iB

INFORMATIEBEVEILIGING

jaargang 18 - 2018

#3

Privacy gaat me aan mijn hart

Catching an insider spy

Terugblik uitreiking Artikel van het Jaar

Last van de Bystander Bug

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

INFORMATION SECURITY *CERTIFICATION TRACK*

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

IT-SECURITY *CERTIFICATION TRACK*

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

PRIVACY & DATA PROTECTION *CERTIFICATION TRACK*

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

ETHICAL HACKING *CERTIFICATION TRACK*

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

BUSINESS CONTINUITY *CERTIFICATION TRACK*

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

(ISC)² ISACA iapp

Preparation courses

- CISSP® Preparation Course
- CCSP® Preparation Course
- CISM® Preparation Course
- CRISC® Preparation Course
- CISA® Preparation Course
- CIPM® Preparation Course
- CIPT® Preparation Course
- CIPP/E® Preparation Course

Hierboven ziet u een greep uit ons portfolio. Bij de Security Academy kunt u terecht voor het behalen van verschillende internationale titels van SECO-Institute®, (ISC)²®, IAPP® en ISACA®.

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

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

CONTINUÏTEIT EN BOEIENDE ARTIKELEN

Mei 2018, de maand van de AVG/GDPR. Je zou verwachten dat het magazine bol zou staan van de aan privacy gerelateerde artikelen. Nou, bol hoeft niet, want een ieder is daar al lang druk mee bezig geweest. Toch? In de afgelopen nummers, en zeker in de Privacy special van vorig jaar, is het onderwerp al genoeg besproken. Interessanter wordt het straks om de ervaringen te bespreken als de wet al een tijdje van kracht is.

Maar in dit nummer is toch wel wát te vinden over privacy. Zo was er de uitreiking van het artikel van het jaar 2017; twee van de drie artikelen van de prijswinnaars gingen over privacy. Het CIP heeft een aantal gratis tools, waaronder voor de GDPR/AVG ondersteuning, die zeker de moeite waard zijn. Ad Reuijl schrijft daarover. En uiteraard in dit nummer een redactioneel 'Achter het Nieuws' over het van kracht worden van de AVG/GDPR.

Zoals u merkt, is ondergetekende na iB1 weer de hoofdredacteur. Het aangekondigde roulerend hoofdredacteurschap werkt niet echt om redenen die Lex Dunn in het voorwoord van iB2 heeft aangegeven. We hebben via verschillende wegen een oproep gedaan om redacteuren te werven en potentiële auteurs te interesseren om een bijdrage te leveren. Inmiddels heeft een aantal mensen zich gemeld voor beide zaken. In ieder geval twee nieuwe redacteuren. Goed nieuws! Zeker voor de continuïteit van het magazine. En ook enkele auteurs hebben op korte termijn artikelen aangeleverd voor dit nummer. Waarvoor dank!

Wat valt er in deze uitgave dan verder te lezen, behalve de eerder genoemde privacy gerelateerde artikelen? Naast het juryrapport met betrekking tot het artikel van het Jaar 2017 voegde juryvoorzitter Jurgen van der Vlugt een beschouwing toe over de artikelen van afgelopen jaren. Bovendien schreef hij een opiniestuk over het 'Bystander Effect': "Iedereen stond erbij en keek ernaar en deed verder niets". Hij nodigt de lezer graag uit om te reageren. Verder schreef Vincent de Vries aan de hand van zijn Masterthesis een artikel over de 'Insider Spy threat (Catching an Insider Spy)'. Een pakkend artikel met weer een andere invalshoek (spionage) en hoe de 'spy' gevangen kan worden. Gert Kogenhop bespreekt de inbreng van Nederland bij de herziening van ISO22301 (de BCMS standaard) die onderweg is. Met een oproep aan mensen die er aan willen meewerken. Van Jan Wessels en Olaf Streuker een verslag van het European Cybersecurity Challenge 2017 oktober 2017. Daar zijn een paar zaken opgevallen, die zij beschrijven in 'Wie of wat is de security professional in 2018?' Zeker interessant is ook het artikel van Ilan Barda over de convergentie tussen SCADA/ICS en fysieke beveiliging (oftewel in het artikel OT genoemd, Operational Technology, in tegenstelling tot IT). 'Last but not least' in deze uitgave weer de rubriek 'Het bestuur in beeld', dit keer van de hand van Jasmijn Ogink, en de vaste columns van Rachel Marbus, The Attributer en Berry.

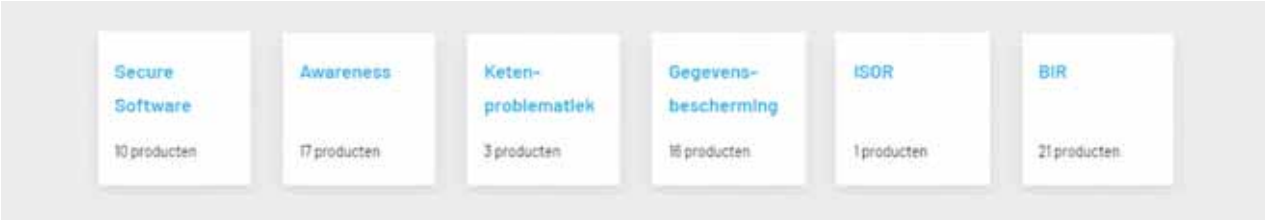
Kortom: voor elk wat wils! Veel leesplezier.
Tom Bakker

In dit nummer

Voorwoord - **3**
CIP Producten: die mag je niet missen! – **4**
Integratie van cyber security en fysieke beveiliging – **6**
Herziening business continuity management norm ISO 22301 onderweg - **8**
Het bestuur in beeld: Jasmijn Ogink – **9**
Column Privacy - Privacy gaat me aan mijn hart – **11**
Catching an insider spy – **12**
Wie of wat is de security professional in 2018 - **20**
Terugblik uitreiking artikel van het jaar - **22**
Column Attributer – Threat Modelled- **25**
Last van de Bystander Bug – **26**
Achter Het Nieuws – **28**
Column Berry – To Facebook or not to Facebook - **31**

CIP PRODUCTEN: DIE MAG JE NIET MISSEN!

Het Centrum Informatiebeveiliging en Privacybescherming is een publiek-private netwerkorganisatie die bestaat uit participanten en kennispartners. Participanten zijn (semi-)overheidsorganisaties en andere non-profit organisaties, waarvan medewerkers meedoen aan één of meer van de werkverbanden in het netwerk. Kennispartners zijn marktpartijen die met een convenant verbonden zijn en een hoeveelheid uren hebben toegezegd in de samenwerking.



Categorieën downloadbare producten CIP

Vanuit het principe 'voor allen, door allen' deelt het CIP kennis op alle mogelijke manieren. Zo zijn er onder andere themagerichte sessies, 'practitioner communities', een digitale samenwerkingsomgeving en conferenties. Ook stelt het CIP kennis ter beschikking in de vorm van samen uitgebrachte handreikingen, materialen voor gebruik in bewustzijns-campagnes, serious games, et cetera. Inhoudelijk variëren de onderwerpen van Secure Software Development tot Privacy Self Assessment workshops. De producten zijn door iedereen vrij te gebruiken onder de open source licentie Creative Commons Naamvermelding-GelijkDelen. Eventuele vrijwillige financiële bijdragen worden altijd gebruikt voor de versterking van de samenwerking.

Producten CIP voor iedereen beschikbaar

Het CIP wil als samenwerkingsplatform een relevante bijdrage leveren aan de informatieveiligheid in Nederland. Vandaar ook dat iedereen kan beschikken over de producten. Het is ook toegestaan om eigen varianten te maken, mits je de herkomst (de naam CIP) eraan blijft verbinden en dezelfde creative commons licentie gebruikt voor het nieuwe product.
Op https://www.cip-overheid.nl/ vind je alle downloadbare producten. Ze zijn gebundeld in de volgende categorieën.

Secure Software (in het bijzonder de productlijn Grip-op-SSD) is van belang als je de veiligheid van je applicaties wilt zekerstellen. Het gaat hier om basisbeveiligingseisen die een opdrachtgever in aanbestedingen en contracten kan gebruiken als veiligheidseisen aan het op te leveren softwareproduct. Deze eisen zijn zowel bruikbaar in de relatie tussen opdrachtgevers en leveranciers als tussen

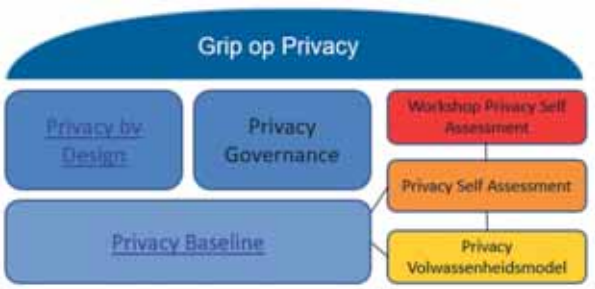
Een wel hele leuke vorm van het creëren van awareness is het doen van één van de serious games van het CIP

producteigenaren en ontwikkel- of onderhoudsafdelingen. Ze zijn concreet en testbaar. Het is een invulling van security by design op het terrein van de software.
Op de site van Forum voor Standaardisatie wordt Grip-op-SSD inmiddels ook aanbevolen: als iedereen deze eisen zou hanteren, zou ons landschap aanzienlijk beter beschermd zijn tegen 'hacken en lekken'.

Awareness-producten zijn talrijk. Zo kun je beschikken over een basisset van eenvoudige e-Learningmodules, die je zelf als sources kunt downloaden, naar believen kunt veranderen voor je eigen doel en die je kunt opnemen in je eigen Leer Management Systeem. Er is een handreiking voor de opzet van awareness programma's. Ook een verzameling CIP-casts: korte filmpjes, in de vorm van interviews met host Brenno de Winter, die in enkele minuten een IB&P-onderwerp uitleggen. Een wel hele leuke vorm van het creëren van awareness is het doen van één van de serious games van het CIP: bestrijd met een groep collega's, relaties of klanten een hacker die het je moeilijk maakt en beperk de schade die hij toebrengt. Leren door ervaren!

Op Ketengebied heb je met de 'Keten Service Library' een gesystematiseerde inventarisatie van keten governance practices in handen. Een relatief nieuw product is de 'Handreiking Bestuurlijke Communicatie bij Crises'. Dit document met vooral de twee krachtige bijlagen is zeer aan te bevelen voor iedereen die in ketens werkt. In dit document is nu eens niet uitgegaan van de technische, oplossingsgerichte communicatie, maar is de blik gericht op communicatie naar stakeholders.

Privacybescherming is een thema dat onder druk van de nieuwe Europese wetgeving zeer veel aandacht heeft



Productlijn Grip-op-Privacy

gekregen binnen de CIP-productontwikkeling. Met de productlijn Grip-op-Privacy wil CIP organisaties te hulp komen om privacy management op orde te krijgen en te houden. De Privacy Baseline vertelt wat je op orde moeten hebben in de organisatie (de AVG vertaald in 13 hanteerbare principes). De handreiking Privacy bij Design is het instrument dat ontwerpers, architecten et cetera in de ontwerpfase helpt privacy-vereisten direct mee te nemen bij de ontwerpkeuzen. Met de Privacy Self Assessment – PriSA (volledig gebaseerd op de baseline) toets je hoe jouw organisatie ervoor staat en geeft het tool aan wat je nog te doen hebt. Als je de self assessment door meerdere collega's laat invullen, kun je in een workshop in gesprek gaan op basis van een door CIP geconsolideerd groepsresultaat en elkaar verrijken met de diverse inzichten. In deze workshop vul je het plan dat het tool je aanreikt nog aan met eigen bevindingen tot een stevig plan van aanpak. De PriSA is ook goed te gebruiken als PDCA-instrument om periodiek de voortgang in kaart te brengen en bij te sturen.

Voor vragen aan het CIP ga naar:
www.cip-overheid.nl/contact/

Ad Reuijl is directeur van het CIP. Hij is sinds medio 2009 werkzaam bij het UWV. Vanaf 2012 heeft hij het CIP opgezet. Ad is bereikbaar via ad.reuijl@uwv.nl

INTEGRATIE VAN CYBER SECURITY EN FYSIEKE BEVEILIGING VOOR BETERE BESCHERMING OT-NETWERKEN

Geïntegreerde systemen voor fysieke beveiliging bestaan al jaren. Denk bijvoorbeeld aan een videobewakingssysteem dat gekoppeld is aan een systeem met scanpasjes dat het toegangsbeheer en de gebruikersrechten regelt. Maar integratie van cyber security en fysieke beveiliging? Dat is een ander verhaal.

