iB

INFORMATIEBEVEILIGING

jaargang 18 - 2018

#5

1.500.000 collega's gezocht

Aan de slag met NIS NIB

SIEM lessons learned bij autoturven

Blog: Vrouwen in de cybersecurity

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

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

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers

HET GAAT GOED MET IB

In iB1 van dit jaar kondigde Tom Bakker aan dat elk nummer door een andere redacteur in de rol van hoofdredacteur begeleid zou gaan worden. Helaas is dat ons niet helemaal gelukt. In iB2 deed ik een oproep om nieuwe redactieleden te zoeken. En dat is ons wel gelukt! We hebben een heleboel reacties gehad en de redactie van iB is behoorlijk uitgebreid. In iB3 meldde Tom nog dat er twee nieuwe redacteuren waren gevonden, maar ondertussen staat de teller al op zeven (jawel, 7)! In dit nummer stellen Bianca Brooijmans, Nicole van Deursen en Chris de Vries zich alvast aan u voor, in het volgende nummer volgen de anderen.
Ook moet ik u op deze plek verontschuldigingen aanbieden voor de misser aan het einde van iB4: ondanks zorgvuldige controle en een correcte proefdruk ging er toch iet mis en werd de column van Berry (Een nieuwe bril) twee keer afgedrukt.

Onze herhaalde oproepen om artikelen hebben hun vruchten afgeworpen. Het zal u niet vreemd voorkomen dat we ook dit keer weer aandacht voor de AVG hebben: een onderzoek naar aanbieders van AVG gerelateerde diensten en het toekomstperspectief van Privacy Management. Ook aandacht voor de informatiebeveiliger: SVB zoekt 1.500.000 collega's (?) en Vrouwen in Cybersecurity (ja, die zijn er ;-). Tevens komen ICS (SCADA of OT) netwerken en systemen aan de orde. En de gebruikelijke columns van Rachel Marbus, de Attributer en natuurlijk Berry.

Tot slot: helaas is de zomer alweer voorbij, maar we kunnen ons verheugen op het jaargetijde van de beurzen, tentoonstellingen en seminars. Als u dit leest, is het jaarlijkse Security Congres van PvIB, NOREA en ISACA NL Chapter alweer achter de rug en zijn we onderweg richting de InfoSecurity beurs in Utrecht. Wellicht zie ik u daar. Ik wens u in elk geval veel leesplezier met deze uitgave van iB.

Lex Dunn

In dit nummer

ONLINE COMMUNICATIE OVER DE AVG

Begin 2018 gebeurde wat al langer was voorspeld. De vraag naar en het aanbod van AVG-diensten kwam in een stroomversnelling. Op niet eerder voorgekomen wijze en schaal werd offline en online geadverteerd voor de meest uiteenlopende diensten en oplossingen die allemaal iets met de AVG te maken zouden hebben. Het was een interessant en leerzaam proces om te volgen, temeer daar vanuit Europa nog meer ingrijpende maatregelen te verwachten zijn.

Onderzoek

De meeste IB'ers hebben echter vanaf januari weinig tijd zich in de kwaliteit en kwantiteit van de uitingen te verdiepen, voor hen is het immers alle hens aan dek om klanten te helpen de deadline te halen. CompLions-GRC uit Deventer heeft een goede aanleiding hier wel bij stil te staan. De medewerkers worden tijdens de gesprekken met klanten en prospects namelijk in toenemende mate geconfronteerd met onbekende partijen en oplossingen. Daarbij is meerdere keren te horen dat aan de vraagzijde verwarring heerst en men door de bomen het bos niet meer kan zien.

Om te begrijpen wat er aan de hand is, wordt daarom de opdracht gegeven voor onderzoek naar de manier waarop online over de AVG wordt gecommuniceerd en geadverteerd. Eerste doel van het onderzoek is te achterhalen met welke boodschappen potentiële afnemers van AVG-diensten online in contact komen en van wie die zijn. De resultaten zullen primair voor intern gebruik worden aangewend.

Door de bril van

Bij het bepalen van de scope van het onderzoek is ook met de opdrachtgever afgestemd dat de gekozen invalshoek niet de techniek mocht zijn. Omdat de AVG iedereen in een organisatie raakt en een onderwerp is voor bij de koffiemachine wordt uitgegaan van "iedereen is op zoek naar informatie". Er wordt dus nadrukkelijk niet naar de communicatie gekeken door de bril van alleen een CISO, CTO of IB'er.

Methode

Het onderzoek heeft een eenvoudige opzet. Een aantal veel voorkomende zoektermen en zinnen is geselecteerd. Deze termen bestaan uit de feedback van eerdere gesprekken met marktpartijen en zijn gereduceerd tot die zoektermen. Die worden ingevoerd in zoekmachines waarbij de automatische aanvullingsopties aanstaan. Dat leidt tot zoekbegrippen als "AVG voor het MKB" en "Hoe word ik GDPR compliant". Deze termen worden op verschillende manieren en tijdstippen in zoekmachines ingevoerd. Hiervoor wordt gebruik gemaakt van zowel computers, tablets als smartphones met verschillende operating systems. Het online gaan gebeurt via verschillende VPN-aanbieders en gaat zowel via kabel, xDSL als twee mobiele netwerken. Van de meeste devices worden na elke zoeksessie de cookies verwijderd.

Naast het gericht zoeken wordt met meerdere identiteiten op Twitter en LinkedIn gevolgd wat er aan pushberichten over de AVG/GDPR voorbij komt. Dit alles levert binnen een week een forse hoeveelheid input, die te herleiden is tot ongeveer 80 verschillende websites of bedrijven. Die input wordt vervolgens uit praktische redenen gelimiteerd. Aanvankelijk is het de bedoeling de uitingen van de 50 meest genoemde bedrijven verder te analyseren. Dat blijkt echter zoveel tijd te vergen dat dit wordt teruggebracht tot 36 websites, dat komt ongeveer overeen met de eerste drie pagina's zoekresultaten.

Onduidelijkheid troef

Een van de redenen waarom het in kaart brengen van de 50 meest genoemde aanbieders van AVG-diensten zo veel tijd vergt, is dat een deel van de websites uitblinkt in onduidelijkheid. Geringe transparantie is een rode draad die door het hele onderzoek loopt. Ook bij de beperking tot 36 websites moet worden vastgesteld dat één op de zes websites sterk de indruk geeft dat de dienstverlening die online wordt gepromoot bij nader inzien weinig met de AVG te maken heeft. Wat hier zichtbaar wordt, is zowel de kracht van SEO als de mogelijkheid een veelgebruikte term te claimen voor iets anders.

Wat verder opvalt is dat een deel van de ondernemers die via de zoekmachines en pushmeldingen een hoge ranking heeft, niet actief is op de Nederlandse markt. Dit ondanks het feit dat de Nederlandse taal steeds leidend is bij de zoekopdrachten en aangenomen online identiteiten. Bij nadere bestudering is die groep in te delen in AVG-dienstaanbieders die vooral internationale bedrijven als doelgroep zien en een aantal aanbieders die vooral op zoek is naar resellers. Dat die laatste categorie de nodige verbazing wekt, spreekt voor zich.

Nadat de top 36 is vastgesteld en voor een eerste keer onder de loep is genomen, valt nog iets op. Een aantal bekende namen uit de Nederlandse IT- en consultancysectoren ontbreekt. Waarom dat het geval is lijkt alleen maar te verklaren te zijn door de spaarzame online activiteiten. Dat is een lastige conclusie, mede omdat ze voor andere diensten wel goed vindbaar zijn.

Twee indelingen

Geprobeerd is de groep met 36 websites te categoriseren. Dat is gedaan om duidelijker te krijgen met wat voor soorten bedrijven, die AVG-diensten aanbieden, een brede groep geïnteresseerden in contact komt. Dit levert zeven verschillende soorten aanbieders op, die als negen categorieën zijn weergegeven:

- Accountants – big 4
- Accountants – top 10
- Privacy- en AVG-consultants
- Overige consultants
- Detacheerders
- Big 5 IT-dienstverleners

Rashid Niamat is journalist en schrijft onder andere voor ISP Today. Rashid is te bereiken via rashid@niamatmediagroup.nl

- Generieke IT-dienstverleners
- Bijzondere securitydiensten
- Auditors

Als controleslag is de indeling nog langs de oorspronkelijke 80 websites gehouden. Alle serieuze bedrijven lijken daarmee in te delen. Iemand op zoek naar ondersteuning om AVG compliant te worden zal een dergelijke indeling waarschijnlijk ook herkennen en al dan niet bewust hanteren om een match te vinden.

Wat hij ongetwijfeld ook zal doen, is kijken naar de werkterreinen. Dan stelt hij de vraag wat de corebusiness of de focusgebieden van deze AVG-specialist is. 36 websites en een handvol zoekwoorden ingeven, levert deze tabel op.

- Financiële consultancy
- Verandermanagement
- Juridische consultancy
- Overige consultancy
- End-user communicatie
- IT-diensten
- Bijzondere security diensten

Deze tweede tabel helpt te begrijpen waar het eerder genoemde "door de bomen het bos niet meer kunnen zien" vandaan komt. Om AVG compliant te worden en blijven is een brede focus nodig. Dat komt ook naar voren door het ingeven van zoekwoorden. Een aantal van de gevonden specialismen dat dan naar boven komt, zal de nodige vragen oproepen, helemaal na het lezen van de online uitingen. Menigeen zal zich afvragen of hij ook met dit soort partijen contact moet opnemen, want ze lijken onmisbare diensten te verlenen. Het vinden van een eensluidend en helder antwoord op de websites en profielpagina's is flink lastig gebleken. Om dat te illustreren is langer stilgestaan bij de drie laatste categorieën.

Bouwblokken

Tijdens het onderzoek zijn meerdere bedrijven gevonden die "end-user communicatie" als focus hebben. De aandacht daarvoor is terecht. Consumenten krijgen immers meer mogelijkheden voor inzage in wat er over hen is opgeslagen en het recht data te laten wissen. Dat impliceert dat tal van front- en backoffice handelingen moeten worden aangepast. Die processen en de feitelijke communicatie hierover naar klanten en interne organisaties is een specialisme waarin door deze categorie wordt voorzien. Hoewel erg veel aandacht aan deze aspecten van de AVG wordt besteed, betreft het maar een deel van de veranderingen die door de AVG noodzakelijk worden.

Een andere groep bedrijven die een rol claimt bij AVG compliant worden, zijn de IT-dienstenleveranciers. Dit is een brede noemer voor bedrijven die alles leveren en onderhouden van netwerkinfrastructuur tot werkplekken. Deze bedrijven wijzen terecht op bijvoorbeeld de noodzaak van veilige opslag, transport en verwerking van data. Het zijn belangrijke onderwerpen, maar net als de communicatie is het een beperkt deel van de plichten en taken die te linken zijn aan de AVG.

Tenslotte zijn er nog de echte security vendors. Uit de websites en profielpagina's blijkt dat zij de AVG meenemen als een extra aandachtspunt. Zij gebruiken de AVG opvallend vaak om naast de hardware en software ook consultancy te leveren. De manier waarop zij communiceren, valt tijdens de onderzoeksperiode mede op omdat zowel grote als kleine aanbieders erg makkelijk FUD (Fear, Uncertainty and Doubt) inzetten. In een aantal gevallen leek de websitebezoeker zelfs op het verkeerde been te worden gezet door te suggereren dat met een enkel product of dienst alles zou zijn geregeld. Of hier sprake was (of is) van slordigheid of onkunde valt buiten de scope van het onderzoek.

