar zet de Digital Security Group zich onder leiding van professor Bart Jacobs zich in voor verantwoorde onthullingen. Onder de inmiddels veertig onderzoekers bevinden zich veel specialisten in RFID systemen. Dit zijn chips die middels elektromagnetische golven op afstand zijn uit te lezen, zoals de Mifare classic die wordt gebruikt in toegangspassen en de OV-chipkaart. Vanuit academische interesse en maatschappelijk belang, zijn al veel smartcards, tokens en e-readers door hen geopend. Eind 2012 was het elektronische autoslot aan de beurt.

Zo'n slot werkt als volgt. Als je de fysieke sleutel in het slot steekt, stuurt een lezer in dat slot een signaal naar een chip in de autosleutel. Eerst gaan er wat nummers heen en weer om te kijken of de chip en lezer echt zijn, vervolgens geven ze elk een nummer dat uniek is voor dat specifieke slot en die sleutel van die auto. Klopt alles, dan kan de auto gestart worden. Draden lostrekken en starten, zoals in de film, kan dan niet meer. Hoe deze berekeningen worden uitgevoerd is geheim.

Roel Verdult -die ook de Mifare classic kraakte- richtte zich op de Megamos Crypto chip. Die wordt gebruikt in de sloten van Porsche, Audi, Bentley, Lamborghini en alle Volkswagens. Op internet kocht hij een Tango Programmer. Met dit apparaat kun je sleutel en slot programmeren. Het bevat het geheime algoritme waarmee de berekeningen worden uitgevoerd. Door steeds de input en output te variëren en te kijken wat er gebeurde -reverse enginering- kwam hij achter het algoritme.

Nu kon hij elke elektronisch sleutel van auto's met Megamos startonderbrekers namaken. Maar dat was natuurlijk niet zijn doel. Hij wilde zijn bevindingen samen met collega Bar›s? Ege en Flavio Garcia van Birmingham University publiceren op de aanstaande USENIX computer security conferentie. Die was pas in augustus 2013, dus er was genoeg tijd om de eigenaar van het systeem in te lichten zodat die tijdig maatregelen kon nemen.

Alleen, wie is er eigenaar? Het algoritme is van het bedrijf Thales. Die heeft een ander bedrijf EM toestemming gegeven het te gebruiken in hun RFID chips. Weer een ander bedrijf Delphi gebruikt deze chips in hun sloten en sleutels en verkoopt dit systeem aan de fabrikanten die het in de auto's installeren. De onderzoekers gingen voor de chipleverancier en benaderde EM in november 2012. Ondertussen begonnen ze te schrijven aan hun artikel "Dismantling



Figuur 1: SHA-512 hash van het artikel

Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer." Deadline voor de Usenix conferentie: 25 juni.

EM reageerde pas in februari en op 6 juni was er dan eindelijk een meeting. Delphi was er ook bij. De leveranciers van de chips en de sloten vroegen de onderzoekers of zij bepaalde delen van het algoritme niet wilden publiceren. Lastig, want zo konden ze niet precies laten zien wat het probleem was, en bewijzen dat ze het algoritme ook werkelijk hadden achterhaald. In belang van deze bedrijven wilden ze het wel overwegen. Aan het eind van de meeting krijgen de onderzoekers een e-mail van een advocaat van Volkswagen. De autofabrikant heeft de High Court of England and Wales gevraagd een gerechtelijk bevel uit te voeren en publicatie tegen te gaan. Dat verzoek is de dag ervoor ingewilligd.

De zitting is 25 juni, de dag van de deadline van hun artikel [1]. De aanklager beroept zich op de Human Rights Act. In artikel 12, over de vrijheid van meningsuiting, staat namelijk dat een rechter een publicatie mag tegenhouden als je daar overtuigende argumenten voor hebt. Hij stelt dat het algoritme vertrouwelijke informatie is. Het onthullen ervan schaadt de vertrouwelijkheid en faciliteert diefstal van miljoenen Volkswagens. Het algoritme moet onrechtmatig verkregen zijn door de maker van de Tango Programmer. Wie de Bulgaarse site van de verkoper Scorpio bezoekt, ziet meteen dat dit illegale software is, volgens de advocaten van Volkswagen.

De verdediging stelt dat de onderzoekers het algoritme hebben achterhaald middels legale apparatuur en methoden: reverse enginering. Onthulling van het beveiligingslek is juist wel in het publieke belang: als criminelen het kunnen weten, moet ook het publiek er van op de hoogte zijn. Geheel volgens de Leidraad Responsible Disclosure van het NCSC hebben de onderzoekers EM zes maanden de tijd gegeven er iets aan te doen. Het is niet de schuld van de onderzoekers dat Volkswagen niet is ingelicht. Bovendien: hoe kan het dat Volkswagen hen aanklaagt? Zij zijn immers niet de eigenaar van het algoritme.