In een doorsnee bedrijfsomgeving heeft zo'n integratie weinig meerwaarde, omdat er niet zo veel overlap is tussen meldingen op het gebied van cyber security en meldingen met betrekking tot de fysieke beveiliging. Maar nu kritieke infrastructurele netwerken steeds verder geautomatiseerd worden, wordt de potentie van zo'n integratie opnieuw bekeken. Bij onbemande, afgelegen locaties van nutsbedrijven kan het zinvol zijn om gegevens uit systemen voor fysieke beveiliging in verband te brengen met netwerkactiviteit: dit kan belangrijke indicaties opleveren van kwaadwillige activiteit.

Helaas is het traditionele gat tussen cyber security en fysieke beveiliging vaak ook terug te vinden in de organisatiestructuur van nutsbedrijven: in veel organisaties is cyber security het domein van de afdelingen IT of Operations, terwijl de afdeling Beveiliging verantwoordelijk is voor de fysieke beveiliging. Organisaties die een geïntegreerd systeem willen implementeren, moeten daarom één enkele proceseigenaar aanwijzen voor het volledige, geïntegreerde proces.
Hoe ver de verschillende systemen geïntegreerd moeten worden om netwerkverkeer te beveiligen – en wat dat mag kosten – is uiteraard afhankelijk van het soort risico waaraan het netwerk blootstaat, de gevolgen van een eventuele aanval en de vraag of zo'n aanval ook op andere manieren kan worden opgespoord. Wel biedt het feit dat fysieke beveiliging en cyber security al parallel aan elkaar zijn georganiseerd in onderstations de mogelijkheid om beide systemen te integreren zonder veel extra investeringen.

Gezien de toegevoegde waarde van integratie van cyber-fysieke beveiliging bij afgelegen, onbemande kritieke locaties en de mogelijkheden om dit te implementeren als onderdeel van door de netbeheerder geplande (en nu nog gescheiden) veiligheidsmaatregelen, hebben wij een geïntegreerde oplossing ontworpen die nutsbedrijven eenvoudig kunnen toepassen.

Reikwijdte geïntegreerde cyber-fysieke beveiliging

Laten we als voorbeeld eens kijken naar wat het gebruik van geïntegreerde cyber-fysieke oplossingen kan opleveren voor elektriciteitsleveranciers. Zij beheren vele verschillende locaties. De bedreiging kan hier twee vormen aannemen: (i) iemand dringt het netwerk van buitenaf binnen door het te hacken, en (ii) iemand verschaft zich toegang tot het netwerk door fysiek een complex binnen te gaan en verbinding te maken met een server of een ander apparaat

(in sommige gevallen wordt een netwerk besmet door malware die op de laptop van een monteur is geladen zonder dat deze dat weet). In het laatste geval kan een geïntegreerde oplossing voor fysieke beveiliging en cyber security een rol spelen.
Een onderscheid dat we ook moeten maken, is of een persoon het onderstation legaal betreedt, namelijk wanneer een monteur onderhoudswerkzaamheden moet uitvoeren op de locatie, of zich illegaal toegang verschaft tot de locatie.
In het eerste geval, wanneer een monteur de locatie in verband met gepland onderhoud bezoekt, zijn de doelen van het geïntegreerde systeem:

1. Het authenticeren van de toegangsgegevens van de bezoeker – bij voorkeur door middel van een authenticatie in meerdere stappen – voordat deze naar binnen kan, EN het authenticeren van de tijd en de reden van de toegang, aan de hand van een goedgekeurde werkopdracht.
2. De monteur alleen in verband met de klus toegang tot het netwerk geven: hij heeft alleen toegang tot de fysieke en logische zones op de locatie en binnen het netwerk gebaseerd op de werkopdracht. Elke afwijking van de werkopdracht levert dan een melding in het systeem op en zo nodig kunnen de betreffende apparaten of subnetwerken losgekoppeld worden van het OT-netwerk. Tijdens de onderhoudswerkzaamheden wordt de normale bedrijfsmodus van het IDPS (Intrusion Detection and Prevention System) voor het netwerksegment waarin het onderhoud wordt uitgevoerd aangepast, zodat de activiteiten van de monteur gevalideerd worden door specifieke regels die speciaal voor de werkopdracht zijn ingesteld. Door deze dynamische validatie worden de activiteiten van de monteur beperkt en vastgelegd zonder zinloze meldingen te genereren.
3. Het gebruik van fysieke apparaten (videobewaking, scanpasjes, biometrische scanmiddelen et cetera) om te bepalen waar de monteur zich binnen de locatie bevindt. Indien de monteur afwijkt van de werkopdracht door een ruimte te betreden waar hij niet voor geautoriseerd is, of door verbinding te maken met een niet-geautoriseerd apparaat of een niet toegestaan commando te geven (of dat nu met opzet of per ongeluk gebeurt), is het doel om de schade te beperken door het betreffende apparaat of netwerksegment los te koppelen.
   In het geval dat iemand zich illegaal toegang verschaft tot de locatie (binnendringen), zijn de doelen van het systeem:

a) Voorkomen dat de betreffende personen het onderstation kunnen betreden door middel van fysieke hindernissen zoals hekken en platforms, en als indringers er toch in slagen de hindernissen te passeren, de plek van binnenkomst te detecteren en de indringers te volgen bij hun gang door de locatie met behulp van een videobewakingssysteem dat verbonden is met het systeem voor toegangsbeheer.
b) Minimaliseren van de schade door het afkoppelen van de betreffende apparaten en subnetwerken door middel van een DPI-firewall (deep packet inspection), om de aanval binnen dat ene netwerksegment te houden. Deze DPI-firewalls werken met dynamische activering van persoonsgebonden regels voor cyber security, dus de standaardregels zullen alle netwerkactiviteiten die de indringer wil uitvoeren, blokkeren.
c) Het verhogen van het alarmniveau voor de rest van het netwerk en het waarschuwen van de beheerder en de verantwoordelijke autoriteiten, zodra onregelmatigheden worden geconstateerd, door fysieke beveiligingsapparaten of door het IDS dat het lokale netwerk bewaakt.

Samenvatting

Voor het correleren van de data van de systemen voor cyber security en fysieke beveiliging van een organisatie, om tot een echt geïntegreerde oplossing te komen, is geen expertise in cyber security nodig. De beste cyber-securitytools zijn in staat het netwerk zelflerend te maken en onregelmatigheden zelfstandig te melden. Integratie met de fysieke beveiliging vereist instelling van cyber-beleid per onderhoudsklus in hetzelfde systeem als dat voor de fysieke uitvoering, en een weergave van meldingen uit beide domeinen in hetzelfde systeem. Om een geïntegreerd systeem met succes te kunnen implementeren, moet ten slotte ook de gesplitste verantwoordelijkheid voor cyber security en fysieke beveiliging worden veranderd in een centraal overzichtspunt.

Ilan Barda is de CEO van Radiflow, een vooraanstaande leverancier van industriële cybersecurity oplossingen voor kritische infrastructuur. Ilan heeft ruim twintig jaar ervaring in de security en telecom-industrieën. Hij is bereikbaar via Ilan_b@radiflow.com

HERZIENING BUSINESS CONTINUITY MANAGEMENT NORM ISO 22301 ONDERWEG

In het voorjaar van 2012 werd de eerste ISO norm voor Business Continuity Management (BCM) gepubliceerd. Deze standaard 'ISO 22301:2012 Societal security – Business continuity management systems – Requirements' is inmiddels vertaald en daardoor tevens beschikbaar als 'Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit – Eisen'. Deze vertaling is gemaakt door leden van de BCM en Crisismanagement normcommissie bij NEN. Nu ligt daar een nieuwe uitdaging; dat is de Nederlandse inbreng verzorgen voor de herziening van de norm dit jaar.

BCM gaat over het zo optimaal mogelijk voorbereid zijn op het onverwachte, het vermogen van een organisatie om na een verstorend incident producten of diensten te blijven leveren op aanvaardbare, vooraf vastgestelde niveaus. Nu er zo'n vijf jaar ervaring is opgedaan met de norm, die grotendeels was gebaseerd op een Engelse 'voorganger', is het een uitstekend moment om deze positieve en negatieve ervaringen om te zetten in uitsluitend verbeteringen van de norm. Echter, er zijn meer dan 160 landen aangesloten bij ISO, men dient zodoende goed voorbereid ten strijde te trekken om de Nederlandse verbeterpunten om te zetten in wijzigingen in de norm. De Nederlandse inbreng komt voornamelijk van de leden en hun eventuele achterban, waaronder toonaangevende bedrijven uit verschillende sectoren, alsmede certificatie instellingen, het Business Continuity Institute plus trainings- en consultancybedrijven. Het gaat hier om de eisen voor certificering, niet een vrijblijvend setje richtlijnen, daarom behoeft elk voorstel tot aanpassing, toevoeging of het verwijderen van clausules een sterk argument en verdient alles een weloverwogen beslissing.

De norm wordt door een groot aantal organisaties in Nederland gehanteerd als de standaard om serieus met dit onderwerp aan de slag te gaan en een solide managementsysteem te implementeren. Een deel hiervan wil tevens dat een onafhankelijke certificatie instantie hier een oordeel over velt en, bij het voldoen aan de gestelde eisen, een ISO 22301 certificaat afgeeft. Meestal komt deze wens voort uit een eis van een grote klant of van een 'autoriteit', maar steeds meer ook vanuit de organisatie zelf of van de aandeelhouders, zoals het eerlijk gezegd ook zou moeten zijn. Elke organisatie dient dit te regelen, om in geval van een ernstige verstoring zo snel mogelijk weer haar producten en diensten te kunnen leveren met zo min mogelijk schade. Of dit nou het gevolg is van een brand, ICT uitval, cyber crime, logistieke problemen als gevolg van extreem weer of uitval van gas, elektra of water. Overigens wordt ook de leidraad (guidance) ISO 22313 vaak gehanteerd, die vanzelfsprekend tegelijkertijd wordt herzien om synchroon te blijven lopen. Momenteel wordt gewerkt aan de Working Draft (WD). Verwacht wordt dat in enkele stappen en bijeenkomsten van de wereldwijde werkgroep via de Draft International Standard (DIS) en de Final Draft International Standard (FDIS) nog eind dit jaar, uiterlijk begin 2019, de herziene versie beschikbaar zal zijn. De verwachting is dat er geen drastische - noem het inhoudelijke - wijzigingen zullen zijn, echter wel meer duidelijke eisen en een eenduidige aanpak onder de High Level Structure van ISO, waar deze norm overigens in 2012 de eerste 'gebruiker' van was. Wie op de hoogte gehouden wil worden of wil meedenken, kan zich uiteraard bij NEN melden.

Gert Kogenhop is lid van de BCM + en voorzitter van de NEN BCM & CM normcommissie. Hij is bereikbaar via www.bcmplus.nl of per e-mail: gk@bcmplus.nl.

Dit artikel is eerder verschenen in Kwaliteit in Bedrijf, nr.2 Maart 2018

JASMIJN OGINK

Ik heb er, voor het schrijven van dit stuk, eens mijn originele reactie bijgezocht op de bestuursvacature zo'n drie jaar geleden.

3-2015 "Ik las het bericht op de site van het PvIB vanochtend dat er een vacature is voor een bestuurslid. Ik ben sinds de zomer werkzaam in het vakgebied van informatiebeveiliging als business consultant IT risk management & compliance. In mijn functie help ik organisaties aantoonbaar normen zoals de ISO27001 na te leven, waarbij ik me inzet dat het gezonde beoordelingsvermogen en het managementsysteem van een organisatie voorop staan en niet ondersneeuwen in de regeldruk.
Informatiebeveiliging vind ik een machtig mooi vakgebied waar ik me verder in ga ontwikkelen. Naast het vakgebied zelf heb ik veel interesse in de effecten van digitalisering en automatisering in de breedte: op onze maatschappij en op het gebied van kennisdeling, privacy en ethiek. Het multidisciplinaire en het breed georiënteerde karakter van het PvIB spreekt mij aan."

Ik had op dat moment net een switch gemaakt van facility management naar infosec consultancy. De brug tussen deze twee verschillende rollen was mijn kennis van managementsystemen en compliance. Maar het vakgebied van informatiebeveiliging was zo goed als nieuw voor mij, hoewel het me wel meteen 'machtig mooi' leek. Ik wil graag betrokken zijn bij wat ik doe. En daarom zocht ik naar manieren om extra aansluiting te vinden bij wat informatiebeveiliging inhoudt, bij de mensen, de ontwikkelingen, de kennisbronnen. Het lidmaatschap van en de bestuursfunctie bij het PvIB hebben me die kans ruimschoots gegeven. Meer nog; ik voelde me vanaf het begin welkom!
Hetzelfde wens ik voor de andere leden van het PvIB; dat je je welkom voelt en aansluiting vindt. Het PvIB heeft daarin een functie als toegankelijk platform en als exchange point waar iedereen zich vrij voelt om zijn/ haar bijdrage te leveren.

