08/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 8 - 2013

OP WEG NAAR INTERNET OF EVERYTHING

AANSTORMEND TALENT VERDIENT EEN PODIUM

DE VALKUILEN VAN SECURITY MONITORING

AGILE IN INFORMATIEBEVEILIGINGSPROJECTEN

EUROPESE PRIVACYWETGEVING: DE ROUTE NAAR COMPLIANCE

FOX IT

for a more secure society

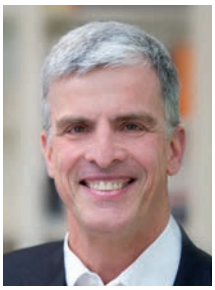
FOX-IT voorkomt, onderzoekt en beperkt de meest serieuze cyberdreigingen met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. Onze aanpak combineert slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. We ontwikkelen producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

FOX-IT.COM

Fox zoekt nieuwe Foxers

FOX-IT groeit en bloeit. Om deze reden zijn wij over de volle breedte van ons werk op zoek naar hackers, Forensic Experts, Pentesters, Developers (Python / C++), Hardware Engineers en Fraude analisten. Een Foxer is nieuwsgierig, kritisch en talentvol.
Je draagt bij aan de missie van FOX-IT: having fun in making technical and innovative contributions for a more secure society

Interesse om bij ons te komen werken?
Bel of mail Walter Doorduin 06 41901011 of doorduin@fox-it.com.



VOORWOORD

In de jaren tachtig, voordat virussen echt een breed probleem werden, heb ik een programma geschreven om mensen bewust te maken wat een virus kon doen op een PC, in Turbo Pascal. Dit is een DOS programma, waarbij DOS niet "Denial-of-Service" betekent, maar "Disk Operating System". Het programma ging recursief alle mappen door op de primaire schijf en toonde de melding "<file name> deleted". Er werd niets weggegooid, en dat meldde het programma ook aan het eind. Het maakte het echter wel duidelijk voor mij hoe eenvoudig dat te doen is.

Eind jaren negentig was ik 's morgens vroeg bij een klant aan het werk en maakte van de gelegenheid gebruik om mijn CMG e-mail binnen te halen. Ja, in die tijd moest je nog inbellen om je e-mail op te halen, dit is voordat er wifi guest netwerken bestonden. Het viel me gelijk op dat er een vreemde e-mail tussen mijn boodschappen stond: een liefdesverklaring van een manager. Je vermoedt dat er iets vreemds is, maar ik ging pas aan malware denken toen ik er nog twee meer kreeg. De "I love you" worm was in volle gang bezig. Die ochtend kreeg ik er nog honderden liefdesverklaringen erbij. Bij dit stuk malware was de verspreiding zelf die last gaf, maar nog steeds bleef die last daartoe beperkt. Later heb ik nog eens meegemaakt dat alle computers op de afdeling 's morgens hun luidspreker lieten toeteren.

Inmiddels zijn we ruim 25 jaar verder. Virussen heten tegenwoordig malware en die malware is een groot probleem. Niet alleen Windows PC's lopen gevaar, andere gevarenbronnen zijn Adobe producten en Java programma's. Uiteindelijk moet je alle programmatuur die van niet-vertrouwde bronnen afkomt of niet via een veilig kanaal komt als potentieel gevaarlijk zien.

Nu hebben we CryptoLocker als malware, een programma dat selectief je databestanden versleuteld. Dat is bijna zo goed als weggooien. Met het verschil dat het proces omkeerbaar is. Tegen betaling van 2 Bitcoin (ongeveer 1600 Euro) kun je je bestanden laten ontsleutelen. Er zijn berichten dat dit inderdaad lukt. Maar dan moet je het wel betalen binnen 72 uur, want anders vertienvoudigd het bedrag. En de server waar jouw sleutel op bewaard wordt, moet niet inmiddels van het internet verwijderd zijn door opsporingsdiensten. Voor de criminelen is het natuurlijk wel belangrijk dat het ontsleutelen goed werkt, want reputatie is alles, het geld moet binnen kunnen blijven komen.

Meer dan ooit is digitale hygiëne belangrijk geworden. Goede backups maken. En 'goed' in deze context is 'meerdere versies bewaren' en 'off-line zijn'. Een veilig netwerk gebruiken. Geen open wifi netwerk meer gebruiken. Je eigen netwerk beveiligen met WPA2. Patches bijhouden. Firewalls gebruiken, tegen malware scannen. En natuurlijk ook niet klikken op links in e-mail en niet overal hetzelfde wachtwoord gebruiken.

Ook voor internet providers is CryptoLocker een groot probleem. Zij worden natuurlijk aangekeken door hun klanten als die er achter komt dat alle bestanden op zijn PC versleuteld zijn. En moeten de radeloze klant vertellen dat er geen redden aan is als er geen backup is. Het is geen wonder dat ze er toe overgaan om bij het detecteren van malware activiteit de verbinding te blokkeren, hoe vervelend dat ook is voor de klant die het overkomt.

De malware strijd wordt feller. Een nieuwe ronde met nieuwe kansen. Nieuwe kansen voor beide zijden. ●

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto Omslag: Grand Canyon

OP WEG NAAR INTERNET OF EVERYTHING

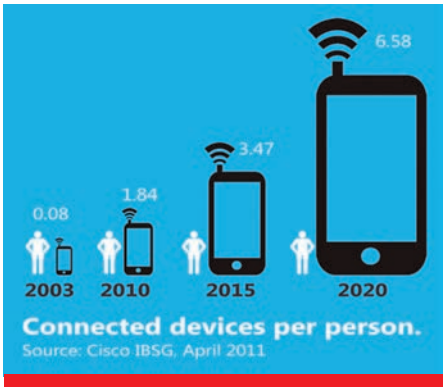
ALLES COMMUNICEERT MET ALLES

Ronald Eygendaal is werkzaam als principal security consultant bij eygendaals services (www.eygendaals.nl) en heeft meer dan twintig jaar ervaring in bewaking & beveiliging, technische beveiliging, fraude onderzoek en informatiebeveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsmanagers Nederland (VBN).

De Britse technologie pionier en medeoprichter van het Massachusetts Institute of Technology (MIT) Kevin Ashton staat bekend als de 'bedenker van Internet of Things. De term "het internet van dingen" is een visie waarin systemen in staat zijn om via het internet verbinding met elkaar en met de fysieke wereld te hebben.

Tijdens de Cisco Live 2013 conferentie in Orlando, waar 20.000 IT-beslissers aanwezig waren, heeft Cisco CEO John Chambers de volgende levensfase van Internet of Things aangekondigd waarbij Things wordt vervangen door Everything (oftewel IoE). Hierbij worden volgens John Chambers mensen, data, dingen via het internet aan elkaar gekoppeld. Het Internet of Everything gaat niet alleen over machine to machine communicatie maar ook over machine to people communicatie en in de optiek van Cisco zelfs over people to people communicatie. Kortom, een volledige vermenging dus van communicatie tussen mens en mens, mens en machine, en machine en machine. Dat alles moet leiden tot meer kennis en productiviteit. Een van de fundamenten onder Internet of Everything is de steeds verder gaande convergentie tussen kantoorautomatisering (IT) en procesautomatisering (OT) en fysieke beveiliging. Cisco is hierin een van de leidende spelers.

De slag om te komen tot het Internet of Everything is gaande en snel evoluerende. Het is heterogeen en omvat zowel verticale als horizontale producten en diensten. Het kan worden toegepast in zowel wired als wireless infrastructuren. Deze infrastructuren kunnen zich zowel binnenshuis als buitenshuis bevinden. Het Internet of Everything infrastructuur wordt bevolkt door apparaten welke variëren van computers tot "smart devices" welke 'slimme' functionaliteiten bezitten, dit vanwege de infrastructuren en diensten waarop zij aansluiten. Een smart device is een elektronisch apparaat, wat verbinding heeft met andere apparaten of netwerken zoals Internet, Bluetooth, Near Field Communication (NFC), WiFi, 3G en 4G. In basis zijn het op IP-technologie gebaseerde apparaten. Het Internet of Everything *faciliteert* consumenten en bedrijven en heeft invloed op alle aspecten van het dagelijks leven in de moderne samenleving.



Aantal verbonden apparaten per persoon (Bron: Cisco)

Op IP-technologie gebaseerde infrastructuren spelen hierbij een cruciale rol. Het Internet of Everything moet een intelligente, beheerbare en veilige infrastructuur bieden welke op kan schalen tot miljarden contextbewuste apparaten. Het intelligente netwerk luistert, leert en reageert met open interfaces voor betere beveiliging, grotere eenvoud, betrouwbaarheid, continuïteit, innovatie, en misschien wel meer comfort als ooit tevoren.

Eisen IoE apparaten

Het moge duidelijk zijn dat het Internet of Everything eisen stelt aan de apparaten die worden toegepast. Grofweg zijn er vijf belangrijke kenmerken vast te stellen waaraan apparaten moeten voldoen. Deze kenmerken zijn:

1 Ieder aangesloten apparaat dient te beschikken over *eigen uniek IP adres* wat wordt gebruikt voor identificatie en communicatie.
2 Elke aangesloten apparaat, mobiel of vast, dient een *unieke (soms virtuele) locatie* te hebben, dit is noodzakelijk om de onderliggende communicatieinfrastructuren zo efficiënt te laten werken.
3 Er is sprake van een situatie waarin een apparaat *informatie dient te verwerken of te generen.*

Alles met alles verbonden (Bron: Flickr)

De hoeveelheid informatie waar we het hier over hebben, zal de door mensen voortgebrachte informatie al snel gaan overstijgen.

4 Er zijn *complexe voorzieningen voor security*, analyse en beheer benodigd die het mogelijk maken groepen apparaten te formeren die via IP-netwerken met elkaar verbonden zijn.

5 Bij het verwerken of generen van enorme hoeveelheden data zijn *tijd en locatie van cruciaal belang*.

Aan het Internet of Everything zitten ook kwetsbaarheden, sterker nog, het is waarschijnlijk voor kwaadwillenden een zeer interessant doelwit om aan te vallen. Met de groei van het Internet of Everything zullen de kansen op aanvallen alleen maar toenemen. Het is dus van cruciaal belang dat security zeer veel aandacht krijgt, maar dan wel zo dat daarmee het Internet of Everything ook weer niet onbruikbaar wordt.

De beveiliging van Internet of Everything kan voor een groot deel worden gefaciliteerd vanuit de netwerkarchitectuur. Door deze architectuur op te bouwen in lagen ontstaat de mogelijkheid de beveiliging per laag te regelen. In de aller-onderste laag bevinden zich de zogenaamde end-points. Dit zijn embedded systemen, sensoren, actuators, cameras en dergelijke. Kortom een zeer gevarieerd spectrum van apparaten, met allerlei cpu-types, OS'en, geheugenstructuren en -omvangen en dergelijke. Veel van die apparaten zijn zeer goedkoop en verrichten slechts één functie. Er zijn reeds vele end-points in het veld voorzien van de mogelijkheid om aan te sluiten op een IP-netwerk. Echter ondanks de mogelijkheid om aan te sluiten is het daadwerkelijk aantal aangesloten end-points nog laag. Soms komt dat doordat de benodigde infrastructuur niet aanwezig is, in een aantal andere gevallen staan de kwaliteitssystemen en de regelgeving dit soort apparaten niet toe. Zo zijn er bijvoorbeeld infrarood detectors te koop welke kunnen worden aangesloten op een IP-netwerk. Maar staat het kwaliteitssysteem voor inbraakdetectie installaties, de zogenaamde BORG-regeling, het gebruik van IP infrarood detectors niet toe. Gelukkig kunnen veel end-points autonoom functioneren.

Boven de laag met de end-points bevindt zich de multi-service edge laag. In deze laag bevindt zich netwerkapparatuur welke verbinding heeft met de end-points. De multi-service edge laag faciliteert een reeks van protocollen en technieken. Dit zijn zowel vaste als draadloze technieken zoals Zigbee, (*open standaard* voor draadloze verbindingen tussen apparaten op korte afstand), IEEE 802.11, 3G en 4G. Vanwege de grote diversiteit aan protocollen en technieken speelt security hier een belangrijke rol. Voorkomen moet worden dat end-points onbeschermd zijn, de security services binnen multi-service edge laag hebben hierbij een belangrijke rol. Zoals eerder aangegeven is peer-to-peer verkeer tussen end-points een belangrijk gegeven in het kader van netwerkefficiëntie. Boven de multi-service edge laag bevinden zich het IP/MPLS-core netwerk en de datacenters met al hun mainstream IT-beveiligingsmechanismes.

Fysieke beveiliging

Binnen de fysieke beveiliging speelt de overgang naar IP-technologie al jaren, althans als we de branche mogen geloven. In de praktijk zien we in één gebouw vaak nog een fysieke scheiding tussen de verschillende IP-netwerken. Vaak wordt het IP-netwerk voor het kantoorautomatisering fysiek gescheiden van het ook op IP-technologie gebaseerde beveiligingsnetwerk. Ook de proces