Rechter Justice Birss vindt dat Volkswagen zeker gezien kan worden als aanklager en wijst op jurisprudentie. Uit de zogenaamde Cream Holdings zaak kwam namelijk naar voren dat als de oorspronkelijk gedupeerde van een publicatie – in dit geval Thales - een sterke zaak heeft, een ander ook in diens plek kan aanklagen als dat nodig is. Maar eigenlijk is Volkswagen volgens hem ook gedupeerde: "Their products depend on the secrecy of the Megamos Crypto algorithm."

Aan de rechter het oordeel of deze onthulling verantwoord is. Hij vindt van niet, want met deze publicatie wordt een nieuwe manier om auto's te stelen publiek gemaakt. Hij vindt academische vrijheid een groot goed, maar "I think the defendants' mantra of "responsible disclosure" is no such thing. It is a self-justification by defendants for the conduct they have already decided to undertake and it is not the action of responsible academics." Hij verbiedt de onderzoekers hun artikel te publiceren.

Verdult, Garcia en Ege kunnen het artikel ook niet meer aanpassen, want de deadline is die dag en het kan niet nog een keer door de peer review. Typisch voor cryptografen publiceren ze in plaats daarvan de hashfunctie van hun tekst, die het artikel terugbrengt tot een unieke code van 128 tekens. Mocht later nog eens iemand de Megamos kraken, dan kunnen zij aantonen hoe zij dat nu al hadden gedaan.

Twee maanden later verschijnt Verdult toch op de USENIX Security Conference, zonder artikel, maar wel met een presentatie die is gecontroleerd door juristen en begint met disclaimers [2]. Hij mag geen technische details geven en geen vragen beantwoorden. Zijn verhaal gaat over hoe zij andere elektronische autosleutels hebben gekraakt, Responsible Disclosure en reverse engineering. Tussendoor zegt hij dat het met Megamos net zo ging. Op de laatste slide staat "Historical claim" met de hash van het artikel dat hij daar had willen presenteren (figuur 1). Het artikel is echter nog steeds niet gepubliceerd.

Links:
[1] Uitspraak gerechtshof:
http://www.bailii.org/ew/cases/EWHC/Ch/2013/1832.html
[2] Presentatie Verdult op USENIX:
https://www.usenix.org/conference/usenixsecurity13/dismantling-megamos-crypto-wirelessly-lockpicking-vehicle-immobilizer

SCHOENMAKER BLIJF BIJ JE LEEST

De discutabele rol van de accountant

Door verschillende incidenten staat de rol van de accountant ter discussie. Zowel zijn controlefunctie als zijn adviesfunctie. Gebieden waar zijn rol op het spel staat zijn risicosignalering, beheersing en rapportering aan stakeholders. Volgens Piersma en Couwenbergh wassen accountantskantoren steeds vaker hun handen in onschuld door erop te wijzen dat risicoanalyse niet hun opdracht is en geven ze aan dat het hen ontbreekt aan normen om hierover uitspraken te kunnen doen.

Yuri Bobbert MSc is PhD onderzoeker aan het IT Alignment & Governance Institute van de Universiteit van Antwerpen op het gebied van Business Information Security Governance. Ook is hij als Lector Business Information Security verbonden aan NOVI University of Applied Sciences en is hij CEO van B-Able. Hij is te bereiken via yuri.bobbert@b-able.nl.

Een soortgelijke valkuil ontstaat bij technology (IT) risicobeheersing. Dit is een gebied waar de accountancy-wereld steeds meer commerciële kansen probeert uit te nutten, gezien het feit dat IT audits onderdeel uitmaken van de jaarrekening. Naast de IT audit (controle) verschuift zijn functie steeds meer naar advies. Echter, uit empirisch onderzoek onder Nederlandse controleplichtige organisaties blijkt dat de analyse en de controle door de accountantskantoren op informatie systemen "hoog over" plaatsvinden. De nadruk ligt op vertrouwelijkheid en integriteit van de data, minder op informatievoorziening, uitwisseling en continuïteit van informatie systemen. Dat dient bij integraal IT-risicomanagement wel te worden onderzocht.