En dat is broodnodig. We zien een steeds grotere maatschappelijke interesse in het beschermen van informatie en persoonsgegevens. Gevoed door het referendum over de Wiv, de komst van de AVG en de nodige schandalen, voelen steeds meer mensen zich betrokken bij het onderwerp.
Ook in het bedrijfsleven is dat het geval, de marketingafdeling vraagt zich actief af onder welke voorwaarden reclamemail mag worden verstuurd en developers hebben te maken met het vertalen van 'privacy by design' naar de praktijk. Zo zien we steeds meer een expliciete verwevenheid van informatiebeveiliging met andere disciplines. Dat vraagt een opstelling van alle betrokkenen gericht op samenwerking en kennisdeling. En wij hebben vanuit onze informatiebeveiligingsexpertise een grote invloed op de bouwstenen die gelegd worden voor de verdere vormgeving van de informatiemaatschappij.

Juist doordat we veel verschillende disciplines hebben binnen de vereniging, kunnen we onze kennis verrijken en zorgen voor kruisbestuiving. Dat bereiken we denk ik met name op onze bijeenkomsten, waar we elkaar spreken. Het vakgebied dat we delen, maakt dat we altijd wel gesprekstof hebben met een ander lid. Ik hoop dat iedereen deze bijeenkomsten als laagdrempelig ervaart en zich welkom voelt.

Inmiddels houd ik me in mijn werk met veel plezier bezig met privacy en security rond klantgegevens en slimme meters bij een netbeheerder. Als algemeen bestuurslid zet ik me in de breedte voor de vereniging in en, meer specifiek, als connectie met onze Young Professionals commissie en het onderwerp opleidingen. Als ik nu terugkijk naar mijn motivatie om bestuurslid te worden, kan ik zeggen, dat wat ik toen schreef nog steeds klopt. En ik vind informatiebeveiliging inderdaad ook nog steeds een 'machtig mooi' vakgebied.

THALES

THE MULTI-CLOUD ERA CREATES NEW ENCRYPTION CHALLENGES

Key Findings from the 2018 Global Encryption Trends Study

Data is the lifeblood of a successful business in today's world, but the balance of using it effectively and protecting it properly is pushing enterprises to the brink. With more organisations using multiple cloud providers to store and process their data, while at the same time needing to demonstrate compliance with increasingly stringent regulations, it is essential to have a data protection strategy that is up to the task. No core technologies are more fundamental to data protection than encryption and key management.

We've just released the results from our Global Encryption Trends Study (1) which once again show positive growth in the use of encryption across a wide variety of use cases. For example:

- 43 percent of respondents reports that their organization has an encryption strategy applied consistently across their enterprise
- 39 percent encrypts extensively in public cloud services, a number which has grown significantly just in the past year

An interesting aspect of the 2018 report is that encryption drivers have shifted towards protecting specific sensitive information, not just checking the compliance box. Compliance remains a significant driver for performing encryption, however, it has been surpassed for the first time by protecting enterprise's intellectual property and customer's personal information. Now, we've seen a multi-year trend of increasing cloud adoption with organizations looking to use the flexibility and scalability of services offered by Amazon Web Services, Microsoft Azure, Google Cloud, and more. According to the report, 61 percent of the respondents is using more than one public cloud provider, and 71 percent plans to in the next two years.
Data discovery was cited as a huge challenge (67 percent) for organisations this year. By storing data in several different places, it's harder for organisations to find and keep track on their data, which is important in the face of today's more stringent compliance regulations. Additionally, the use of multiple cloud providers can take users down the road of using multiple native cloud encryption tools, which in turn makes it difficult to instantiate a consistent encryption and key management policy using those different tools. Multiple tools can also increase the likelihood of mistakes, such as configuration errors, which are already cited as the most significant threat to sensitive data or confidential data by 47 percent of the respondents. Organisations can benefit from taking a single pane of glass approach (2) to managing keys and bringing their own encryption (BYOE) to the cloud, simplifying the administrative aspects of encryption and key management.

Cloud encryption was nascent five years ago, but adoption has accelerated greatly. And of course, we cannot forget about GDPR and the looming May deadline. We see substantial evidence in this year's study of its effect – one example is the increase in data discovery challenges, particularly in countries such as the UK, Germany, US, The Netherlands, Belgium and France. No matter what happens over the next year, encryption will continue to be a crucial part of any security and data protection strategy. When everything else fails, data-centric methods such as encryption – with best-practice based key management – wrap a protective layer around data to thwart those that seek unauthorized access to it. Scalable, cloud-friendly encryption isn't a luxury or insurance policy. It is a necessity to protect the data which is the lifeblood of the business. To get a copy of the 2018 Global Encryption Trends Study please send an email to Johan.vanderWelle@thales-esecurity.com

References

(1) www.thalesesecurity.com/2018/global-encryption-trends-study
(2) www.thalesesecurity.com/solutions/use-case/cloud-security

Mr. Rachel Marbus
@rachelmarbus op Twitter

PRIVACY GAAT ME AAN MIJN HART

Er zijn een aantal zaken in het leven waar mijn hart sneller van gaat kloppen. Mijn dochter die in mijn oor fluistert: "Ik hou van jou". Een prachtig schone golf die omrolt en de surfer die erin duikt om hem helemaal door te rijden. De bescherming van grondrechten en dan in het bijzonder het recht op privacy.

De afgelopen 1,5 jaar was een waanzinnige rit. Want hoe je het ook wendt of keert, het draaien van een wetsimplementatieprogramma is een pittige opgave. Zeker als je dat doet naast alle andere dagelijkse werkzaamheden. Met een waanzinnig team stond ik aan de lat om te kijken hoe we alle verwerkingen in kaart brengen, wat privacy by design nou betekent in de praktijk, hoe we moeten omgaan met dataportabiliteit en hoe je iedereen binnen het bedrijf niet alleen bewust maakt, maar ze ook nog een arsenaal aan kennis meegeeft om toe te passen in de praktijk.

Dat ging niet altijd van een leien dakje. Het duurde - voor ons gevoel – een eeuwigheid voor de organisatie in beweging kwam. En soms wisten we zelf ook niet zo goed wat nu de juiste weg was. Dat is natuurlijk niet gek, iets nieuws moet door alle partijen in de praktijk 'uitgevonden' worden. En dan blijkt maar weer eens dat een wetstekst zich niet altijd zo lekker laat uitvoeren in het echte leven. Maar, omdat privacy in ons hart zit, gaan we vrolijk door om die mooie dag – Towel Day – te halen.

Soms kregen we ook best forse tegenslagen te verwerken. Het gaat je niet in je koude kleren zitten als je met een klein team keihard werkt en je een slecht rapportcijfer krijgt van de meester. Want, natuurlijk kan het altijd beter en wie eens goed onder allerlei stenen gaat kijken, vindt daar altijd wel een vies beestje. Dat slechte rapportcijfer voelt dan toch wel ineens heel persoonlijk en dat heeft uiteraard ook te maken met de privacy in het hart meedragen. Ik besef me overigens dat de meester dat wellicht niet begrijpt (of het deert hem niet), maar we hadden er toch best een slapeloze nacht van.

Bij het naderende einde (of is het nou eigenlijk pas het begin?) merk ik dat de druk gigantisch toeneemt en dat mensen het onmogelijke beginnen te verwachten van de privacyspecialisten. Sorry, wij kunnen niet alle door jou gemaakte fouten uit het verleden ineens voor je wegwissen. Maar we doen wel onwijs ons best om je te helpen. Wij kunnen ook niet meer zo heel hard, we zijn al 1,5 jaar een marathon aan het lopen namelijk.

Afgelopen vrijdag voelde ik mijn hart. Daar, die plek waar mijn liefde voor privacy zit. Het deed zeer en klopte te snel. Ik voelde me ook een beetje benauwd. En dat was echt flink schrikken. Mijn hart heeft te hard gelopen zei de dokter me. En mijn bloeddruk wil ook te hoog pieken. Dus met 25 mei in het zicht moet ik een pasje terugnemen. Het tempo moet omlaag en de stress moet naar beneden. Ik heb mijn handdoek alvast klaargelegd. Dan kan ik op het strand liggen naast mijn dochter terwijl we naar epic surfers kijken en prachtige golven. En dan fluister ik in haar oor hoeveel ik van haar hou.

CATCHING AN INSIDER SPY

The insider threat is a risk that comes from the people within the organisation, such as (ex-) employees, contractors, business partners and third parties (1). Some experts argue that employees are the biggest threat to companies, because they have legitimate credentials and access to data and systems which can cause much damage when abused (2). There are many definitions of the insider threat. The CERT Division of the United States Software Engineering Institute defines the insider threat as: "a current or former employee, contractor, or business partner who has or had authorized access to an organisation's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems" (1). The perpetrator is called a malicious insider.

One of the key aspects of a malicious insider, according to Eric Cole, an industry recognized security expert, is that they "have access and in most cases will exploit the weakest link that gives them the greatest chance of access, while minimizing the chances that they get caught" (2).

A good example of a malicious insider from the perspective of the US Government is Edward Snowden, who worked as a contractor with access to classified information. He was stationed at the NSA (3). Snowden downloaded thousands of classified NSA documents and leaked them to journalists (4) and allegedly to the Russian Government (5). The NSA is considered one of the most technologically sophisticated organisations in the world and failed to detect this incident (4).
A malicious insider can cause tremendous impact on an organisation, because malicious insiders may commit fraud, sabotage data or steal information like intellectual property (6). Stolen information can be sold to the highest bidder or leaked to competitors, which might hinder the competitive advantage of the organisation. Other negative effects include possible monetary loss of the organisation, financial instability, loss of customers and loss of customer confidence (2). Apart from the impact on the organisation, stolen information may indirectly pose a threat to its clients as well.

Acts of sabotaging data or stealing information are often part of (cyber)espionage (7). Espionage is the act of obtaining information considered secret or confidential using "human sources (agents) or technical means" (8). There are two different types of espionage: industrial espionage, which is conducted for commercial purposes, and international espionage, which is conducted by Government entities for the interest of the nation (9).

According to the Dutch General Intelligence and Security Service (AIVD), espionage is a serious threat for organisations in The Netherlands (7). They state on their website that Dutch organisations are structurally under espionage attacks and incidents have already occurred in a variety of sectors like the defence sector, the high-tech sector, the chemical and energy sector, the health sector and the water management sector (7).

To minimize (cyber)espionage risks, organisations are advised to implement mitigative controls (depending on their maturity level). These controls have in most cases a passive and restrictive nature, which means that they prevent espionage from happening to a certain extent. Mitigative controls include central log collection, network segmentation, network filtering,
access control and strict security policies.

The downside of this 'passive' approach is that the organisation only reacts after an incident is reported or a possible leak is discovered. There is a considerable chance that information can be stolen without the organisation taking notice.
A more active approach in identifying insider spies is needed. Therefore, the goal of this research was to develop a prototype of a technical system that can detect insider spies. By detecting insider spies in an early stage, the impact on the organisation can be minimalized. To achieve this goal, the following main research question has been formulated: "Which technical indicators of compromise can be defined and used to detect common behavioural traits and patterns of insider spies within organisations?"

To answer the research question multidisciplinary research was conducted. Insider spies have specific behavioural traits and patterns associated with their motivations and enablers (social science), which can (partly) be detected

Vincent de Vries is werkzaam bij Fox-IT als CISO en als manager van het Security, Quality en Compliance team. Hij heeft dit artikel geschreven op basis van zijn thesis voor de executive masteropleiding Cyber Security waar hij de technische track heeft gevolgd. In deze master gaat aandacht uit naar zowel technologische als juridische, bestuurskundige, economische en psychologische aspecten van digitale veiligheid. Vincent is te bereiken via devries@fox-it.com of via LinkedIn (linkedin.com/in/vincentdev)

by monitoring the technical systems they abuse (computer science).

Literature review and unstructured interviews with domain experts were carried out to establish the body of knowledge regarding insider spies. This research revealed multiple indicators of compromise, which might be used in identifying insider spy activity. Subsequently, exploratory data analysis was conducted based on the CRISP-DM process (10) on log data as a case study. This log data was provided by an organisation interested in benefitting from the results of the research and was anonymised before usage.

The goal of the exploratory data analysis was to determine the main characteristics of the collected log data, to prepare this log data for automatic analysis and to determine the value of the available log data in relation to the earlier defined indicators of compromise.
The data analysis provided multiple additional indicators and a good understanding of the relevance and value of the collected log data.
A prototype system was developed to automatically detect the defined indicators in the log data. This prototype was developed in line with the design-science research guidelines defined by Hevner et al (11).
This article describes the motivations, enablers, the behavioural traits and the patterns associated with insider spies. Furthermore, the article describes some indicators of compromise which can be used by organisations to gain more control on this threat.