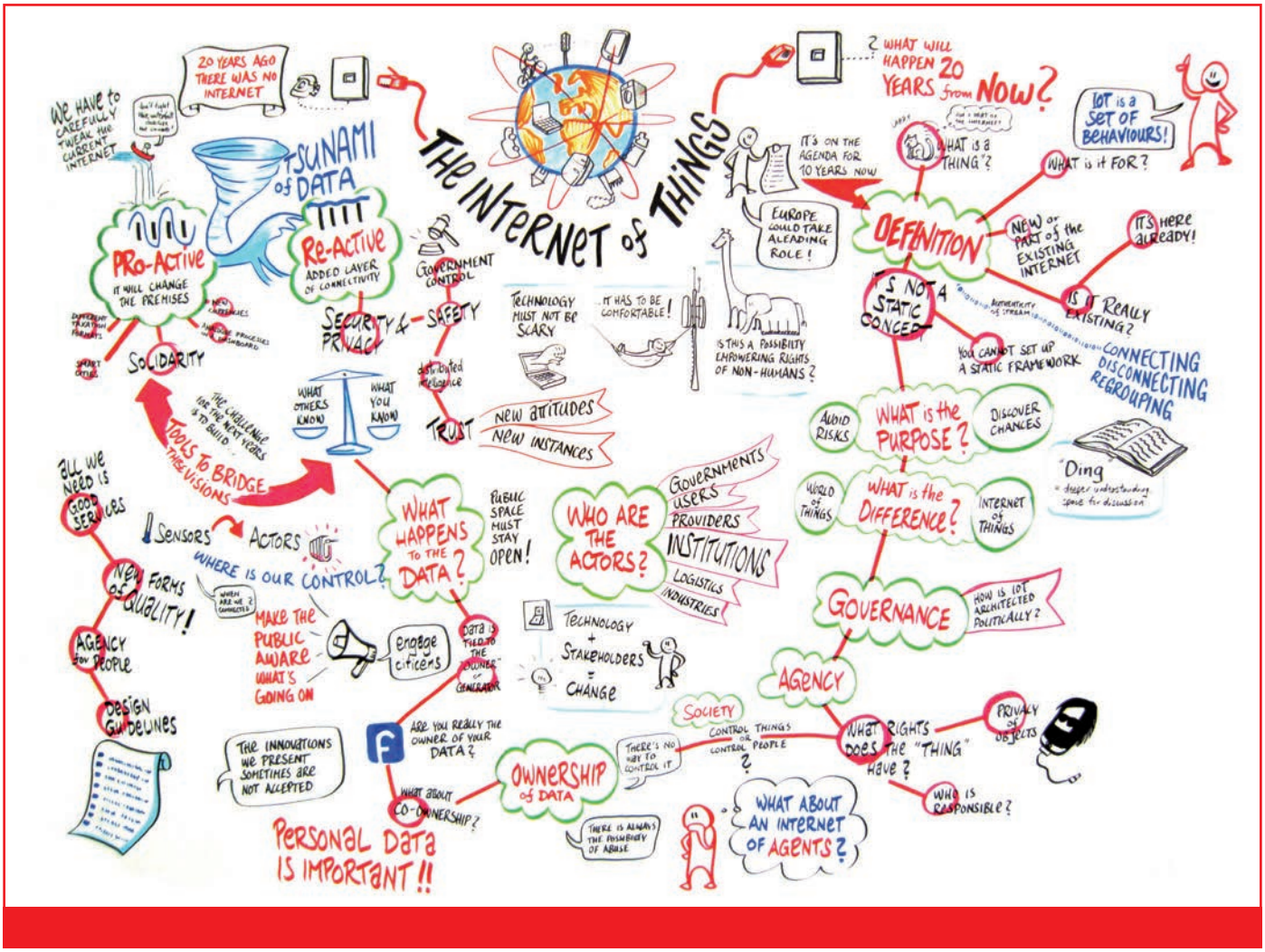
automatiseringsnetwerken (PCS, SCADA) zijn heel vaak gescheiden van de overige IP-netwerken. Door deze praktijken worden de fundamenten van de Internet of Everything visie geweld aan gedaan. Alhoewel Cisco inzet op Internet of Everything en ook fysieke beveiliging daar in wil meenemen beperkt Cisco zich tot toegangscontrole en videosurveillance. Andere fysieke beveiliging onderwerpen, zoals inbraakdetectie, passen nog niet in de Internet of Everything visie van Cisco. Toch zou het in theorie mogelijk moeten zijn om de functionaliteit inbraakdetectie te faciliteren vanuit het Internet of Everything. Zoals reeds eerder beschreven zijn er bijvoorbeeld infrarood detectoren te koop welke kunnen worden aangesloten op een IP-netwerk. Ook zou men in plaats van infrarood detectoren camera's met motion detection kunnen gebruiken. Hiermee zou het mogelijk moeten zijn om met de data die uit de end-points (lees infrarood detectoren & camera's) komt deze functie te creëren.

Marktbeweging

De beweging naar convergentie tussen kantoorautomatisering en procesautomatisering en fysieke beveiliging is in de markt duidelijk voelbaar. De eerste aanbestedingen waarin men deze convergentie vraagt, staan in de markt. In deze aanbestedingen lees je de natuurlijke spanning tussen het traditionele denken en de Internet of Everything gedachte. Ook Kristian Steenstrup, research vice-president bij de onafhankelijk marktanalist Gartner signaleert dat de aard van de procesautomatisering aan het veranderen is. Deze systemen en de onderliggende technologieën krijgen steeds meer de kenmerken van de mainstream IT. Dit ziet hij ook terugkomen in de platforms, software, beveiliging en communicatie. Volgens Steenstrup worden IT-leiders beïnvloed door de convergentie van mainstream IT en procesautomatisering. Ook in de bestuurskamer dringt ondertussen door dat ze met convergentie kostenbesparend kunnen worden en dat hierdoor efficiënter management kan plaatsvinden. Hoewel de uitdagingen van de integratie convergentie tussen kantoorautomatisering (IT) en procesautomatisering (OT) en fysieke beveiliging groot zijn, zijn er wel genoeg voordelen te noemen: gestroomlijnde budgetten, gecoördineerde planning, consistente technologische beslissingen en een gemaximaliseerde koopkracht. ●

Links

http://www.hays.co.uk/features/HAYS_411714
http://iotevent.eu/
http://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf
http://www.slideshare.net/CiscoIBSG/internet-of-everything



EEN KIJKJE IN DE KEUKEN VAN DE JBIS-AWARD 2013:

AANSTORMEND TALENT VERDIENT EEN PODIUM

Sandra Kagie is freelance tekstschrijver/journalist (website: www.sanscriptproducties.nl; twitter @SanSanscript). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'. Dit artikel is geschreven naar aanleiding van de uitreiking van de Joop Bautz Information Security Award op 9 oktober 2013. Meer informatie hierover is te vinden op www.jbisa.nl. Op deze website zijn ook de scripties van de twee genomineerden te vinden.

'Ware eyeopeners'. Met deze woorden typeert juryvoorzitter Pieter van Dijken de scripties van de twee genomineerden voor de Joop Bautz Information Security Award 2013. Zowel de uiteindelijke winnares, Christina Höfer, als runner-up, Hugo Ideler, hebben in de ogen van de juryvoorzitter met respectievelijk eMobility en cloud computing een actueel thema bij de kop gevat en hierbij nadrukkelijk de bescherming van de privacy van de gebruiker centraal gesteld. Het zijn mede hierdoor bijdragen aan het vakgebied van de informatiebeveiliging waar vakgenoten in zijn ogen kennis van móeten nemen.

In het geval van de scriptie van Christina Höfer betreft haar bijdrage een antwoord op de vraag 'hoe betaling van het opladen van elektrische auto's aan een laadpaal is te organiseren zónder dat de privacy van de automobilist in het geding komt'. De inmiddels afgestudeerde studente van de Universiteit Twente stelt in haar scriptie, getiteld 'Privacy-Preserving Charging for eMobility', dat er binnen het momenteel gangbare oplaad- en afrekenprotocol veel te weinig aandacht is voor privacyaspecten. Zogenoemde Personally Identifiable Information van degene die zijn auto oplaadt aan een laadpaal en ook direct afrekent, is veel te makkelijk traceerbaar voor betrokken partijen. Een situatie waar haar POPCORN-protocol een eind aan maakt.

Mede-genomineerde Hugo Ideler, inmiddels afgestudeerd aan de Technische Universiteit Eindhoven, staat in zijn scriptie uitgebreid stil bij de privacy risico's die cloud computing met zich meebrengt. In zijn werkstuk met als titel 'Cryptography as a service in a cloud computing environment' stelt hij dat gebruikers in de cloud veel te weinig grip hebben op de beveiliging van hun data. Dit tegen aanvallen van hackers, veiligheidsdiensten of malicious insiders. Een onderwerp dat het best kan worden samengevat met de kreet 'Big Data = Big Brother'.

'Dit moeten we niet willen'

De conclusie na bestudering van beide scripties is wat de juryvoorzitter betreft helder: "Dit moeten we op deze manier als samenleving niet willen. We moeten op het gebied van beide technieken, eMobility en cloud computing, als individuele burgers en gebruikers een vuist maken door veel meer aandacht te vragen voor de bescherming van onze privacy."

"Het moet in de nabije toekomst mogelijk zijn om onze elektrische auto anoniem op te laden. En hiervoor automatisch te betalen zonder dat de verschillende betrokken instanties, zoals energiemaatschappijen, op elk moment volledig op de hoogte zijn van onze whereabouts", meent hij.

En als het gaat om cloud computing moet in zijn ogen het onzichtbare (de cloud) weer tastbaar worden gemaakt. "Alleen de eigen sleutelbos van een gebruiker van de cloud mag nog toegang geven tot de gegevens die hij er heeft opgeslagen", stelt hij onomwonden.

De beide scripties vertegenwoordigen volgens de juryvoorzitter en ook volgens collega-jurylid en secretaris van de jury, Kelvin Rorive, een enorme actualiteitswaarde. Cloud computing

is met toepassingen als Facebook en Dropbox immers niet weer weg te denken uit onze maatschappij. En met anno 2013 naar schatting twintigduizend auto's met een stekker op de Nederlandse wegen, geldt dit langzamerhand ook voor de elektrische auto en de daarbij behorende laad-infrastructuur. Streven van de regering is zelfs dat het elektrische wagenpark in Nederland in 2020 niet minder dan tweehonderdduizend auto's telt.
De noodzaak van zowel vakgenoten als 'gewone gebruikers' om op de hoogte te zijn van de bezwaren omtrent privacy die zowel Christina als Hugo in hun scripties aan de kaak stellen, is wat beide heren betreft dan ook evident. "We zitten er op te wachten", vat Pieter van Dijken de mening van de jury over de twee scripties beknopt samen. En juist dit laatste uitgangspunt vormt een van de vier criteria waaraan een scriptie moet voldoen om in aanmerking te komen voor de Joop Bautz Information Security Award (JBISA), de jaarlijkse scriptieprijs voor Nederlandse studenten op het gebied van informatiebeveiliging. Een initiatief van het Platform voor InformatieBeveiliging (PvIB), ISACA dat staat voor vertrouwen in en waarde uit informatiesystemen en NOREA, de beroepsorganisatie van IT-auditors.

De vier criteria

Maar natuurlijk is dit genoemde criterium dat door de organisatoren van de prijs wordt omschreven als 'Praktische relevantie' niet het enige criterium waarop inzendingen beoordeeld worden. Studenten die in aanmerking willen komen voor de prestigieuze prijs, waaraan een bedrag van tweeduizend euro is verbonden, moeten met hun scriptie aan nog drie criteria voldoen: theoretische diepgang, vernieuwing en toepasbaarheid. Waarbij de laatste twee punten volgens Kelvin Rorive dit jaar de doorslag hebben gegeven in het voordeel van Christina. De jury heeft haar scriptie dan ook beoordeeld met de kwalificatie 'zeer goed' op alle criteria. Terwijl in het geval van Hugo's scriptie volgens hem binnen de jury enige bezorgdheid bestaat over de brede toepasbaarheid van zijn benadering in de echte wereld.

Uitzonderlijk talent

Wat zowel Christina als Hugo volgens de jury van de Joop Bautz Information Security Award heeft bewezen, is dat Nederlandse opleidingen en kennisinstituten uitzonderlijk talent op het gebied van informatiebeveiliging herbergen en afleveren. Deze talenten in het zonnetje zetten door ze op het jaarlijkse Security Congres een podium te geven, is een belangrijke doelstelling van de JBISA-verkiezing. De genomineerden hebben dan ook allebei naar aanleiding van hun scriptie een presentatie gegeven op het Security Congres dat onlangs op 9 oktober door ISACA, NOREA en PvIB is georganiseerd.

"We willen aanstormend talent prikkelen een bijdrage te leveren aan de ontwikkeling van ons vakgebied", legt Pieter van Dijken uit. "Daarbij willen we vakgenoten laten zien waar hun aankomende collega's zoal mee bezig zijn. Zo proberen we in de geest van de naamgever van onze award mensen bij elkaar te brengen en te enthousiasmeren om sámen te komen tot nieuwe activiteiten en initiatieven op het gebied van informatiebeveiliging in Nederland."
De juryvoorzitter hoopt en verwacht dat de scripties van Christina en Hugo hieraan een bijdrage zullen leveren. En natuurlijk ziet hij voor de JBISA-verkiezing van volgend jaar weer graag een aantal kwalitatief hoogstaande scripties tegemoet van studenten van Nederlandse hogescholen en universiteiten.
"We dagen deze studenten dan ook uit ons de komende jaren opnieuw te verrassen met hun vernieuwende inzichten", aldus Kelvin Rorive. "Er wordt op Nederlandse hogescholen en universiteiten zoveel onderzoek gedaan op ons vakgebied. We zijn er als jury daarom van overtuigd dat er nog veel meer scripties worden geschreven waarvan wij op de hoogte moeten zijn", stelt hij uitdagend.

De genomineerden aan het woord

Een oproep waar de genomineerden voor de JBISA 2013 zich van harte bij aansluiten. "Dankzij mijn deelname aan de verkiezing is mijn scriptie niet alleen beoordeeld door mijn begeleiders aan de TU/e, maar ook door gerenommeerde mensen uit de praktijk van de informatiebeveiliging", geeft Hugo Ideler aan. Een leervolle ervaring, zoals hij het noemt, die hem weer nieuwe inzichten heeft opgeleverd.

"Dit vooral omdat je in het gesprek met de jury over je scriptie wordt gedwongen om na te denken over wat jouw werkstuk zou kunnen veranderen in het leven van mensen", aldus de runner-up.
Deze praktische insteek van de jury spreekt ook winnares Christina Höfer erg aan. "Ik ben zelf namelijk een enorme voorstander van toepasbaar onderzoek", vertelt ze.
Dat juist dit criterium voor de jury van doorslaggevende betekenis is geweest om haar uit te roepen tot winnaar 2013, noemt ze daarom 'extra mooi'.
En ook heeft zij het net als Hugo als stimulerend ervaren om tijdens het Security Congres met vakgenoten over haar scriptie te praten. "Op die manier ga je je afstudeeronderwerp toch weer vanuit andere invalshoeken bekijken. In mijn geval bijvoorbeeld vanuit de financiële kant", geeft ze aan.

Beide talenten, inmiddels afgestudeerd, hopen dat ze met hun verhaal anderen kunnen overtuigen in de komende jaren ook deel te nemen aan de JBISA. "Het biedt je als student toch een mogelijkheid om wat meer bekendheid te krijgen in de wereld van de informatiebeveiliging", aldus Hugo. "Zo mag je op het Security Congres je idee pitchen. Een mogelijkheid waarvan ik gretig gebruik heb gemaakt."

Toepassingen in de toekomst?
Voor de toekomst hopen zowel Christina als Hugo natuurlijk dat de security-oplossingen die zij in hun respectievelijk scripties hebben aangedragen daadwerkelijk toegepast gaan worden in de dagelijkse praktijk. Wat het POPCORN-protocol van Christina betreft heeft zij haar hoop voor de brede implementatie hiervan gevestigd op ISO/IEC. Haar protocol waarmee de behoefte aan privacy van de elektrische rijder wordt ingewilligd, borduurt namelijk voort op de huidige ISO/IEC 15118-norm. "De Europese norm die momenteel alle aspecten van oplaadcommunicatie voor elektrische voertuigen beschrijft", legt ze uit.
Met haar benadering op basis van cryptografische innovaties vult ze de hiaten in deze norm in waardoor deze de toets van een privacy assessment wel doorstaat. Mede door contacten die bijvoorbeeld haar professor heeft met ISO/IEC hoopt Christina dat haar protocol in de toekomst het fundament zal zijn van een standaard protocol voor betaling voor eMobility met behoud van privacy voor de elektrische rijder. En de extra aandacht die haar scriptie dankzij het winnen van de JBSIA 2013 heeft gekregen, kan hieraan volgens haar zeker een bijdrage leveren.

Iets dat volgens Hugo ook geldt voor de nominatie die hij voor zijn scriptie in de wacht sleepte. Wat hij in elk geval met zijn scriptie heeft willen bereiken is dat mensen en bedrijven beter nadenken over welke gegevens ze wel en niet in de cloud willen opslaan. De recente onthullingen van klokkenluider Edward Snowden rond het afluisterprogramma PRISM hebben volgens hem de noodzaak hiertoe pijnlijk blootgelegd.
En zoals uit zijn scriptie blijkt, is er een oplossing. "De 'crypto VM', een extra virtuele machine die tussen de virtuele machine van een cloud gebruiker en de software van de cloud provider in wordt geplaatst", legt Hugo uit. "In combinatie met de eerste benodigde stap: de komst van een certificaat waaruit blijkt dat een cloud provider alleen software gebruikt waarmee het onmogelijk is data van klanten te lezen, geeft deze 'crypto VM' de cloud gebruiker de gewenste zelfbeschikking."
Het vertrouwen in de cloud zal volgens Hugo dankzij de implementatie van deze oplossing toenemen. "En dus is de security-oplossing zeker ook in het belang van de providers", stelt hij. En juist deze win-winsituatie geeft hem het vertrouwen dat zijn oplossing in de echte wereld toegepast gaat worden. "Waarschijnlijk niet helemaal zoals ik het in mijn scriptie heb voorgesteld, maar zeker in een afgeleide vorm", voorspelt hij.