Wat deze drie categorieën gemeen hebben, is dat ze als noodzakelijke bouwblokken gelden. Ze zijn onmisbaar om organisaties AVG compliant te krijgen. Als bouwblokken komen ze echter pas tot hun recht in een groter geheel. Het zijn nadrukkelijk geen losstaande of universele oplossingen. Of iedere website bezoeker dat tijdig door heeft, valt te betwijfelen

Doelgroepen

De potentiële afnemer zal waarschijnlijk verder nog kijken naar het soort klanten waarmee de aanbieder van AVG dienstverlening gewend is te werken. Websites die melding maken van klantgroepen door te verwijzen naar klantcases, noemen bijna allemaal overheden als actieve klanten. Zorginstellingen en financials worden ook met enige regelmaat genoemd. In scherp contrast hiermee staat het aantal verwijzingen naar het reguliere MKB. Zelfs het MKB+ wordt opvallend weinig genoemd als klantgroep. Dat enterprises of internationals weinig worden genoemd is minder opvallend, zij zullen eerder bij de Big 4 uitkomen. Tenslotte valt op dat er onder de 36 websites slechts twee aanbieders zijn die specifiek NGO's en not-for-profits als doelgroepen vermelden. Het selecteren van de juiste aanbieder op basis van ervaring met de sector of bedrijfsomvang is daarmee op basis van de online uitingen en referenties voor de meeste MKB ondernemers best lastig.

Hoewel er goede redenen zijn het criterium klantgroep te laten meewegen bij een beslissing, is er in het geval van de AVG-communicatie een belangrijke beperking. In de meeste gevallen is ten tijde van het onderzoek niet bekend of de genoemde klanten te linken zijn aan AVG-trajecten. In de klantcases die als downloads of persberichten voorhanden waren, was de AVG bijzaak en niet hoofdzaak.

Aanbod

Op basis van de websites en andere bronnen is vanuit prospect perspectief ook op zoek gegaan naar het antwoord op de vraag: "wat leveren deze bedrijven concreet?" Die vraag leidt tot een onwerkbare en onvergelijkbare hoeveelheid informatie. Het gebrek aan transparantie is zeer nadrukkelijk zichtbaar. Daarom is de vraag vervangen door de vier volgende:

- Levert men een complete analyse en inzicht in processen en techniek?
- Wordt de kennis (realtime) bijgehouden of is het een momentopname?
- Is er sprake van kennisoverdracht, zodat de klant het zelf kan bijhouden?
- Is het een standalone dienst of kan het met andere diensten gecombineerd worden?

De vragen zijn sturend in de zin dat ze overeenkomen met wat het C-level waarschijnlijk wil weten.
Door deze vier vragen wordt ook duidelijk dat het eerdergenoemde categoriseren (dat ook door de aanbieders zelf wordt gedaan!) te grofmazig is. Feitelijk blijkt binnen elke categorie een scheidslijn te lopen die te maken heeft met de mate waarin uren schrijven de basis van de dienstverlening is. Dat lijkt grotendeels te verklaren waarom sommige diensten eigen kennis en inbreng door de afnemer meer benadrukken of als USP benoemen. In andere gevallen wordt daar minder helder over gecommuniceerd.

Footprint

En dan is er nog de footprint, een component waar waarschijnlijk weinig bij wordt stilgestaan. Een behoorlijk deel van het aanbod dat via Google.nl, adwords, advertenties en artikelen aan Nederlandse ondernemers is getoond tijdens de onderzoeksperiode heeft nadrukkelijk niet de Nederlandse lezer als doelgroep op het oog. Deze formulering is niet bedoeld als diskwalificatie.
Het wordt genoemd omdat er vooralsnog weinig reden is aan te nemen dat deze organisaties, die bijna uitsluitend in het Engels communiceren, de Nederlandse verhoudingen begrijpen. Dat een aantal ondernemers zich nadrukkelijk positioneert als partner voor Amerikaanse ondernemers met klanten in de EU doet de vraag opkomen of hier sprake is van partijen die de Nederlandstalige markt bedienen.

Belangrijk signaal

Het zal na voorgaande niet verbazen dat twee brancheorganisaties, Nederland ICT (1) en VNO-NCW (2), in januari 2018 het belangrijke signaal hebben afgegeven niet zomaar op elk aanbod in te gaan. Dat is in lijn met de bevindingen van dit onderzoek en met wat recent nog via een duidelijke waarschuwing van de toezichthouder is bekend gemaakt (3). Tijdens de testperiode zijn meerdere bedrijven opgevallen waarvan de SEO inspanningen (die soms al jaren terug zijn gestart!) indrukwekkender zijn dan de geclaimde kennis en dienstverlening. Wat precies wordt geleverd, is lang niet altijd duidelijk. Wie online op zoek is naar informatie over tijdsbeslag of een prijsindicatie komt in bijna alle gevallen van een koude kermis thuis.

Het gebrek aan transparantie en vooral het aantal minder serieuze aanbieders is reden geweest met de opdrachtgever van het onderzoek te overleggen of de markt niet gewaarschuwd moet worden. Besloten is dat niet te doen, maar het voor interne doeleinden bedoelde verslag online (4) te plaatsen. Met het verslag kan eenieder een indruk krijgen van het aanbod voor AVG-diensten zoals dat begin 2018 online zichtbaar was. Zij zullen begrijpen waarom het voor de meeste geïnteresseerden makkelijk was door de bomen het bos niet meer te zien. Het is nog steeds voor niet-professionals lastig een goed beeld te krijgen van het relevante aanbod.

Gelukkig zijn er lichtpuntjes. Er zijn aanbieders die wel serieus zijn en transparant communiceren over wat zij leveren en met welke doelgroepen een match mogelijk is. Er is een checklist opgenomen die de lezer helpt bij het maken van de voor hem juiste keuzes.

Links

(1) www.nederlandict.nl/diensten/helpdesk-avg
(2) www.vno-ncw.nl/forum/zo-bereid-je-je-als-ondernemer-voor-op-de-nieuwe-privacy-wet
(3) www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-waarschuwt-voor-misleidend-avg-keurmerk
(4) www.complions-grc.com

1.500.000 COLLEGA'S GEZOCHT!

Dat was de titel van de wervingscampagne bij de SVB om medewerkers te vinden die een stap durven te maken naar de boeiende wereld van Privacy of Informatiebeveiliging. Heeft de SVB dan zoveel medewerkers nodig? Nee gelukkig niet, maar volgens de kenners is dit het aantal medewerkers wat er de komende jaren wereldwijd extra nodig is om de ontwikkeling van de digitale dreigingen het hoofd te bieden. En daar wil de SVB een steentje aan bijdragen. Daarnaast past het goed binnen het mobiliteitsprogramma waarbinnen de SVB haar medewerkers stimuleert om zich te ontwikkelen en te bewegen, binnen- en buiten de SVB.

Het doel van de wervingscampagne bij de SVB was om 10 medewerkers te vinden die zich wilden omscholen tot Privacy Coördinator of Information Security Officer. Niet alleen vakkennis, maar echt voldoende vaardigheden bijbrengen om het vak volwaardig te kunnen uitoefenen, al dan niet bij de SVB zelf. Men dacht in eerste instantie aan ongeveer 10 medewerkers, maar dat pakte anders uit.
De eerste berichtgeving op intranet en de narrow-casting binnen de SVB leverde dermate veel belangstelling op dat er in plaats van één, uiteindelijk twee informatiesessies werden georganiseerd. In totaal kwamen er ongeveer 150 medewerkers op die sessies af. Kennelijk was de wervende tekst succesvol geweest. Iedere sessie duurde 2 uur en in die tijd legde Jaap Halfweeg (CISO) uit wat het traject behelst en wat de vakgebieden globaal inhouden. Daarbij werden niet alleen de positieve aspecten van deze vakgebieden belicht, maar ook de minder leuke kanten. Hedy Wijdoogen (HR) gaf een toelichting op de kosten en de eigen bijdrage van het traject en hoe de selectie van deelnemers zou gaan plaatsvinden. Daarna was er een interactieve pub-quiz en sloot men af met een borrel, waarbij meerdere bestaande ISO's en Privacy Officers aanwezig waren om vragen te beantwoorden.

Kennismaken met IB en Privacy

Uiteindelijk waren er 50 medewerkers die belangstelling hadden voor de opleiding. Dit overtrof alle verwachtingen. De bedoeling was dat uit deze groep een selectie gemaakt zou worden voor het volgen van een 'snuffel'-cursus. Een tweedaagse kennismakingscursus die er op gericht was om de medewerkers een heel goed beeld te geven van de inhoud van de opleiding en de vakgebieden en daarnaast om de deelnemers te beoordelen op geschiktheid. Dat laatste was van tevoren bij de deelnemers bekend. Daarom zaten er ook interactieve sessies in, zoals het spelen van het CIP Cyber Crisis Game. Het resultaat was dan ook een advies aan de kandidaten. Deze snuffelcursus werd verzorgd door een extern bureau.

Omdat de belangstelling zo groot was, besloot de SVB om alle gegadigden uit te nodigen voor de snuffelcursus. Dit omdat daarmee toch een grotere en gemotiveerde groep (50 personen) een hoger kennisniveau van Privacy en IB zouden krijgen, wat op zich al een waarde heeft voor de organisatie. Er werden drie groepen gevormd die afzonderlijk van elkaar de training kregen. Om deel te mogen nemen moest men wel een motivatiebrief schrijven en werden een aantal eisen gesteld. Zo was het een vereiste dat men Engels kan lezen en dat men toch wel een HBO werk/denkniveau bereikt moest hebben.
De snuffelcursus was een succes en uit de cursus gaven uiteindelijk 33 medewerkers zich op voor de opleiding. Om definitief ingeschreven te worden, moesten alle medewerkers een assessment (via internet) doorlopen om te toetsen of ze over de juiste competenties en het vereiste

Jaap Halfweeg is sinds 2 jaar werkzaam bij de SVB in de functie van Chief Information Security Officer. Hij is verantwoordelijk voor alle aspecten van informatiebeveiliging, business continuity en privacy. Jaap is bereikbaar via JHalfweeg@svb.nl.

werk/denkniveau beschikken. Alle 33 medewerkers kregen een persoonlijk gesprek. Wat SVB verraste was dat veel medewerkers al langer met een belangstelling voor Privacy en/of IB rondliepen of zelfs al met een eigen traject bezig waren. Er bleek dus een groep verborgen talenten in de organisatie te zitten. Daar kom je dus ook niet eenvoudig achter en alleen door individueel te praten vind je die groep.

Een groep vol diversiteit

Van de 33 medewerkers bleken er uiteindelijk 28 geschikt te zijn. 15 voor IB en 13 voor Privacy.
De verscheidenheid was groot. Deelnemers kwamen uit alle 'windrichtingen' van de samenleving en hadden de leeftijd variërend van 29 tot 60 jaar. Voor de IB-kant was er maar één vrouw en de rest mannen. Voor de Privacy kant hadden weer meer dames dan heren belangstelling.
De SVB had initieel het idee dat een groep van 10-12 haalbaar moest zijn. Echter na overleg met de interne stakeholders werd besloten dat alle 28 in opleiding konden gaan. In eerste instantie moesten medewerkers een eigen bijdrage betalen. Toen dat fiscaal lastig bleek, heeft SVB ervoor gekozen dat alleen medewerkers een deel van de kosten terug moeten betalen, als zij de studie niet afmaken.

Twee intensieve ' in-house' opleidingen

De twee opleidingstrajecten zijn inmiddels in volle gang en worden gehouden op de vrijdag bij de SVB zelf. De Privacy-opleiding duurt 15 dagdelen met veel huiswerk en de IB-opleiding duurt 33 hele dagen. Voor beide richtingen zijn externe partners aangetrokken die deze trajecten verzorgen. De doelstelling is naast het doceren van vakinhoudelijke privacy- en IB-kennis, ook een aantal andere onderwerpen aan de orde te stellen. Het gaat daarbij om zaken als beroepsethiek, communicatie met management en schriftelijk/mondeling rapporteren. Gedurende de opleiding wordt ook geoefend met het oplossen van echte cases, het uitvoeren van riskassessments en PIA's. Daarnaast zijn er meeloopdagen georganiseerd waarbij de deelnemers een of meerdere dagen meelopen met specialisten binnen en buiten de SVB. Daarvoor zijn er al contacten met de Amsterdam IT Circle en collega organisaties zoals het UWV. Eén deelnemer start binnenkort met een 6 maanden durende stage bij het Openbaar Ministerie.
Beide richtingen worden afgesloten met een formeel examen. In het geval van de Privacy is dat een internationaal erkend CIPP/e certificaat en in het geval van de IB-richting zijn er twee opties: een CISSP examen (niet het certificaat) voor de meer IT gerichte deelnemers en het CISM examen voor de wat algemenere IB gerichte deelnemers. Het volledige certificaat is niet haalbaar, omdat men niet over de vereiste vijf jaar praktijkervaring beschikt. Desondanks geeft dit hen aanzienlijk meer kans op de arbeidsmarkt. Het halen van de examens is echter niet het hoofddoel van de opleiding.
De IB deelnemers zijn lid geworden van het PvIB en hebben zich allen ingeschreven bij het CIP en het Information Security Forum (SVB is lid). Een van de deelnemers gaat dit jaar mee naar het jaarlijkse ISF Congres in Las Vegas. De selectie voor het congres is middels een loterij uitgevoerd. Voorwaarde is dat deze persoon een presentatie aan de hele groep geeft na terugkomst.