Common motivations and enablers of insider spies

The first step in this research was to establish and explore the body of knowledge regarding insider spies. This contributed to the overall understanding of the insider spy threat and gave insights on how to detect their actions.

During the research four leading theories have been identified describing the motivations and enablers of insider spies. These theories are: 1) the five core motivations, 2) the suggested motives for spying (MICE), 3) the RASCLS framework and 4) the enablers and motivations of spying insiders identified by the FBI. These theories have been compared and merged during the research. Based on the comparison, the five core motivations have been extended with one additional core motivation.

The five core motivations were developed by Dr. Julie E. Mehan. These core motivations encourage and enable employees to become malicious insiders (regardless of the nature of the insider activity) (6). The five core motivations are: greed, ideology, ego, revenge and opportunity.

One of the most powerful motivators for insider threats is greed (6). Dr. Jeevan D'Souza defines greed as "the selfish desire to possess wealth, substances, objects, people, power, status, appreciation or attention far beyond what is required for basic human comfort" (12). According to the insider data collection study conducted by the British Centre for the Protection of National Infrastructure (CPNI), financial gain was the "single most common primary motivation" for malicious insiders (13) and was identified in 47 percent of the cases as the main motivator.

The research conducted by the CPNI, which is part of the United Kingdom's MI5 security service, included 120 UK-based insider cases from both the public and private sector (13), where there was significant damage to the organisation (13). The data analysis and collection took place between 2007 and 2012. The information on the incidents was collected by "reviewing case files, paperwork, and through formal interviews with key personnel who had knowledge of the individual" (13). A structured interview protocol was used to "ensure, where possible, the same type of information was captured for each case" (13).

The second core motivation is ideology which can be defined as a "set of beliefs about how the world or a set of behaviours should be" (6). Edward Snowden and Chelsea Manning are both examples where ideology seems to play an important role. Snowden released information because he feared a surveillance state (14), "to encourage other whistleblowers" (14) and because "he loves the concept of privacy" (15). Chelsea Manning released information "out of love for her country" and "a sense of duty to others" (16). According to the CPNI insider data collection study, ideology was the primary motivation in 20 percent of the studied insider cases (13).

The desire for recognition or retribution is at least greed's equal (6). According to the dictionary, ego is the "I or self of any person; a person as thinking, feeling, and willing, and distinguishing itself from the selves of others and from objects of its thought" (17). Malicious insiders felt disgruntled in some cases because they never received a response they believed they deserved (18). They "rationalize that their activities are justified" (6) and carry out their malicious act. According to the CPNI insider data collection study, in 14 percent of the cases, the desire for recognition was the motivator (13). David L. Charney claims in his paper titled 'True Psychology of the Insider

Insider spies tend to show certain behavioural traits and patterns before, during and after their malicious acts.

Spy' that injuries to human pride and ego are at the root of most cases of insider spying (19).

The fourth core motivator, revenge, is relatively uncommon for malicious insiders. It was the main motivator in only 6 percent of the cases studied by the CPNI (13). Malicious insider activities motivated by revenge often involve "acts of sabotage and unauthorized theft of intellectual property or government information" (6). An example of revenge can be found in the "Maroochy water breach". Vitek Boden worked for a company called Hunter Watertech that was responsible for the installation of the SCADA radio-controlled sewage equipment for the Maroochy Shire Council (20). In 1999 Vitek Boden left after disagreements with the company and tried to get a job at the local Council but was refused. Consequently he decided to take revenge on his previous employer and the Council by launching attacks on the radio-controlled SCADA sewage equipment (20). His attack caused "800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel" (20).

Opportunity, the fifth core motivator, is "a favourable juncture of circumstances" (21) and can be a motivation on itself, but mostly it only enables malicious insiders to commit their crimes. This is one of the enablers that can be controlled to a certain extent by the organisation itself. Organisations should have strict security controls, processes and procedures to inhibit and deter an employee's opportunity to commit a malicious insider action (22).

The comparison of the above-mentioned theories highlighted the absence of a sixth powerful motivation in the original five core motivations indicated by Dr. Mehan, the possibility of being influenced by a third party. Coercion is part of the suggested motives for spying (MICE) and influence can be exerted using the recruitment principles from the RASCLS framework.

Besides the motivations of an employee to become an insider spy, the organisation itself plays a part in enabling the would be spy. The organisation is in most cases the factor that motivates or provides opportunities to malicious insiders even though organisations might be justified and right in doing so (e.g. by treating the employee in a certain way). Malicious insiders can be motivated, amongst others, by poor management practices including a lack of management oversight, failure to address individual issues and failure to manage and resolve workplace issues (13). Due to the lack of management oversight, insider activities can be conducted either unnoticed or they are not addressed when noticed. Failure to address individual issues and failure to resolve workplace issues appear to contribute to the level of employee disaffection (13). Employee disaffection can escalate into employees taking revenge on the company.

Behavioural traits and patterns associated with insider spies

Insider spies tend to show certain behavioural traits and patterns before, during and after their malicious acts.

Behavioural traits

The CPNI, the FBI and the US-CERT focused on the workplace behaviour of an insider spy. They defined several suspicious workplace behaviours that might indicate that an employee is a malicious insider.

When an employee is engaged in unusual and unnecessary copying activities, this might be an indication of an insider spy. Unusual copying activities include copying sensitive files from servers, removing the classification from classified documents and copying printed documents at departments other than one's own (in the case a copier is available at the department of the employee) (13)(23)(24). It is also possible for an insider spy to, for example, photograph sensitive documents with a smartphone.

Another indicator can be found in unusual IT activity. This behaviour includes, amongst others, key-word based searches on subjects that are not related to one's work, in sensitive databases or on network shares (13)(23), increased computer usage shortly before foreign travel, using remote access functionality while on vacation, at odd times or when on sick leave (13)(23) and disregarding IT-policies by installing personal software or plugging private hardware in their computers (23).
Unauthorised handling of sensitive information might be an indicator. This includes storing and carrying sensitive

information without need or authorisation (13)(23). When an employee violates or ignores security policies, this might be an indicator as well (13).

Besides these behaviours, malicious insiders might show an unusual interest in matters outside the scope of their duties, particularly in foreign entities or business competitors in the case of espionage (24). They might have unexplained wealth (they buy things they cannot reasonably afford with their salary) (23) and they might take short trips to foreign countries for a limited amount of time for unclear reasons. They can show "unusual interest in personal lives of co-workers" (23) and they might be overly enthusiastic to work overtime, late at night, odd times or in the weekend (24). In some cases, malicious insiders have concerns that they are being investigated. They may leave traps to detect searches (23).

Insider spy patterns

The researched theories all focus on a specific part of the insider spy attack. The focus is either on the psychology of an insider or on the attack pattern the insider follows. During the research, it became evident that there is no model that combines both the psychology perspective and the attack pattern perspective of an insider spy attack. There is a clear gap between both views and it appeared to the researcher that only the FBI and the Institute of Electrical and Electronics Engineers (IEEE) tried to map the whole attack chain. However, they lack the psychology insights of the insider threat due to their focus on the attack pattern. To fully understand the insider spies and their attack patterns there is a need for a model that combines both views and that integrates those into a kill chain. This model should illustrate the phases and stages an insider spy attack passes, so organisations can take measures to minimalize the insider spy risk.
Based on the established body of knowledge through expert interviews and the extensive literature review, an insider spy kill chain was developed that illustrates the structure of an insider spy attack. This kill chain contains five phases including 14 stages and is illustrated in Figure 1. The phases in the model are: the Life Experiences phase, the Shift of Allegiance phase, the Attack Preparation phase, the Active Attack phase and the Post-Attack phase.

During the Life Experiences phase, the insider might develop predispositions which establish the basis for future decisions. This basis can enable or motivate an insider spy to commit a malicious act when experiencing multiple stressful life events in a short time period (25). Subsequently, during the Shift of Allegiance phase, the insider spy experiences multiple stressors, shows concerning behaviour and reaches a tipping point on which the insider spy will start with his/her malicious actions due to the earlier

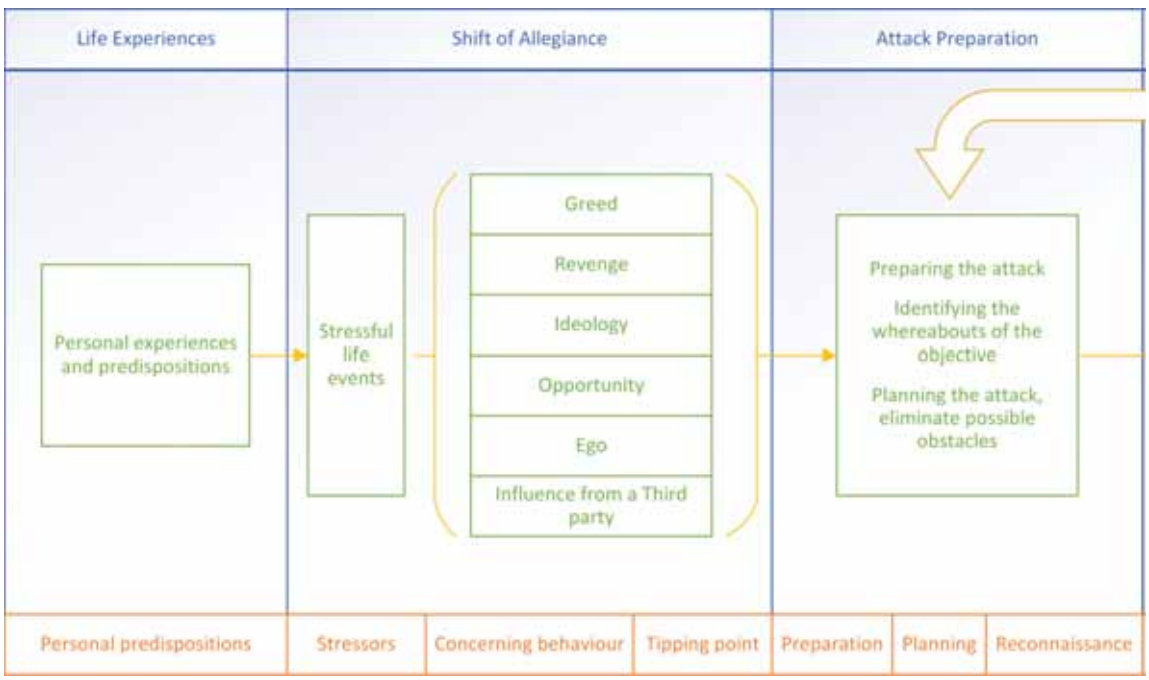


Figure 1 – The insider spy kill chain

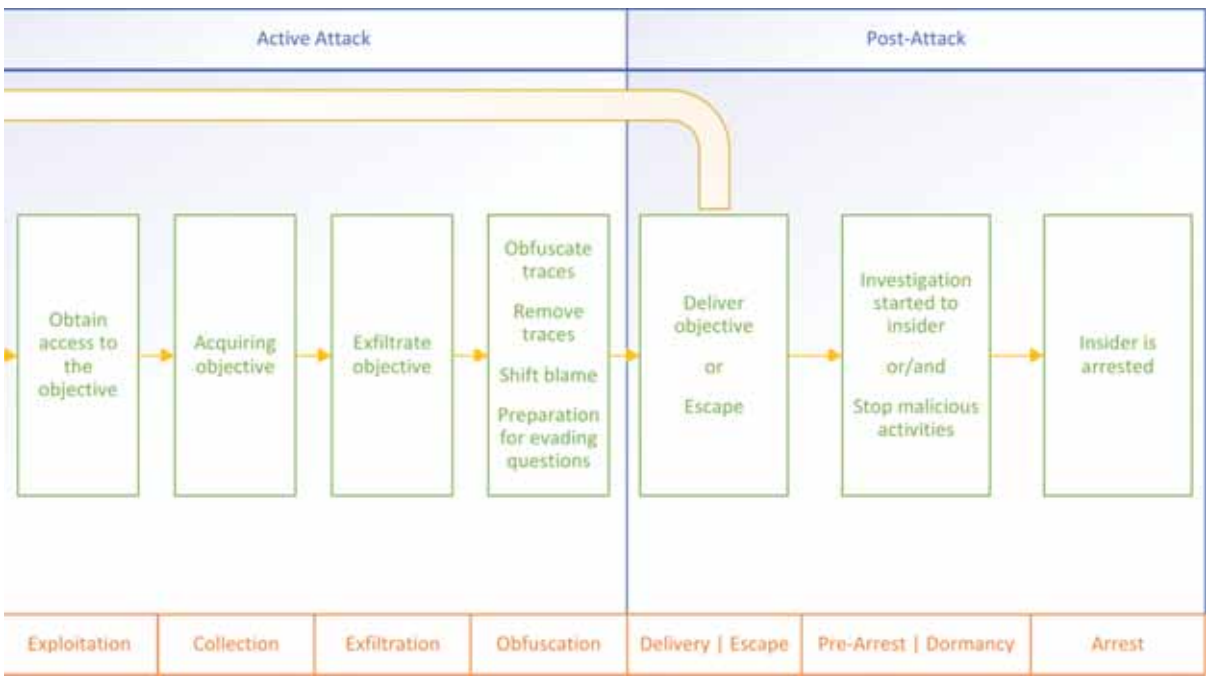
defined six core motivations and enablers for spying (greed, revenge, ideology, opportunity, ego and the influence from a third party).