Zoektocht naar krenten in de pap
Een dosis gezond vertrouwen en enthousiasme dat de jury van de JBISA graag ziet. Het zijn immers deze eigenschappen die studenten er volgens Pieter van Dijken toe zetten om bijzondere prestaties te leveren. "En laat dat nu net zijn waar wij naar op zoek zijn: de krenten in de pap die het vakgebied van informatiebeveiliging nieuw elan geven. Talent dat we ook graag volgend jaar en de jaren daarna een podium geven", besluit de juryvoorzitter van de Joop Bautz Information Security Award enthousiast. ●

DE VALKUILEN VAN SECURITY MONITORING

Dr. ir. Tom Kleiberg is security consultant bij Pinewood.
Tom is te bereiken via Tom.Kleiberg@pinewood.nl en http://nl.linkedin.com/in/tjkleiberg

Security monitoring is een belangrijke maatregel met als voornaamste doel tijdig en adequaat te kunnen acteren op bijzondere of afwijkende gebeurtenissen. Security monitoring gaat verder dan systeembewaking of compliance monitoring. Waar compliance monitoring vooral (automatisch) toeziet op naleving van wet- en regelgeving door controle op de *aanwezigheid* van maatregelen, bewaakt security monitoring continu de informatieveiligheid door óók de correcte *werking* en *effectiviteit* van maatregelen inzichtelijk te maken. Security monitoring biedt actueel inzicht in de gedragingen in de ICT-infrastructuur en door betekenis te geven aan bepaalde ICT-gebeurtenissen kan alert en adequaat gereageerd worden op afwijkende en risicovolle situaties.

De belangrijkste aanleiding voor veel organisaties om te starten met security monitoring is gelegen in compliance. Standaarden en baselines als PCI-DSS en Baseline Informatiebeveiliging Rijksdienst (BIR) schrijven voor dat security monitoring wordt toegepast binnen de organisatie en zodoende wordt vaak ijverig gestart met aanschaf van tooling, gevolgd door implementatie. In de praktijk blijkt echter dat de weg naar een succesvolle implementatie en aanwending is behept met vele valkuilen. De toegevoegde waarde van security monitoring wordt vaak niet bereikt of zelfs gezien door organisaties. Want afgezien van de vaak forse financiële investeringen, blijkt regelmatig dat organisaties die wel security monitoring geïmplementeerd hebben, na een "succesvol" implementatietraject stuiten op een teleurstellende opvolging. De inzet van security monitoring moet daarom zeer goed doordacht worden vóór aanschaf van tooling en de betrokkenheid van de organisatie is daarbij onontbeerlijk. Dit artikel gaat in op de voornaamste valkuilen en misverstanden.

Valkuil 1 - ICT als promotor

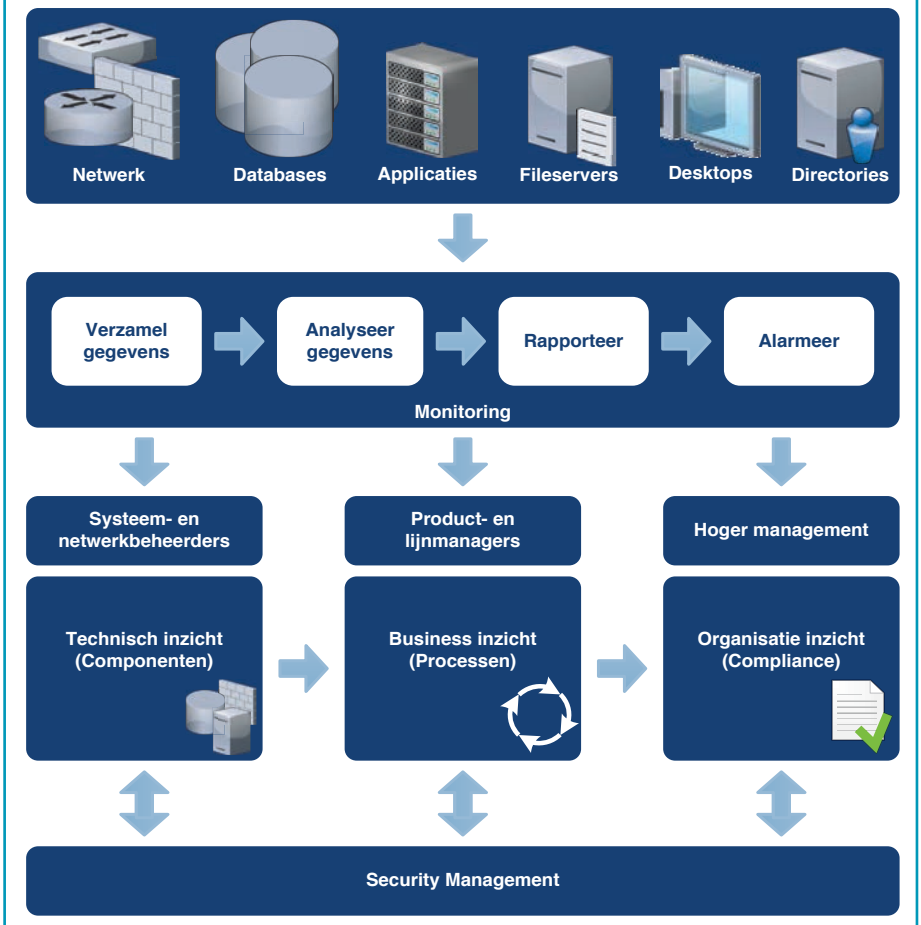
Organisaties die security monitoring vanuit een compliance behoefte initiëren, behandelen dit vaak als een technisch vraagstuk. Hierdoor belandt de projectuitvoering en opvolging bijna automatisch bij ICT. ICT heeft ogenschijnlijk het grootste belang bij security en krijgt als zodanig de rol van promotor naar zich toegeschoven. Hierdoor ontstaat de perceptie dat security monitoring vooral ICT-processen ondersteunt en geen directe toegevoegde waarde heeft voor de business. De betrokkenheid van de business is daardoor niet vanzelfsprekend. Security monitoring is echter *juist* een business tool en ondersteunt deze door risico's, ten gevolge van ICT-gedragingen, inzichtelijk te krijgen en dus beheersbaar te maken. ICT is verantwoordelijk voor de operationele staat van systemen, maar kan de *business value* van de informatie op deze systemen niet inschatten. De business is nodig om aan te geven welke informatie belangrijk is en hoe deze informatie geïnterpreteerd moet worden. Het is daarom essentieel de business vroegtijdig te betrekken bij het project en ze bekend te maken met de mogelijkheden van security monitoring (tools). Zorg dat de doelstellingen van security monitoring aansluiten bij de business doelstellingen en laat tijdens het project bijvoorbeeld regelmatig wat rapportages zien. Zo leert de business de mogelijkheden kennen van security monitoring, inclusief de uitgebreide toepassingen ervan. Dit leidt tot een verbeterde acceptatie en inzet van security monitoring en verhoogt de toegevoegde waarde.

Valkuil 2 - Technisch beheer wordt te laat aangehaakt bij de implementatie

Security monitoring bestaat uit het verzamelen en analyseren van (veel!) informatie. Afstemming over welke informatiesystemen moeten aanleveren en in welke vorm is essentieel. De medewerking van beheerders is hierbij onmisbaar. Zij weten welke configuratie-onderdelen belangrijk zijn, wat het formaat is van de logs en welke betekenis gegeven moet worden aan verschillende ICT-gebeurtenissen. Beheerders zitten echter lang niet altijd te wachten op dergelijke implementaties. Hun primaire taak is ervoor te zorgen dat "hun kindje" in de lucht blijft, er geen verstoringen optreden, etc. Zodra er sprake is van installatie van een agent, er aanpassingen nodig zijn op het systeem of extra koppelingen aangelegd moeten worden, ontstaat er vaak weerstand. Neem deze weerstand weg door beheerders ervan te overtuigen dat deze tools ook voor hen waardevol zijn. Laat zien hoe deze tools hun werk gemakkelijker kunnen maken doordat ze bepaalde taken uit handen nemen. Voorkom hiermee ook dat beheerders zich gecontroleerd voelen, omdat een security monitoring tool hun "fouten" kan detecteren. Dergelijke tools helpen de beheerder juist verder en dragen bij aan het kwaliteitsproces.

Valkuil 3 - Processen voor gebruik en onderhoud van de tools worden pas na oplevering ingericht

Doordat security monitoring tools zijn gekoppeld aan veel informatiebronnen, vereisen ze veel onderhoud en worden ze onvermijdelijk onderdeel van diverse (ICT) processen. Regelmatig kom je tegen dat vergeten wordt nieuwe systemen toe te voegen aan de security monitoring tool of dat bijwerken van een bewaakt systeem leidt tot een onleesbaar logformaat, met als gevolg dat deze bron wegvalt. Voorkom deze problemen door vooraf processen



Security monitoring in een schematische weergave

in te richten voor het beheer van de security monitoring tools en beoordeel de impact op bestaande ICT-processen. Wacht dus niet met het inrichten en wijzigen van deze processen totdat het ICT-implementatietraject is afgerond, maar zorg ervoor dat er voldoende aandacht is voor de periode erna.

Valkuil 4 - Er is niet nagedacht over een security organisatie die past bij de security monitoring

Security monitoring resulteert bijna automatisch in meer meldingen over je ICT-omgeving. Deze meldingen zullen afgehandeld moeten worden en dit verlangt een verandering in de organisatie. Adequaat en alert reageren op afwijkend ICT-gedrag vereist in de eerste plaats dat specialistische kennis aanwezig is voor de analyse van de verzamelde gegevens op relevante afwijkingen. Daarnaast is het van belang dat de juiste rollen, taken en verantwoordelijkheden belegd zijn binnen de organisatie. Op het moment dat een calamiteit zich voordoet, moeten deze bekend zijn, zodat men niet ten tijde van de calamiteit nog moet uitvinden waar de verantwoordelijkheden liggen. Bedenk vooraf welke personen betrokken moeten worden bij het afhandelen van de meldingen en welke informatie nodig is in geval van een calamiteit. Zorg ervoor dat in situaties waar op basis van 24x7 gealarmeerd moet worden, de organisatie dit kan ondersteunen.

Valkuil 5 - Tot aan het vinkje… En niet verder

Leveranciers van security monitoring tools spelen handig in op compliance vraagstukken door voorgeprogrammeerde sets aan te leveren voor het bewaken van de compliance status. Hierdoor wordt de indruk nog verder versterkt dat men na de implementatie achterover kan leunen en de tool zijn werk kan laten doen. Men is compliant en hoeft zich vervolgens voor een jaar geen zorgen meer te maken. Tot de volgende audit… Wat de auditor dan vaak aantreft is een security monitoring tool die nauwelijks nog is afgestemd op de werkelijke situatie. De ICT-omgeving is dermate veranderd dat niet langer (de juiste) informatie wordt verzameld. Daardoor mist men veel loginformatie van de afgelopen periode en kan de auditor niet beoordelen of zich geen bijzonderheden hebben voorgedaan in de voorbije periode. Bovendien ligt er voor de ICT-organisatie weer een hoop werk klaar om ervoor te zorgen dat de omgeving weer correct gemonitord wordt. Dit brengt vaak veel extra kosten met zich mee. In enkele gevallen leidt het er zelfs toe dat het monitoringsysteem opnieuw dient te worden geconfigureerd en men feitelijk weer vanaf nul moet beginnen. Bedenk dus dat ook voor compliance toepassingen het noodzakelijk is beheer in te richten. De voorgeprogrammeerde sets zijn vooral een hulpmiddel, de werkelijke kracht komt nog steeds uit de organisatie zelf.

Valkuil 6 - Gebrek aan resources

Tot slot is de tijd die de ICT-organisatie heeft voor security monitoring een probleem. Regelmatig wordt de uitvoering van ICT-projecten ondergebracht bij beheer. Zij zijn echter al overbelast met beheerwerkzaamheden en kunnen onvoldoende tijd vrijmaken voor zo'n ingrijpend project (waarvan ze zelf ook niet altijd het belang zien). De prioriteiten moeten van bovenaf duidelijk worden gemaakt en bij "bovenaf" moet dus ook duidelijk zijn dat de implementatie gedragen moet worden door de organisatie. Er moeten (aanzienlijke) resources vrijgemaakt worden bij beheer, zowel tijdens als na de implementatie. Duidelijke communicatie over hun rol hierin is daarom onontbeerlijk. Zorg ervoor dat voldoende projectbudget wordt ingeruimd tijdens de implementatie en houd hierbij rekening met de complexiteit van deze projecten. Bedenk eveneens dat na oplevering er extra taken komen te liggen bij beheer. Houd dus ook hier rekening met extra resources om zo te komen tot een succesvol project!