Een ongelukje zit in een klein hoekje, getuige het recente faillissement van Impairment Resources in de Verenigde Staten of, dichter bij huis, het faillissement van Diginotar. Een ander voorbeeld uit de praktijk is de verhoogde controle op gebruikers-autorisaties en het gebruik van sterke wachtwoorden bij toegang tot financiële data. Vergelijkbaar met de paspoortcontrole op een vliegveld. Dit helpt natuurlijk niet tegen de 'kwade' opzet van de gebruiker. Sterker nog, veel van de ondervraagden geven aan dit wachtwoordbeleid een vorm van schijnveiligheid en zeer belemmerend te vinden. Iedereen kent het probleem van een vergeten wachtwoord na een vakantie en de frustratie die dat met zich meebrengt. Een direct gevolg hiervan is de toename van post-its met wachtwoorden onder toetsenborden.

Het motto lijkt "Alles voor de handtekening op de jaarrekening". De kennis van de accountant, en zelfs van zijn IT-auditafdeling schiet te kort als het gaat om diepgaande kennis van IT-systemen en de adequate af- en bescherming ervan. De kennis en focus richt zich bij controles meer op methode en proces dan op de inhoud van materie en context van het te auditen object. Zeker als deze gevirtualiseerd, gedistribueerd, extern staan (cloud computing) of dynamische koppelingen hebben met derden. De informatiesystemen waar kritische financiële data op staan, de toename van digitale verbindingen met de "boze" buitenwereld en de exponentiële groei van digitale bedreigingen (virusverspreiding, diefstal, hacks) zorgen ervoor dat de accountant, het spreekwoordelijke schaap met vijf poten moet zijn. Vergelijk het met een schoenmaker die orthopedisch advies moet gaan geven.

De klantvraag om technische risicoanalyses en de daaruit voortvloeiende technische interventies synchroon te laten lopen met het beleid (In de meerderheid van de gevallen is er zelfs geen beleid) blijkt in de praktijk een hoofdpijndossier. Simpelweg omdat de vertaling van beleidskaders naar "pure" technische interventies complex is en onderhevig aan snelle verandering. Een wachtwoordbeleid is simpel te verwoorden en door te voeren, de noodzaak en effectiviteit daargelaten. Echter een virtuele scheiding van publieke en bedrijfskritieke data blijft voor veel organisaties complex, en dus wordt het niet gedaan. Je kunt dit vergelijken met je kast met de bedrijfsadministratie in de centrale lobby plaatsen en de voordeur wagenwijd open laten staan.

Waar de CEO veelal blindvaart op "ons zal dat niet gebeuren" of "wij hebben daar maatregelen voor getroffen" is het noodzakelijk dat zij zelf (laten) toetsen of dat ook echt zo is. Desnoods door een externe deskundige die niet in opdracht van de IT afdeling of zelfs de auditor werkt, maar in opdracht van een aansprakelijk (accountable) orgaan, veelal dus het bestuur. Om in accountancy-termen te blijven "vertrouwen is goed, controle is beter". Bij deze controle is de "hoog over" methode door de omgeschoolde account niet meer toereikend. Diepgaande materiekennis van potentiële risico's, kans en de impact ervan is nodig, zeker als de bedrijfsvoering grotendeels afhankelijk is van IT systemen.

Geen wonder dat het World Economic Forum zich buigt over wat weleens corporate's volgende nachtmerrie kan zijn en mogelijk de risicoanalyse van de accountant zal missen. Zeker als de hoeveelheid financiële transacties en de afhankelijkheid van het informatiesysteem sterk toenemen en parallel de informatiebehoefte exponentieel groeit. Het Centraal Bureau Statistiek rapporteerde eerder al over de toenemende economische schade en de koppositie die Nederland hierin vervult. Zowel overheid als bedrijfsleven kunnen hier niet langer aan de zijlijn blijven staan. Zij moeten deze risicobeheersing proactiever gaan aanpakken.

Een goed voorbeeld is Zuid-Afrika, daar heeft de overheid strikte "corporate governance" kaders voor technologie-risico's analyses vastgesteld (King report). Op het World Economic Forum werd het volgende voorgesteld: "Map highly interconnected key risks in the cyberspace and networked ecosystem and illustrate how they might unfold, while addressing the causes to identify effective intervention". Dit kunnen we vertalen naar een "digitale stakeholder analyse". Een van de meest principiële corporate governance praktijken die inzage geeft in digitale risico's die zakenpartners kunnen brengen en die accountancy IT audit mogelijk over het hoofd ziet. Voor een accountant wellicht complex en kennisintensief, maar voor een belegger of potentiële overname-kandidaat wel degelijk van belang. De keuze ligt bij de organisatie om dit transparant voor de markt te maken. In de VS tonen studies aan dat gedegen IT risico management juist concurrentie-voordeel kan bieden omdat de markt de organisatie ziet als een betrouwbare digitale handelspartner (Harvard Business School).