Kennis in de praktijk brengen via werkervaringsplekken

Als onderdeel van het SVB mobiliteitsprogramma kent de SVB zogenaamde werkervaringsplekken (WEP). Dit is om medewerkers tijdelijk ervaring op te laten doen in ander werk en waarbij uiteindelijk een definitieve aanstelling soms ook mogelijk is. Sinds januari zijn er vijf Privacy WEP plekken beschikbaar en vier voor IB. Alle plekken zijn vanuit de opleidingstrajecten gevuld en in veel gevallen zal dit leiden tot een vaste aanstelling. Dit levert ook een aanzienlijke besparing op aan wervingskosten. De verwachting is dat de SVB nog meer kandidaten kan gebruiken. De SVB denkt aan een tweede ronde (er is al een wachtlijst) waarbij ook gekeken wordt om dit samen met nog een aantal andere bedrijven te doen. Binnen de SVB is men trots op het feit dat men met deze opleidingen inspeelt op uitdagingen van nu: die van de eigen mobiliteit, voldoende IB- en Privacy-specialisten binnen de eigen organisatie en helpen om het wereldwijde tekort te verminderen. Al is dat laatste natuurlijk slechts een druppel op een gloeiende plaat.

Tips & lessons learned bij het ontwikkelen van een studieprogramma IB & Privacy:

- Er zitten meer medewerkers met potentieel in je organisatie dan je zou vermoeden;
- Het wervingstraject levert al veel awareness op bij diegenen die belangstelling tonen en zorgt voor een olievlekwerking;
- Geef een reëel beeld over de vakgebieden, dus niet alleen een positief verhaal;
- Breng een incentive aan om de cursus af te maken (eigen bijdrage, of zoals SVB het nu heeft georganiseerd met het terugbetalen van gemaakte kosten);
- Denk goed na over de inhoud van het opleidingspakket. Het doel is niet alleen stof te behandelen waar men het examen mee haalt, maar vooral ook om de functie later goed uit te kunnen voeren;
- Gebruik je netwerk voor stageplekken;
- Richt een eigen stand-alone plek in waar men met pen-test tooltjes kan oefenen.

Mr. Rachel Marbus
@rachelmarbus op Twitter

NOSTRADAMUS

Iedereen heeft van die momenten in het leven waarop je denkt "auw, dat is jammer zeg, dat valt me toch een beetje tegen". Dat moet toch ogenschijnlijk ook het geval zijn geweest voor heel veel mensen nadat 25 mei voorbij gegaan was zonder dat er ook maar iets bijzonders gebeurde. Voor mijzelf was het ook in het geheel niet indrukwekkend, maar dat kwam vooral omdat ik vlak voor 25 mei van de dokter te horen kreeg dat ik voorlopig niet meer mocht werken en niet eens aan werk mocht denken. De dag werd voor mij daarmee een rustdag, waarvan ik eigenlijk ook niet eens meer weet wat ik nu precies gedaan heb.

Maar goed, je hoeft ook geen Nostradamus te zijn om te kunnen voorspellen dat 26 mei en de dagen erna flink zouden gaan tegenvallen. Hypes duren altijd maar kort en daarna dondert de aandacht weer heel snel terug naar een plateau-niveau. Nu hoop ik natuurlijk dat het basisniveau wel wat hoger is geworden dan voor de hype en als je over een lange periode terugkijkt, is dat ook zeker het geval. Waar twintig jaar terug eigenlijk alleen academici debatteerden over het recht op privacy, zie ik dat nu eigenlijk bijna iedereen wel – noodgedwongen – met privacy bezig is. Of het debat daarmee altijd even scherp is en of de juiste klemtoon wordt gelegd? Daarover valt ook weer te debatteren…

Maar even terug naar die relatieve stilte die er nu heerst over privacy. Laat je niet in slaap sussen en voor de gek houden door mensen die zeggen dat het allemaal wel weer een onsje minder kan met die privacy (helaas zijn die er alweer/nog steeds). De wet is echt strenger dan we gewend waren onder de voorgaande privacywet en de toezichthouder is zich aan het hergroeperen. Met veel meer mensen. En die gaat echt niet stil blijven zitten. Natuurlijk heb ik liever dat iedereen, net zoals ik, een echt privacygekkie is en vanuit het hart en de ethiek naar de privacy van personen kijkt. Maar dat is natuurlijk niet zo en dus hier toch even het waarschuwende 'er gaat echt handhaving komen'-vingertje. Ik hou er ook meteen weer mee op hoor.

Feit is dat privacy nu bijna meer dan ooit, een noodzakelijke voorwaarde is voor onze vrije samenleving. En dat het ook niet meer weg te denken is uit de normale bedrijfsvoering en het overheidsleven. Overal wordt nog steeds naar privacyhelden gezocht die de boel in goede banen moeten leiden. En gelukkig komen er steeds meer specialisten bij. Zelf ben ik langzaam weer een beetje begonnen met werken en dat is heel erg fijn, want maanden niet aan privacy denken is voor mij een beetje teveel van het goede. Ik heb er zin in, want voor een specialist is de periode na nieuwe wetgeving eigenlijk de allermooiste die er is. Nu gaan we namelijk pas echt praten over de reikwijdte van die nieuwe wet en wat dat dan allemaal betekent in de praktijk.

VIJF STAPPEN OM DE VEILIGHEID VAN UW INDUSTRIËLE CONTROLE-SYSTEEM TE EVALUEREN

Het eerste artikel in iB3 van Ilan Barda, CEO van Radiflow, ging in op de integratie van cyber security en fysieke beveiliging om een betere bescherming van OT-netwerken te bewerkstelligen. Dit artikel behandelt vijf stappen om de veiligheid van uw industriële controlesysteem te evalueren.

Afgaand op de omvang van cyberaanvallen op organisaties die industriële controlesystemen (ICS, Industrial Control Systems) gebruiken, mogen we ervan uitgaan dat de kans groot is dat iemand zal proberen om uw systeem te hacken en storingen te veroorzaken die de veiligheid en betrouwbaarheid van het netwerk beïnvloeden. De vraag is niet óf, maar wanneer dit gebeurt.
Om zo'n aanval en de gevolgen ervan te voorkomen, raad ik bedrijven die industriële controlesystemen gebruiken aan om een eenvoudige veiligheidscontrole uit te voeren op hun ICS-netwerken, voordat ze een duur adviesbureau inhuren. Deze elementaire veiligheidscontrole bestaat uit een aantal eenvoudige stappen. U heeft hiervoor geen specifieke kennis van cyber security nodig, maar u moet de controle wel goed voorbereiden. In het algemeen wordt bij een veiligheidscontrole gekeken of het netwerk zich gedraagt zoals ontworpen, en of er geen zwakke plekken zijn die processen kunnen beschadigen of verstoren of de

netwerkactiviteit veranderen. Vijf stappen om een veiligheidscontrole met succes te doorlopen:

1. controleer het bestaande netwerkplan;
2. leg het netwerkverkeer vast;
3. verwerk de vastgelegde gegevens;
4. vergelijk de verwerkte gegevens met het netwerkplan;
5. spoor zwakke plekken in het netwerk op.

Controleren van de geplande netwerkstructuur

Bij de controle van de netwerkstructuur maakt u onder andere een grondige analyse van het netwerkplan van uw ICS, met een focus op de onderliggende architectuur van het ICS-netwerk: de integratie tussen de IT- en de OT-netwerken, leveranciers, interne verbinding, externe verbindingen, onderhoudswerkzaamheden etc.
Nadat de beheerder deze structuur goedgekeurd heeft, kunt u overgaan tot de volgende stap.

Vastleggen van netwerkverkeer

Het doel van de tweede stap is te begrijpen wat er daadwerkelijk binnen het ICS-netwerk gebeurt. Al het netwerkverkeer binnen het ICS wordt vastgelegd met behulp van een apparaat dat op uw netwerk aangesloten wordt via mirroring op een passieve poort (om verstoring van het netwerk te voorkomen). Zodra het apparaat met een switch verbonden is en de port mirroring op de switch geconfigureerd is, wordt al het netwerkverkeer vastgelegd met behulp van tools als TCPdump.

Verwerken van de vastgelegde gegevens

Deze stap is bedoeld om het vastgelegde verkeer zichtbaar en leesbaar te maken, zodat het vergeleken kan worden met de netwerkstructuur die oorspronkelijk gepland was. Met behulp van een tool als Wireshark kan de beheerder PCAP-bestanden op een intuïtieve manier bekijken en inzicht krijgen in het gedrag van het netwerk.
Om het daadwerkelijke verkeer te kunnen vergelijken met het netwerkplan moeten onder andere de volgende gegevens verwerkt worden:

- de communicatie tussen apparaten;
- het soort protocollen tussen apparaten;
- de poorten die tijdens elke sessie gebruikt worden, inclusief informatie over de functiecodes voor industriële protocollen;
- de periode dat het apparaat met het netwerk verbonden is (de eerste en de laatste keer dat het wordt gezien);
- de typen apparaten per leverancier;
- het verkeer dat apparaten veroorzaken.

Vergelijken van de feitelijke gegevens met het plan

De volgende stap, na het verwerken van de gegevens, is het controleren of het netwerk draait zoals bedoeld was in de ontworpen, geplande structuur. Bij deze stap moet u uiterst zorgvuldig te werk gaan, want hier worden de eventuele niet-geautoriseerde activiteiten opgespoord. De uitkomst van deze stap is een lijst van alle verdachte gegevens, d.w.z. onbekende IP-adressen, links, protocollen en apparaten die grote hoeveelheden verkeer veroorzaken.

Ontdekken van zwakke plekken

Bij de laatste stap wordt de lijst, die bij het vergelijken is aangemaakt, geanalyseerd om te bepalen of het verdachte verkeer veroorzaakt is door menselijke fouten. Bijvoorbeeld een netwerkbeheerder die vergeten is om een poort te sluiten die door een technicus voor specifieke onderhoudswerkzaamheden is gebruikt. Dit had natuurlijk meteen moeten gebeuren na het afronden ervan.
Als u kwaadwillige activiteit ontdekt, bijvoorbeeld een niet-geautoriseerde verbinding met een onbekend IP-adres, dan raad ik u aan om een bedrijf in te schakelen dat gespecialiseerd is in dit soort gevallen. Maar voordat die met hun werk beginnen, kunt u nog wel een aantal dingen doen:

- Bepalen of de kwaadwillige activiteiten netwerkprocessen hebben verstoord.
- Controleren of het IP-adres waar de niet-geautoriseerde verbinding mee gemaakt is zich buiten het ICS-netwerk bevindt.
- Online naar meer informatie zoeken over het onbekende IP-adres, bijvoorbeeld op de website van ICS-CERT, en controleren of andere apparaten ook een verbinding proberen te leggen met hetzelfde IP-adres.