Samenvattend kan worden gezegd dat betrokkenheid van de business bij security monitoring van vitaal belang is. Niet alleen tijdens het voortraject, maar ook na oplevering blijft betrokkenheid essentieel. Maak hierbij wel een realistische inschatting van de inzet en benodigde resources, zodat aan de verwachtingen kan worden voldaan. Dit verhoogt de kans van slagen van security monitoring projecten aanzienlijk en draagt bij aan een succesvolle opvolging! ●

COLUMN: PRIVACY

TIEN ZAKEN DIE U MOET WETEN OVER PRIVACY VOOR 2014

Met wat doorstemmendheid van wetgevers wordt 2014 een mooi privacywetten-jaar. De Wbp wordt opgesierd met een meldplicht datalekken en vanuit de EU komt een privacyverordening die alle lokale wetten in een klap moet vervangen. Hieronder een aantal hoogtepunten voor 2014:

1. **De meldplicht datalekken**: De Nederlandse meldplicht datalekken komt eraan in 2014. Vanaf dat moment bent u verplicht elk lek in de beveiliging waarbij persoonsgegevens betrokken zijn, te melden bij het CBP. Wat is dan een lek in de beveiliging? Dat kan variëren van het verliezen van een USB-stick, het gehackt worden tot het verkeerd adresseren van een e-mail of het per ongeluk bij de vuilnis zetten van het papieren archief. Ik hoor u denken "dat is nogal wat zeg…". En dat klopt, naar verwachting zullen er zeker 60.000 meldingen gedaan worden in het eerste jaar. En, moet ik dan echt alles melden? Ja, vooralsnog wel, want de wettekst en de uitleg laten geen ruimte voor kwijtschelding van de meldplicht in bagatel-zaken.
2. **De Privacy Officer**: Een carrière-switch aan het overwegen? Dan zou ik serieus denken over privacy. 2014 wordt namelijk het jaar van de Privacy Officer. Althans, het jaar waarin veel bedrijven een vacature uit moeten zetten. Alle overheids-organen zijn straks verplicht er een te hebben. Daarnaast ook alle bedrijven die voor tenminste 12 maanden achter elkaar de gegevens van 5.000 betrokkenen verwerken of als de kernwerkzaamheden bestaan uit het monitoren van personen of als deze bestaan uit het verwerken van gevoelige gegevens.
3. **De bewerkersovereenkomst**: Uiteraard sluit u altijd een bewerkersovereenkomst af indien anderen in uw opdracht persoonsgegevens verwerken. U zult een aantal wijzigingen moeten doorvoeren. De beveiligings-clausule moet meer uitgebreid omschreven worden (onder meer duidelijker de eisen vastleggen). Daarnaast moet u een clausule opnemen over de meldplicht datalekken, waarbij de bewerker verantwoordelijk wordt voor het doen van de melding.
4. **Nog even over die meldplicht datalekken**: U krijgt trouwens een boete als u geen lijst bijhoudt van datalekken en ook als u geen melding doet bij het CBP of aan de betrokkenen. Alles ter waarde van 450.000 euro per overtreding.
5. **Toestemming**: Een veelgebruikte rechtsgrond voor gegevensverwerkingen. Straks bent u verplicht bewijs te leveren dat u toestemming hebt verkregen. Alles moet vastgelegd en gedocumenteerd worden.
6. **De beveiliging van persoonsgegevens**: Ik besef me dat ik nu voor eigen parochie sta te preken. Maar, voor juristen is het even wennen. De beveiligingsparagraaf in de verordening is vrij uitgebreid, althans, eindelijk is rekening gehouden met de kernbegrippen binnen de informatiebeveiliging. Er dient securitybeleid te zijn vastgelegd waarin integriteit, confidentialiteit, beschikbaarheid en weerbarstigheid centraal staan. Regelmatig dient er getest te worden of alles nog netjes werkt en de effectiviteit van zowel beleid als maatregelen dient geëvalueerd te worden.
7. **Nog even over die Privacy Officer**: Betrokkenen krijgen onder de verordening het recht om persoonlijk contact op te nemen met de Privacy Officer. Diens naam en contactgegevens moeten dus ook duidelijk kenbaar worden gemaakt. Eerlijk is eerlijk, als Privacy Officer van Nederlandse Spoorwegen weet ik niet wat er straks allemaal op me af gaat komen als iedereen bij mij persoonlijk kan aankloppen. En ik maak me ook wel een klein beetje (echt een klein beetje maar hoor) zorgen. De eerste doodsbedreigingen aan het adres van een Privacy Officer – ik noem vanwege privacy even geen namen – zijn afgelopen jaar namelijk al binnengekomen doordat diens naam publiek kenbaar was gemaakt. Misschien wilt u punt 2 van deze lijst nu toch heroverwegen.
8. **Data protection day**: 28 januari wordt het jaar ingeluid met Data protection day.
9. **Misschien krijgen EU onderdanen eindelijk ook rechten tegen de USA**: Reding is met de USA aan het onderhandelen over zogenaamd "judicial redress". Onder judicial redress zouden EU onderdanen het recht krijgen om juridisch op te treden tegen privacyschendingen door de USA. Of het ook echt zo ver zal komen, is nog maar de vraag. Obama heeft gezegd open te staan voor het beperken van de bevoegdheden van de NSA, hetgeen natuurlijk nog niet hetzelfde is als de NSA kunnen aanklagen.
10. **Privacy pictogrammen**: Wist u dat u straks privacy pictogrammen dient te voeren om duidelijker kenbaar te maken wat er met persoonsgegevens gebeurt? Ik heb geprobeerd zonder begeleidende tekst de pictogrammen te lezen en moest constateren dat het toch vrij slecht met mijn privacy-gok-kennis gesteld is. Ik had slechts 2 van de 6 direct goed. De laatste had ik in ieder geval fout. Het pictogram waar-mee kenbaar wordt gemaakt dat gegevens niet onversleuteld worden bewaard, is een plaatje van een open slotje... Ja jeetje! Dat heeft toch elk security-minnende PvIB-er dan fout!

Op naar een privacy-proof 2014! ●

Mr. Rachel Marbus, @rachelmarbus op Twitter

AGILE IN INFORMATIEBEVEILIGINGSPROJECTEN

Thomas van Vooren is Principal Consultant bij Everett, een gespecialiseerd systeemintegratie- en adviesbureau op het gebied van Identity oplossingen. Als adviseur en projectmanager heeft hij de afgelopen 15 jaar opdrachtgevers in de financiële sector en (semi-)overheid geholpen met de realisatie van Identity oplossingen. Thomas is lid van Everett's Vision Board en is Expert Group Lead voor Identity & Access Governance. Thomas is bereikbaar via thomas@everett.nl

Projecten in het algemeen, en dus ook die op het gebied van informatiebeveiliging, zijn per definitie verandertrajecten. Of het nu gaat om het werken aan de cultuur van de organisatie ten aanzien van informatiebeveiliging, de introductie van beheersmaatregelen, of de invoering van software die deze dient te ondersteunen; de status quo verandert. Een kritieke succesfactor voor het slagen van projecten is dan ook het meenemen en begeleiden van de business en andere stakeholders in deze verandering. De toepassing van een agile projectaanpak biedt hier de nodige handvatten voor. Dit artikel is een handreiking voor de praktische invulling en toepassing van agile voor informatiebeveiligingsprojecten.

Agile vindt zijn oorsprong in projecten rondom de invoering van informatietechnologie, waarbij vertegenwoordigers van verschillende methodieken zoals Extreme Programming, Scrum en DSDM met elkaar het *agile manifesto* [1] hebben opgesteld. In dit agile manifesto zijn de kernwaarden beschreven die ten grondslag liggen aan een agile aanpak.

Kernwaarden van een agile aanpak

"Wij laten zien dat er betere manieren zijn om software te ontwikkelen door in de praktijk aan te tonen dat dit werkt en door anderen ermee te helpen. Daarom verkiezen we:

- *Mensen en hun onderlinge interactie boven processen en tools*
- *Werkende software boven allesomvattende documentatie*
- *Samenwerking met de klant boven contractonderhandelingen*
- *Inspelen op verandering boven het volgen van een plan*

Hoewel wij waardering hebben voor al hetgeen aan de rechterkant staat vermeld, hechten wij méér waarde aan wat aan de linkerzijde wordt genoemd."

Een agile aanpak en diens kernwaarden herbergt eigenschappen die je helpen een aantal gewenste effecten te realiseren die nodig zijn om een veranderproject succesvol uit te voeren. Voor projecten op het gebied van informatiebeveiliging onder meer, omdat deze vaak worden gezien als "moetje" en dat eisen en wensen onder invloed van wet- en regelgeving voortdurend aan verandering onderhevig zijn. Mijn ervaring is dat het draait om de volgende eigenschappen en effecten:

- Betrokkenheid: met de nadruk op samenwerking en interactie - zonder onderscheid te maken tussen project en de lijnorganisatie - worden mensen onderdeel van de verandering. Het effect hiervan is dat draagvlak verbetert, er een betere afstemming tussen project en haar afnemers ontstaat en dat stakeholder management op een natuurlijke manier plaatsvindt.

- Geleidelijkheid: het iteratief en geleidelijk doorvoeren van oplossingen heeft als effect dat weerstand wordt geminimaliseerd. Mensen houden immers niet van grote en plotse veranderingen. Bovendien zorgen frequente en zichtbare resultaten voor de voortdurende toetsing van gemaakte keuzes waardoor, indien nodig, snel bijgestuurd kan worden. Ofwel: als je faalt, faal dan snel.

- Flexibiliteit: door het openstaan voor verandering is het mogelijk snel en direct bij te sturen naar aanleiding van voortschrijdende inzichten of wijzigingen in wensen en eisen. Daarnaast is het niet ongebruikelijk dat het project en diens afnemers enige tijd nodig hebben om tot een gemeenschappelijk beeld te komen van de vraag en daarbij passende oplossingen. Dit vraagt om een aanpak die onder meer faciliteert dat (in)richtingskeuzen gaande weg verlegd kunnen worden.

Informatiebeveiligingsprojecten worden gezien als "moetje"

Praktische invulling en toepassing van agile

Als adviseur en projectmanager ben ik zelf betrokken geweest bij projecten op het gebied van informatiebeveiliging in het algemeen en identiteit- en toegangsbeheer in het bijzonder. Op basis van mijn ervaringen heb ik hieronder een aantal voorbeelden opgenomen als concrete en praktische invulling van agile voor

informatiebeveiligingsprojecten. Daarbij is gebruik gemaakt van de vier agile kernwaarden als logische groepering.

Mensen en hun onderlinge interactie boven processen en tools

- Via het oprichten van een klankbordgroep met mensen uit de lijnorganisatie die regelmatig bijeenkomt, ontstaat een bruikbaar instrument voor de afstemming tussen project en haar afnemers. Zo heb ik bij het consolideren van een aantal autorisatiebeheerprocessen binnen verschillende business units van een bedrijf gebruik gemaakt van een klankbordgroep. Deze klankbordgroep bestond uit een mix van zogenaamde IT-contactpersonen die managers ondersteunen bij het regelen van toegang voor hun medewerkers, afdelingsmanagers en lokale security officers. Op basis van de dynamiek en input van deze diverse groepen zijn nieuwe autorisatiebeheerprocessen vastgesteld die voldeden aan beveiligingsbeleid en konden rekenen op draagkracht in de uitvoerende lijnorganisatie.

- Door mensen bij elkaar te brengen en bijeenkomsten te faciliteren komt besluitvorming sneller tot stand dan wanneer vertrouwd wordt op een formeel change- of besluitvormingsproces. Als voorbeeld hiervan heb ik met systeemeigenaren en security operations een gewijzigd controleproces van accounts en rechtenstructuren in systemen voorbereid. Met de automatisering van dit proces kon deze namelijk niet "as is" worden overgenomen. Op basis van de praktijkervaring van direct betrokkenen is een voorstel voor de gewijzigde inrichting voorgelegd aan de proceseigenaar binnen information risk management. Met deze aanpak kwamen we tot een proces dat praktisch werkbaar was voor de operationeel verantwoordelijken en voldeed aan de toetsingseisen vermeld in het beleid.

- In projecten probeer ik zo veel mogelijk gebruik te maken van afdelingsmanagers in de voorlichting op de werkvloer. Mijn ervaring is dat informatie eindgebruikers beter bereikt en effectiever is dan wanneer gebruikt gemaakt wordt van bijvoorbeeld publicaties op het intranet of in te haken op algemene periodieke mailingen. Belangrijkste reden hiervoor is dat de communicatie veel gerichter wordt; zowel in de inhoud van het bericht als het moment waarop aandacht van de ontvanger gevraagd wordt. Een bijkomend voordeel is dat de betrokkenheid van afdelingsmanagers uitnodigt tot terugkoppeling over keuzes in het project en zo zorgt voor een verbeterde afstemming.

Als je faalt, faal dan snel

Werkende software boven allesomvattende documentatie

- In alle projecten waarbij software wordt geïntroduceerd, lever ik in korte cycli nieuwe versies van software op om zo regelmatig terugkoppeling van eindgebruikers te krijgen voor vervolgleveringen. Als software aansluit bij de werkwijze van de organisatie is de kans immers groter dat deze vanzelf wordt gebruikt. Een voorbeeld hiervan is de invoering van een oplossing voor registratie en toegangsbeheer voor externe medewerkers van een hogeschool. Demonstratie van de software aan autorisatiebeheerders heeft onder meer geleid tot de aanpassing dat getrapte invoer van gegevens mogelijk werd. Dit sloot beter aan bij de dagelijkse praktijk waarbij niet alle relevante gegevens in één keer beschikbaar zijn, maar een vorm van basistoegang tot IT-voorzieningen vaak wel al eerder gewenst is.

- Door eindgebruikers te trainen in een praktijksituatie beklijft de leerstof beter dan met theorie in klassikale vorm en vast cursusmateriaal. Bij een aantal opdrachtgevers heb ik deze vorm toegepast bij de introductie van een proces voor het periodiek beoordelen van toegangsrechten door de direct leidinggevenden en de invoering van daarbij ondersteunende software. Bij de uitrol van dit proces is er iedere keer

voor gekozen om de daadwerkelijke start van het controleproces als trainingsmoment te gebruiken. Daarbij zijn de leidinggevenden in groepen ingepland waarbij ze, naast een plenaire introductie door een instructeur, op een werkplek geholpen werden om voor hun medewerkers het controleproces te doorlopen. Door op deze praktische manier de instructie toe te snijden op de voor de leidinggevende relevante situatie was er sprake van een zeer vlakke leercurve.

- In het verlengde van de training in het vorige punt pas ik liever het gebruik van "cheatsheets" toe dan dat ik uitgebreide werkinstructies of omvangrijke documentatie aan eindgebruikers oplever. Een cheatsheet is bij voorkeur niet groter dan één A4'tje waarin de essentie van het proces en de software is beschreven met een aantal concrete aanwijzingen voor de uitvoering. Door de beperkte omvang van de cheatsheet is het raadplegen laagdrempelig en past deze beter bij de intensiteit van het gebruik dan een dik handboek.

Samenwerking met de klant boven contractonderhandelingen

- Door in de bezetting van een project gebruik te maken van medewerkers uit de lijn worden project en praktijk bij elkaar gehouden. In plaats van een strikte scheiding tussen de project- en lijnorganisatie met allerlei aparte overleggen wordt zo op een natuurlijke manier afstemming verbetert en de ontvangstbereidheid van de lijnorganisatie vergroot. Zo heb ik voor de duur van een project rondom de realisatie van rolgebaseerd toegangsbeheer gebruik kunnen maken van autorisatiebeheerders. Op basis van hun kennis van de tot dan handmatige en centraal uitgevoerde toegangsbeheerprocessen kon ik snel concrete voorstellen voor roldefinities aan de business voorleggen voor verdere afstemming.

- Door business- en IT-activiteiten in samenhang uit te voeren wordt een project wendbaarder. Dit komt doordat afhankelijkheden integraal worden beheerst in plaats van afstemming via harde onderlinge afspraken en onnodige overlegvormen. Dit heb ik onder meer toegepast in een project dat er voor gezorgd heeft dat functiescheiding werd geborgd in kritieke informatiesystemen. Dit is gerealiseerd met behulp van software die continu volautomatisch toegangsrechten van medewerkers toetst tegen een aantal bedrijfsregels. Deze bedrijfsregels zijn door de business analisten en software-specialisten in gezamenlijkheid opgesteld. Daarbij is iteratief gewerkt aan de implementatie van bedrijfsregels zodat deze pasten binnen de mogelijkheden van de software zonder dat de gewenste toetsing die er van uit moest gaan verloren ging.

> Door de instructie toe te snijden op de relevante situatie ontstond een vlakke leercurve

Inspelen op verandering boven het volgen van een plan

- In plaats van implementatie-voorstellen eerst geheel uit te werken op papier pas ik graag prototyping toe tijdens een project. Documenteren kan later altijd nog. Het vroeg en herhaaldelijk tussendoor toetsen, stelt me in staat bij te sturen voordat de beschikbare tijd en het budget geheel aangewend is. Overigens kan prototyping variëren van een proces doorlopen op een whiteboard aan de hand van praktijkvoorbeelden, tot de demo van specifieke softwarefuncties aan een eindgebruiker. De terug-koppeling die ik op die manier krijg, gebruik ik voor het doorvoeren van verbeteringen.