Primaire vraag blijft of de diepgaande complexe technologie kennis die nodig is in deze zeer snel veranderende wereld van cybercriminaliteit ooit van de accountant verwacht mag worden. Of moet de schoenmaker bij zijn leest blijven?

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 4 maart 2014, vond plaats in de Haagse Hoge School / Dutch InnovationFactory te Zoetermeer. In het expertpanel zaten Rudolf van der Maas, manager bij ngCompliance en leverancier van anti-fraude en -corruptie software en Roy Zwartjes, digitaal onderzoeker bij Hoffmann Bedrijfsrecherche B.V. In dit verslag een impressie van de discussie.

VERSLAG

FRAUDE & SECURITY

SECURITY CAFÉ

Het Libor schandaal bij de banken, de bouwfraude met een schaduwboekhouding, de examenfraude bij scholen, de uitkeringsfraude van de Bulgaren, maar ook verkeerd declaratiegedrag van openbaar bestuurders en spookfacturen zijn allemaal vormen van fraude waarbij er een motief is van een persoonlijk gewin. Hoe kunnen security professionals een bijdrage leveren om dit soort uiteenlopende vormen van fraude te voorkomen of detecteren?

Omdat er zoveel vormen van fraude zijn, is er niet één schadebedrag te noemen om de omvang van het probleem te schetsen. Fraude is echter van alle tijden en wordt door de media en techniek steeds zichtbaarder. Volgens Roy Zwartjes neemt fraude toe tijdens crises. Volgens onderzoek van Symantec is voornamelijk het midden- en kleinbedrijf straks slachtoffer van cybercrime. Man-in-the-middle-attacks, spyware, randsomware en social engineering zijn technieken waarmee criminelen eenvoudig middelgrote- en kleine bedrijven geld afhandig kunnen maken. Grote bedrijven hebben in potentie de juiste mensen en middelen om zich hiertegen te wapenen. Neemt niet weg dat fraudeurs vaak inventief zijn en dingen bedenken die beveiligers het nakijken geven.

Anti-fraude is opgezet door de 'business'. Informatiebeveiliging en IT security wordt vaak vanuit de techniek benaderd. Deze twee werelden komen steeds dichter bij elkaar en kunnen elkaar versterken. Om fraude met techniek te kunnen detecteren, moet je snappen wat de waarde is van je informatie. Meestal zijn fraudeurs uit op geld, maar fraude kan met alles wat een economische waarde heeft. Op een school kan het ook gaan om fraude met examens. Het is vreemd als de examenuitslag significant beter is dan voorgaande jaren. Bij een industrieel bedrijf kan het gaan om intellectueel eigendom. Het is vreemd

Gerco Kanbier is directeur van Trust in People – the information protection company.

Hij is te bereiken via gerco.kanbier@trustinpeople.com

Economische waarde en de verwachte werking die nodig is om afwijkingen te detecteren

als jouw concurrent opeens hetzelfde product lanceert. Bij de overheid kan een tender net gewonnen worden door de leverancier waarvan je het niet verwacht. Het is vreemd als het lijkt dat er onderling afspraken zijn gemaakt tussen aanbieders. Bij een beursgenoteerd bedrijf kan het gaan om koersgevoelige informatie. Het is vreemd als er zonder aanleiding veel in dat aandeel wordt gehandeld. Bij een uitkeringsinstantie zijn bankrekeningen veranderd en/of is de uitkeringsstroom opeens verdubbeld. Kortom, je hebt economische waarde en de verwachte werking nodig om afwijkingen te kunnen detecteren.

De werkgever

Als werkgever heb je een vertrouwensrelatie met je medewerkers. Verdenking van fraude zonder bewijs is moeilijk bespreekbaar en in eerste instantie ook af te raden. Echter, op het moment dat een werkgever iemand verdenkt, is er al sprake van een verstoorde arbeidsrelatie, aldus Roy Zwartjes. Als werkgever moet je dus voorzichtig te werk gaan. Je moet continu het bedrijfsbelang afwegen tegen de privacy van een medewerker. De Wet Bescherming Persoonsgegevens (WBP) zegt dat je in principe vooraf moet informeren tenzij er belangen zijn op basis waarvan informeren vooraf schadelijk kan zijn. Het is daarom raadzaam om als werkgever een procedure te hebben afgestemd en vastgelegd met de ondernemingsraad onder welke verdenkingen intern onderzoek gedaan kan worden naar verdacht gedrag van medewerkers. De verdenking moet dan in ieder geval een afwijking zijn op de gedragscode waarvan de medewerker bij aanvang van het dienstverband op de hoogte is. Als werkgever kun je in geval van vermoedens of bewezen fraude aangifte doen bij de politie. De politie zal veelal geen onderzoek gaan doen bij een verdenking van interne fraude. Bezit van kinderporno moet overigens wel altijd gemeld worden bij de politie. Indien de fraude digitaal heeft plaatsgevonden en mogelijk meerdere bedrijven treft, kun je het incident ook melden bij het Nationaal Cyber Security Centrum voor een structurele aanpak op landelijk niveau. De Kamer van Koophandel krijgt ook meer bevoegdheden om wantoestanden met spookfirma's aan te pakken en is dus ook een mogelijk meldpunt.