During the Attack Preparation phase, the insider spy prepares the attack by deciding on a plan and will carry out reconnaissance if deemed necessary. This phase is followed by the Active Attack phase, during which the insider passes through four stages: exploitation, collection, exfiltration and obfuscation. In this phase the insider spy obtains access to the objective, acquires the objective, exfiltrates it and starts obfuscating the traces.

Finally, there is the Post-Attack phase, where the insider spy delivers the objective and/or escapes. After delivery the insider might be asked or feels obligated, in the case of an insider spy motivated by ideology, to collect/deliver more of the objective. That is why the kill chain has a possible loop back to the Attack Preparation phase. When an insider escapes or when colleagues notice suspicious behaviour, the organisation and authorities might start an investigation towards the insider spy. This is where the pre-arrest and dormancy stages described by Dr. D. Charney start (19). The insider might stop its previous activities in these stages or discover surveillance. Only one stage remains which is the arrest stage. During this stage the insider spy clearly did not escape and is successfully incarcerated and brought to justice.

It should be noted that the stages in the insider spy kill chain are not set in stone and some attacks might not encompass every stage. A good example is represented by the obfuscation stage because not all insiders will obfuscate their traces. The kill chain can end at any stage because the insider activity might be noticed and stopped upon detection. For example, during the data collection, technical indicators of compromise could notify the security team of suspicious behaviour which can be the start of an investigation. This means that at every stage, except the Personal Predispositions and the Arrest stages, an investigation can be started.

The first phase (Life Experiences) and the first and second stages of the second phase (Shift of Allegiance) are based on the research of Eric Shaw and Laura Sellers (25). The tipping point stage is based on the results of the literature review and the Attack Preparation phase is based on both the insider threat kill chains of the FBI (26) and the IEEE (27). This is also the case for the stages in the Active Attack phase and the first stage of the Post-Attack phase. The last two stages are based on the insider spy psychology studies of Dr. D. Charney (19).



Common indicators of compromise

This section gives a brief overview of a number of indicators of compromise associated with insider spies. It should be noted that these events or behaviours by themselves do not imply that an employee is an insider spy, although a combination of multiple indicators could be the starting point for an investigation.
The indicators of compromise come in many forms. Below is an overview of the indicators based on how and where they can be detected. Three categories were defined: indicators through social interaction and observations, indicators that can be observed depending on the context and lastly indicators through socio-technical and technical activities.

Social interaction and observations

The following indicators, amongst others, can be detected by employees through social interaction and observations:

- Unusual or unexplainable stress peaks
- Unexplained wealth
- Short trips to foreign countries for a limited amount of time
- Unusual interest in personal lives of co-workers
- Appearing intoxicated at work
- Pattern of significant change from past behaviour, especially relating to increased nervousness or anxiety (28)
- Deterioration of personal hygiene (28)
- Increased friction in relationships with co-workers (28)
- Enthusiastic to work overtime, late at night, odd times or in the weekend
- Pattern of lying and deception of co-workers or supervisors

Detection based on context

The list below contains indicators that can be detected by individuals or by a technical solution depending on where the insider spy activity takes place:

- Unusual and unnecessary copying activities
- Regularly printing on printers in other departments
- Removing data classification from documents or declassifying sensitive files without a good reason
- Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research (28)
- Violating and/or disregarding security policies
- Attempts to enlist others in illegal or questionable activity

Socio-technical and technical activities

The list below contains indicators that can be used to detect suspicious socio-technical and technical behaviour:

- Using remote access functionality while on vacation, at odd times, odd locations (geoIP) or when on sick leave
- Access denied events related to specific zones in the organisation
- Discrepancy between usage of alarm code and physical access to the building
- Outliers in the number of bytes transferred to and from VPN clients
- Inconsistency between the time spent in the building and the declared working hours
- Access denied requests originating from a system assigned to a different user (applicable if all employees have a personal workstation)
- Outliers in privileged user account activities
- Outliers in the size of incoming and outgoing e-mail messages
- Forwarding of internal e-mails to an external e-mail address
- Outliers in file share activity regarding access attempts
- Discrepancy between usage of VPN connection and physical presence in the building

The general technical indicators of compromise from an external attacker must be taken into account as well because an insider spy might apply these techniques.
It should be mentioned that the results of the literature review are mostly based on research conducted in the United States and the United Kingdom. This means that the results of their research might not be fully applicable on malicious insiders in the Netherlands (due to cultural differences), although the results from the literature review and domain experts interviews apply well to six known Dutch insider cases. Further research should be conducted in this area.

Prototype system

The body of knowledge resulting from this research was implemented in a prototype system. The aim of the initial version of the prototype was to detect the technical indicators of compromise in the available datasets.
The results show that a prototype system can detect the defined indicators. The prototype was able to find some unusual events in the log data. However, to improve the prototype and the technical indicators of compromise, further research is needed.

Whether an insider spy will be detected by the organisation depends on his/her level of operational knowledge and security. In the case an insider receives instructions from an intelligence agency, or when an insider is trained by such an agency, operational mistakes are limited and it is likely that information is exfiltrated without detection.

(NB) Due to the size of this article, the results of the exploratory data analysis and the details regarding the prototype system had to be omitted. The researcher is preparing an additional article or blog post on this subject.

References

(1) D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, 'Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1', Published by CERT, Software Engineering Institute, Carnegie Mellon University, www. cert. org, 2009.

(2) E. Cole and S. Ring, 'Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft', 1st ed. Syngress, 2006.

(3) 'Edward Snowden', Biography.com, www.biography.com/people/edward-snowden-21262897.

(4) 'Edward Snowden and the NSA: A Lesson About Insider Threats', Bloomberg.com, 03-Jul-2013, https://bloom.bg/2Knpfss.

(5) 'Was Edward Snowden a Spy? The Answer Remains Classified - Bloomberg', https://bloom.bg/2l4xQlK.

(6) J. Mehan, 'Insider Threat - A Guide to Understanding, Detecting, and Defending Against the Enemy from Within', 1st ed. IT Governance Ltd, 2016.

(7) M. van B. Z. en Koninkrijksrelaties, 'Cyberspionage - Cyberdreiging - AIVD', 10-Jun-2015, www.aivd.nl/onderwerpen/cyberdreiging/cyberspionage.

(8) 'Espionage | MI5 - The Security Service', https://www.mi5.gov.uk/espionage.

(9) I. Staff, 'Industrial Espionage', Investopedia, 29-Mar-2010, www.investopedia.com/terms/i/industrial-espionage.asp.

(10) R. Wirth and J. Hipp, 'CRISP-DM: Towards a standard process model for data mining', in Proceedings of the 4th international conference on the practical applications of knowledge discovery and data mining, 2000, pp. 29–39.

(11) A. R. Hevner, S. T. March, and S. Ram, 'Design science in information systems research', MIS Quarterly, vol. 28, no. 1, pp. 75–105, 2004.

(12) J. D'Souza, 'Greed: Crises, Causes, and Solutions', International Journal of Humanities and Social Science, vol. 5, no. 7, pp. 1–6, 2015.

(13) 'CPNI Insider data collection study - Report of main findings', Apr-2013, https://bit.ly/2Hz9fFY.

(14) K. Hill, 'Why NSA IT Guy Edward Snowden Leaked Top Secret Documents', Forbes, https://bit.ly/2I0YLyA.

(15) G. Greenwald, E. MacAskill, and L. Poitras, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', The Guardian, 11-Jun-2013.

(16) C. Manning, 'Chelsea Manning on the U.S. Military and Media Freedom', The New York Times, 14-Jun-2014.

(17) 'Ego | Define Ego at Dictionary.com', www.dictionary.com/browse/ego.

(18) 'Insider Threats 101: The Threat Within', TrendLabs Security Intelligence Blog, 09-Dec-2014, https://bit.ly/2I16Ymh.

(19) D. L. Charney, 'True Psychology of the Insider Spy', Intelligencer: Journal of U.S. Intelligence Studies, 2010.

(20) M. Abrams and J. Weiss, 'Malicious control system cyber security attack case study–Maroochy Water Services, Australia', McLean, VA: The MITRE Corporation, 2008.

(21) 'Definition of OPPORTUNITY', www.merriam-webster.com/dictionary/opportunity.

(22) Dawn Cappelli, Andrew Moore, and Randall Trzeciak, 'The CERT® Guide to Insider Threats - How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud'). Addison-Wesley Professional, 2012.

(23) 'The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy', Federal Bureau of Investigation, www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

(24) U.S. Department of Homeland Security, Combating the Insider Threat', 02-May-2014.

(25) E. Shaw and L. Sellers, 'Application of the Critical-Path Method to Evaluate Insider Risks', Laos: Operation MILLPOND, 1961 Foundations of Anglo-American Intelligence Sharing The National Intelligence Council, 2009–2014 Evaluating Insider Risk–The Critical-Path Method, vol. 59, no. 2, p. 41, 2015.

(26) HackersOnBoard, 'BlackHat 2013 - Combating the Insider Threat at the FBI: Real-world Lessons Learned', www.youtube.com/watch?v=38M8ta13K0Q.

(27) J. R. C. Nurse et al., 'Understanding Insider Threat: A Framework for Characterising Attacks', in 2014 IEEE Security and Privacy Workshops, 2014, pp. 214–228.

(28) Antonio A. Rucci, 'Protecting Against and Investigating Insider Threats', presented at the Defcon 17, Las Vegas, 2017.

VERSLAG

WIE OF WAT IS DE SECURITY PROFESSIONAL IN 2018?

Bron: ENISA

Op 31 oktober 2017 was ik in Malaga voor een overleg van de ECSO (European Cyber Security Organisation). Het overleg viel samen met de European Cyber Security Challenge 2017, waar nationale jeugdteams tegen elkaar strijden in een 'Capture the Flag'.

Hierbij vielen twee zaken mij op.

1. Onder de 15 teams bevond zich geen Nederlands team, terwijl Nederland rond dezelfde periode wel de officieuze wereldkampioenschappen had gewonnen. Een kans voor het NCSC?
2. Het tweede punt is meer serieus. Slechts in een paar teams zat een vrouw (per team hooguit één), de meerderheid van de deelnemers was dus mannelijk. Zo blijft de ongelijke verdeling van de geslachten in het werkveld wel in stand.

In dit artikel ga ik in op wie of wat nou de security professional is in 2018 met daarnaast een bedrijfsmatige kijk op de security professional.

De security professional van 2018

Mijn beeld van de security professional is voornamelijk gebaseerd op informatie verzameld in een online enquête, onder andere ook via de PvIB is uitgezet, die begin 2017 door 106 mensen is ingevuld (93 mensen hebben de enquête volledig ingevuld). Dit levert het volgende beeld op:

- De gemiddelde security professional is een man, tussen de 35 een 54 jaar oud, met een HBO of Universitaire achtergrond. De studie is veelal gedaan in een economische, wiskundige/ natuurwetenschappelijke of technische richting;
- Het merendeel is in loondienst, waarschijnlijk bij een financiële instelling, of werkzaam in de advisering/zakelijke dienstverlening. Zijn functiebenaming is CISO of ISO, met daarnaast nog consultant;
- De security professional werkt al lang bij het bedrijf; meer dan de helft langer dan 6 jaar. In 5 procent van de gevallen zelfs langer dan 20 jaar. Hij heeft zijn sporen ook al verdiend in de informatiebeveiliging: slechts 16 procent werkt korter dan 5 jaar in de informatiebeveiliging. Dit hangt natuurlijk ook samen met de leeftijdsopbouw;
- De favoriete certificering is CISSP, met CISA en CISM als goede tweede en derde. De certificeringen worden over het algemeen actief onderhouden.