- Door de brede toepassing van software binnen informatie-beveiliging is het nodig dat de softwarevoortbrengers gebruik maken van ontwikkelmethoden die flexibel zijn voor wensen vanuit business en eindgebruikers. Dit uit zich in onder meer tools die ondersteunen in het bouwen en uitrollen van software. Hierdoor kunnen snel nieuwe versies opgeleverd worden zonder dat dit tijd vergt die ten koste gaat van de softwareontwikkeling zelf. Een voorbeeld waarbij dit noodzakelijk was betrof een project voor de insourcing van autorisatiebeheer van ongeveer 50 verschillende soorten aanvragen. Hiervoor was het nodig om de bijbehorende aanvraagformulieren uit een externe tool onder te brengen in een eigen bestaande centrale beheeromgeving. Omdat de insourcing binnen drie maanden moest worden volbracht is gekozen om de formulieren in een hoog tempo iteratief te ontwikkelen. Dit was alleen mogelijk omdat de bouw en uitrol van de software geheel geautomatiseerd was. Hierdoor konden wekelijkse nieuwe versies van bestaande en nieuwe formulieren worden uitgerold voor acceptatie en live gang.

Tot slot

Agile is geen methode. Het schrijft niet voor hoe je een project inricht of een aanpak concreet invult. Agile dient beschouwd te worden als een filosofie, de intentie in wat je doet. Door de kernwaarden toe te passen in de projectuitvoering wordt een project agile en faciliteert het verandering. Ik hoop met een aantal concrete voorbeelden een aanzet gegeven te hebben om de agile kernwaarden zelf toe te passen in de praktijk. ●

Links

[1] http://agilemanifesto.org/iso/nl/

EUROPESE PRIVACYWETGEVING: DE ROUTE NAAR COMPLIANCE

André J. Biesheuvel is bedrijfseconoom, Register Accountant en Register IT Auditor. Hij is meer dan tien jaar partner bij Duthler Associates (www.duthler.nl). Binnen de praktijk is hij verantwoordelijk voor de dienstverlening op het gebied van gegevensbescherming. Biesheuvel is medeauteur van de NOREA uitgave: "Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors".

Guus Bekker is bestuurskundige en heeft een Master in Public Information Management. Hij is consultant bij Duthler Associates (www.duthler.nl) en heeft daarvoor in verschillende functies bij de Rijksoverheid gewerkt. Bekker is binnen de praktijk verantwoordelijk voor de vakinhoudelijke ontwikkeling van gegevensbescherming en in het bijzonder de dienstverlening rond PIA's.

Zoals eerder aangegeven [1] staan privacy en gegevensbescherming volop in de belangstelling. De onthullingen van Edward Snowden over de handelswijze van zijn voormalige werkgever, Booz Allen Hamilton, hebben hier zeker een onuitwisbare bijdrage aan geleverd. Maar ook het besef dat gegevensbescherming leidt tot een paradigmashift waarbij de betrokkene controle krijgt over zijn of haar persoonsgegevens. Het gevolg is dat de kwaliteit van deze gegevens stijgt, kostenopslagen voor risico's van inadequate data worden verlaagd en processen meer effectief en efficiënt worden ingericht. Er is onmiskenbaar een lucratieve businesscase voor betrokkenen, bedrijfsleven en overheid.

Dit artikel vormt het tweede deel van een tweeluikcommentaar. In het eerste artikel is nadrukkelijk ingegaan op het voorgestelde nieuwe rechtskader voor de bescherming van persoonsgegevens binnen de Europese Unie [2], dat op 25 januari 2012 door de Europese Commissie is gepresenteerd. Wij spreken hier van de Europese privacyverordening. De bij deze Europese privacyverordening horende achtergronden zijn beschreven en enkele relevante opgenomen vereisten zijn nader toegelicht. Ook de rol van overige, reeds geldende regelgeving, zoals de Wet bescherming persoonsgegevens (Wbp) en nog komende wetgeving, zoals de voorgestelde Europese richtlijn ten aanzien van netwerk- en informatiebeveiliging (NIB) zijn uiteengezet.

In dit artikel zal eerst worden ingegaan op de meest recente ontwikkelingen rond de Europese privacyverordening. Ook de ontwikkelingen rond de NIB en het wetsvoorstel meldplicht datalekken komen aan bod. Hierna wordt specifieker ingegaan op de potentiële implicaties die deze (Europese) wet- en regelgeving met zich meebrengen voor organisaties ten aanzien van het beschermen van persoonsgegevens. De focus wordt gelegd op beheersmaatregelen. Door het nemen van passende maatregelen en gebruik te maken van bepaalde instrumenten en middelen kunnen organisaties zich beter voorbereiden op de verplichtingen uit komende wetgeving. En zo toewerken naar een aanvaardbaar niveau van compliance.

De focus wordt gelegd op beheersmaatregelen

Stemming rechtskader bescherming persoonsgegevens

De politieke ontwikkelingen op het terrein van privacy en gegevensbescherming volgen elkaar in rap tempo op. De commissie voor Burgerlijke Vrijheden, Justitie en Binnenlandse Zaken (LIBE) van het Europees Parlement heeft op 21 oktober 2013 ingestemd met het ontwerpverslag en de ingediende amendementen. Ook heeft de LIBE-commissie ingestemd met een mandaat om onderhandelingen te starten met de Raad. Enkele voor dit artikel belangrijke voorgestelde wijzigingen op het eerste voorstel van 25 januari 2012 betreffen:

- Als een land buiten de Europese Unie een bedrijf (bijvoorbeeld een zoekmachine, social networksite of een cloud provider) verzoekt om persoonsgegevens, die zijn verwerkt binnen de Europese Unie of die Europese burgers betreffen, te onthullen, dan moet dit bedrijf toestemming vragen aan haar nationale toezichthouder, voordat gegevens verstrekt kunnen worden. Het bedrijf moet dan tevens de betrokkene, degene om wiens gegevens het gaat, informeren over het verzoek tot gegevensoverdracht.
- In het eerste voorstel zijn sancties voorgesteld voor het niet voldoen

aan de gestelde eisen, die kunnen oplopen tot € 1 miljoen of 2% van de wereldwijde jaaromzet. In het nieuwe voorstel zijn deze sancties verhoogd en kunnen ze oplopen tot € 100 miljoen of tot 5% van de wereldwijde jaaromzet. Welk bedrag wordt gekozen hangt af van de vraag of het percentage van de wereldwijde omzet het vaste bedrag al dan niet overstijgt. De boetes zijn niet langer gedifferentieerd naar categorieën en zijn ook niet meer gespecificeerd naar type overtreding.

- Een vereiste voor expliciete toestemming (consent) is opgenomen. Verwerkingen, gebaseerd op deze toestemming, zijn alleen toegestaan wanneer de betrokkene hier expliciet en vrijwillig toestemming voor heeft gegeven. Het intrekken van deze toestemming moet hierbij even laagdrempelig haalbaar zijn als het geven van de toestemming.
- Het "recht om vergeten te worden" is geschrapt. De LIBE-commissie meent dat het recht om gegevens te laten vernietigen dit recht voldoende ondervangt. Dit verzoek moet ook doorgestuurd worden naar derde partijen, waarmee de betrokken persoonlijke gegevens zijn uitgewisseld.

Enkele dagen na deze stemming in de LIBE-commissie verschenen in de media [3] berichten dat onder druk van bondskanselier Merkel en de Britse premier Cameron aanscherping van de Europese regelgeving op het gebied van privacybescherming wordt uitgesteld tot 2015. Dit was besloten tijdens de Europese Top van 24 en 25 oktober 2013 te Brussel, waar onder meer de digitale economie op de agenda stond. [4] Regeringsleiders kunnen via de Raad van ministers van Justitie invloed uitoefenen op het wetgevingsproces in Brussel. Het is dus vooralsnog even afwachten met welke amendementen de Raad van ministers komt. De uitkomsten van

dit politieke proces zouden uitstel kunnen betekenen, hoewel hier ook niet iedereen het over eens is [5], maar zeker geen afstel. Dit blijkt wel uit de afsluitende conclusie met betrekking tot gegevensbescherming van de eerder gememoreerde Europese Top van 24 en 25 oktober 2013:
"Het is belangrijk om het vertrouwen van de burger en het bedrijfsleven in de digitale economie te bevorderen. De spoedige vaststelling van een sterk uniaal algemeen gegevensbeschermingskader alsook van de richtlijn cyberveiligheid is van doorslaggevend belang om de digitale en gemaakte markt in 2015 te kunnen voltooien." [6]

Wetsvoorstel meldplicht datalekken

Op nationaal niveau is op 17 juni 2013 het wetsvoorstel meldplicht datalekken [7] bij de Tweede Kamer ingediend. Het wetsvoorstel geeft invulling aan de kamerbreed aanvaarde motie Recourt [8]. De verplichting tot het melden van datalekken door verantwoordelijken en bewerkers wordt geregeld door aanvullende bepalingen op te nemen in de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw). In het wetsvoorstel is tevens geregeld dat de maximale bestuurlijke boete, die het College bescherming persoonsgegevens (Cbp) kan opleggen bij overtreding van de voorgestelde meldplicht, € 450.000 bedraagt. Deze boete kan ook worden opgelegd bij overtreding van andere bepalingen van de Wet bescherming persoonsgegevens. In feite komt deze laatste wijziging neer op een algehele verhoging van de boetebevoegdheid van het Cbp van 4.500 naar 450.000 euro. [9] De meldplicht van een datalek op nationaal niveau kent een breder toepassingsgebied dan de meldplicht van een datalek op grond van de Europese privacyverordening.

"Het recht om vergeten te worden" is geschrapt

Het is niet gemakkelijk te voorspellen binnen welke termijn de Tweede Kamer over het wetsvoorstel zal gaan stemmen. Zo moeten de staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken bij nota van wijziging op het onderhavige wetsvoorstel nog voorzien in een regeling die strekt tot uitbreiding van de bestuurlijke bevoegdheden van het Cbp. Na het akkoord van de Tweede Kamer moet het voorstel ook nog door de leden van de Eerste Kamer worden geaccordeerd. Niettemin kan het wetsvoorstel meldplicht datalekken in de loop van 2014 van kracht worden.

Gevolgen voor organisaties

Aan de ene kant bestaat er onzekerheid bij organisaties omdat nog volop diverse politieke discussies worden gevoerd op het vlak van gegevensbescherming, ook al is het wel duidelijk dat er hoe dan ook nieuwe privacywetgeving gaat komen. De inhoud van de nieuwe regelgeving zal waarschijnlijk liggen tussen de inhoud van het Commissievoorstel van 25 januari 2012 en het LIBE-voorstel van 21 oktober 2013. Aan de andere kant dient een organisatie zich nu al degelijk en zorgvuldig voor te bereiden op wat er komen gaat, om zich zelf niet onnodig in een lastige positie te manoeuvreren.

Het organiseren van privacybescherming en het zorgdragen voor veilige verwerkingen vormt een steeds belangrijker aandachtspunt voor bestuurders van organisaties. Dit geldt ook voor toezichthouders en accountants in verband met de gevolgen voor het opstellen van de jaarrekening en het jaarverslag door het bestuur en het door de externe accountant goedkeuren van de jaarrekening en het jaarverslag. Als de accountant niet kan vaststellen dat adequate maatregelen zijn getroffen, moet een voorziening voor een mogelijke sanctie worden opgenomen in de verantwoording.
Niet voldoen aan wet- en regelgeving kan, zeker in het voorgestelde Europese rechtskader voor de bescherming van persoonsgegevens, aanleiding zijn voor het opleggen van sancties van materieel belang. Tot slot heeft de in het eerste deel [10] van dit tweeluikcommentaar uiteengezette NIB-richtlijn gevolgen voor organisaties. Op deze richtlijn zijn half oktober 2013 de eerste amendementen ingediend door de Industrie, Onderzoek en Energie (ITRE) commissie van het Europees Parlement. De ITRE-commissie onderstreepte hierbij verheugd te zijn over de voorgestelde richtlijn. [11] Ook met voorbereidingen op deze richtlijn zullen organisaties rekening moeten houden.

Beheersmaatregelen

Een organisatie moet veel werk verzetten om aan de aankomende wet- en regelgeving op het terrein van privacy en gegevensbescherming te voldoen. Het is niet aannemelijk te verwachten dat deze activiteiten binnen enkele maanden kunnen worden gerealiseerd. Er zijn verschillende manieren om de voorbereidingen op de aanstaande privacywetgeving vorm te geven. Gelet op de in dit artikel besproken nationale en Europese wetgeving worden hier enkele beheersmaatregelen en te hanteren instrumenten nader toegelicht. Wij onderscheiden:

- Het verkrijgen en behouden van **overzicht over en inzicht in <u>alle</u> binnen de organisatie aanwezige verwerkingen van persoonsgegevens.**
- Het uitvoeren van een Privacy Impact Assessment (PIA) om compliant te kunnen met (aankomende) wet- en regelgeving en in control te kunnen zijn, wanneer zich een datalek voordoet.
- Het aanstellen van een Functionaris voor de Gegevensbescherming en deze persoon in staat stellen om zijn taken adequaat uit te kunnen voeren.

Ten eerste wordt de blik gericht op het verkrijgen en behouden van **overzicht en inzicht ten aanzien van <u>alle</u> verwerkingen van persoonsgegevens.** Dit is geen simpele opgave en vereist een uitgebreide registratie van alles wat betrekking heeft op de verwerkingen van persoonsgegevens, inclusief de per verwerking genomen maatregelen en ingestelde mechanismes en procedures. Dit is een eerste stap naar het gestructureerd vastleggen van de privacyhuishouding.
Een voor de hand liggende manier voor het vastleggen van de privacyhuishouding is het gebruik maken van een Data Protection Management Systeem (DPMS). Idealiter biedt een dergelijk DPMS een organisatie meer zekerheid over het compliant zijn met de privacywetgeving, inclusief de hieraan gerelateerde wet- en regelgeving. Dit betekent impliciet een kleiner risico op fouten en sancties. Het kunnen aantonen van meer zekerheid ten aanzien van compliance is een eerste gewenste functionaliteit van een DPMS. Een aanvullende gewenste functionaliteit is het verschaffen van inzicht in de van toepassing zijnde verantwoordelijkheden en aansprakelijkheden. Een tweede functionaliteit is het inregelen van "Lifecycle data protection management". Dit begrip is geïntroduceerd in het eerder genoemde nieuwe tekstvoorstel van de commissie LIBE van 21 oktober 2013. Inhoudelijk heeft dit begrip betrekking op de bescherming van gegevens gedurende de gehele levenscyclus van deze persoonsgegevens. Dit gaat dus vanaf het eerste moment van verzamelen van persoonsgegevens tot het verwerken en uiteindelijk het verwijderen van de betrokken persoonsgegevens. De verantwoordelijke dient zich gedurende deze gehele cyclus te focussen op aspecten als juistheid, vertrouwelijkheid en integriteit van persoonsgegevens. Wanneer dit daadwerkelijk aantoonbaar zorgvuldig plaatsvindt, wordt inhoud gegeven aan "data protection by design" [12] Deze gewenste eigenschappen en functionaliteiten gelden natuurlijk naast meer algemene requirements aan een DPMS als flexibiliteit, zodat gemakkelijk met veranderingen omgegaan kan

> Boete kan ook worden opgelegd bij overtredingen van andere bepalingen van de Wbp

worden, zo laag mogelijke kosten en een uitgebreid onderliggend juridisch framework, waarin relevante wet- en regelgeving wordt geduid.