Fraude voorkomen

Om fraude te voorkomen, kun je interne workshops organiseren met je medewerkers om zwakheden van de organisatie op te sporen en preventief te verbeteren. Tegenargument voor deze aanpak, is dat eventuele interne fraudeurs nooit die informatie gaan delen en ze misschien wel op een idee brengen. Een andere suggestie uit het publiek was om kunstmatig gelegenheden te creëren om de verdachte alsnog in de val te lokken. Denk aan de lokfiets die politie gebruikt om fietsendieven te vangen. het uitlokken van misstanden niet altijd mogelijk is en dat daar wet- en regelgeving alsmede proportionaliteit en subsidiariteit niet vergeten mogen worden. Voor grotere bedrijven zijn er ook technische oplossingen die fraude en corruptie in een vroeg stadium kunnen signaleren. Menselijke interpretatie, normalisatie en technische signalering is noodzakelijke combinatie om fraude te detecteren, aldus Rudolf van der Maas. Banken maken gebruik van zwarte lijsten, zodat fraudeurs niet zomaar aan de slag kunnen bij de volgende werkgever. Zo heb je natuurlijk ook de Verklaring Omtrent het Gedrag (VOG), die je kan aanvragen bij de gemeente. Hierbij moet opgemerkt worden dan een veroordeling alleen gemeld wordt als dit relevant is voor de beoogde functie. Zwarte lijsten bestaan voor diverse sectoren (bv Onderwijs, Zorg), maar zijn vaak nationaal georiënteerd en dus te omzeilen door net over de grens te gaan werken. Het aanleggen van zwarte lijsten vereist formele registratie bij het CBP. Het is als werkgever zeker de moeite waard om medewerkers op bepaalde kritische posities in de organisatie te screenen op diploma, voorgaande werkgevers, schulden en veroordelingen. Fraude komt soms spontaan aan het licht als medewerkers op vakantie gaan en andere medewerkers tijdelijk het werk overnemen. Grote schandalen komen tot nu grotendeels door klokkenluiders aan het licht. Mensen die met interne informatie en bewijzen naar buiten treden, zijn formeel strafbaar volgens de bedrijfsregels, maar de klokkenluiderregeling beschermt klokkenluiders enigszins als het een groter maatschappelijk belang dient.
Als controlemiddel voor fraude, kunnen bedrijven een financieel overzicht met alle transacties opvragen bij hun leveranciers of controle doen naar de extra transacties naar de bankrekeningnummers van medewerkers.
Vele fraudeurs zijn geen beroepsfraudeurs; de gelegenheid maakt vaak de boef. De werkgever is echter vaak niet voorbereid op reconstructie van de fraude. Veelal is er gebrek aan digitaal forensisch bewijs en blijft het bij een verstoorde arbeidsrelatie. Naast de schade van de fraude, ben je geld kwijt aan (extern) onderzoek en een schikking met de fraudeur.

LINKS:
Security Cafe: http://www.trustinpeople.com/security-cafe

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

ADVERTENTIES OP WEBSITES VERBIEDEN?

En alweer is er via advertenties op bekende Nederlandse websites malware verspreid, zie: http://is.gd/giKKwT Wordt het zo langzamerhand niet tijd om advertenties volledig te blokkeren? Er zijn diverse tooltjes dit kunnen doen. Maar is dat ook wenselijk? Een groot deel van de internet infrastructuur en de gratis applicaties worden door advertentie-inkomsten gefinancierd. Maar hoe krijgen we dit onder controle?