Het dagelijks werk van de security professional bestaat uit (in willekeurige volgorde):

- implementatie van informatiebeveiliging (vraag is dan wel wat dit precies inhoudt)
- uitvoeren van risicoanalyses voor informatiesystemen et cetera
- in aansluiting hierop informatiebeveiligingsassessments, tests et cetera
- training geven en awareness verhogen
- monitoren van en rapporteren over informatiebeveiligingsrisico's
- opstellen van beleid (richtlijnen en standaarden)

Bedrijfsmatige kijk op de security professional

Op de ISF(1) Grey/Orange Summer Conference in juni 2017 in Frankfurt hebben we het onderwerp professionalisering besproken. Zo'n 50 vertegenwoordigers uit Duitsland, Oostenrijk, Zwitserland, Luxemburg, België en Nederland gaven hun mening over de vraag: "Wat maakt iemand een goede security professional?" De groep was te klein om een echt representatief beeld op te stellen, maar het gaf wel een interessante eerste inkijk.

Personeel

Bedrijfsmatig is het aantrekken van goed opgeleid security personeel op dit moment de grootste uitdaging. Het ontwikkelen en behouden van personeel blijft daarnaast natuurlijk ook van groot belang. Het invullen van een specifieke vacature kost in de regel tussen de zes maanden en een jaar. Er lijkt weinig verschil van mening te bestaan tussen de verschillende bedrijfstakken. Ook is geen duidelijk onderscheid in welke positie het moeilijkst in te vullen is. Van adviseurs tot technisch specialisten – ze zijn allemaal lastig te vinden.

Functieprofielen en opleidingen

Er bestaat een gemengd beeld of standaard functieprofielen helpen bij het aantrekken en behouden van personeel, er is geen uitgesproken voor of tegenstem. Dit beeld bestaat in iedere bedrijfstak en ieder betrokken land. De security professional zelf en de organisatie zijn verantwoordelijk voor de opleiding van de professional. Dat geldt nagenoeg voor elk werkveld. Bedrijven leiden in grote mate zelf op, met daarnaast ook een externe opleiding. Die laatste is vooral in de industrie populair. Een interne opleiding of training 'on the job' vindt plaats in alle werkvelden. Bij de vereiste certificeringen is de top 3: CISSP, CISA en CISM. Hierin zijn geen grote verschillen tussen de landen en werkvelden. De laatste vraag was of standaard onderwijs helpt bij het terugdringen van het tekort aan professionals. Men was hierbij voorzichtig positief; de meeste respondenten gaven aan 'waarschijnlijk wel', een kleine groep antwoordde met een uitgesproken 'ja'. Ook bij het antwoord op deze vraag zijn dus geen grote verschillen tussen de landen en werkvelden.

Conclusie

Het intuïtief bestaande beeld van de security professional (oudere man met een technische/bèta achtergrond) is duidelijk bevestigd in de online enquête. Ook dat certificeringen als CISSP, CISA en CISM veel worden behaald en veel worden gevraagd.

Het werkveld is in de afgelopen jaren verbreed met meer specialistische functies. Denk hierbij aan pen testers, security analisten en ga zo maar door. Dat komt nog niet terug in de enquête. Een reden hiervoor kan zijn dat we in de enquête de verkeerde doelgroep hebben aangesproken. In alle (snelle?) veranderingen in het werkveld met termen als 'agile' en 'devops', zou je ook een verjonging van de professionals verwachten. Die verjonging zie ik wel in mijn omgeving, maar niet in de enquête.

Conclusie is dat er meer onderzoek nodig is naar de ontwikkelingen in het werkveld. Wat zijn de ontwikkelingen in de functies die ontstaan en verdwijnen? Welke zaken pakken DevOps teams zelf op en welke taken blijven echt bij specialistische functies? Hoe ver willen we gaan in het uitsplitsen van capabilities per functie? Een mogelijke kapstok om deze ontwikkelingen te beschrijven is het zeer uitgebreide NICE-framewerk (2) uit de VS.

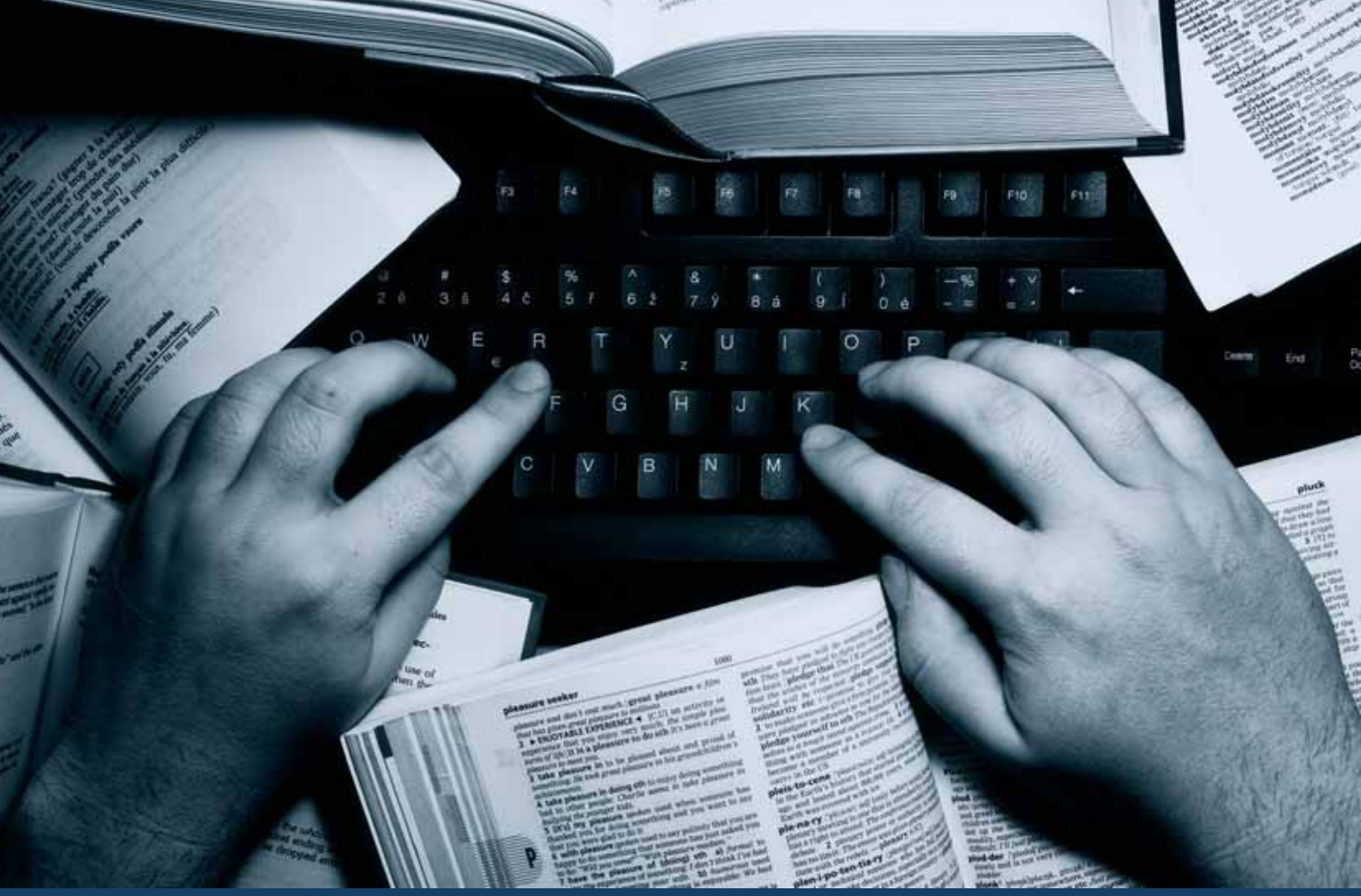
Wordt vervolgd….

Links

(1) Information Security Forum, www.securityforum.org/
(2) NICE Framework: https://bit.ly/2FE8Z3C

(r) Jan Wessels is security officer voor de business line Wholesale bij het Global Information Security Office van Rabobank en lid van de werkgroep QIS. Hij is bereikbaar via Jan.Wessels@rabobank.com

Olaf Streutker is Strategic Advisor bij het Corporate Information Security Office van ABN AMRO Bank en onder andere lid van de stuurgroep QIS en de klankbordgroep dcypher. Olaf is bereikbaar via olaf.streutker@nl.abnamro.com



OEFENINGEN...

Terugblik uitreiking 'Artikel van het jaar'

De artikelprijswinnaars van dit jaar hebben trends gezet en voortgezet, in diverse richtingen. Alf Moens en Sandy Janssen geven in hun verslag van een crisisoefening een helder beeld van wat er zoal voor te bereiden is – en te leren. En hoe je daarover open kunt zijn – en dat allerminst een teken van zwakte is.
De jury had het er weer druk mee dit jaar. Een reeks van artikelen werd doorgekauwd en kritisch beoordeeld. Initiële oordelen en criteria gingen op de helling, kwamen terug, werden bediscussieerd, tot er dan uiteindelijk een top 3 uitkwam. Plus flink wat meta-beoordeling; de trends die de jury door de jaren heen ziet in de artikelen.

Diversiteit

Wat daarbij vooral opvalt, is dat de diversiteit in de loop der jaren alleen maar is toegenomen. Waren vroeger (ja, we worden oud, hopen we!) artikelen typisch van een lengte en diepgang dat altijd nog wel wat semiwetenschappelijke pretenties waren blijven hangen, tegenwoordig is het op allerlei fronten diversiteit wat de klok slaat. En dat is uitstekend! Want dat brengt een stevige verbetering in de leesbaarheid van de stukken met zich mee, en volgens ons ook een veel betere lezing. Voorheen kon een lezer na een bladzijde of twee nog concluderen dat het artikel toch niet zo relevant of interessant was en afhaken. Tegenwoordig is het artikel door de gedownsizede lengte dan al helemaal gelezen. De diversiteit sluit ook aan op de verbreding die we in ons vakgebied hebben zien groeien. Waar het voorheen nog wel mogelijk was om als specialist zo'n beetje alles van informatiebeveiliging te weten tot in de vereiste technische details, tegenwoordig is een 'uomo universale' op ons vakgebied meestal een verkoper, niet een echte deskundige. Daarmee is het extra nuttig voor de lezer om zich zo breed mogelijk te kunnen oriënteren op allerlei ontwikkelingen. De winnaars van dit jaar scoren duidelijk op dit aspect.

Diepgang

Aan de andere kant: er is ook nog steeds behoefte, zeker bij de jury, aan doorwrochte artikelen die wel enigszins in allerlei details en zijlijnen naar volledigheid streven, maar ook heel duidelijke handreikingen geven voor praktische implementatie. In het verleden zat daar soms ook nog wel wat 'stoppen vlak voor de finish' bij, uit commerciële overwegingen. Lezers lekker maken, zodat ze wel een behoefte kregen er 'iets' mee te doen, maar dat aan de hand van het artikel eigenlijk nét niet zelf konden. Zodat ze vervolgens wel het betreffende adviesbureau moesten inhuren om het werkelijk te komen uitvoeren. Terwijl de PvIB natuurlijk, uit hoofde van haar opdracht, liever zo veel mogelijk kennisdeling ziet onder leden, en zeker niet alléén als marketingplatform wil optreden. En we toch in een tijd leven waarin, langzaam, al te langzaam, begint door te dringen dat kennis delen macht is, en gedeelde kennis vermenigvuldigde kennis is voor alle deelnemers. Kennis afschermen, dát is pas improductief. Kennis delen is dus het devies, en ook dat zien we terug in het winnende artikel van dit jaar.
En in het kennis delen, in de breedte, zit uiteraard voor

Sandy Janssen ontving de eerste prijs uit handen van jurylid Jurgen van der Vlugt (l) en kreeg een mooi boeket van Tom Bakker, redactielid van iB Magazine.

uzelf ook een oefening. Nee, geen rampenoefening, denken we. Maar een manier om te zien dat ook uw ervaringen, gedeeld, ons vakgebied in steeds bredere zin verder brengen. Mag de jury komend jaar uw volwaardige, diepgravende, maar 'actionable' artikel beoordelen ..? Wellicht dat u dan ook in de top 3 'Beste artikelen van 2018' of 2019, of …, komt.

Juryrapport

2018, Het jaar van de privacy. Zou dat ook terug te zien zijn in de verkiezing van artikel van het jaar? Er waren zeker een aantal artikelen die het onderwerp aanpakten. Helaas geen artikel dat de nieuwe dataprotectieverordening totaal duidelijk maakt met daarbij een vinklijstje voor elke organisatie. De lezer die dat had willen hebben … PvIB-leden weten vast beter, en zijn ongetwijfeld druk bezig met dit onderwerp.

De jury van 'Artikel van het jaar 2017': Aart Jochem, Jurgen van der Vlugt en Ellen Wesselingh

De jury was aangenaam verrast door het grote aantal prettig leesbare artikelen.