Een tweede activiteit, die goed past in de route naar compliant zijn met privacy wet- en regelgeving, is het uitvoeren van een PIA. Hiermee kan in de beginfase van het aanleggen van bijvoorbeeld een systeem of een gegevensbestand duidelijk gemaakt worden wat de risico's ten aanzien van privacy zijn.
Een PIA kan ook binnen een staande organisatie worden uitgevoerd, waarbij de "IST`-situatie op het gebied van gegevensbescherming wordt beoordeeld. Deze beoordeling is relevant wanneer een organisatie terdege voorbereid wil zijn op een datalek. Naast een datalek bestaan overigens nog meerdere aanleidingen voor het uitvoeren van een PIA.
Zowel private als publieke organisaties, die persoonsgegevens verwerken, zijn na het van kracht worden van het wetsvoorstel meldplicht datalekken verplicht om inbreuken op of het omzeilen van de beveiliging, die leiden tot diefstal, verlies of misbruik van persoonsgegevens te melden. In deze aanstaande wetgeving gaat het erom dat de verantwoordelijke (de organisatie) aantoonbaar zorgvuldig is en voldoende maatregelen heeft genomen om de risico's op een datalek tot een aanvaardbaar minimum terug te brengen. Tijdens het uitvoeren van de PIA wordt bij het beoordelen van de risico's specifiek de aandacht gevestigd op opslag van persoonsgegevens door werknemers op draagbare apparatuur, risico's in de ICT-infrastructuur en de decentrale opslag van persoonsgegevens. Aanvullend is er ook aandacht voor maatregelen en procedures die van kracht worden bij het daadwerkelijk plaatsvinden van een datalek, zoals het communicatieplan voor het naar buiten brengen van de melding en het uit te voeren actieplan, inclusief training van betrokken werknemers in de uitvoering van het actieplan. De resultaten van de PIA worden aan de verantwoordelijke opgeleverd en vormen de basis waarop beslissingen ten aanzien van te nemen maatregelen en in te stellen procedures worden genomen.
Een derde manier om je als organisatie goed voor te bereiden op het zoveel mogelijk compliant zijn met de komende privacywetgeving, betreft het aanstellen van een Functionaris voor de Gegevensbescherming (FG), wanneer deze er nog niet is. De door de Commissie voorgestelde Europese privacyverordening stelt voor publieke organisaties en bedrijven met meer dan 250 werknemers het aanstellen van een FG verplicht. Het tekstvoorstel van de LIBE-commissie stelt dit verplicht voor organisaties die van meer dan 5000 betrokkenen persoonsgegevens verwerken. Ook worden in beide voorstellen eisen gesteld aan de taken van de FG. Om zijn of haar advies- en toezichtstaken goed te kunnen vervullen moet een FG over multidisciplinaire kennis en competenties beschikken. De FG zal voor het vervullen van zijn taken en het dragen van zijn verantwoordelijkheden ondersteund moeten worden met adequate informatie en middelen.

> Ook worden eisen gesteld aan de taken van de FG

De taken zullen zich voornamelijk richten op het creëren van awareness binnen de organisatie, het informeren en adviseren van de verantwoordelijke en de verwerker over hun verplichtingen, toezien op de uitvoering en toepassing van het privacybeleid, het opleiden van medewerkers en het laten uitvoeren van PIA´s en audits. Een in een optimale omgeving goed functionerende FG geeft een stevig fundament voor een succesvolle uitvoering van het privacybeleid.

> "Lifecycle data protection management"

Gedegen voorbereiding is vereist
In dit tweede deel van het tweeluikcommentaar gericht op wet- en regelgeving ten aanzien van privacy en gegevensbescherming zijn de laatste (politieke) ontwikkelingen geduid en is aangegeven wat in de toekomst nog te wachten staat. Vervolgens is specifiek ingegaan op vormen van beheersmaatregelen en instrumenten, die een organisatie nu in het voorbereidingstraject al kan hanteren of uitvoeren.
Het gebruik van een geschikt DPMS, uitvoeren van PIA's en het aanstellen van een FG zijn enkele belangrijke voorbeelden hiervan. Met deze beheersmaatregelen en instrumenten kunnen de eerste stappen op de route naar compliance worden gezet. ●

Links

[1] *Guus Bekker & André J. Biesheuvel: "Europese wetgeving bescherming persoonsgegevens in de schijnwerpers" Informatiebeveiliging, nummer 7, 2013*
[2] *COM(2012), d.d. 25 januari 2012*
[3] *http://www.volkskrant.nl/vk/nl/13524/De-afluisterpraktijken-van-de-NSA/article/detail/3532973/2013/10/25/Woede-over-afluisteraffaire-maar-geen-strafmaatregelen.dhtml*
[4] *De Europese Raad, ook wel Europese Top genoemd bepaalt de algemene politieke beleidslijnen en prioriteiten van de Europese Unie. Met de inwerkingtreding - op 1 december 2009 - van het Verdrag van Lissabon is de Europese Raad een instelling van de Europese Unie geworden.*
[5] *In een nieuwsreport op de Europese nieuwssite Euractiv wordt aangegeven dat door middel van qualified majority voting een eerdere inwerkingtreding ook mogelijk is: http://www.euractiv.com/specialreport-digital-single-mar/commission-push-ahead-data-prote-news-531357*
[6] *Begeleidende nota van: het secretariaat-generaal van de Raad aan: de delegaties Betreft: Europese Raad 24/25 oktober 2013 conclusies http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/nl/ec/139218.pdf*
[7] *Vergaderjaar 2012-2013 Kamerstuk 33 662, nr. 4*
[8] *Vergaderjaar 2011-2012 Kamerstuk 32 761, nr. 22*
[9] *In de memorie van toelichting van wetsvoorstel 33 662 wordt daarover op blz. 18 vermeld: "Verder mag van het Cbp worden verwacht dat het beleidsregels vaststelt omtrent de hoogte en de berekening van de boetes (boetetoemetingsbeleid). Vooralsnog wordt rekening gehouden met tien boetebesluiten per jaar."*
[10] *Guus Bekker & André J. Biesheuvel: "Europese wetgeving bescherming persoonsgegevens in de schijnwerpers" Informatiebeveiliging, nummer 7, 2013*
[11] *http://www.enisa.europa.eu/media/news-items/itre-committe-publishes-draft-opinion-on-the-proposed-nis-directive*
[12] *art. 23 van het nieuw voorgestelde rechtskader voor de bescherming van persoonsgegevens van 21 oktober 2013.*

COLUMN: VERANTWOORDE ONTHULLINGEN#3

TOEN @UID_ DE KAZERNE BELDE MET EEN FABRIEKSWACHTWOORD

HET TELECONFERENTIESYSTEEM VAN DEFENSIE (2012)

Beroepshacker Rickey Gevers, ook wel @UID_, kreeg een tip van iemand van Anonymous: het Nederlandse Ministerie van Defensie zou gebruik maken van een videoconferentie systeem, waarvan niet alle gebruikers hun wachtwoord hebben aangepast. Met het standaard fabriekswachtwoord, dat is te vinden in een handleiding op internet, opende hij de inlogpagina van een topman bij Defensie. Hij toonde dit aan een journalist van de Volkskrant, die eerst zijn advocaat en daarna Defensie belde. Een woordvoerder zei dat het Defensienetwerk veilig was. Maar, als de krant bij de drukker ligt, ziet Rickey dat het systeem uit de lucht is gehaald. Had @UID_ gelijk?

Gevers is, zoals zijn Twitter profiel meldt, een "criminal brought to justice". In 2008 werd hij, na een tip van de FBI, opgepakt door Team High Tech Crime van de Nederlandse politie. Voor het hacken van o.a. de Michigan University heeft hij 18 dagen in de gevangenis gezeten. Daarna heeft hij zijn hackersvaardigheden vooral ingezet om anderen te helpen hun beveiliging op orde te brengen. Soms vrijwillig, maar ook voor commerciële tarieven via het bedrijf Digital Investigation. Niettemin heeft hij nog veel contact met het schemergebied van de hackerswereld, zoals Anonymous.

Op maandag 20 februari 2012 krijgt @UID_ een bericht van de Nederlandse anarchistische hacker @ntisec. Hij had een tip gekregen van Anonymous, maar vindt het lek van dermate hoog kaliber dat hij zijn vingers hier liever niet aan wil branden. Daarom had hij twee journalisten benaderd om het te onthullen, maar dat deden ze niet. Of @UID_ ernaar wilde kijken. Dat wilde hij wel en hij kreeg de handleiding van het Cisco videoconference system, een IP-adres en de opdracht in te loggen met het default wachtwoord.

Rickey logt in en ziet tot zijn verbazing de pagina van directeur marinebedrijf A.J. de Waard. Hij checkt vervolgens de IP-adressen, telefoonnummers en namen of dit wel echt het systeem van Defensie is. Het klopt. Vervolgens probeert hij nog wat andere pagina's in het systeem. Het blijkt dat hij eindeloos veel wachtwoorden kan intypen en dus andere accounts gewoon met brute force zou kunnen openen. Gevers is geschokt en weet niet goed hoe hij dit naar buiten moet brengen. Hij wil natuurlijk niet weer de gevangenis in. Hij schakelt daarom, net als @ntisec, een journalist in: Victor de Kok van de Volkskrant. Rickey weet namelijk dat deze krant goede advocaten heeft.

Die woensdag ontvangt Rickey journalist De Kok op zijn studentenkamer om samen in te bellen. Rickey achter de laptop en de journalist continue aan de telefoon met zijn advocaat. Ze loggen in als de directeur marinebedrijf en bellen de directie van de Jan de Noordazaal, een kazerne in Den Helder. Helaas, er wordt niet opgenomen. Ze zouden ook kunnen bellen naar warroom@denhaag NL of testsite@US, maar dat lijkt ze te link. De journalist belt daarom zelf met de gewone telefoon naar de kazerne om het lek te melden. Daar wordt hij direct doorverbonden naar een woordvoerder die in eerste instantie niet begrijpt wat er aan de hand is en later terugmeldt dat er niets aan de hand is, omdat het betreffende systeem niet in gebruik is. Rickey ziet echter aan de logfiles dat het systeem een uur geleden nog is gebruikt en zeker niet door de minsten. Daar heeft de woordvoerder geen weerwoord op. De Kok gaat over tot de onthulling en kopt vrijdag 24 februari "Communicatie Defensie eenvoudig te kraken". Dit wordt direct overgenomen door andere journalisten, waaronder ook een parodie van GeenStijl, die het bekijken waard is. Bij Defensie zijn ze er inmiddels achter wat er aan de hand is, want Rickey ziet dat het systeem offline is gehaald. Wat is er gebeurd? Ik heb daarom ook contact opgenomen met Defensie. Het bleek te gaan om woordvoerder Maarten Hilbrandie. Die heeft direct na het telefoontje van de journalist naar hun communicatiesystemen gekeken en zag niets vreemds. Die staan ook niet online. Pas toen kwam hij erachter dat er nog een ander systeem was, dat wel via internet ging. Dat was inderdaad tegen de regels in en de zeven installaties werden donderdagavond 21:25 offline gehaald. Dat was maar goed ook, want de krant lag toen al bij de drukker. Niet echt een verantwoorde onthulling dus. Maar het heeft wel geholpen.

Hoe is het eigenlijk afgelopen met Arjen de Waard, de directeur die tegen de regels in het onveilige systeem gebruikte? Als ik hem bel, reageert hij vrij luchtig: "Ja, ze hadden weleens dat fabrieks-wachtwoord moeten veranderen. Was niet zo netjes. En nee, de hack heeft voor hem geen negatieve consequenties gehad."

Volgende keer in *Verantwoorde onthullingen#4*: "I hacked KPN, and all I got was this lousy T-shirt." ●

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

Links

[1] http://rickey-g.blogspot.nl/2012/02/maandag-de-20ste-word-ik-getipt-door.html?spref=tw

[2] http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3199980/2012/02/24/Communicatie-Defensie-eenvoudig-te-kraken.dhtml

[3] http://www.geenstijl.nl/mt/archieven/2012/02/communicatiesysteem_defensie_g.html

MARTIJN VEKEN STELT ZICH VOOR

Als vers redactielid vind ik het leuk om mijzelf aan de lezers van dit blad voor te stellen. Ik ben 39 jaar en woon met mijn vrouw en 3 kinderen in het prachtige Stompetoren. Ik werk al enige jaren bij SNS REAAL als penetratietester en digitaal forensisch onderzoeker. Dit werk vind ik fantastisch omdat, om dit goed te kunnen uitvoeren, je echt precies moet weten hoe systemen en applicaties werken. Tot op bit-niveau. Naast het werk bij SNS REAAL heb ik met twee vrienden een eigen bedrijf waar we ons ook met dit soort technische beveiligingsvraagstukken bezig houden. Dit bevalt goed en daarom ga ik mij vanaf begin 2014 fulltime met dit bedrijf bezighouden.

Er is vaak een opvallende gelijkenis tussen mijn werk en dingen waar ik mij in mijn vrije tijd mee bezig houd. Het vakgebied waar ik in werk, vergt een aardige investering in de vorm van het onderhouden en uitbreiden van kennis. Maar mijn werk is ooit begonnen als mijn hobby en ook tegenwoordig gaat dit nog naadloos in elkaar over. Naast het opnemen van kennis beleef ik ook veel genoegen aan het delen ervan. Ik schrijf graag artikelen en blogposts en geef zo nu en dan ook presentaties over de technische aspecten van de informatiebeveiliging. Vandaar dat ik het ook erg leuk vind dat ik in de redactie van dit blad mag plaatsnemen!

Mijn andere grote hobby stamt nog uit de tijd dat computers nog niet tot elke hoek van ons bestaan waren doorgedrongen. Het gaat hier om een Porsche 912 uit 1969, een geweldige auto om mee te rijden. Ik heb deze auto in 4 jaar tijd volledig gerestaureerd en ken deze auto dus ondertussen tot op bout-niveau.

Het mag dus duidelijk zijn dat ik iets met techniek heb en dit is dus ook wat ik kan bijdragen aan de inhoud van dit blad. Ik kijk er naar uit om hier de komende tijd mee bezig te zijn.

Martijn Veken

VERSLAG

SECURITY CAFÉ – BIG DATA & SECURITY

Gerco Kanbier is directeur van Trust in People – the information protection company.
Hij is te bereiken via gerco.kanbier@trustinpeople.com

Big data wordt door Gartner gedefinieerd als "high volume, high velocity and high variety". Is big data een nieuwe hype of een andere naam voor Security Information Event Management? Welke organisaties zijn bezig met big data? Wat zijn de kansen en risico's van big data? Kun je op basis van het Safe-Harbour convenant tussen VS en EU opvragen wat er over mij persoonlijk is vastgelegd bij de NSA? Als privacy-data wordt gestolen door een interne medewerker en dit op eigen houtje publiek maakt, is de organisatie daarvoor dan eindverantwoordelijk en kan hiervoor een boete worden opgelegd door de toezichthouder? Bij websites testen we vaak of via SQL-injection data te manipuleren is. Hoe bewaak je de integriteit van big data-bronnen als dat gebaseerd is op NoSQL-technologie zoals Hadoop? Kortom, een hoop vragen waar het panel in 45 minuten op los kon gaan.