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

CONCREET AAN DE SLAG MET DE NIS/NIB

Wegwijs in de cybersecurity-wetgeving voor aanbieders van essentiële diensten

In mei dit jaar werd Directive (EU) 2016/1148 (1), ook bekend als de NIS Directive of in het Nederlands NIB-richtlijn, van kracht in de Europese Unie. Het was niet de enige cybersecurity-wet- en regelgeving die Nederlandse bedrijven recent zagen voorbijkomen. Veel aandacht ging uit naar de eveneens in mei in werking getreden AVG/GDPR. Slechts een paar maanden eerder - per 1 januari 2018 - werd de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) volledig van kracht. En om het afkortingencircus compleet te maken is de NIS/NIB in Nederland in de nieuwe Cybersecuritywet (Csw) uitgewerkt en direct daarna omgedoopt tot de Wet beveiliging netwerk- en informatiesystemen (Wbni). Met al deze afkortingen en opeenvolgende nationale cybersecurity-strategieën is er een kans door de bomen het bos niet meer te zien. Voor Aanbieders van Essentiele Diensten (AED's), de focus van de NIB-richtlijn, ligt de situatie nog iets gecompliceerder. Aanbieders voor wie dit geldt, worden uiterlijk 9 november 2018 aangewezen.

In de praktijk kunnen organisaties die binnen de NIB-invloedssfeer liggen, zoals partijen in de sectoren energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater en digitale infrastructuur, toch nu al aan de slag met het treffen van maatregelen om aan de toekomstige regelgeving te voldoen. Want dankzij de opeenvolgende nationale cybersecurity-strategieën is bestaande wetgeving al een goede indicatie van wat vanuit compliancy voor de NIB nodig zal zijn. Zo zal in de nieuwe Cybersecuritywet (Csw) veel nadruk worden gelegd op zowel de zorgplicht als ook de meldplicht. De zorgplicht betekent dat de aangewezen organisaties passende en evenredige technische en organisatorische maatregelen nemen om hun ICT te beveiligen. Ook moeten zij passende maatregelen treffen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. De meldplicht houdt in dat incidenten met aanzienlijke gevolgen gemeld moeten worden bij de toezichthouder en het NCSC.

Operational Technology onder vergrootglas

In veel van de AED's zal met name het Operational Technology (OT) domein onder het vergrootglas komen te liggen, aangezien de doelstelling van de wetgeving vooral is gericht op het veilig en weerbaar houden van de essentiële diensten die deze partijen voor de samenleving leveren. En juist binnen dit OT-domein is met een pragmatische aanpak nog heel veel winst te behalen. Een risico gedreven aanpak is belangrijk om daarin juiste keuzes te maken. Daarbij is inzicht in de bedrijfsrisico's die de organisatie loopt cruciaal. Denk hierbij aan risico's als financieel verlies, productieverlies, persoonlijke veiligheid, reputatieschade als ook milieuschade. Op basis van deze risico's kan worden bepaald welke maatregelen getroffen moeten worden om de risico's tot een aanvaardbaar niveau terug te brengen.

Uit ervaring blijkt dat basale security-maatregelen vaak al heel veel effect sorteren. Zaken als een goede segmentatie van het netwerk, goede fysieke en logische

Auke Huistra, partner bij Applied Risk, een internationale specialist op het gebied van de beveiliging van industriële controlesystemen. Hij is bereikbaar via ahuistra@applied-risk.com.

toegangscontrole, het controleren van gebruik van draagbare media (bijv. USB-sticks), anti-virus, een passende patching cyclus, logging en monitoring, back-up and restore, en 'last but not least' een goede incident response capaciteit, hebben het meest effect. Enerzijds om de kans op een incident te verkleinen, anderzijds om de impact van een eventueel incident zo klein mogelijk te houden. De genoemde maatregelen zijn voor de IT-omgevingen veelal al ingericht, maar staan binnen het OT-domein vaak nog in de kinderschoenen.

Uitvoeren risico assessment

Bij een risico-assessment wordt eerst de bestaande organisatie doorgelicht en geïnventariseerd wat de kritieke bedrijfsprocessen zijn. Op basis daarvan wordt gekeken welke IT- of OT-systemen/netwerken deze kritieke processen ondersteunen. Het hebben van dit inzicht is belangrijk om een goede inschatting te kunnen maken wat de daadwerkelijke risico's zijn van de gevonden kwetsbaarheden. Immers dan pas kan de kans en impact worden ingeschat.

Een belangrijke standaard bij het uitvoeren van risico assessments op het OT-domein is de IEC 62443 standaard. Deze richt zich specifiek op OT-omgevingen. Bij Applied Risk hebben we risico assessments ontwikkeld die bestaan uit twee delen. Het eerste deel betreft het beoordelen van de aspecten mens, organisatie en processen, alsmede de fysieke security. In het tweede gedeelte worden de technische controls getest. Met een dergelijke bewezen methodiek kan in korte tijd bepaald worden waar de verbeterpunten liggen, welke prioriteiten er zijn en wat globaal de kosten van een verbeterprogramma zijn. Zo kan bijvoorbeeld in de technische assessments snel bepaald worden wat kwetsbaarheden en risico's zijn aan de hand van een bibliotheek aan bekende dreigingen en kwetsbaarheden. In deze database is een grote diversiteit aan ICS/SCADA-oplossingen en leveranciers terug te vinden. Door het bijhouden van relevante externe bronnen, middels eigen onderzoek en vooral ook door het uitvoeren van een grote hoeveelheid assessments is onze database inmiddels flink gegroeid en biedt daarmee steeds meer waarde bij het uitvoeren van de assessments.

De uitkomsten van risico assessments en het opvolgen van de aanbevelingen die hieruit voortkomen, dragen bij aan het voldoen aan de zorgplicht.

Incident response en meldplicht

Inmiddels is ook binnen industriële omgevingen de realiteit doorgedrongen dat het niet een kwestie is van of een incident zich zal voordoen, maar wanneer. Het opzetten van een effectief Incident Response(IR)-plan is dan ook een belangrijke stap. Zoals gezegd functioneert Incident Response binnen industriële controlesystemen wel net anders dan binnen IT-omgevingen. Zo ligt opnieuw opstarten van systemen, een logische IR-stap in IT-omgevingen, in OT-systemen veel gevoeliger. Niet alleen is interruptie van het industriële proces wel het laatste waar een plantmanager op zit te wachten, ook is de kans van vernietiging of vervuiling van forensische sporen groot. Niet alle apparaten zijn namelijk voorzien van log-systemen waar achteraf informatie kan worden uitgelezen. Ook kunnen bijvoorbeeld PLCs niet eenvoudig vanuit een image worden hersteld, zoals dat wel mogelijk is bij bijvoorbeeld een server of een laptop. Opzetten van effectieve monitoring van de netwerkactiviteit en netwerkintegriteit is essentieel om incidenten te kunnen detecteren. Een uitgebreid Incident Response-plan geeft inzicht in waar assets en processen elkaar raken en mogelijk afhankelijk zijn en of en hoe ze verbonden zijn aan het netwerk. Op die manier kan worden bekeken hoe en waar een aanval of infectie kan worden ingedamd. Leg vast wie gebeld moet worden ingeval van een incident. En stel een gespecialiseerd IR-team samen waar zowel het management, de juridische afdeling, engineering, de technische staf, beveiliging, relevante leveranciers en een ICS-securityspecialist in vertegenwoordigd zijn.

Vanuit de wetgeving is het daarbij belangrijk om bij het overschrijden van bepaalde drempelwaardes qua productieverlies (ten gevolgde van IT-verstoringen) een notificatie te doen bij de aangewezen nationale autoriteit. Dit valt onder de eerdergenoemde meldplicht. Dit blijkt in de praktijk geen sinecure te zijn, aangezien er vele verschillende onderdelen van het bedrijf betrokken zijn bij dit meldproces. Denk hierbij bijvoorbeeld aan de business, legal, informatiebeveiliging, IT en crisismanagement.

Aan de slag

Het digitaal veilig houden van het operationele proces en daarmee het waarborgen van de continuïteit van industriële omgevingen en vitale infrastructuren is een flinke kluif. Via een risico gedreven en holistische aanpak kunnen organisaties twee vliegen in één klap slaan. Ze zijn zelf digitaal weerbaarder en voldoen tegelijkertijd ook aan zorg- en meldplicht, zoals die is opgenomen in Wet beveiliging netwerk- en informatiesystemen. Ga dus direct hiermee aan de slag!

Referenties

(1) .eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515595408542&uri=CELEX:32016L1148

PROVENANCE ASSURED

"Trust but verify"
– Russian proverb.

Earlier this year The Attributer published an article entitled `Fake Protected'. This new article revisits the same topic but from a different perspective. We are living in a time of increasing outbreaks of `fake news' in particular, and `fake information' in general. How do we establish the provenance of data and the information that it encodes? Perhaps the more important question to ask is: are we looking at the wrong metadata? The issue is exploitation of trust without verification. This problem undercuts our fundamental security foundations.

One of the earliest trust-with-verification mechanisms was the handshake. Since most of the world is right-handed, the extended open palm of the right hand signalled that both parties were unarmed, therefore the handshake was safe. In the virtual environment where only some senses are invoked, the ability to verify is compromised. There is no eye contact, no body language and no assessment of dress codes and other signals of personal identity and integrity. This phenomenon is witnessed frequently with autonomous systems where subtle changes to signs and other environmental objects become significant problems for systems that cannot verify content.

Content can be verified when contextually examined. This activity requires not only more effort, but also re-thinking our security paradigm and designing new solutions that capture contextual information. Capturing contextual data provides the ability to gain new insights from old events. Consider the case of fake news. There are three critical characteristics of `news' that can be examined: computational linguistics (CL), pattern-spread (PS) and source provenance (SP). CL can be used to identify and quantify linguistic markers of deceptive speech. PS can use signal gathering techniques to identify normal and anomalous propagation patterns, and SP can be used to examine the history of the author and publisher.

The Oxford English Dictionary defines provenance as: `the place of origin or earliest known history of something'. As a secondary definition it says: `the beginning of something's existence; something's origin'. In one of the sentence examples it gives this usage: `False provenances and certificates of authenticity are favourite tools of cheats and should never be accepted blindly.' You bet!

In 2017 a report on fake news mentioned that discrediting a reporter can be done for $50,000 and a fake protest can be created for $200,000. The relatively low cost associated with both of these acts suggests that they will become more frequent. Serious journalists may be fooled once or even twice, but not repeatedly. These same journalists will have a body of work that can be examined through archived data by using CL to classify their work. The work history can be scored and trended indicating whether the veracity score of the reporter's work is improving or worsening.

A Jigsaw Research (2018) found that while the majority of people rely on the television, followed by the Internet as sources for news, a full 82% of young people (16-24 years) prefer the Internet. The same Internet that is vulnerable to injection of non-verified data as discussed above. Furthermore, when trusted sources are attacked and discredited the trust model further erodes. This results in sentiments listed below:

"The only people I trust to tell me the truth are my Facebook friends".

"I only use Facebook and Twitter to get news and information about the world. I don't trust the other media".