Maarten Hartsuiker

We zijn eraan gewend geraakt. Gratis nieuws, gratis de weersvoorspelling, gratis social media, gratis muziek, gratis films... Waarom betalen als het ook gratis kan? Maar voor niets gaat natuurlijk de zon op. Vanuit onze sterke behoefte naar gratis diensten, zijn de online verdienmodellen van organisaties inmiddels voor een groot deel gericht op het in kaart brengen van onze interesses waarmee vervolgens passende advertenties worden getoond.

Om deze interesses in kaart te kunnen brengen en passende advertenties te tonen, vertrouwen website-eigenaren op grote advertentiebrokers en slimme profileringsoplossingen. Het vertrouwen in deze partijen, waaronder soms onbekende tussenpersonen en ondoorzichtelijke advertentiemarktplaatsen, is zelfs zo groot dat website-eigenaren deze partijen vrijwel ongelimiteerd toegang geven tot alles dat jij met de website deelt en van de website opvraagt. Deze controle wordt gedeeld via kleine blokjes javascript. Op het moment dat je als website-eigenaar zo'n enkel regeltje javascript in de website opneemt, geef je de externe partner de mogelijkheid om je bezoekers beter te leren kennen en passende advertenties te plaatsen. Met vergelijkbare stukjes javascript integreren we content zoals "social buttons", Google Maps of externe "libraries" zoals jquery in onze site. De veiligheid van de website is hiermee even krachtig geworden als de veiligheid van de websites waar deze programmacode vandaan wordt gehaald. We erven met deze werkwijze feitelijk de kwetsbaarheden van onze partners. Het is daarom niet vreemd dat veel grote websites, waaronder Groupon, Arke en Zalando, met malvertising te maken hebben gekregen. Het inladen van onvertrouwde content is een onderdeel van het internet ecosysteem geworden. Websites zijn afhankelijk geworden van de diensten van de grote tech-reuzen en advertentiebrokers. En in het grote geld van de online advertentie-inkomsten lijkt een incidentele malvertisingscampagne collateral damage te zijn geworden. Als website-eigenaren zouden we daarom terughoudender moeten zijn met het plaatsen van "slechts dat ene regeltje code" en zouden we onze beveiligingswensen krachtiger moeten laten horen. Vraag als afnemer je advertentieleverancier eens welke maatregelen hij heeft getroffen om jouw website tegen malvertising te beschermen. En probeer altijd passende geheimhoudings- en beveiligingsafspraken te maken met partijen waarvan je programmacode in je website opneemt.

Lex Dunn

Advertenties op websites: als regulier internet gebruiker heb je daar een soort haat-liefde verhouding mee. Meestal kijk ik er


Lex Borger


Maarten Hartsuijker


Lex Dunn


Ronald van Erven

overheen, maar soms zit er iets tussen dat je aandacht trekt. Zelf probeer ik dan de website te vinden buiten het advertentie mechanisme om, het gaat per slot van rekening niemand wat aan wat mijn specifieke interesses zijn (als ik op een advertentie uit de krant reageer weet ook niemand dat). Maar wat mij vooral stoort, zijn die irritante pop-ups, pop-overs en hoe ze allemaal ook mogen heten, zeker als ze ook nog (veel) geluid produceren. Omdat ik ook de bedreiging van met malware geïnfecteerde advertenties serieus neem, heb ik maar weer eens een ad-blocker geïnstalleerd. Als adverteren op internet geen inkomsten voor de adverteerders meer oplevert, zullen ze er mee stoppen. En dan rijst de vraag: wat betekent dit voor ons als regulier internet gebruikers? Google haalt het grootste deel van zijn inkomsten (en winst) uit advertenties. Stel dat deze wegvallen, zou Google dan nog zijn zoekmachine in de lucht houden? Ook sites als Youtube (met ondertussen meer dan één miljard bezoekers per maand) zouden dan mogelijk niet meer beschikbaar zijn. Recentelijk las ik een artikel in Quest (nr. 122 van April 2014, pagina 27) waarin een wetenschapper opmerkt dat als Youtube ooit zou stoppen, dit door de Verenigde Naties overgenomen zou moeten worden. En wat te denken van de hele internet infrastructuur? Een groot gedeelte wordt uit "eigenbelang" in de lucht gehouden, maar een niet onbelangrijk deel is weer afhankelijk van advertentie inkomsten. En wat te denken van de vele gratis apps in de Android, Apple IOS of Microsoft store? De meeste zijn gratis omdat de programmeur(s) inkomsten genereren via de advertenties. Volgens mij zouden we daarom de bedrijven die advertentie programma's aanbieden moeten aanpakken. Zij zouden zeker moeten stellen dat er geen geïnfecteerde advertenties getoond kunnen worden op de websites of in de apps, die hun programma gebruiken. Kan dat? Ja, net zo goed als anti-malware op een PC kan. Bekende malware kan gedetecteerd en dus verwijderd worden, (nog) onbekende malware zal de uitdaging zijn.

Ronald van Erven

Alles rondom malware is terug te brengen naar gemak, er snel en flitsend uitzien, cosmetisch en vooral GRATIS!! En vandaag de dag lift malware ook gratis mee in marketingware, die je weer opgedrongen krijgt via cookies of like buttons. Neem nu het verkopen van klant gegevens door banken. De storm barste los. Maar veel banken hebben op hun telebankier websites ook een facebook like button. En mensen vinden het leuk om hierop te klikken. Het is gewoon leuk om je sociaal te uiten. En dat zonder te weten wat er onder water allemaal aan persoonsinformatie weglekt of wat je aan nieuwe informatie in de vorm van malware binnen krijgt.
Sterker nog onlangs had ik een discussie met IT-professionals over het hergebruik van code en het "hardenen" van applicaties. De stelling was "moet jij als operationeel verantwoordelijke weten welke code (of services) op jou machines draait". Is hardening nog wel van deze tijd? Er worden zoveel code stukjes hergebruikt dat ook de professionals niet meer weten wat er allemaal in meekomt. Combineer dit met een "internet of everything" dat continu met elkaar verbonden is en je hebt een mooi platform voor malware verspreiding. Als alles maar functioneel werkt, het er lekker sexy uitziet, het snel en vooral gratis is! Dit gesprek maalde nog dagen bij mij door met vragen als:
Is informatiebeveiliging en privacy niet iets van de oude knarren die zich krampachtig vasthouden aan vroeger, de tijd dat malware spannend en iets unieks was? Is het met de vercommercialisering van internet niet all-in-the-game en geaccepteerd? Moeten we niet weer terug naar zuinig leren ontwikkelen en je verantwoording nemen voor elke code-regel? Het had nadelen maar ook veel voordelen als je op de aspecten privacy en kennis van je software code lette.

Lex Borger

Malware komt op je computer terecht door een bug of een click. Bugs bestrijd je door bij te blijven met je updates. Besmettingen door clicks doe je zelf, maar het is soms behoorlijk onduidelijk waar je op klikt. Met advertenties blokkeren bestrijd je in beginsel beide vormen, maar alleen als ze binnenkomen als advertentie. De advertenties mis je dan ook. En, zoals gezegd in de inleiding, veel internetdiensten worden bekostigd middels advertenties. Alternatieven zijn nodig: het is veel te eenvoudig voor externe software om jouw computer binnen te komen. Wat nu als actieve elementen altijd in een sandbox draaien of, beter nog, als de externe bron gewoonweg niet wordt toegestaan? Oracle laat Java nu zo werken. Hier kan Adobe een voorbeeld aan nemen. Nu zijn advertenties ook wel kampioen aandacht trekken met actieve elementen. Een gedragscode tegen gebruik hiervan, of minstens matiging, staat gelijk aan het Damrak een beter aanzien geven door de lichtreclames grotendeels te verwijderen. Websites mogen ook een beter aanzien hebben. De ad-blocker mag dan advertenties blokkeren die zich niet houden aan de code.

IMF
INTERNATIONAL MANAGEMENT FORUM

Trainingen in uw vakgebied
Certified Ethical Hacker (CEH)
CISM
Certified in Risk and Information Systems Control (CRISC)
CISSP
Cloud Security (CCSK)
Identity Management & Access Control
Informatiebeveiliging
ISO 27001 Lead Implementer
ISO 27001 Lead Auditor

€ 200,- korting voor PvIB-leden

www.imf-online.com/partner/pvib | info@imf-online.com

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
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (ANWB)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

ADVERTENTIE ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
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 2014
De abonnementsprijs in 2014 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

creative commons

Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-GelijkeDelen 3.0 Nederland licentie (CC BY-SA 3.0).
ISSN 1569-1063

WhatsApp

WAT MOET IK NU?

Deze week viel mijn oog op een berichtje dat uiteindelijk door de gehele media is overgenomen, namelijk dat we weer een miljardair in ons midden hebben, Jan Koum. Op zich een hele prestatie als je na vijf jaar bikkelen aan het cross-platform product Whatsapp uiteindelijk de titel miljardair overhoudt. Deze Oekraïense programmeur vestigde zich in de Verenigde Staten (wat een geluksvogel dat hij zijn geboorteland de rug heeft toegekeerd) en begon als immigrant in Amerika als afwashulp en verzorger van zijn zieke moeder. De tranen biggelen over het toetsenbord terwijl ik dit schrijf, maar laten we voorop stellen dat ik het Jan van harte gun.

Toen ik Whatsapp begon te gebruiken vroeg ik mij wel eens af waarom zou iemand zoveel investeren in infrastructuur en medewerkers zonder dat daar een verdienmodel tegenover staat: geen reclame inkomsten; geen commerciële uitingen; gewoon gebruikers het mogelijk maken om kosteloos (nou ja, officieel 79 eurocent per jaar) foto's, filmpjes, berichten en dergelijke te versturen. De nachtmerrie van de telecom bedrijven die hun verdienmodel op telefoontikken en SMS inkomsten hadden ingericht zagen de inkomsten verdampen en de eerste abonnementsvormen zijn al op de markt waar geen telefoontikken en geen SMS-bundels meer verkocht worden. Louter en alleen data wordt nog verkocht.

Terug naar Jan. Jan zat op een gegeven moment met een blikje Cola en zijn voeten op het bureau toen Mark Zuckerberg binnenkwam. Mark wilde de winkel van Jan wel overnemen. Hij ging naast Jan zitten en nam ook een blik Cola, voeten op het bureau en hij begon de onderhandelingen met 1 miljard euro. Jan krabt zich op het achterhoofd en zwijgt langdurig. Mark kreeg het benauwd en al snel gaven ze elkaar een hand bij de stand van 13 miljard euro. Ik ben nog van de oude stempel en reken vaak nog even terug naar de vertrouwde florijn. Jawel, ruim 30 miljard gulden was Jan rijker gedurende één blikje Cola. "Maar," vroeg Jan zich af, "Hoe kan ik de wereld vertellen dat Facebook een overname doet van 13 miljard euro terwijl mijn bedrijf dat lang niet waard is?" Facebook gaat de data van Whatsapp niet gebruiken is de officiële bewering. Maar waarom dan toch wel een groot bedrag vrijgemaakt voor deze overname? Volgens de verklaring van Facebook zijn de doelstellingen van Facebook en Whatsapp hetzelfde, namelijk de hele wereld met elkaar verbinden. Facebook ziet in Whatsapp een aanvulling daarop. De ruim een miljard Facebook-gebruikers en de 500 miljoen 'Whatsappers' is inderdaad een grote groep mensen. Er zal wel wat overlap zijn, maar toch.

Het kan toch niet zijn dat Mark Zuckerberg gek is (iets wat ik inderdaad echt niet geloof) en gewoon een enorm kapitaal uitgeeft aan data waarvan hij zegt dat hij die beslist niet gaat gebruiken? Wat is een bedrijf waard? Economen hebben daar ongetwijfeld moeilijke formules voor. Toch geloof ik niet dat dit bedrijf zoveel waard is. De 79 eurocent per gebruiker per jaar (die ik overigens slechts eenmaal betaalde) is geen echte vetpot. Zou Zuckerberg de zelfde fout maken als de Telegraaf groep die dacht dat Hyves een geweldig platform was om voet aan de grond te krijgen op het social media gebeuren? Twee jaar later bestond Hyves niet meer, weg 40 miljoen euro. Misschien ben ik te argwanend, misschien wordt de data inderdaad niet uitgewisseld. In de eerste klas van de kleuterschool beweerde ik ook dat Sinterklaas en Zwarte Piet niet bestonden. Iedereen zei dat ik gek was, zelfs de lerares. Ik ga bij mijn provider weer een abonnementje halen met SMS tegoed.

Groetjes Berry

Secure Link
Infrastructure Security Solutions

Gezocht!
Security Engineer

SecureLink is sterk groeiende en is daardoor op zoek naar Security Engineers die ons team komen versterken!

Als Security Engineer heb je diepgaande kennis op het gebied van onze security en networking producten. Je wilt met uitdagende technologieën van leidende security vendoren projectmatig werken. De combinatie van enerzijds de security technologie en anderzijds de integratie met de networking technologie is iets waar je jouw energie in kwijt kunt. Je krijgt veel zelfstandigheid om security oplossingen te pre-stagen, implementeren en onderhouden.

Benieuwd? Kijk dan op www.securelink.nl/vacatures

Integrated Networking Security Solutions

SecureLink is een vooraanstaande Benelux georiënteerde security en networking integrator. SecureLink onderscheidt zich door haar geïntegreerde security en networking specialisatie, voorname vendor statussen, managed services en hoge klanttevredenheid.

Go Secure!

SecureLink Nederland B.V. | Trapezium 224 | 3364 DL SLIEDRECHT | T +31 88 1234 200 | info@securelink.nl