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 25 juni 2013, werd wederom bij Koetjes & Kalfjes te Zoetermeer georganiseerd. Op LinkedIn hadden de inmiddels 700 leden van de groep voor het onderwerp "Big Data & Security " gestemd. In het expertpanel Michiel Toes, commercieel directeur van SMT en specialist op het gebied van Big Data en Security management oplossingen. Hans Teffer, CISA en Register IT auditor, gespecialiseerd in het ontwerpen en creëren van holistische security monitoring omgevingen en Sander Klous, hoofd Data & Analytics bij KPMG en binnenkort hoogleraar Big Data Ecosystems aan de Universiteit van Amsterdam. Hier volgt een impressie van de discussie.

Sander Klous stelt als eerste dat er een verschil is tussen "Big Data for Security" en "Security of Big Data". "Big Data for Security" biedt mogelijkheden op het gebied van fraudedetectie zoals bij zorgverzekeraars en preventie zoals bij terreurbestrijding bij de NSA. Bij "Security of Big Data" gaat het om de betrouwbaarheid van die informatie en wie toegang heeft tot die informatie.

De meeste big data initiatieven zijn al enige jaren geleden opgestart, aldus Hans Teffer. Google is in 2004 met hun BigTable database gestart. Facebook, Amazon en de NSA begonnen met hun varianten daarop in 2007. Hans ziet big data niet als een hype, maar als een 'mainstream' implementatie voor overheden en grote bedrijven.

Logfiles kunnen een schat aan informatie te bevatten, mits je weet waar je naar op zoek bent. ArcSight, LogLogic, Splunk en Hadoop zijn voorbeelden van software applicaties om grote logverzamelingen te analyseren. ArcSight (HP) en LogLogic zijn in de markt vooral gepositioneerd als SIEM-oplossing en richten zich op realtime security en compliance waarbij vooraf bekend is wat je zoekt. Splunk en Hadoop (Apache) zijn gebaseerd op NoSQL-technologie en worden vaak gebruikt als ongestructureerd data-archief waarop analyses realtime, maar ook achteraf alsnog uitgevoerd worden. Dit wordt zowel voor beveiligingsdoeleinden, fraudedetectie als analyses gebruikt. Het mooie van Splunk, alsdus Michiel Toes, is dat analyses achteraf nog uitgevoerd kunnen worden, omdat je alle logdata opslaat. Soms weet je naar aanleiding van (APT) incidenten pas veel later waarop je moet letten in de logfiles. Bewezen analyses zoals aankoopgedrag of surfgedrag kunnen vervolgens weer gestructureerde input zijn voor een datawarehouse.

> Soms weet je pas later waarop je moet letten in de logfiles

Het analyseren en vastleggen van klantengedrag is gekoppeld aan privacy-wetgeving. Met big data zijn er nogal wat uitdagingen op gebied van privacy. Indien klanten bijvoorbeeld toestemming hebben gegeven voor een 'cookie' ten behoeve van commerciële en/of analysedoeleinden, dan is er nog geen toestemming om andere bronnen - waar ook toestemming voor is - aan elkaar te koppelen. Als er namelijk nieuwe informatie over deze klant ontstaat, door verbanden te leggen en bronnen aan elkaar te koppelen, dan moet dit vooraf en duidelijk worden verteld aan die klant. Deze klant moet een overzicht van zijn gegevens kunnen opvragen en eventueel eisen dat zijn gegevens verwijderd worden. De vraag is hoe die verantwoordelijkheid in de organisatie belegd is en of hier toezicht op is. Het is

namelijk gemakkelijk om dit technisch te realiseren zonder dat een klant dit door heeft. Volgens Sander Klous is het voor big data-systemen belangrijk om toegangsmaatregelen te ontwerpen op het niveau van rapportages, zoekfunctionalteit en business logica. Hiermee moet voorkomen worden dat een analist kan inzoomen op de details van een individuele gebruiker, als daar geen toestemming voor is verleend. Dit wordt ook wel 'Granular Access Control' genoemd.

De onthullingen van Edward Snowden over het publieke geheim dat NSA 'ons' bespioneert is echt een mediahype. Voor welke doeleinden de NSA namelijk binnen- en buitenland mag bespioneren, is gewoon bij Amerikaanse wet geregeld. Je kan je afvragen waarom sommige doeleinden in dit soort wetgeving is aangenomen, maar dat is anno 2013 een feit. Het verschil met een totalitaire staat, is dat dit valt en staat met toezicht op misbruik of oneigenlijk gebruik door derden. Dit soort wetgeving geldt overigens bijna voor alle inlichtingendiensten wereldwijd. Gegeven deze wetgeving is de wens voor een onafhankelijke internationale toezichthouder geboren. Inlichtingendiensten mogen net zomin als banken 'valsspelen', ook al is dat beschreven in de kleinste lettertjes van een wetsartikel. Het is op sommige punten immoreel en onethisch voor lokale belangen. Gezien de recente leerpunten uit de bancaire sector, is aangescherpt en internationaal toezicht bij inlichtingendiensten ook nodig als het gaat om bescherming tegen misbruik van gegevens. De overheid en inlichtendiensten hebben een serieuze verantwoordelijkheid dat informatie nooit in handen valt van iemand met andere/kwade bedoelingen. Ik verwacht namelijk niet dat de hacker straks toestemming gaat vragen bij het College Bescherming Persoonsgegevens voor een big data-store van de NSA, omdat de doeleinden van de nieuwe eigenaar zijn veranderd.

Inlichtingendiensten mogen net zomin als banken 'valsspelen'

Als data wordt gestolen door een interne medewerker en dit tegen de contractuele afspraken op eigen houtje publiek maakt, is de organisatie daarvoor dan eindverantwoordelijk? We kunnen technisch, juridisch en organisatorisch veel dingen beveiligen, maar incidenten blijven gebeuren. Een CD met alle zwitserse bankrekeningen, een USB-stick met alle medische gegevens van patiënten of alle diplomatieke documenten over een dubieuze oorlog, het gebeurt gewoon. Dit probleem is misschien alleen te verzekeren. Echter, ik heb nog geen juridische claims gezien van slachtoffers naar de organisatie of overheid die eindverantwoordelijk is. Noch heb ik toezichthouders boetes zien uitdelen.

Bij big data wordt vaak gebruik gemaakt van gedistribueerde systemen, met in veel gevallen duplicatie van data, wat vaak ten goede komt aan de beschikbaarheid van informatie. Deze data wordt ongestructureerd opgeslagen, echter de exacte lokatie van data elementen is moeilijk te bepalen. Juridisch kan dat een probleem zijn, als je zelf niet weet waar de data opgeslagen is. Meestal wordt dan wetgeving gehanteerd die geldt waar het hoofdkantoor gevestigd is. Daarnaast is het nog maar de vraag of logfiles op die verschillende locaties beschermd zijn.

Ongestructueerde data zoals log-files zijn over het algemeen niet beveiligd zoals gestructueerde databases. Je kan dus eenvoudig log-bestanden aanpassen met onjuiste analyses en beslissingen tot gevolg. De integriteit en vertrouwelijkheid van deze big data-stores moet dus anders beveiligd worden. Daarom dient er een vorm van security monitoring opgezet te worden rond Big Data-stores waarin gelet moet worden op de integriteit van log-files, wie toegang heeft tot welke data, het soort analyses dat wordt uitgevoerd en de volledigheid van informatiebronnen monitoren, alsdus Hans Teffer.

Tot slot een voorbeeld van een big data-ecosystem: Talend-software kan je gebruiken om verschillende databronnen aan een big data-systeem te koppelen op basis van NO-SQL Splunk-technologie. Rapportages en analyses uit Splunk vormen dan weer input voor een datawarehouse.

CC by Rena Schild / Shutterstock.com

Links

Security Cafe: informatie beveiliging community in Nederland www.trustinpeople.com/security_cafe.php

COLUMN: ATTRIBUTER

IDENTIFIED

All human interactive protocols depend upon our ability to *identify* one another. In this article we examine *identification* in terms of SABSA Business Attributes. It seems at first glance to be extremely simple, but when you start to look closely, it is full of both subtlety and complexity.

First of all we shall establish the concept of the *core identity*. Each of us as individuals has a core identity. You are you, I am me, and we shall evermore be so. When we die our core identity dies with us but its existence is recorded in history books and in the minds of those that knew us. When a new baby is born, a new core identity is created. Core identities are not recycled. However, the core identity that is contained within each of us needs to be externalised for interaction with other people, and so we now move to the concept of *identifiers*. We can immediately see that there is a huge difference between *core identity* and an *identifier* associated with that core identity. As humans we think most often in terms of names and other information that can be recorded in language as being the nature of *identifiers*, but the truth is much more fundamental than that.

Consider what you may often see on television: a large beach area covered with hundreds of thousands of penguins. To us they all look the same. The saying goes, if you have seen one, you have seen them all. You know what a penguin looks like and you can *identify* it as being a penguin, but probably not as a specific penguin. For the penguins it is quite different. First, they do not have the linguistic concept of *penguin*, but still they know the difference between their own species and another animal. Secondly, they can recognise and identify other individuals with which they are acquainted. Each penguin in a bonded pair pair knows exactly which other one is their mate, and they all know which bundles of fluff are their own chicks. They can distinguish physical features, sounds and smells as *innate identifiers*. Let us call these *core identifiers* because they are physically linked to (and indeed part of) the *core identity*. Perhaps modern advances in DNA identification belong to this class of *core identifiers* too.

Humans have evolved complex sophisticated societies based on language and communication, in which *external identifiers* can be created as linguistic information. *Names* are inherited and given, and along with *date of birth* and *place of birth* this combination of data can provide a unique form of *identification* for each individual. The *core identifiers* such as the face and sound of voice are used more as *authenticators* these days, as in the case of *photoID*. A passport associates a face picture with a name, date of birth and place of birth, to *authenticate* that the presenter of the passport is indeed the authentic owner of those pieces of information. The key to creating any strong *core identifiers* and *authenticators* is a strong *registration* process, such as the registration of all births with the authorities.

What then is *identity theft*? It is certainly not the theft of a core identity, but the theft of sufficient *identifiers* to *impersonate* someone else's core identity.

Each core identity has associated with it a number of *personae*, with each *persona* being one aspect of that individual's life. Each of us has many *personae*: as a citizen, as a medical patient, as a family member, as a member of a club or society, as an employee of a company, and so on. Each *persona* in your collection is represented by a selection of your *identifiers* and other personal identity attributes, now perhaps including new *identifiers* such as *membership numbers, address details* and many more. However, because you share some details with other people in support of your relationship with them, you do not choose to share all of your details. This is the issue of personal *privacy*. Privacy is the right to segregate your *personae* from one another so that knowledge of one *persona* does not reveal knowledge of the others, and may not reveal your *core identifiers* unless you so choose. People who live 'double lives', such as spies, criminals and unfaithful spouses, may even wish to hide their core identity with a *false identity*. In some cases this will extend into the need for an *anonymous* or *unidentified* persona. Quite legitimately, many people register on Internet sites with an *avatar* and a *screen-name*, which are examples of *anonymous identifiers*.

This shows that *identity management* is a complex subject, one that requires the consideration of many related SABSA Business Attributes. That is why the concept of SABSA Attribute Profiling is so powerful and so necessary for analysing the requirements for identity management. ●

The Attributer

ONBEKENDE CERTIFICERINGEN VOOR IB PROFESSIONALS

Jim de Haas PSP CIPP/IT, security consultant bij Vest Informatiebeveiliging.
Jim is per e-mail bereikbaar via j.de.haas@vest.nl

Het is mijn ervaring dat security professionals in hun werk steeds vaker te maken krijgen met privacy vraagstukken. Zeker in cloud computing projecten is de link naar privacy aspecten helder. Privacy maatregelen geheel overlaten aan juristen is misschien niet verstandig. Het is beter om basiskennis over privacy op te doen en de dialoog met collega's van de juridische afdeling aan te gaan.

Certificering voor privacy
De International Association of Privacy Professionals (IAPP) is de grootste en meest complete privacy community. IAPP is opgericht in het jaar 2000, heeft meer dan 13.000 leden in 78 landen. Vergelijkbaar met ISACA biedt deze organisatie de mogelijkheid tot certificering en 'members only content'.

IAPP certificeringen zijn inmiddels een wereldstandaard op het gebied van privacy en privacy professionals. Er zijn twee certificeringprogramma's: CIPP en CIPM. Het CIPP programma kent vijf varianten: United States; Canada; Europe; U.S. Government en IT. Deze laatste is het meest toegankelijk voor IT/Infosec security professionals, omdat voor de andere teveel juridische kennis nodig is. Een CIPP/IT begrijpt het privacy-aspect in de ontwikkeling, uitrol en auditen van IT-producten en -diensten. Voor meer volledige informatie is er een CBK beschikbaar. CIPP/IT is ontworpen zodat het goed aansluit bij certificeringen, zoals CISM CISA en CISSP.

De CIPM certificering gaat een stap verder dan CIPP en vraagt ervaring met de governance van privacy programma's. Security managers die een privacy programma moeten implementeren en onderhouden hebben baat bij een CIPM certificering. Voorwaarden voor beide certificeringen zijn: IAPP lidmaatschap; behalen van het basisexamen en verdiepingsexamen. Relevante werkervaring wordt niet gevraagd.
Voor het vasthouden van de certificering is een IAPP lidmaatschap nodig (uiteraard 'in good standing') en tien CPE punten per jaar. CPE punten kunnen worden behaald bijvoorbeeld via IAPP conferenties. De eerstvolgende conferentie in Europa is 10-12 december in Brussel. Voor meer informatie over IAPP en haar certificeringen zie https://www.privacyassociation.org.

Certificering voor fysieke beveiliging
Over de integratie van informatiebeveiliging en fysieke beveiliging wordt al jaren gesproken. Er zijn echter weinig bedrijven die deze integratie daadwerkelijk voor elkaar hebben. Managers uit de respectievelijke domeinen kijken elkaar argwanend aan en werken nauwelijks samen. Voor security professionals die de kloof willen overbruggen naar de wereld van fysieke beveiliging is ASIS International een interessante organisatie.
ASIS International biedt standaarden, opleidingen en certificeringen aan professionals op het gebied van fysieke beveiliging. ASIS heeft meer dan 38.000 leden wereldwijd. ASIS standaarden zijn beschikbaar voor leden en dekken het hele spectrum af; maatregelen, managementsysteem, auditen en continue verbetering. ASIS biedt drie internationaal geaccrediteerde certificeringen: PCI; PSP en CPP. PCI is voor de Professional Certified Investigator met ervaring in case management, bewijsvergaring en case presentatie. CPP is voor ervaring security managers en voor vele IT/Infosec professionals een brug te ver, omdat we eenvoudigweg niet voldoende werkervaring opdoen als security manager. PSP is voor Physical Security Professionals met ervaring in site surveys, ontwerp en toepassing van maatregelen. PSP is voor IT/Infosec security professionals de meest toegankelijke certificering. Voor het behalen van een PSP certificering is vijf jaar relevante werkervaring nodig (geverifieerd bij drie referenties) en het behalen van een examen (125 meerkeuze vragen, computer based). Ter voorbereiding op het examen is een set van acht boeken beschikbaar. Dit materiaal gaat over risicoanalyse, security management, business continuity management en vooral over fysieke beveiligingsmaatregelen. Voor het vasthouden van een PSP certificering zijn 45 CPE punten nodig, over een periode van drie jaar. Voor meer informatie over ASIS zie https://www.asisonline.org. Begin april 2014 is de ASIS European Conference & Exibition in Den Haag.