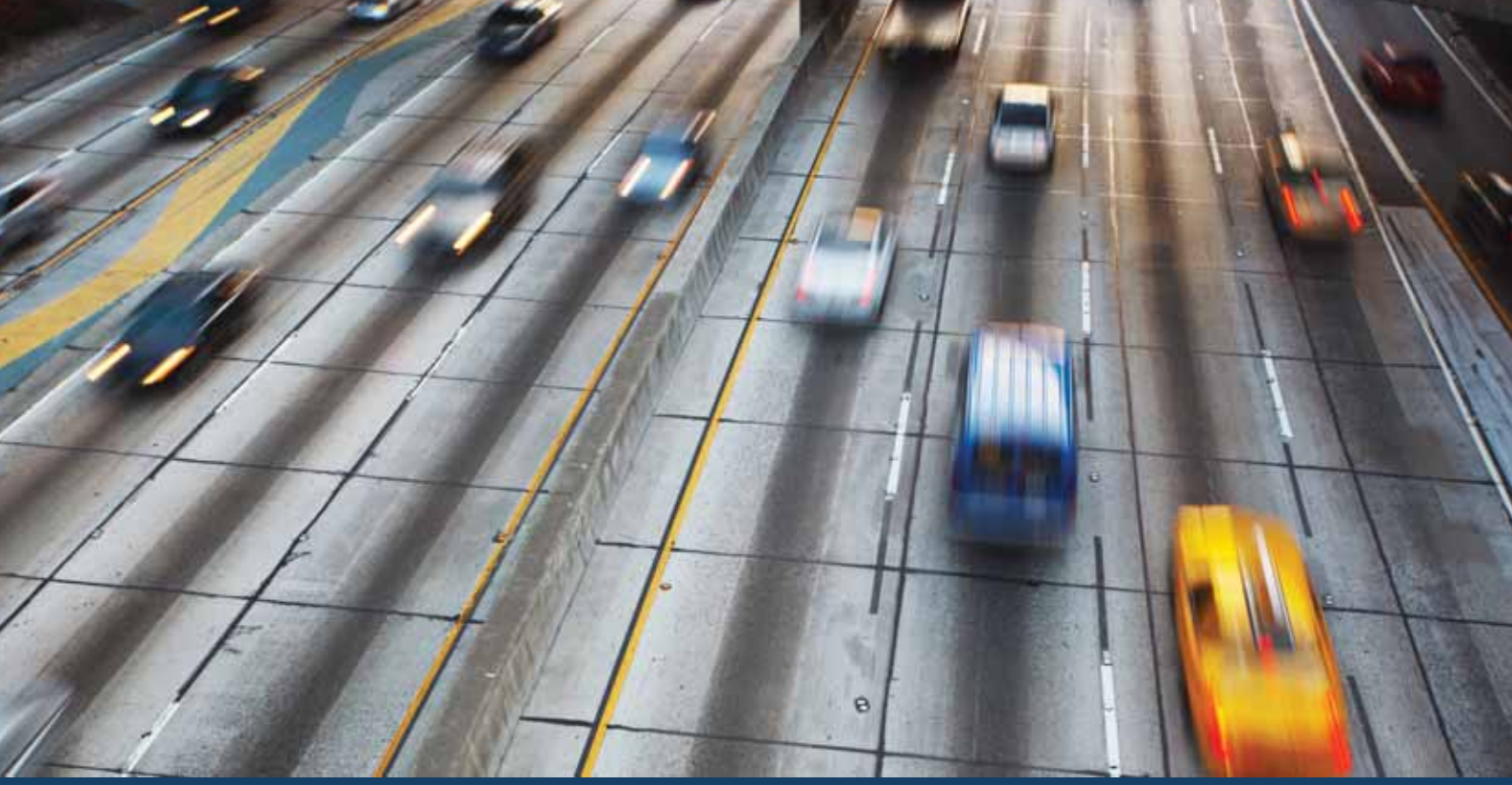
The truth about fake news is complex. Consider the BREXIT referendum where voters, young and old, educated and uneducated, supported leaving. The messages were crafted to appeal to the voters' deeply held values and beliefs. These messages were crafted to demographic groups identified by the very social media that people increasingly rely on for their news.

Countering fake news will require reliance on technical and non-technical solutions. The ability to critically assess information in this digital world is a topic that should be included in every school and college curriculum. The issue is to do with three major things: what is the source of the information? Do you trust that source? Can you verify the data? It will require more SABSA Thinking .

The Attributer (with thanks to Dr Char Sample for her advice)

The Attributer

https://www.ofcom.org.uk/__data/assets/pdf_file/0024/116529/news-consumption-2018.pdf

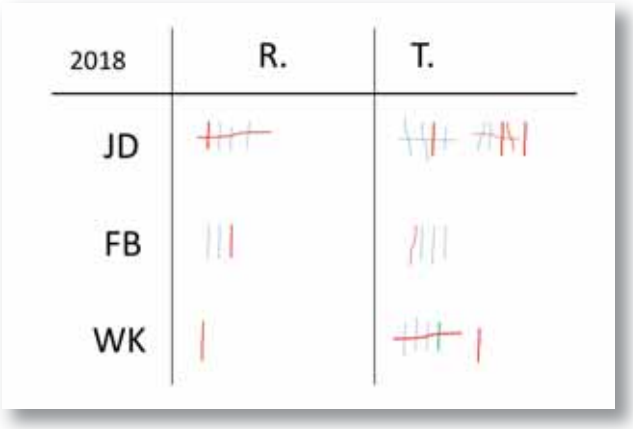


SIEM LESSONS LEARNED BIJ AUTOTURVEN

Ook afgelopen vakantie turfden mijn vriendin en ik tijdens onze reis door Duitsland weer auto's. Bij dit spel houden bestuurder en bijrijder op een turflijst bij hoe vaak ze bepaalde voertuigen zien. Het gaat bij ons om John Deere tractors, Flix reisbussen en vrachtwagencombinaties van Wolter Koops. Ervaring leerde ons dat deze voertuigen vaak genoeg rondrijden om het spel zin en spanning te geven. Degene met de meeste streepjes wint het recht de ander te trakteren op gebak of een Japans buffet, al naar het zo uitkomt. Het houdt ons bezig en alert op lange trajecten van soms honderden kilometers rechte Autobahn. Door de onvoorspelbaarheid (soms zie je er uren geen en dan drie tegelijk) levert het ook mooie herinneringen en associaties: aan ander werk (Deere), aan andere vakanties (Flix) en zelfs aan een toekomstige erfenis. Want Wolter deelt zijn achternaam met mijn vriendin, en mogelijk blijkt zij - pas over vele jaren natuurlijk! - bij het verdelen van de erfenis een verre achternicht te zijn. Die dan bijvoorbeeld één zo'n wagen krijgt. Dat zou al ontzettend mooi zijn!

Eerdere vakanties toonden aan dat de landbouwers in de diverse Bondslanden niet allemaal hetzelfde merk tractor gebruiken. Afhankelijk van waar je rijdt, zie je veel of weinig van die knalgroene JD-jongens met een horizontale gele streep op de motorkap. Het zijn nogal uit de kluiten gewassen knapen, die qua aanschafprijs starten bij een flinke starterswoning. Je kan ze dus goed herkennen, zeker als bijrijder die nu eenmaal meer tijd en aandacht heeft voor de omgeving dan voor de snelweg zelf. De Flix-reisbussen hebben ongeveer dezelfde groene kleur, maar er staat met grote witte letters "Flix-bus" op de zijkant. Deze busmaatschappij concurreert met de trein op trajecten tussen steden waar geen goed treinalternatief is. Soms zie je wel een enkele keer een Flix-bus aankomen of vertrekken in een grote stad (we tellen namelijk ook lopend!), maar de meeste bussen zie je onderweg. Op de langgerekte stukken tussen grote Duitse steden en dus zoals gezegd eigenlijk nooit langs een treinspoor. Ze zijn natuurlijk zo groot als een autobus. En het wifi-netwerk van de bus heeft als SSID ook iets met Flix. Ja inderdaad, als je het eigen rijtempo nauwkeurig afstemt op dat van zo'n bus, kun je onderweg vanuit je eigen auto gratis op internet. Heb ik "gehoord". De Wolter Koops vrachtwagens zijn wit, minstens zo groot als één Flix-reisbus en er staat met enorme zwarte letters "Wolter Koops" op beide zijkanten. Als bijrijder zie ik ongeveer evenveel WK-wagens rijdend als stilstaand op de truckerrustplaatsen naast de snelweg. Een Wolter Koops chauffeur die al vroeg op de werkdag aan het rusten is, suggereert dat het voor die dag alweer verdiend is, en dat wakkert onze hoop op een kleine erfenis aan. Plaats en tijd van de waarneming heeft dus wel een positieve invloed op de teller, maar dat nemen we niet mee in de telling.

Als lezer denkt u nu: wat heeft dit met security te maken? "Wat zijn de zaken waarop u let in uw SIEM?", vraag ik dan terug. Welke "anomalies" (gekkigheden) worden er opgespoord op uw netwerk? Wat zijn de signaleringen van



gebeurtenissen waarvoor ze u letterlijk uit bed mogen bellen en bij welke u denkt laat maar gaan? Is dat een vaste verzameling van gebeurtenissen of stopt u ook weleens met het tellen van één ervan?

De gedefinieerde incidenten en events in een SIEM (Security Incident & Event Monitoring) systeem moeten immers ook voldoende opvallend en daarmee goed herkenbaar zijn. Als ze per stuk ook nog groot zijn, is de investering in de aanschaf van een SIEM en wat nog duurder is, het inrichten daarvan, gemakkelijker te verantwoorden. Dit geldt zeker voor de eerste gevallen (of "use cases") die in de monitoring worden opgenomen. Je gaat immers niet lopen zoeken naar securityzaken die nooit of zeer zelden optreden. Je weet dat ze kunnen en dus ooit zullen (wet van Murphy) optreden, alleen niet precies wanneer en met welke frequentie. Aan de andere kant zie je een John Deere tractor vrijwel nooit in het stadscentrum en er staat geen enkele Flix-reisbus volgeladen met passagiers stationair te draaien in een weiland, terwijl de bestuurder zijn boterhammen zit op te eten. Toegegeven, ik heb zelf één keer drie Wolter Koops vrachtwagens in colonne achter elkaar zien rijden, maar dat is dan ook mijn persoonlijk record van ruim 10 jaar

Robert Metsemakers is Enterprise Security Officer bij Achmea IT. Robert is bereikbaar via metsemakers@live.com. (Dit artikel is geschreven op persoonlijke titel).

spotten. Je krijgt op den duur een gevoel voor waar en wanneer je ze zult zien. Zoals je ook, wanneer er halverwege de reis een achterstand in bijvoorbeeld getelde Flix-bussen ontstaat, een gevoel kunt hebben dat alles nog niet verloren is en dat het verschil op het resterende traject nog ingehaald kan worden.

Aan het eind van de monitoring-periode (dag, week of kwartaal) heb je - bij een goede selectie van waar te nemen gebeurtenissen - dus vrijwel zeker een aantal turfstreepjes bij verschillende gebeurtenissen kunnen zetten. Sommige soorten komen vaker voor dan je vooraf had verwacht, andere juist minder. Over die mee- of tegenvallers kun je dan nog eens verder nadenken. Ook kun je de security-afdeling op gebak trakteren. Dat kan zowel bij hoge (= goed opgelet zodat je ze ziet!) als bij lage aantallen (= goede preventie gedaan zodat het niet meer vaak gebeurt!).

Maar helaas, de werkelijke gekkigheden op het netwerk ga je zo niet vinden. Want in de SIE-monitoring (één M is genoeg) wordt meestal vooral (of zelfs uitsluitend) gelet op vooraf gedefinieerde, goed herkenbare objecten en gebeurtenissen. Op het bekende werk dus, dat al eens eerder in de eigen organisatie is waargenomen en daardoor in de eerste plaats te definiëren was. Maar om een werkelijke knaller te maken, moet je het onverwachte doen, leerde ik van mijn grootvader. Hij had het daarbij weliswaar over het invullen van het toto-formulier, waarmee hij wekelijks gokte op de uitslagen van voetbalwedstrijden. Het beschikbare prijsbedrag wordt daarbij verdeeld onder de goede voorspellers. Met het team van toen zou Ajax elke voetbalwedstrijd van Willem II winnen, maar dat wist iedereen en iedereen gokte dus ook op die uitslag. Om de kans op een grote toto-prijs te verhogen, vertelde opa mij, moest je dus juist Willem II van Ajax laten winnen op je formulier. "Contrair beleggen" is ook zoiets: kopen als iedereen zijn aandelen verkoopt. Met andere woorden: je moet uitkijken naar iets dat je nog nooit gezien hebt.

Bij mijn eerste security-cursus hoorde ik dat fraudeurs wachten tot iedereen van kantoor weg is om dan hun gemene slag te slaan. Het was daarom nuttig om in de monitoring te kijken naar aanlogpogingen op het systeem (toen: het centrale mainframe) buiten de normale kantooruren. Fraudeurs gingen destijds ook nooit met vakantie. Want gingen ze wel een keertje weg, dan zou de bedrijfswinst die periode ineens veel hoger zijn en zouden hun malversaties aan het licht komen. Dus waren ook medewerkers die dagelijks aanlogden gedurende een lange periode interessante gevallen voor de security-monitoring. Ook de werkzaamheden van systeembeheerders, met name als het via "inbelverbindingen" van buiten het pand gebeurde, moest in die tijd met argusogen worden gevolgd. Immers die beheerder zat daar zomaar thuis te werken, zonder oogtoezicht of sociale controle. Dit soort security-monitoring is door het always on ("ubiquitous") internet concept geheel onderuit gehaald. Er zijn nu immers gebruikers die meerdere keren per dag (ha!) naar hun e-mail kijken en daarvoor steeds opnieuw aanloggen op hun smartphone met een pincode, vingerbeweging of vingerafdruk. Ook als zij met vakantie zijn. Daardoor is een aantal in de loop van jaren of decennia bekend geworden voor security-monitoring interessante gebeurtenissen eigenlijk niet meer relevant. Ook in een bos moet regelmatig het dode hout worden verwijderd om zo de wezenlijke zaken over te houden.

Naast de bovengenoemde voertuigen (JD, FB, WK), speur ik tijdens reizen ook naar Mercedessen met vleugeldeuren, Porsche sportwagens (maar niet de jeeps) en Italiaanse auto's eindigend op een "i" (maar niet Auto Bianchi). Zeg maar alles waar in Nederland enorm veel BPM op wordt geheven. Dat zijn voor mij de echte verrassingen en van zo'n mooi stuk techniek kan ik echt genieten, zelfs al rijd ik er zelf niet in. Wat ik leuk vind, is dat Ferrari en Lamborghini ooit ook als tractorbouwer zijn begonnen; van Maserati weet ik dit niet, maar het zou best kunnen. In de verzameling zaken waar ik naar kijk, beste lezer, zit dus zeker wel een structuur, rode lijn of achterliggende bedoeling (hint!).

En dan let ik ook nog op of motorrijders, vrachtwagen- en buschauffeurs (alle merken bij alle drie) elkaar groeten, via het opsteken van de niet-schakelhand of een wijsvinger of met een kort lichtsignaal. Dit is natuurlijk geen wettelijke verplichting en mijn vriendin wordt gek van de meldingen die ik aan haar doe als het eens een keertje niet gebeurt. Maar het is wel een schade beperkende preventiemaatregel voor het geval je als chauffeur met pech langs de weg staat, met je exotische mechanische motortechniek of je kostbare lading mensen, dieren of platte TV's. Een ander lid van jouw groep chauffeurs zal, is de gedachte, eerder geneigd zijn voor een groeter te stoppen en je te helpen met een krik, telefoontje of goede raad.

Toegegeven, deze gewoonte zorgt er niet voor dat je nooit pech krijgt, maar het helpt wel bij het oplossen ervan. Het is vergelijkbaar met het aanbrengen van security-patches. Als je software leverancier zelf aangeeft dat er iets niet goed zit of zelfs ontbreekt in het door jou

gebruikte pakket of systeem en hij biedt ook nog een oplossing aan? Dan zal er echt wel iets aan de hand zijn. En dus kun je security-patches maar beter metéén bij het beschikbaar komen installeren, heb ik altijd gedacht. Wie als gebruiker weleens een vergadering over releaseplanning heeft bijgewoond, kent het gelukzalige gevoel als je verzoek ("feature request" heet dat tegenwoordig) wordt opgenomen in de komende release en bij security-patches is het dan nog gratis ook! Je vermijdt er inderdaad niet mee dat een collega op een link in een phishing-mail klikt en daarmee toestemming geeft voor het installeren van malware (bijvoorbeeld ransomware). Maar de schade wordt er allicht wel door beperkt omdat de grote, algemeen bekende security-gaten in elk geval niet meer kunnen worden misbruikt op een juist en volledig gepatchte machine.

Ik adviseer overigens wel om een installatie-procedure in te richten om zoveel mogelijk medewerkers te voorzien van de nieuwste security-patches. In plaats van een monitoring-procedure op te stellen die opspoort hoeveel machines van welke medewerkers (gesorteerd per afdeling) er helaas nog niet gepatcht zijn om dit dan aan de hoogste directie te gaan rapporteren. Af en toe komt het voor dat een organisatie het SIEM-systeem ook voor deze laatste soort compliance-metingen inzet. Vanuit mijn principe "security-patches van de leverancier altijd en snel toepassen" zijn niet-gepatchte machines geen echte gekkigheden, en zou je dit eigenlijk niet moeten doen. Ik heb namelijk liever een rapportage over een klein aantal SIEM-use cases die er werkelijk toe doen.

Afgaan van een inbraakalarm bij het rekencentrum is niet zo boeiend, want het kan ook een vogel zijn die tegen een raam botst en beduusd verder vliegt. Dat het alarm afgaat zonder dat er iemand in het systeem is gekomen, hoef je eigenlijk niet eens te weten. Geen alarm en ook niemand binnengedrongen, is de meestal geldende situatie. Je wilt dus eigenlijk alleen een melding krijgen wanneer de inbrekers binnen zijn, zonder dat het inbraakalarm is afgegaan. Zo'n melding is natuurlijk niet eenvoudig, maar met het combineren van data en diverse metingen kom je een heel eind. Als je organisatie zich met zijn producten louter richt op de Nederlandse markt en midden in de nacht zijn er forse versleutelde bestanden verzonden via internetverbindingen naar IP-adressen in China? Dan is dat eerder data-exfiltratie door een APT-groep dan een noeste arbeider die 's nachts speciaal naar kantoor is gekomen om een enorme PDF met product- of polisvoorwaarden te verzenden aan een expat prospect in China. En daarmee heb je dan toch een echte anomalie te pakken, die verder onderzocht en opgelost kan worden. Als je vervolgens de oorzaak van de gekkigheid oplost met behulp van preventieve maatregelen, dan is er eigenlijk geen goede reden meer om zo'n geval als monitoring use case op te nemen in het SIEM-systeem. Want het kan door de getroffen maatregelen immers niet meer gebeuren!

Samenvatting

1. Zorg in je SIEM-systeem voor duidelijk gedefinieerde te monitoren zaken, die werkelijk kunnen optreden en herkenbaar zijn (bijvoorbeeld John Deere green);
2. Maar staar je niet blind op die verzameling en zoek ook steeds naar nieuwe opvallende gebeurtenissen (denk aan vleugeldeuren);
3. Kijk periodiek kritisch naar de use cases in je SIEM: zijn ze nog steeds relevant? en durf te schrappen (zoals monitoren op aanloggen tijdens vakantie);
4. Durf ook uit te breiden. "Normale" waargenomen gebeurtenissen kunnen op een ongewone tijd, in een ongebruikelijke richting of heel vaak (frequentie) of veel (bandbreedte) toch weer abnormaal worden en daarmee tóch een anomalie (gekkigheid) zijn (zoals een 4,3 GB file 's nachts naar Bejing);
5. En bedenk: degene die de meeste gekkigheden vindt, mag de ander (die er vervolgens veel uitzoekwerk aan heeft) trakteren op taart of een Japans buffet.

SMART HUMANITY 2018

daar moet je bij zijn!

Donderdag 13 december 2018, EYE Amsterdam

SMART HUMANITY, powered by KNVI, is HET event waar je 24 uur lang alles hoort over vijf thema's:

- **Smart GLAM**
  (Galleries, Libraries, Archives, Musea)
- **Smart Me & Ethiek**
- **Smart Mobility**
- **Smart Industries**
- **Smart Cities**

Uniek 24-uurs programma
Daar wil jij toch bij zijn? Een hele nacht, dag en avond gevuld met tal van lezingen over dé onderwerpen die momenteel hot topic zijn binnen ons vakgebied!
Vanaf middernacht vindt bovendien 24 uur lang een hackaton plaats.

Zie, beleef, voel en praat mee!

Hoofdsponsor:

EBSCO | knvi | smart humanity

Meld je nu aan voor dit unieke 24-uurs event met een passe-partout!

www.smarthumanity2018.knvi.nl

Als PVIB lid met korting naar Smart Humanity 2018 Schrijf je nu in!

Tijdvak 1	€ 75
Tijdvak 2	€ 100
Tijdvak 3	€ 125
Tijdvak 4	€ 125
Tijdvak 5	€ 250
Passe-partout (24 uur)	€ 495

VROUWEN IN CYBERSECURITY: HOE EEN TWEET LEIDDE TOT EEN GEDRAGSCODE VOOR SECURITY EVENEMENTEN

In augustus is de IN Security Code of Conduct[1] gepubliceerd. Het doel is om te beschrijven wat het verwachtte gedrag en houding is van mensen die evenementen bijwonen, waaronder sprekers, sponsors, partners, facilitaire medewerkers en organisatoren. Organisaties van security conferenties of evenementen kunnen de gedragscode overnemen in hun voorwaarden voor deelnemers.

Het PvIB organiseert ook regelmatig evenementen. Deze evenementen zijn veel kleiner dan de grote commerciële evenementen waar bovenstaande gebeurtenissen over gaan. Een belangrijke regel uit de gedragscode van het PvIB is dat commercie tot het absolute minimum wordt beperkt. Commerciële partijen zijn niet nodig om de activiteiten uit te voeren en daarmee wordt ook de kans kleiner dat ludieke, maar slecht uitgevoerde acties, voorkomen. Het uitgangspunt bij PvIB-activiteiten is dat iedereen zich veilig moet voelen, ongeacht leeftijd, geslacht, voorkeuren en achtergronden. Gelukkig heeft het PvIB nog nooit een dergelijke misstand gemeld gekregen. De algemene indruk van onze leden is dat onze gemeenschap van nature al een veilige omgeving is omdat iedereen persoonlijk lid is, daarvoor betaald en dat de leden daardoor kunnen vertrouwen dat ze met vakgenoten spreken. Voor het melden van situaties is overigens al een bestaande mogelijkheid: Debbie Reinders ondersteunt elk evenement persoonlijk door altijd op het event aanwezig te zijn en is daarmee toegankelijk voor het melden van allerlei situaties. Ze kan gezien worden als vertrouwenspersoon.

De gedragscode is opgesteld als concrete actie naar aanleiding van gebeurtenissen op Infosecurity Europe[2][3] in juni. Jane Frankland, een Britse voorvechter van diversiteit in cybersecurity, maakte een foto van 'booth babes' op een stand en plaatste die op Twitter met de opmerking dat ze teleurgesteld was over deze seksistische marketing methode. De organisatie van Infosecurity trof direct maatregelen, maar de storm was al ontstaan. Jane Frankland werd bedolven onder positieve en vooral ook negatieve reacties. De storm werd opgemerkt door Newsweek, Computer World[4], Forbes[5] en andere media. Het leidde zelfs tot enkele meldingen door vrouwen van ongewenste intimiteiten op security evenementen.

Om een positieve wending aan de storm te geven is er direct een initiatief gestart om een gedragscode op te stellen. De gedragscode beschrijft wat acceptabel gedrag is, hoe slachtoffers het kunnen rapporteren en wat er aan gedaan wordt. Het document somt enkele voorbeelden van ongewenst gedrag op en duidt op het belang van dat organisatoren van een evenement een procedure hebben om meldingen te behandelen. Het idee is dat organisatoren van evenementen de gedragscode kunnen steunen als teken van hun normen en waarden, en dat ze het kunnen opnemen in hun voorwaarden voor deelname.

Links

(1) http://cybersecuritycapital.com/event-code-of-conduct/
(2) https://www.newsweek.com/cyber-firm-blasted-using-booth-babes-major-security-conference-964472
(3) http://jane-frankland.com/women-in-red-ball-gowns-at-infosec-why-i-spoke-out/
(4) https://www.computerworld.com.au/article/644508/push-code-conduct-help-fight-sexism-security/
(5) https://www.forbes.com/sites/kateoflahertyuk/2018/08/15/sexual-harassment-in-the-cyber-security-industry-how-one-woman-is-fighting-back/#7500520576e2

VOORSTELLEN NIEUWE REDACTIELEDEN

Met gezond verstand en een pragmatische aanpak kijk ik vooral naar wat past bij en binnen de organisatie.

Bianca Brooijmans

Enige maanden geleden las ik over de functie van redactielid bij het magazine Platform voor Informatiebeveiliging en was meteen geïnteresseerd. Zelf vind ik het altijd erg inspirerend om te sparren met - en leren van andere professionals in het veld en lees vele (achtergrond) artikelen. Ik ben ervan overtuigd dat we alleen continu kunnen verbeteren als we onze (eigen) ideeën toetsen en bijstellen. Met trots stel ik me in deze editie voor als nieuw redactielid van PvIB en ben blij hier te mogen bijdragen aan kennisdeling.

Mijn naam is Bianca Brooijmans en sinds 2000 werkzaam bij Enovation bv, al 35 jaar dé partij op het gebied van elektronisch berichtenverkeer en uitwisseling van standaarden in de zorg. De laatste 10 jaar ben ik o.a. actief op het gebied van informatiebeveiliging. Mijn expertise ligt op het gebied van privacy en opzet & onderhoud van "het systeem" d.w.z. hoe ben ik aantoonbaar in control. Denk daarbij aan de diverse normen als ISO27001, NEN7510 en hoe verhoudt de AVG zich daar toe. Je kunt privacy immers niet garanderen zonder adequate informatiebeveiliging. Ik ben Functionaris Gegevensbescherming binnen onze groep en adviseer daarnaast ook zelfstandig diverse bedrijven buiten de zorg op het gebied van Informatiebeveiliging & Privacy.

Ik ben wars van onnodige, dure en dubbele administratie en geloof niet in "moetjes". Met gezond verstand en een pragmatische aanpak kijk ik vooral naar wat past bij en binnen de organisatie. Daarom geloof ik ook in een kenniscentrum zoals het PvIB met achtergrondinformatie, best practices en leasons learned - laten we vooral van elkaar blijven leren. Informatie beveiligen, privacy garanderen, herhaalbare kwaliteit leveren en continu verbeteren is hard werken, ik help je er graag bij, dus als je een interessant artikel hebt, feedback wil geven op bestaande artikelen of wil sparren over een vraagstuk, laat het me gerust weten.

Nicole van Deursen

Toen ik de oproep zag voor nieuwe redactieleden heb ik direct gereageerd. Als kind schreef ik al verhalen en knipte en plakte ik zelf mijn eigen tijdschriften in elkaar. Dat ik communicatiewetenschap ging studeren was een logisch gevolg. In mijn vroege carrière heb ik organisaties geadviseerd over kwaliteitsverbetering van processen en het voorlichten van medewerkers over beleid en procedures. Vanaf het jaar 2000 adviseer ik over informatiebeveiliging, met name over awareness, compliance en risicoanalyse. Ik ben nogal een studiebol en altijd aan het bijleren: of het nu gaat om het leren van een nieuwe taal, een nieuwe wet, onderzoeksvaardigheden, statistiek, software voor data visualisatie of design: ik vind het allemaal interessant. Tegenwoordig hou ik mij vooral bezig met kwalitatief onderzoek, schrijven en visuele communicatie. Ik heb heel veel zin om bij de redactie van het magazine aan de slag te gaan, omdat daar al mijn interesses bij elkaar komen.

Ik heb heel veel zin om bij de redactie van het magazine aan de slag te gaan, omdat daar al mijn interesses bij elkaar komen.

Toen ik kans zag om de risico's in de I(C)T-wereld beter te leren kennen en mijn kennis daaromtrent te verdiepen door lid van het PvIB te worden, aarzelde ik geen minuut.

Chris de Vries

Chris de Vries, al meer dan 25 jaar zelfstandig bedrijfsadviseur die in het dagelijks leven altijd al geconfronteerd is geweest met risico's en hoe deze te beheersen. Begon als kredietbeheerder bij de bank (jaren `80 – 7 jaar `fulltime' faillissementen behandelaar) daarna meer dan geïnteresseerd computer enthousiast. Ook daar zag ik de risico's vaak opduiken. Toen ik kans zag om de risico's in de I(C)T-wereld beter te leren kennen en mijn kennis daaromtrent te verdiepen door lid van het PvIB te worden, aarzelde ik geen minuut. In de tussentijd al jarenlang trouw deelnemer aan de lezingen en recentelijk in de werkgroep Ketenveiligheid. Een onderwerp dat mij ook aanspreekt vanuit de waardeketengedachte van Porter.
Momenteel ben ik druk doende om het Structura-model toe te gaan passen in het bedrijfsleven, maar ik zie ook kansen in onze Informatiewereld en zelfs bij de sportwereld. Ik vertrouw er namelijk op dat mensen de kern zijn van het betrouwbaar, secuur en integer werken en dus ook van Informatieveiligheid. Innovatie boeit mij. Nederland is altijd al het land van de introductie van innovaties. De reden is, zo heb ik mij laten vertellen, in de acceptatiegraad van innovaties door Nederlanders, onze onbegrensde re-engineering behoefte van alles wat wij in handen krijgen (F16; pantserinfanterievoertuigen; APP-toepassingen enz.) en dat wij het best gedocumenteerde volk van de wereld zijn. 'Big data' was al voor de uitvinding van dit begrip een essentieel bestanddeel van Nederland.
Al het bovenstaande maakt dat wij in een interessante tijd leven, met veel kansen, opties en levens-verrijkingen, echter, ook van de daaraan gekoppelde bedreigingen als identiteitsdiefstal, fraude en inbreuken op de persoonlijke levenssfeer. Dat alles maakt dat ik geïnteresseerd ben en blijf in Informatie Beveiliging. En daarom zei ik volmondig "ja" op de uitnodiging om deel te gaan nemen aan de redactie.

HET TOEKOMST - PERSPECTIEF VAN PRIVACY MANAGEMENT

Zijn we door de AVG-hype allemaal in paniek? Geloven we écht dat de letter van de wet regeert? Of verliezen we de werkelijke essentie uit het oog? Deze advertorial van Smile roept op tot een beetje nuchterheid.

Fatsoenlijk omgaan met persoonsgegevens wordt de norm

Dankzij de katalyserende werking van de AVG/GDPR realiseren steeds meer mensen zich dat hoe we nu omgaan met dataprivacy bepalend is voor hoe toekomstige generaties zich in deze wereld kunnen bewegen. Fatsoenlijk omgaan met persoonsgegevens wordt de norm en iedere organisatie zal aan deze norm moeten voldoen. Logisch dus dat we met z'n allen naarstig op zoek zijn naar hulpmiddelen voor AVG-compliance. Naast begrip voor en inzicht in dataprivacy in relatie tot het eigen werkterrein, vormt het implementeren van (verbeter)maatregelen zoals een goed privacy beleid en een juridisch beproefd verwerkingsregister een grote uitdaging voor organisaties. Wat daarbij opvalt is de neiging om het onderwerp dataprivacy geïsoleerd op te pakken. Misschien kun je dit niemand kwalijk nemen, de overheid brengt het onderwerp immers ook op een geïsoleerde manier onder de aandacht, maar toch zou je verwachten dat men intussen wel beter weet.

Terug naar de essentie, we zeggen A maar doen B

Waar kwaliteitsmanagement zich ooit vooral bezighield met `de kwaliteit van producten en diensten aan klanten' kwamen daar de afgelopen decennia steeds meer taken bij. Door de ontwikkelingen op het gebied van Arbo & Milieu werd de kwaliteitsmanager een KAM- of QHSE-manager. De klantgerichtheidshype legde een verbinding tussen kwaliteitsmanagement en processen als feedbackmanagement, CRM en marketing. En wat meer recent zorgde de nieuwe ISO 9001-norm ervoor dat de kwaliteitsmanager een flinke stap richting risicomanagement moet gaan maken, een transitie die nog volop gaande is.
Langzaamaan raken we ervan doordrongen dat ook vakgebieden als Business Continuity Management en Governance, Risk & Compliance niet los van kwaliteitsmanagement kunnen opereren. Integratie wordt de nieuwe standaard. Alleen op die manier kunnen we voldoen aan de steeds complexer wordende eisen en het almaar toenemend aantal stakeholders. De roep om managementsystemen terug te brengen naar hun essentie klinkt daardoor steeds harder door. Het zijn hulpmiddelen die bij moeten dragen aan het verwezenlijken van de organisatiedoelen, geen doelen op zich.
Voor het vakgebied privacy management is dat natuurlijk niet anders. De AVG/GDPR is geen doel op zich, het gaat om de geest van de wet. Privacy raakt ons allemaal en het is goed dat we beschermd worden. Omdat dat niet vanzelfsprekend blijkt, zijn regels nodig. Regels die duidelijkheid geven en bijdragen aan een veiligere samenleving. Het doel is niet het uitvoeren van de regel, maar het verbeteren van de samenleving. `Gewoon' fatsoenlijk omgaan met elkaars gegevens als nieuwe kwaliteitseis.

De angst voor boetes en imagoschade regeert

Toch lijken we het onderwerp dataprivacy nog steeds volledig geïsoleerd en als doel op zich aan te pakken. Vanwege de dreigende AVG `deadline' van 25 mei voerden veel organisaties in een sneltreinvaart maatregelen door, uit angst voor boetes en imagoschade. Alsof privacy management iets eenmaligs is, dat je door `even een projectje te doen' goed kunt regelen. Paniek

voert veelal de boventoon. Wat als ik de boot mis? Wat als ik niet op tijd klaar ben? Ben ik wel volledig op de hoogte? Hoe gaat de Autoriteit Persoonsgegevens straks handhaven? Zijn de nieuwe regels niet in strijd met verplichtingen die voortvloeien uit andere wetten? We maken elkaar gek met juridische kaders en lijken het allemaal beter te weten. Eenoog is koning in het land der blinden. Maar onderhuids knaagt de onzekerheid.
Zijn we door de privacy hype uit het oog verloren waar het echt om gaat? Geloven we werkelijk dat de letter van de wet regeert? Verliezen we opnieuw de essentie uit het oog? De kern van ieder bedrijf is en blijft leveren wat de klant eist en verwacht. Zonder een intrinsieke motivatie voor kwaliteit in de breedste zin van het woord heb je als bedrijf feitelijk geen bestaansrecht. Dataprivacy is anno nu simpelweg een van de kwaliteitseisen waar rekening mee gehouden moet worden, niet meer en niet minder. Als je dat als bedrijf nog niet deed, is het creëren van bewustwording en het initiëren, implementeren én borgen van (verbeter)maatregelen uiteraard best een flinke klus. Maar maak het niet ingewikkelder of groter dan nodig. En zoek aansluiting bij wat er al is.

Voorbij de AVG-hype

Als de hype straks gaat liggen, zullen we wakker worden en terugkijken met een glimlach en misschien ook wel een klein beetje schaamrood op de kaken. 'Was er echt een moment dat we helemaal in de ban waren van de AVG/GDPR?'. 'Hadden we echt het idee dat we dit als geïsoleerd thema konden oppakken?'. egen die tijd heeft onze angst plaatsgemaakt voor vertrouwen. Bemerken we dat de privacy wet ons allemaal op persoonlijk niveau een gunst heeft verleend. Fatsoenlijk omgaan met persoonsgegevens is dan iets dat net zo vanzelfsprekend is als goede arbeidsomstandigheden en maatregelen gericht op een beter milieu. Een integraal onderdeel van het (kwaliteits)managementsysteem van iedere organisatie. Bedrijven komen er niet meer mee weg als er op dit vlak wordt 'gesjoemeld'. Op dat moment is de ware geest van de wet opgestaan. Tot die tijd ploeteren we nog even een tijdje door.

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.

PRINSJESDAG - WAT BETEKENT DAT VOOR CYBER SECURITY?

In de recent uitgesproken troonrede heeft koning Willem Alexander namens het kabinet de intentie uitgesproken om meer te investeren in de cyber veiligheid van de BV Nederland.

Zie bijvoorbeeld dit artikel: https://www.security.nl/posting/577545/Kabinet+investeert+miljoenen+extra+in+bestrijding+cybercrime). Wat denken onze redacteuren daarvan, gaat dit helpen cyber security op een hoger peil te brengen, of is het meer pleisters plakken op slagaderlijke bloedingen?

Fook Hwa Tan

Op 18 september 2018 was het weer Prinsjesdag. Dit jaar gaf de koning in de troonrede aan dat meer zal worden geïnvesteerd in de digitale veiligheid van BV Nederland. Dit jaar al zal een additionele 30 miljoen euro worden vrijgemaakt. Maar gaat dit daadwerkelijk helpen?
Het is mooi om te zien dat de overheid steeds meer haar verantwoordelijkheid neemt op het cyber domein. In Nederland hebben we steeds meer digitaal contact met de overheid. Veel overheidsinstanties zijn bezig met de verdere digitalisering van haar processen. Het is daarom belangrijk, dat ook op dit terrein de overheid voldoende investeert. Hierdoor zal in de komende jaren onze digitale hartslag verder worden versterkt. Wat betekent dit voor bedrijven? We zien dat veel organisaties cybersecurity op de agenda hebben staan of minimaal op het netvlies hebben. Ook de privacywetgeving en wetgeving over de nieuwe bevoegdheden van politie en inlichtingendiensten hebben hieraan bijgedragen. Wat je echter nog wel ziet is dat veel organisaties vaak de basis van cybersecurity nog niet op orde hebben. Misschien zelfs wel de basis van Informatietechnologie zelf. Het is daarom mijn hoop dat gezien de stappen van de overheid in de komende jaren, ook het bedrijfsleven en dan vooral de kleinere bedrijven meer prioriteit gaan geven aan cybersecurity om in ieder geval de basis goed te krijgen. Bedrijven moeten realiseren dat ze hierin een eigen verantwoordelijkheid hebben.

Maar wat mogelijk nog belangrijker zal zijn is dat cybersecurityspecialisten zich beter gaan inleven in wat de primaire processen en belangen van de organisatie zijn. De cybersecurityafdeling binnen organisaties is vaak nog een afgezonderde afdeling, die zich te weinig bezighoudt met waar de organisatie voor staat en hoe daarmee de continuïteit van de organisatie wordt geborgd. We moeten meer gaan denken zoals de rest van het bedrijf om een beter en gefundeerder advies te kunnen geven aan het management over cybersecurity. Met deze invalshoek zal cybersecurity net als andere innovaties in een organisatie goed kunnen worden afgewogen. Al met al zal de aangekondigde investering tijdens Prinsjesdag helpen bij het verhogen van het peil van cybersecurity. Maar we hebben nog een lange weg te gaan. Overheid en bedrijven moeten zowel afzonderlijk als samen te werk gaan om cybersecurity op een niveau te krijgen dat voldoende is voor burgers en klanten om vrij te kunnen handelen in Nederland. We moeten echter niet opgeven, maar juist elke stap in de goede richting aanmoedigen!

Patrick Dersjant

Voorkomen is beter dan genezen. Dat is een dooddoener, en dat weet ook elke beveiligingsexpert. Met allerlei maatregelen proberen we met zijn allen juist te voorkomen dat kwaadwillenden aan de haal gaan met onze gegevens, systemen en in toenemende mate andere


Maarten Hartsuijker


Lex Dunn


Patrick Dersjant


Fook Hwa Tan

`connected things'. Dan is een half miljoen uittrekken voor het bevorderen van veilige hard- en software niet veel. De 30 miljoen extra voor dit jaar blijken netjes over de verschillende departementen verdeeld te zijn. Een echte visie en focus lijkt niet te herkennen, of het moet de versterking van het Nationaal Cyber Security Centrum zijn. En hoewel dat ook voorlichtende taken heeft, ligt daar de focus toch meer op het opsporen en verhelpen van incidenten (en de informatie uitwisseling daarover).
Doe je echter en stapje terug en kijk je niet meer naar de bomen, maar naar het bos, kun je dat `uitsmeren' ook positief bekijken. Onder één gemeenschappelijke noemer hebben alle ministeries opeens de opdracht gekregen `iets' aan informatiebeveiliging te doen. En hoewel dan het te besteden bedrag dit jaar misschien klein is, loopt dat wel op de komende jaren. Dat zorgt aan bestuurstafels voor de broodnodige discussie, want over het uitgeven van geld wordt altijd gepraat. Nu dit geld `geoormerkt' is, dus voorbehouden aan een bepaald onderwerp, gaat de discussie per definitie ook over dat onderwerp zelf. Waarmee de bewustwording en aandacht voor het onderwerp ook in de top van de overheid weer een broodnodig extra zetje krijgt.

Maarten Hartsuijker

Het functioneren van onze samenleving is volledig afhankelijk geworden van ICT. En onenigheden in de wereld worden steeds vaker uitgevochten binnen het digitale domein. Het is dus niet meer dan logisch dat cyberveiligheid prominent op de agenda staat. Extra financiële ruimte helpt uiteraard om de veiligheid te verbeteren, mits het goed wordt ingezet.
Vergeleken met de investeringen die de grote spelers doen in offensieve en defensieve capaciteiten is 95 miljoen natuurlijk een schijntje. Maar persoonlijk vind ik scherpe budgetten wel een goede prikkel afgeven. Zeker aan de offensieve kant, waar momenteel een race plaatsvindt die alleen interessant is voor landen die offensieve middelen verkopen. Budgettaire beperkingen dwingen ons tenminste om dubbel zo goed na te denken over waar elk dubbeltje het meest effectief kan worden ingezet. Daar waar het de Wet Computercriminaliteit III betreft, kan dit wat mij betreft zeker geen kwaad. Als er minder geld beschikbaar is voor het massaal tappen van verkeersstromen en het leveren van een bijdrage aan een sector die kwetsbaarheden geheim houdt om inbraken op systemen te faciliteren (wat ons allemaal onveiliger maakt), dan juich ik dat van harte toe. Al gaat er natuurlijk ook een risico van uit.
Want als we bijvoorbeeld wél geld hebben voor het aanschaffen van de tapapparatuur, maar geen geld meer hebben om de analyse van al die data goed uit te voeren, dan is samenwerking met derden hier een aantrekkelijk alternatief. Maar daar waar analyses als een "vriendendienst" worden verricht, geldt waarschijnlijk het op internet o zo bekende adagium: if you're not the customer, you're the product. Gaat dit extra bedrag cybersecurity op een hoger plan brengen? Het draagt er zonder twijfel aan bij. Maar ik hoop dat er (gezien de garantie op incidenten die er ongeacht de investeringen blijft) in het budget toch ook rekening is gehouden met de aanschaf van wat extra pleisters.

Lex Dunn

Hoeveel geld is nodig om de BV Nederland op cybergebied voldoende weerbaar te maken? Geen mens die het weet. We proberen al jaren een inschatting te maken van wat cyberincidenten ons als maatschappij kosten. Als je de verschillende jaarlijkse rapporten daarover naast elkaar legt, blijkt dat dit een moeizame exercitie is, gezien de grote verschillen. Dan is het ook moeilijk te bepalen of de in de begroting opgenomen bedragen voldoende zijn. Het gaat er nu om de toegezegde bedragen op een goede manier in te zetten. Versterking van het Nationaal Cyber Security Centrum als een CERT lijkt een goede zet, maar helaas blijft dit nu ook weer beperkt tot de overheid en de vitale sectoren van de BV Nederland. En juist binnen het overige bedrijfsleven, vooral in het MKB en bij non-profit organisaties en verenigingen doen zich steeds meer cyberincidenten voor. Samenwerking binnen Europa is ook een goede zaak, want cybercriminaliteit is nooit beperkt gebleven tot landsgrenzen. Maar dan moet je dus ook de samenwerking uitbreiden naar de rest van de wereld. Om die cybercriminaliteit gericht en effectief te kunnen bestrijden is het uiteraard nodig om te weten wat er speelt, en dus zoveel mogelijk aangiftes binnen te krijgen. Maar dan moet je er wel wat mee gaan doen, dus meer cybercops inzetten. En waar halen we die vandaan? Door de recente invoering van de AVG is de beschikbare arbeidspool al behoorlijk uitgeput. Er moet dus snel instroom vanaf de opleidingen (zowel mbo als hbo en wo-niveau) beschikbaar komen, enerzijds door verkorte opleidingen te introduceren voor omscholers (denk aan het PION-programma van jaren terug) en anderzijds jongeren te interesseren in het vakgebied. En dat zijn nou juist zaken die ik mis in het verhaal.

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
Bianca Brooijmans
Patrick Dersjant
Nicole van Deursen
Rik van Dijk
Lex Dunn
Maarten Hartsuijker
Lilian Knippenberg
Hugo Leisink
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
José Broekhuizen
Lisa Petersen
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

TO FAKE OR NOT TO FAKE

Toen mijn vader nog leefde zei hij altijd tegen mij: "Berry, het staat in de krant dus is het waar". Ik heb dat lang geloofd, want waarom zou mijn vader daar over liegen. Hetzelfde zei hij overigens ook over bepaalde beroepsgroepen die volgens mij ook niet altijd de waarheid zeiden. De informatie die mijn vader ter beschikking stond, was ook vele malen beperkter dan de informatie die mij nu ter beschikking staat. Inmiddels ben ik wat ouder en ben ik opgegroeid met internet. Alle positieve en negatieve dingen kreeg ik daar gratis bij. Ik ben wel erg blij met het internet ondanks het feit dat ik in dit onvolprezen blad ook vaak het tegenovergestelde riep. Laten we het een haat-liefde verhouding noemen. Een aantal zaken heb ik ook links laten liggen, waar Twitter wel een van de bekendste is. Ik ben redelijk lang van stof en vind de hoeveelheid karakters te beperkt. Het tweeten is aan mij niet besteed, ik ben zelfs voor de inleiding van deze column al meer karakters kwijt. Toch is de president van het machtigste land ter wereld in staat om via Twitter te communiceren. In mijn ogen redelijk gewaagd, maar wie ben ik. Trump noemt Twitter een van de bronnen van fake news. Facebook heb ik altijd wel grappig gevonden hoewel, de meeste mensen niet eens weten dat ik erop zit, want echt actief kan ik mijzelf op Facebook niet noemen. Ik beschouw het ook meer als een vorm van het tonen aan de hele wereld hoe boeiend je leven is en hoe lekker je gisteren weer met al je vrienden gegeten hebt. Ik vind het goed. Volgens Trump is ook Facebook een vergaarbak van fake news. Wat ik wel geweldig vind, is het gebruik van Google, ja ik weet dat ze precies weten wat ik allemaal zoek en ze willen graag al je foto's en al je mail op hun schijven zodat ze die rustig kunnen doorspitten. Een zoekopdracht is geweldig en mijn teleurstelling was dan ook groot toen ik las dat Trump van mening is dat de zoekresultaten van Google gemanipuleerd worden. Tja, dat zou kunnen. Dat de zoekopdrachten ook bewezen feiten bevat laten we maar even voor wat het is. Dat veroordelingen van zijn medewerkers door hem als fake news worden beschouwd is een beetje sneu van meneer Trump. Hij gaat zelfs zo ver dat hij van mening is dat de rechtse media genegeerd worden en de linkse media die alles ter plekke bedenken voorrang wordt gegeven. Als dat het geval is dan heeft hij gelijk dat er censuur wordt gepleegd. Het moet ook een vervelend gevoel zijn als je het idee hebt dat iedereen tegen je is. Dat hij verklaringen van het Witte Huis tegenhoudt over de heldendaden van de overleden John McCain dat is geen censuur, dat is alleen maar schandalig.
Misschien had mijn vader toch wel gelijk over het waarheidsgehalte van de kranten.

Berry

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

NIEUW IN ONS PORTFOLIO

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®**, **IAPP®**, **ISC²®** en **ISACA®**.
Daarnaast biedt de Security Academy een aantal specialistische opleidingen aan. Denk hierbij aan opleidingen als Mobile Security, Identity and Access Management of Social Engineering.
Voor het complete overzicht, meer informatie en cursusdata kunt u terecht op onze website.

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