Ook dit jaar boog de jury zich over een lijst met kanshebbers. De criteria die de jury daarbij hanteerde: is het een interessant en/of actueel onderwerp dat toch nog jarenlang relevant blijft, heeft het artikel een originele invalshoek of zet het aan tot denken? En niet onbelangrijk: is het gewoon een goed leesbaar artikel, dat door de structuur de zaken helder op een rijtje zet en dat de lezer concrete aanknopingspunten geeft om met de materie aan de slag te gaan? De jury was aangenaam verrast door het grote aantal prettig leesbare artikelen. Na ampel beraad kwam de jury tot de volgende top drie:

Winnaars

1. Alf Moens en Sandy Janssen
'OZON: Bruggen bouwen'

2. Ksenia Kondratova
'Do's en Don'ts bij profiling'

3. Simone van der Hof
'Rechten van kinderen onder druk'

Drie ...
Op plaats drie is geëindigd 'Rechten van kinderen onder druk' van Simone van der Hof. Een belangrijk onderwerp dat zeker te denken geeft over de brede werking van ons vak. Dat ziet de jury graag meer. Het artikel adresseert een spanningsveld dat met de introductie van 'informed consent' in de algemene verordening gegevensbescherming ontstaat als het gaat om de privacy van jonge kinderen. Het artikel gaat in op de problematiek en waarom de standaardoplossing niet werkt. Daarna komen suggesties die helpen andere oplossingsrichtingen te bedenken. Vraag is of de juridische kwestie goed past voor de doelgroep. Maar zondermeer een helder artikel dat een belangrijk onderwerp aansnijdt.

Twee ...
'Do's en Don'ts bij profiling' van Ksenia Kondratova, wederom een juridisch vraagstuk. De auteur geeft een helder verhaal dat wettelijke kaders rondom profiling op een rijtje zet. Het is goed leesbaar en lezers in de doelgroep krijgen zo meer begrip van de valkuilen en nuances van profileren van gebruikers. De jury had graag net iets minder herhaling van punten gezien, en meer eigen analyse of invalshoeken en handvatten over hoe dan te handelen in bepaalde situaties. Niettemin een belangrijk onderwerp dat hiermee op de kaart is gezet, en gaarne voorzien van een aanbeveling aan allen om hier verder mee te gaan.

Één ...!
En op de eerste plaats, het artikel van het jaar: 'OZON: Bruggen bouwen' van Alf Moens & Sandy Janssen. Een artikel zoals de jury ze graag leest: goede structuur, relevant onderwerp, interessante verbreding naar algemenere toepassing, en gewoon lekker leesbaar bovendien. De jury was unaniem in de hoge score van dit artikel, dat het actuele en relevante onderwerp van crisisoefeningen behandelt. De auteurs beschrijven de samenwerking tussen verschillende organisaties om een sector brede crisisoefening te doen. Een helder verslag van een indrukwekkende oefening, waarbij zowel inzicht in de voorbereiding als in de uitvoering wordt gegeven. Daarnaast worden een aantal aanbevelingen gedaan die ook andere sectoren kunnen toepassen, met een link naar verdiepende informatie.

Onder dankzegging overigens voor alle werk het afgelopen jaar blijft de jury nog met één vraag aan de iB Magazineredactie zitten: waar staat dat OZON toch voor?

THREAT MODELLED

The Attributer has become aware that threat modelling is enjoying some popularity at the moment. However, most of what is written and said about it makes little sense. It's not the role of this column to 'name and shame', but if you doubt what is said here, just type the words 'threat modelling' into your favourite search engine and read what it brings up. There is the widespread confusion between 'threat' and 'vulnerability'. A threat is a potential action against you, carried out by someone or something called a 'threat actor'. The action may be malicious or accidental, intentional or unintentional. The actor may be an individual human, or a group of humans acting together in joint enterprise, or it may even be a natural event with no human action involved (such as a flood or an earthquake). Vulnerability is a weakness in your system. The weakness may be concerned with poor design and construction of your technology, or with inadequate processes, or with the incompetence of people doing their jobs, or some combination of these three factors. Threats can exploit vulnerabilities to cause negative impacts on your business objectives. Threats and vulnerabilities are related, but they are not the same thing. A threat is only dangerous if there is a vulnerability that it can exploit. A vulnerability is only a problem if there is a material threat that can exploit it. Got it?

Consider a simple SABSA domain model in which there are two domains. 'Your Systems' is a sub-domain of 'Environment' in which those systems exist (the super-domain). For those readers not familiar with SABSA domains, they are sets and sub-sets and the graphic is a Venn diagram. That means that everything in the sub-set (sub-domain) is also part of the super-set (super-domain).

Threats are found in the super-domain. They emanate from the systems environment. However, there is something known as the 'insider threat' which originates in the sub-domain – which is also part of the super-domain. Insider threats are usually subversive members of staff acting against the organisation. Vulnerabilities are never found in the environment outside the Your Systems sub-domain – they are properties in the systems themselves, not properties of the environment. This clarity of detail is essential in any threat-modelling framework. A methodology that begins by advising you to look at Your Systems (applications, infrastructure, databases, etc.) is beginning in the wrong place, heading in the wrong direction and will finish up with the wrong model.

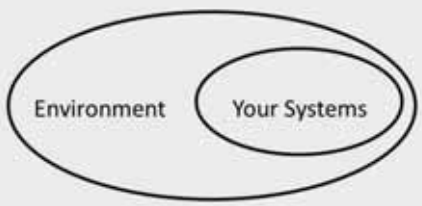


Figure 1 - Venn diagram

To analyse the threat in more detail you need to look at the threat actor with three questions: what are their capabilities to act? What is their motivation for acting? And what opportunities do they have to act against you? There may also be inhibitors (making action less likely), catalysts (triggering action) and amplifiers (making action more likely) that influence the actor's motivation. Nowhere in this threat model is there mention of vulnerability. Modelling vulnerabilities is an entirely different type of activity.

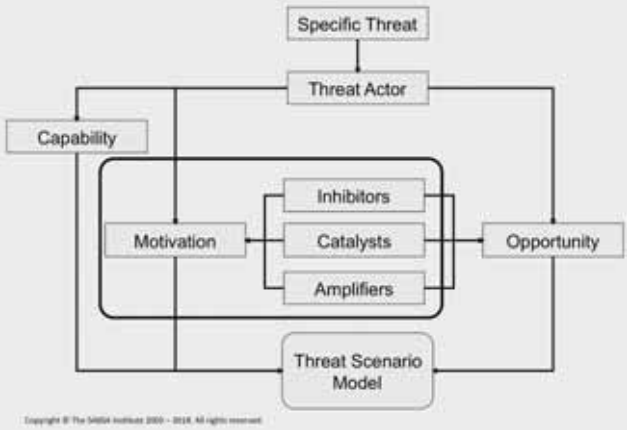


Figure 2 – Threat model

Using SABSA thinking for threat modelling has several advantages: it begins by looking at your business and understanding why an adversary might want to attack you – what's in it for them – their motivation, together with their ability to mount an attack. It then adopts a sound conceptual model of the anatomy of a threat as opposed to vulnerability. Finally it allows you to predict the most likely types of threat and the target assets because you understand what the adversary is trying to achieve. This allows you to focus your defences more effectively and efficiently than if you attempt to cover all possibilities all of the time. Looking at your defences is where vulnerability becomes relevant.

The Attributer

LAST VAN DE BYSTANDER BUG

Hebt u daar nou ook zo'n last van, de Bystander Bug …? Vast wel, zonder dat u het doorhebt. Want waar in de psychologie allang het Bystander effect bekend was, zien we dat nu eigenlijk op dezelfde manier terugkomen in ons aller benadering van nieuwe media.

Ooit was het fenomeen slechts merkbaar als een 'ander' met de auto in het water was beland. Velen stonden er dan omheen, en niemand deed wat. Typisch het Bystander Effect – allen stonden erbij en keken ernaar, wachtend tot iemand anders wèl zou ingrijpen. Zonder besef dat iedereen toch kon worden geacht die ander te zijn; iedereen zou toch al wat hebben kunnen doen. Maar ja, initiatief nemen als die iedereen om ons heen stilstaat en toekijkt… dat bleek niet zo vaak in de aard, de kuddegeest van het beestje te zitten en dus gebeurde het nogal eens dat niemand wat deed.

Open source software

Dit vertaalde zich meer recent naar de benadering van open source software. Daar was toch immers één van de belangrijke kwaliteitswinsten, dat werkelijk iedereen waar ook ter wereld inzage kon hebben in de broncode, die daardoor als vanzelf véél beter was, veel minder bugs bevatte dan closed-source 'proprietary' software. Want ja, als slechts een klein clubje ontwikkelaars kan en wil testen met te weinig tijdbudget, dan blijft er van alles mis met de software die uiteindelijk de wereld in wordt gestuurd. Nee, dan open source: uit den treure getest door Jan en alleman. Toch?

Of… bleek bij diverse bugs die in open source software werden gevonden, dat we er met z'n allen al decennia lang op vertrouwden dat al die anderen het monnikenwerk wel zouden hebben gedaan..? Sendmail, Heartbleed et cetera toonden vooral aan dat zulk vertrouwen zéér wijd verbreid was – iedereen ging er vanuit dat iedereen behalve wijzelf er wel naar gekeken zou hebben. Waarom? Dat mag Joost weten; typisch hoe het Bystander Effect werkt. Eigenlijk is dat een bugje in onze logica, die toch al met zo veel warnings door de compiler komt. Een te groot vertrouwen in de ander. Te weinig zin om zelf zekerheid te verkrijgen.

Netwerk Effect

Maar dat alles lijkt alweer een hele tijd geleden hè? Inmiddels zijn we alweer een fase verder in ons leven. Waarin niet alleen de aller-nerdigsten plotseling overwegen om hun Facebook-account op te zeggen, omdat er (vooral) op een ander continent iets was met de verkiezingen en marketing-spam en … nou ja, iets. Dus maakt iedereen zich zorgen: "Ja, nee, 't is net wat u zegt, ik snap er ook weinig van, maar erg hè dat allemaal?" Bovendien, Facebook verlaten is best lastig (nee hoor!), daarom roept iemand vanuit de EU op om een eigen platform te ontwikkelen. Alsof dat nog kan; het Netwerk Effect verslaan. Terwijl er al zo'n grote samenhang was tussen het Netwerk Effect en het Bystander Effect; denk daar maar eens over na en Google dan nog eens op 'Asch conformity experiment'.
En ziedaar, nu Facebook sleutelt aan de privacy-voorwaarden en standaardinstellingen, denkt een flink aantal van ons (nou ja) al direct weer: "Ah, ze doen iets, dus dan is het wel weer ok", en gaat over tot de orde van de dag. Makke schapen zijn makkelijk te scheren en zelfs Arjan Lubach krijgt de mensen niet mee.

Hoe krijgen we dat voor elkaar?

We willen dus kritisch denken en handelen. Helaas is onze maatschappij daar nogal arm aan. En spiegelt de (privacy-)apathie zich aan de manier waarop in veel organisaties met informatiebeveiliging wordt omgegaan. Geen wonder dat de mens de zwakste schakel wordt genoemd; terwijl iedereen erop vertrouwt dat anderen wel voor informatiebeveiliging zullen zorgen, worden kritische geesten al gauw als veel te lastig bestempeld en monddood gemaakt. Of ze kunnen vertrekken, zodat we allen weer bystander zijn. De enkele goeden niet te na gesproken overigens.
Terwijl er zo veel katten zijn die de bel aangebonden moeten krijgen! Mijn vraag aan u is daarom nu: Hoe krijgen we dat voor elkaar …?

Ir.drs. J. van der Vlugt CISA CRISC, Jurgen, is zelfstandig professional voor information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl

Achter Het Nieuws

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

... Mocht u er nog aan moet beginnen: heel veel succes! Wellicht kunnen onderstaande links u op weg helpen:
https://bit.ly/2BRFHga
https://rvo.regelhulpenvoorbedrijven.nl/avg/#/welkom

25 MEI: DAG VAN DE WAARHEID

Met vrij grote zekerheid ontvangt u dit nummer van uw lijfblad op 25 mei. Een dag als alle andere? Of toch niet? Vandaag treedt formeel de Algemene verordening gegevensbescherming (AVG) ofwel de General Data Protection Regulation (GDPR) in werking in heel Europa. Vanaf deze dag wordt er 'gehandhaafd' door de verschillende toezichthouders. In Nederland is dat de Autoriteit Persoonsgegevens (AP). De afgelopen maanden is er op velerlei fronten aandacht gegeven aan deze nieuwe wetgeving, ook in ons aller lijfblad zijn er al diverse artikelen over dit onderwerp gepubliceerd. Maar is de BV Nederland er echt klaar voor? In de rubriek Achter het Nieuws geven enkele redacteuren hun (ongezouten) mening.


Maarten Hartsuijker


Lex Dunn


Tom Bakker


Rachel Marbus

Rachel Marbus

Niemand is ooit echt helemaal klaar met privacy. En dat is maar goed ook. Het recht op privacy is een fluïde recht, het verandert met de tijd mee. Ooit vonden we - in een ver verleden - de opkomst van de fotografie intens spannend. En dan vooral vanuit de gedachte dat een menselijk portret heel makkelijk vastgelegd kon worden en verspreid via pamfletten. Nu denken we na over de gevolgen van Artificiële Intelligentie en robotisering en wat dat dan allemaal voor privacy, vrijheid en autonomie betekent. En een decennium na nu hebben we weer iets nieuws om over na te denken. En zo heeft elke verdere technologische ontwikkeling weer haar weerslag op privacy en wat wij willen dat ermee beschermd wordt. Het enige dat privacy voor eens en voor altijd heeft vastgelegd, is dat er een beschermde ruimte rondom de persoon is, waar niet zomaar in getreden mag worden. Maar waaruit die ruimte opgemaakt is, dat bepalen we doorlopend samen.

Maarten Hartsuiker

Ik heb nog geen bedrijf horen zeggen dat ze volledig klaar zijn voor de AVG. Het is een deadline als vele anderen: wachten met het in kaart brengen van
acties tot het min of meer te laat is. Om vervolgens flink te schrappen in de ambities om er op 25 mei min of meer klaar voor te zijn. Ofwel: het Minumum Viable AVG-Product. Is dat erg? Nee, wat mij betreft niet. De BV Nederland is nog nooit in zo'n korte tijd zoveel veiliger geworden als de afgelopen maanden. De focus op veiligheid en privacy was en is enorm. Maar veel organisaties zullen uit tijdsdruk veel processen nog handmatig hebben ingericht (denk aan het recht op inzage, verwijdering of bevriezing). En vrezen de workload die hieruit zou kunnen gaan volgen. We zijn er dus nog niet. 25 mei is wat mij betreft geen einddatum, maar een tussenstop waar vanuit versneld zal moeten gaan worden om de bescherming van de gegevens van ons allemaal écht waar te maken.

Tom Bakker

Men verwacht dat ongeveer de helft van de organisaties en instellingen klaar zal zijn op 25 mei. Ik krijg vaak de vraag: "Wat gebeurt er als we niet klaar zijn? Krijgen we dan een boete?" Ik zeg dan dat er niets gebeurt, zolang je geen aan privacy gerelateerd incident hebt. Maar goed, de AVG was al langer van kracht, dus dat is niks nieuws. Er is nog veel onduidelijkheid hoe je de juiste maatregelen moet nemen. Er wordt wel aan gewerkt door werkgroepen om guidance te ontwikkelen. Veel organisaties en instellingen worstelen er toch wel mee. Zo kreeg ik via een bestuurslid van de tennisclub (hij doet de ledenadministratie) de vraag of de ledenlijst op de nieuwe website gepubliceerd mag worden onder het mom van: "Jij hebt er verstand van". Ik zei dat dat niet mag, tenzij je toestemming hebt van de leden. De KNLTB (de Tennisbond) voegde daar nog aan toe: "Alleen als de ledenlijst achter een besloten gedeelte op de website te vinden is." Maar in een uitzending van Radar kwam aan de orde, dat diezelfde bond de persoonsgegevens van hun aangesloten leden aan derden 'verkoopt'. Men spekt daar de kas mee (sponsoren). Is besloten door de ledenraad(?). Volgens de geïnterviewde jurist mocht dat wel. Vreemd. Mij is niets gevraagd. Of heb ik toch iets aangevinkt destijds? Dan nog een uitzending van VPRO's Tegenlicht over algoritmes. Dat gaat nog leuk worden. Op basis van Big (persoons) Data worden de algoritmes gevoed. Iedereen enthousiast over wat er allemaal kan aan voorspellende mogelijkheden. Ik vind het maar eng qua privacy. Hoe past de GDPR/AVG daarin?

Lex Dunn

Is de BV Nederland klaar voor de AVG? Ik denk het niet. Op grond van mijn eigen waarnemingen tijdens congressen en seminars is er vooral veel gepraat over de nieuwe wetgeving, maar zijn lang niet alle bedrijven en organisaties er helemaal klaar voor. Het zal dan ook interessant zijn om te zien hoe de Autoriteit Persoonsgegevens gaat handhaven. En vooral wat het grote publiek zal doen. Er is in de media ruimschoots aandacht gegeven aan de 'nieuwe' rechten van de data subjecten, en wellicht dat deze of gene die rechten in de praktijk wil toetsen. Het sturen van een mailtje (of brief) met de vraag: "Wat heeft u van mij aan data, en waar komt dat vandaan?" is redelijk simpel, maar het beantwoorden van die vraag kan nog een hele uitdaging zijn. Vooral voor bedrijven en organisaties, die te maken hebben gehad met fusies, overnames, samenwerkingsverbanden et cetera kan het nog een hele kluif worden om uit dat zeer diverse applicatie landschap de gevraagde persoonsgegevens boven water te krijgen. Dus: is de BV Nederland klaar voor de AVG: ik denk het niet (maar ik weet zeker dat een aantal privacy specialisten er ondertussen wel klaar mee zijn ;-)

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Tom Bakker
Lex Dunn
Maarten Hartsuijker
Hugo Leisink
Rachel Marbus
Bart van Staveren

BLADMANAGEMENT
MOS bv
Deirdre Bernard
José Broekhuizen
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
Jan van de Vis
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2018 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

Beeld: Shutterstock.com

TO FACEBOOK OR NOT TO FACEBOOK

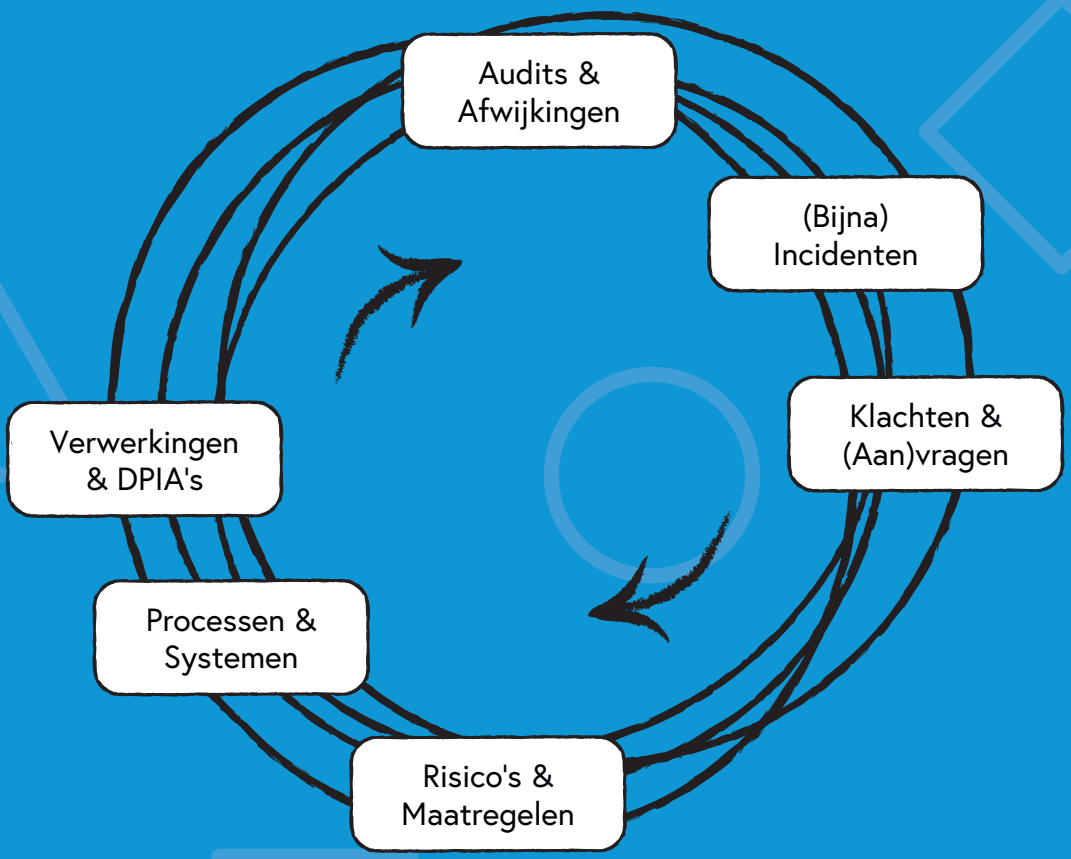
Zoals bekend mag worden verondersteld, hoor je er tegenwoordig niet meer bij als je niet mee doet op social media. Het zal u wellicht verbazen, maar één van de eerste social media omgevingen in Nederland was Hyves. Gemaakt door een paar vrienden die eigenlijk een heel ander doel hadden met de omgeving, en in eerste instantie kwam eigenlijk alleen de familie van deze makers op de omgeving.
De makers hadden het gevoel dat Hyves wel eens een succes kon worden, en met hun collega studenten uit Amsterdam werd Hyves populair in de omgeving Amsterdam. In 2004 waren 3.000 'vrienden' actief op Hyves. Vanaf 2005 verdubbelde het aantal leden bijna iedere week en halverwege 2005 waren er een miljoen leden. Het ging dus snel, maar toen Jan Peter Balkenende lid werd, was het hek helemaal van de dam. Uiteindelijk waren er 10 miljoen leden en verkochten ze alles aan TMG (Telegraaf Media Groep). Toen kwam Facebook op en haalde Hyves in. Hyves stopte en Facebook groeide door naar meer dan 2 miljard leden. Het verdienmodel was eenvoudig: tegen betaling kunnen bedrijven gericht adverteren en daarbij is de informatie over hun potentiële klanten natuurlijk van zeer groot belang. Zelfs onze zorgverzekeraars schromen niet om zogenaamde 'tracking pixels' te plaatsen, waarmee informatie verzameld wordt. Als je dat als klant niet wilt, stop je gewoon met Facebook en wordt er geen data meer doorgesluisd. Wat echter niet mag, is data van je klanten stiekem doorsluizen naar bedrijven of deze data laten verrijken en dan verkopen. Daar ging Facebook de fout mee in! Zij verkocht meer dan 90.000.000 klantgegevens aan een gespecialiseerde club die een vertrouwd aandoende naam heeft: Cambridge Analytica. Cambridge Analytica interpreteerde de gegevens echter alleen maar met het doel om klantdata beter te kunnen aanbieden aan adverteerders of politieke groeperingen. Die op hun beurt veel beter en gerichter hun boodschappen kunnen verspreiden, om op die manier op een ongeoorloofde manier voordeel te halen tijdens, bijvoorbeeld, verkiezingen. Trump zou op die manier best eens de Amerikaanse verkiezingen gewonnen kunnen hebben, louter en alleen door dit soort manipulaties en het verspreiden van nep nieuws om de meningen van de kiezers te kunnen beïnvloeden. Doet Facebook dit allemaal illegaal? Niet alles. Het gebruik van data van Facebookers om op die manier de juiste advertenties te kunnen tonen, is toegestaan. Zoek maar eens naar een wasmachine en je komt op diverse sites advertenties over wasmachines tegen. Het verkopen van data zonder dat de gebruiker dat weet, is wel verboden. Alle 'vrienden' erbij verkopen eveneens. Zal het daarmee stoppen? Nee hoor, al in 2015 werd de enorme bak met gegevens verkocht, het werd pas wereldkundig in 2018. Zit er meer in de pijplijn? 100 procent zeker! Wat kan ik er aan doen? Niets meer. Gewoon met onmiddellijke ingang afscheid nemen van Facebook en je 'vrienden' vragen hetzelfde te doen.
Het vervelende is, dat het Facebook eigenlijk allemaal niet zoveel uitmaakt; Zuckerberg moest op het matje komen bij de Amerikaanse Senaat en komt er, na een dagje "Sorry!" roepen, achter dat zijn vermogen aan het eind van de dag een aantal miljarden hoger is.

Ik zit niet meer op Facebook, dus zoek mij niet. Mark Zuckerberg heeft nu nog maar 106.814.391 volgers.

Berry

De meest complete Privacy / AVG / GDPR Software

smile



- Makkelijk en veilig in gebruik
- Voor en door gebruikers ontwikkeld
- Juridisch beproefd
- Completer dan andere systemen
- SaaS en OnPremise geleverd

Start nu gratis! Kijk snel op: privacysuite.eu