Veel van de PvIB leden hebben één of meer beroepskwalificaties in de vorm van certificeringen als CISSP, CISA en CISM achter hun naam staan. Maar er is meer. In dit artikel presenteert Jim de Haas enkele certificeringen waarvan veel mensen nog niet op de hoogte zijn. Tijd om daar wat aan te doen…

Secure Link
Infrastructure Security Solutions

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.

Je nieuwe functie als Security Engineer

In verband met onze groei zijn we op zoek naar een Security Engineer die ons team wil 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 kunnen pre-stagen, implementeren en onderhouden.

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

Go Secure!

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

BOEKBESPREKING

Titel : De zwakste schakel in de informatiebeveiliging Menselijke aspecten rond de bescherming van gegevens.
Auteur : Jan de Boer (Capgemini)
Blz : 67

Jan de Boer is de auteur van het artikel van het jaar 2010. Daarom vinden wij het interessant als hij iets publiceert. Dit boek is een rapport van praktijksituaties die Jan tijdens zijn werkzaamheden als Social Engineer (SE) is tegengekomen.

Aan de hand van veel voorbeelden worden psychologische mechanismen toegelicht en worden tegenmaatregelen benoemd.

De beveiliging zit in de mens zelf

Deze kunnen direct gebruikt worden in een bewustwordingsprogramma voor de hele organisatie of speciale doelgroepen zoals de bewaking, receptie of secretaresses.

Mensen zijn zich doorgaans niet bewust van de manier waarop zij zich een mening vormen of reageren op een verzoek. Profiteurs kunnen daar misbruik van maken. Door hier aandacht aan te besteden in een bewustwordingsprogramma, gericht

Mensen vertonen voorgeprogrammeerd gedrag

op SE kan de weerbaarheid tegen manipulatie vergroot worden.
Dit wordt in de hoofdstukken uitgelegd aan de hand van psychologische trucs.

1. Wie geeft, die krijgt: Wederkerigheid
2. Maar schiet wel een beetje op!: onmiddelijke invloed
3. Wie A zegt, zal wel B moeten zeggen: consistentie
4. Mensenmassa is kracht: sociale bewijskracht
5. Leuke mensen hebben de halve wereld: sympathie
6. Naam en faam: autoriteit
7. "Hebbe, hebbe, hebbe": schaarste

"Het informatietijdperk maakt de consument dommer" by Robert Cialdini

Het gaat te ver in dit boekverslag om elke truc en gegeven voorbeeld uitgebreid te beschrijven. Ik ben van

mening dat elke beveiligingsprofessional dit rapport moet lezen. Het is goed te doen en leest makkelijk weg.

Het seminar "De psychologie van het overtuigen" is sowieso een aanrader. Erg inspirerend. ●

Ronald van Erven

http://www.nl.capgemini.com/bronnen/de-zwakste-schakel-in-de-informatiebeveiliging
http://www.denkproducties.nl/assets/document/miniboekje-cialdini2012.pdf

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

ADOBE

Adobe werd gehackt. De gebruikersgegevens van bijna 3 miljoen gebruikers is gestolen. Adobe ging met de billen bloot. Zo leek de hack van Adobe door het bedrijf zelf erkend te worden en volgens verwacht draaiboek te lopen. Maar toen kwam het bericht naar buiten dat het om 38 miljoen gebruikers gaat, vervolgens ging dit aantal omhoog naar 110 miljoen en 150 miljoen. Zo bleek dus dat Adobe helemaal niet kon bepalen hoeveel gegevens gestolen waren, en alleen die gegevens die op hackerssites gevonden werden, werden meegeteld. De belangrijkste meldingssite wordt een derde partij, Lastpass [1], die een gedetailleerde analyse maakt van de gestolen wachtwoorden en gebruikers in staat stelt te bevestigen hoe slecht ze er voorstaan. Bovenop dit alles bleek Adobe de gegevens helemaal niet volgens de geldende best practices beveiligd te hebben. Wat ging hier mis? Wat kunnen we hieruit leren? Wat betekent dit voor de gebruikers in kwestie?

Lex Dunn

Adobe heeft een flinke vertegenwoordiging op Microsoft PC's en ook op veel andere apparaten. Hun PDF Reader en Flash Player zijn waarschijnlijk de meest meegeleverde tooltjes op nieuwe PC's, laptops en zelfs smartphones. Als bekend wordt dat Adobe slachtoffer is geworden van een hack lijkt dat in eerste instantie wel mee te vallen voor de gemiddelde eindgebruiker, immers om PDF Reader en Flash Player te kunnen gebruiken hoef je niet direct een account bij Adobe te hebben. Maar er zit meer achter: als de hackers bij de database met gebruikersgegevens zijn gekomen, hebben ze dan misschien ook source-code van PDF Reader, Flash Player of andere Adobe software buit gemaakt? Als ze daar de hand op hebben weten te leggen, kunnen we nog wel wat verwachten aan nieuwe zero-day aanvallen. En dan maak ik me nog niet eens zoveel zorgen over de grootschalige "hit & run" aanvallen, maar meer over de Advanced Persistent Threats. Er zijn diverse rapporten beschikbaar over de modus operandi van APT's, en het overgrote deel maakt gebruik van PDF documenten om high-risk, high-profile gebruikers ertoe te verleiden die te openen, en zo de deur open te zetten voor de aanvallers. Wanneer die aanvallers beschikken over de source-code van PDF Reader is er eigenlijk nog maar één remedie mogelijk: PDF Reader (en Flash Player) geheel verwijderen, en met alternatieve tooltjes gaan werken. Zelf gebruik ik voor PDF documenten de Foxit Reader (nee, die is niet van Ronald 🙂, en heb ik de Flash Player helemaal laten vallen. Je "Internet experience" wordt er niet echt minder van (voor zakelijk gebruik), sterker nog, je hebt ook geen last meer van "drive by" exploits via de Flash advertenties op de bekende sites. Een ander zorgpunt is dat als Adobe "hackable" blijkt te zijn, hoe staat het dan met andere grote spelers? Ik noem een

paar geheel willekeurige voorbeelden: FaceBook, Google (als je een Android toestel wilt gebruiken moet je een Google account hebben, en raad eens waar die logingegevens zijn opgeslagen), maar ook minder voor de hand liggende kandidaten (in Nederland) als Wehkamp, BOL.com, Conrad etc. Die hebben ook grote hoeveelheden klanten, die digitaal bestellen, en dus hun logingegevens bij deze bedrijven achterlaten. En we weten allemaal dat op een gegeven moment de creativiteit voor het verzinnen van wachtwoorden een beetje op is, en dat wachtwoorden worden "hergebruikt" voor andere sites.
Oplossing: geheel afschaffen van wachtwoorden (heb ik al eens eerder in een AHN column gesuggereerd), en vervangen door een mechanisme met (minimaal) twee-factor authenticatie en eenmalige inlogcodes. Zijn daar kandidaten voor? Jawel, DigiD (maar dat is misschien onderwerp voor een komende AHN).

Tom Bakker
Het lek bij Adobe waarbij van 150 miljoen klanten de gegevens op straat liggen is onacceptabel. Beduidend meer dan Adobe zelf heeft toegegeven. Dat lekken is een probleem op zich, maar wat mij is opgevallen in een artikel hierover in de Guardian [2] is dat op papier formeel de wachtwoorden van klanten encrypted waren opgeslagen. Dus een vinkje van eventuele toezichthouders/ auditors. Maar het bleek een zeer eenvoudige encryptiemethode te betreffen (ECB). Adobe gebruikte voor alle wachtwoorden dezelfde key. Dat betekent dat dezelfde wachtwoorden ook dezelfde representatie hebben als ze zijn versleuteld. Met de bijbehorende wachtwoordhints kun je proberen heel wat wachtwoorden te achterhalen. Deze wachtwoordhints waren overigens niet versleuteld.

Ook volgens het Guardian artikel heeft iemand dat geprobeerd en een top 100 gepubliceerd van de meest gebruikte wachtwoorden bij Adobe. Het bleek dat '123456' het meest gebruikt werd als wachtwoord. Door maar liefst 1.9 miljoen mensen. Achterhaald via de hints. Wachtwoorden als 'qwerty' en 'password' scoren ook hoog.
Het blijkt dus weer dat afgezien van het lek, de mens toch ook hier weer de zwakste schakel is. Eenvoudige wachtwoorden was een probleem en blijft blijkbaar een probleem.
Ik verwacht niet dat het zo omgaan met wachtwoorden zal veranderen. Ergens begrijp ik het ook wel.
We moeten zoveel wachtwoorden onthouden. Ik sluit mij aan bij het idee dat we nodig van de wachtwoorden af moeten en over moeten gaan op minimaal twee factor authenticatie. Digid is een goede kandidaat.

Maarten Hartsuijker
We zien ze steeds vaker: bedrijven waar na een computerinbraak blijkt dat ze de accountgegevens van gebruikers onveilig opslaan. Mocht je als lezer ook de regie hebben over een webomgeving met gebruikersaccount, dan volgen hier een aantal tips voor het veilig(er) omgaan met deze accounts.

1. Beveilig inlogschermen altijd met SSL. Hiermee zijn de gegevens ook tijdens het transport beschermd.
2. Gebruik een hashingmethode voor het opslaan van wachtwoorden. Een hash is een onomkeerbare "encryptievorm". Hashes representeren een wachtwoord, zonder dat hackers gestolen hashes naar wachtwoorden kunnen vertalen.
3. Hash altijd een statisch geheim (van bijvoorbeeld 16 willekeurige karakters) en een dynamisch gegeven (bijvoorbeeld het user-id van de gebruiker) mee met het wachtwoord. Dit wordt ook wel een "salt" genoemd en bemoeilijkt het aanvallen (brute forcen) van een grote hoeveelheid gestolen hashes.
4. Bereken hashes met een krachtige hashingmethode, zoals SHA256 of PBKDF2. Doordat er voor het aanvallen van krachtige hashes meer CPU cycles nodig zijn, wordt ook hiermee misbruik van gestolen hashes bemoeilijkt.
5. Geef gebruikers suggesties (bijvoorbeeld middels een wachtwoordmeter) voor het kiezen van sterke wachtwoorden of dwing het gebruik van sterke wachtwoorden technisch af. ●

Links

[1] https://lastpass.com/adobe/
[2] http://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check#!

COLOFON

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

Redactie
Lex Borger (hoofdredacteur, werkzaam bij Ideas to Interconnect), e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

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

Advertentieacquisitie
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 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN: BERRY

ONDER DE BOVENWERELD

In de begin periode van de mobiele telefoons (waarvan de eerste exemplaren eigenlijk niet mobiel waren omdat je een zware externe accu moest meezeulen) waren hele andere merken populair dan vandaag de dag. Het is verbazingwekkend hoe snel een mens de toenmalige populaire producten vergeet. Als voorbeeld even de mobiele telefoons van die tijd. Als je geen Nokia had dan hoorde je er niet echt bij. Trots legde je de Nokia op tafel bij verjaardagen en partijen, nu zou je de Nokia diep in je zakken laten zitten. Ik ga nu niet vertellen hoe het Nokia verging en de verliesgevende jaren zich opstapelden. Desastreuse resultaten en topman na topman werd vervangen. Nokia kreeg geen voet meer aan de grond en leek uiteindelijk ten onder te gaan. Zelfs de nieuwe topman Stephen Elop lukte het niet om de koers van Nokia weer omhoog te laten gaan, nog sterker, het werd alleen maar minder. Tot het moment dat wereldkundig gemaakt werd dat Nokia overgenomen zou worden door Microsoft. De aandelen schoten omhoog en iedereen leek blij behalve de Finnen die onzekerheid vreesden voor de banen van 32.000 werknemers. Later kwamen de twijfels over de verkoop. Dat Stephen Elop van Microsoft komt is op zich niets geheimzinnigs aan, maar het is wel toevallig. Stephen was wel een gewiekste manager. Hij zag de aandelen zakken en zakken (waarschijnlijk had hij daar geen rol in) en hij zou zijn contract hebben laten aanpassen. Een van de zaken die hij zou hebben laten schrappen was de regel dat hij na zijn Nokia avontuur een jaar lang niet voor concurrenten mocht werken. Hij is dus vrij om te gaan werken waar hij wil. Saillant detail, deze wijziging zou doorgevoerd zijn op de dag dat de overname bekend gemaakt zou worden. Een tweede wijziging zal Elop uiteindelijk ruim 18 miljoen euro opleveren hetgeen hij uitgekeerd kreeg als de aandelen zouden opveren nadat ze lange tijd gezakt waren. Het laten zakken was al gelukt en alle aandelen zouden echt wel omhoog gaan als er een overname bekend gemaakt zou worden. Een week na de overname werd bekend dat de huidige topman van Microsoft (Steve Balmer) gaat stoppen. Een nieuwe kandidaat wordt gezocht en wat denk je ? Juist Stephen Elop's naam wordt ook genoemd als de beoogd opvolger van Balmer. Je zou bijna denken dat hij een aantal jaren geleden gewoon door Microsoft naar Finland is gestuurd om daar Nokia in te lijven. Nu kan hij terug naar Amerika om het roer over te nemen van Balmer.

Natuurlijk is het allemaal te toevallig voor woorden en heeft het helemaal niets te maken met een perverse drang om zoveel mogelijk geld bij elkaar te schrapen. Een bedrijf bijna ten onder laten gaan en er dan zelf van profiteren, ik ben bang dat mijn fantasie met mij op de loop gaat, maar het zou in theorie kunnen. Als dit verhaal op zich stond zou ik het niet eens noemenswaardig vinden, maar er zijn meerdere voorbeelden te noemen van slecht functionerende bestuurders die uiteindelijk "hun conclusies" trekken en met een hele dikke portemonnee ervan doorgaan. Nu is dit toevallig een voorbeeld dat niet uit de financiële wereld komt, maar als ik daar begin met voorbeelden te noemen zal dit veelgeprezen blad deze uitgave iets zwaarder worden. Ik kan het toch niet laten één voorbeeld te noemen namelijk die van onze meest eerlijk overkomende bank. De Rabobank gaat dealtjes aan met collega banken om er beter van te worden ten koste van anderen. Ordinaire bedriegerij die gelukkig een boete oplevert van een derde van de jaarlijkse winst van de Rabobank. Natuurlijk neemt ook iemand hier zijn verantwoordelijkheid, de bestuursvoorzitter stapt op, 8 weken voor zijn pensioen, een bank achterlatend die ineens niet meer als de meest betrouwbare bank wordt gezien. Het vertrek van Rijkman Groenink bij de ABN AMRO Bank bespreek ik maar niet, dit is al heel vaak besproken. Bedrijven gaan ten gronde aan de wellust van bestuurders terwijl wij ons in ons vak eigenlijk alleen bezighouden met de onderwereld en de risico's die daar vandaan komen. Ik onderschat de risico's uit de onderwereld niet en alle lezers hebben ook een rol in een vakgroep die ontstaan is door en tegen de risico's die onze geautomatiseerde omgevingen dagelijks lopen, maar ik ben bang dat de risico's uit de bovenwereld vele malen groter zijn en funest voor de bedrijfsvoering. Misschien moeten we iets meer oog hebben voor de risico's uit de bovenwereld. ●

Groetjes, Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. 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 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. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru