IB Cover 43 Restyle - 2019_Opmaak 1 09-07-19 13:00 Pagina 1

INFORMATIEBEVEILIGING MAGAZINE

- Amerikaanse en Nederlandse jongeren worden cyberheroes in Rotterdam
- Cybercriminaliteit: ver-van-mijn-bed-show tótdat je er zelf wakker van ligt
- Een kijkje over de grens
- 20 manieren om je securitycarrière te blokkeren

JAARGANG 19 - 2019 - EDITIE 4

Ad Pagina2 IB4_Opmaak 1 11-07-19 14:57 Pagina 1

SRC
Secure Solutions

srcsecuresolutions.eu
info@srcsecuresolutions.eu

CISO
masterclass

Kennis brengt je naar de top,

de CISO Masterclass zet je aan het stuur!

Najaarseditie 2019: 30 & 31 oktober, 1 november

Meer informatie: cisomasterclass.nl / 079 – 360 4268

TSTC
ICT en Security Trainingen

Fast Track Certified Information Systems Security Professional CISSP
26–30 augustus 2019

Fast Track Certified Cloud Security Professional CCSP
26–30 augustus 2019

Fast Track Certified Data Protection Officer CDPO
16–20 september 2019

Fast Track Certified Chief Information Officer C|CISO
4–8 november 2019

www.tstc.nl

IB4_2019 Voorwoord & Inhoud_Opmaak 1 11-07-19 15:06 Pagina 3

Wil de echte informatiebeveiliger nu opstaan?

De wat oudere lezers herinneren zich misschien nog het televisieprogramma 'Wie van de Drie'. Dan zaten er drie personen die allemaal dezelfde naam en hetzelfde beroep uitspraken. Het panel moest door middel van slimme vragen raden wie de echte beroepsuitoefenaar was.

Het zou een leuk spel zijn tijdens een PvIB-bijeenkomst: "Mijn naam is … en ik ben informatiebeveiliger." Het panel zal wekenlang bezig zijn met vragen stellen en waarschijnlijk nooit tot een conclusie komen, omdat elke ib'er in de praktijk heel uiteenlopende taken heeft te vervullen.

In iB-Magazine proberen wij dan ook om zoveel mogelijk verschillende artikelen op te nemen die de volle breedte van ons vakgebied omvatten. Een enkele keer verzamelen we juist weer een heleboel artikelen die bij één thema horen, zoals in het vorige iB-Magazine - waar de focus lag op privacy-onderwerpen.

Deze keer laat dit magazine juist de diverse uitersten van ons vak zien. De onderwerpen variëren van menselijke communicatie tot techniek, van internationale samenwerking tot verzekeringen en van informatiemanagement tot neurowetenschap.

Het is dan ook geen makkelijke taak om de beroepsprofielen die door het PvIB zijn ontwikkeld uit te werken in competenties en leerdoelen van opleidingen voor informatiebeveiligers. Ook daar publiceren we deze keer een artikel over, want nadenken over wie onze toekomstige ib'ers moeten zijn en wat zij allemaal moeten kunnen, is van cruciaal belang. Technische kennis is slechts een deel van de vereiste competenties. In de woorden van Richard van Hooijdonk (lees hier meer over in dit magazine): "Kinderen van nu moeten we opleiden met filosofie, antropologie, psychologie en sociologie, zodat zij morgen de uitleggevers kunnen zijn."

Nicole van Deursen en Chris de Vries

Rectificatie iB-3
De auteursinformatie van Kim Reijnen in iB-3 was onjuist. Het artikel was geschreven door Kim Reijnen van Kim Reijnen, Legal Support & Training. Kim is een freelance privacyrecht adviseur, trainer en CIPP/E gecertificeerd. Kim is tevens coördinator van het privacyrecht nieuws bij SDU. Kim is te bereiken via kim@kimreijnen.nl en linkedin.com/in/kimreijnen.

IN DIT NUMMER

3 Voorwoord - Wil de echte informatiebeveiliger nu opstaan?
4 Een individuele ondernemer aan het woord over cyberzelfvertrouwen
6 Verslag van een PvIB-themabijeenkomst: Maesbruggen III
8 Amerikaanse en Nederlandse jongeren worden cyberheroes in Rotterdam
10 Is de routetabel wel veilig?
15 Column Privacy - #Doeslief tegen de FG
16 Cybercriminaliteit: ver-van-mijn-bed-show tótdat je er zelf wakker van ligt
18 Communicatie en informatiebeveiliging
21 Column Attributer – Governed
22 Een kijkje over de grens
25 Blog - 20 manieren om je securitycarrière te blokkeren
30 Verslag Security Bootcamp 2019
37 Bestuur in beeld - Kelvin Rorive
38 Masteropleiding Technische Cybersecurity gebaseerd op PvIB-beroepsprofiel
42 Refactor de factoren
44 Achter het Nieuws – Bitcoin: to be or not to be?
47 Column Berry - Het is allemaal nep

IB4 Cyberzelfvertrouwen_Opmaak 1 09-07-19 13:04 Pagina 4

Jeroen Salemink is econoom en mede-eigenaar van Iconica Development BV. Jeroen is bereikbaar via jeroen@iconica.nl.

Een individuele ondernemer aan het woord over cyberzelfvertrouwen

IB4 Cyberzelfvertrouwen_Opmaak 1 09-07-19 13:04 Pagina 5

Cybersecurity is een containerbegrip, maar wat is 'cyber'? Volgens Wikipedia is cyber 'een voorvoegsel dat gebruikt wordt voor iets wat met internettechnologie samenhangt'. Dat is mooi. Dan heb ik een cybertelefoon, een cyberbedrijf en ik schrijf nu een cyberblog.

Ik wil dit moment gebruiken om mijn mening over het belang van bewustwording omtrent cybersecurity te etaleren. Het nieuws staat er vol mee, mensen spreken erover, je leest over de grootschalige datalekken en diefstal van miljoenen euro's. Dat de nieuwswaarde hoog is begrijp ik, maar als je naar de echte risico's kijkt, zijn die miljoen diefstallen van een euro een veel grotere last voor de gemiddelde MKB'er en particulier dan die ene diefstal van een miljoen euro.

Het is interessant eens wat dieper in de materie te duiken bij al die kleine oplichtingen en diefstallen. Vaak is menselijk handelen de oorzaak. Mensen trappen in frauduleuze mailtjes, klikken op vreemde linkjes, geven telefonisch te veel informatie weg of vertrouwen onbekende mensen te snel. Respons van het bedrijf is vaak - naast technische verbeteringen - protocollen en beleid wijzigen. Medewerkers worden verplicht ieder kwartaal een nieuw wachtwoord aan te maken, of kunnen alleen nog inloggen met two-way authentication. Super slim, maar wederom is de sleutel tot succes de manier waarop het beleid wordt uitgevoerd door de medewerkers. Als het wachtwoord nu 'k0nlJn005' is, kan je raden wat het de volgende keer gaat worden. Mensen houden niet van repeterende handelingen, het wordt ervaren als een tijdrovende drempel die hen in het werk belemmert. Automatisch inloggen en overal hetzelfde wachtwoord bieden dan uitkomst. Klinkt als een open deur, maar je zal je verbazen hoe vaak het voorkomt.

Menselijk handelen

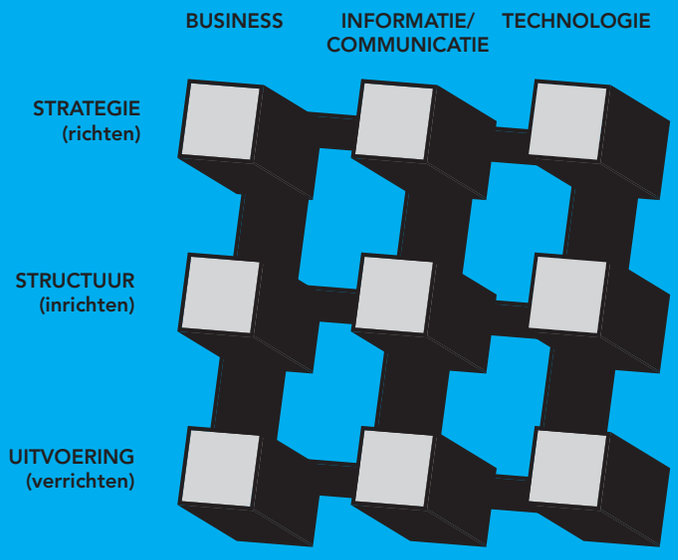
Daarnaast is de persoonlijke kant van fraude interessant. Als een medewerker een fout begaat, zou dat bij de interne controle boven moeten komen, maar hoelang loopt de organisatie dan al risico? Hoe sneller het kenbaar wordt, hoe sneller er gehandeld kan worden. Maar durven medewerkers hun fout te melden. Is je organisatie hierop ingericht? Is er een vertrouwenspersoon waar anoniem gemeld kan worden? Wat doet de organisatie met de medewerker? Ontslag omdat hij een paar duizend euro schade heeft veroorzaakt of contractverlenging omdat er net een paar duizend euro in de medewerker is geïnvesteerd? Daarnaast zijn vennoten van kleine organisaties een interessante groep. Bij kleine bedrijven kan een vennoot vaak zelf offertes aanvragen, goedkeuren en betalen. Dat maakt 'CEO-fraude' bij kleine bedrijven interessant. Een paar duizend euro valt in de cijfers vaak wel weg te werken. Vertelt de directeur dat ook aan zijn mede-vennoten? En wat doet dat met het vertrouwen van zijn mede-vennoten in het financieel beheer van de organisatie?

Leren van fouten

Uiteindelijk ligt menselijk handelen ten grondslag aan veel cybercriminaliteit. Stukje bewustwording over de risico's, over de do's en don'ts en een stukje kennis bijbrengen is even belangrijk als de 'harde' kant van cybersecurity: de organisatie veilig inrichten en het juiste beleid met bijbehorende protocollen opstellen. Maar we moeten niet doorslaan. Privé heb ik geen verzekering tegen ontvoering door buitenaardse wezens (schijnt echt te bestaan). Als dat gebeurt is de impact groot, maar de kans dat het gebeurt is klein; een gecalculeerd risico. We moeten een balans vinden tussen sublieme beveiliging en een werkbare situatie voor de medewerkers. Ten grondslag aan deze balans ligt een culturele verandering in het bedrijfsleven. Fouten maken mag, maar leer als organisatie van de fouten. Zorg dat medewerkers zich vertrouwd genoeg voelen om zaken bespreekbaar te maken en zie deze individuele fouten als collectieve leerpunten, evenals de individuele fouten collectieve risico's vormen.

Als we nog eens opnieuw naar de definitie van cybersecurity kijken, vertelt Google ons dat security vertaald kan worden als 'veiligheid', maar ook als 'bescherming' en 'zelfverzekerdheid'. Dat het dak spreekwoordelijk altijd lek is, is een gegeven. Maar weten wat de risico's zijn, weten hoe om te gaan met veiligheidsvoorschriften, weten wat het 'laaghangende fruit' is, dat zorgt - naast aantoonbare bescherming - voor een stukje zelfverzekerdheid. Voor een doorsnee weldenkend mens, die zichzelf geen cyberexpert noemt, is dat misschien wel het hoogst haalbare doel. Ik reken mijzelf tot deze groep en mij levert bewustwording en de daaruit voortvloeiende zelfverzekerdheid in ieder geval goede nachtrust op.

Nicole van Deursen is redacteur bij iB-Magazine.
Je reactie op dit artikel kan je sturen naar IBmagazine@pvib.nl.



Figuur 1 - Het negenvlaksmodel.

Maesbruggen III: verslag van een PvIB-themabijeenkomst

De Maesbruggen-III-avond stond in het teken van het model van Maes en hoe we de kloof tussen strategisch en operationeel kunnen overbruggen. Het was alweer de derde van een serie bijeenkomsten over dit thema.

De serie begon in 2014 met de probleemstelling van de kloof in het model van Maes. Rik Maes is hoogleraar Informatiemanagement aan de Universiteit van Amsterdam en publiceerde in 2003 het 'Amsterdamse negenvlak voor informatiemanagement' (1). Het negenvlaksmodel is een ordeningsschema voor vraagstukken van informatiemanagement.

Vraagstukken over informatiemanagement (en informatiebeveiliging) gaan over strategie (richting geven), structuur (inrichten) en operations (uitvoeren). In het model lees je deze onderwerpen van boven naar beneden.

Maes zelf stelt dat het interessantste aan dit model is wat er niet in benoemd wordt: de belangrijkste problemen en oplossingen schuilen in de verbindingen. De Maesbrugavonden gaan over een veelvoorkomende spagaat waarin informatiebeveiligers zich bevinden: de kloof in de verbindingen tussen de strategie van de business en de technische operatie. Je kunt dit verbeelden als een diagonale kloof door het model heen, van linksonder naar rechtsboven.

IB4 Verslag NvD_Opmaak 1 11-07-19 15:09 Pagina 7

Het negenvlaksmodel is een handig hulpmiddel om je taken als informatiebeveiliger in kaart te brengen

In 2014 was de eerste avond waar men discussieerde over architectuur, BISL, ITIL, en scenario's (verhalen) als middelen om de kloof te overbruggen. In 2018 ging de thema-avond over de organisatietypen van Mintzberg. Deze derde avond, in juni 2019, onderzocht drie mogelijke bruggen om de kloof te dichten: verhalen vertellen, tekststrategie, en aspecten binnen een professionele bureaucratie.

Overbodige informatie

De eerste presentator (Laurens Coenen, business continuity officer bij de Volksbank) was een schoolvoorbeeld van een verhalenverteller. Het publiek hing aan zijn lippen. Helaas is 30 minuten presentatietijd niet altijd genoeg als je veel wilt vertellen … Opvallend was dat juist de boodschap in deze presentatie was dat overbodige informatie zoveel mogelijk beperkt moet worden als je een kloof wilt overbruggen. Dit geldt vooral bij crisisplannen. Ten tijde van een crisis kun je niet verwachten dat het crisisteam 80 pagina's aan strategische beleidsdocumenten ter hand neemt. Wil je mensen tot actie aansporen dan moet de informatie simpel en makkelijk te vertellen zijn.

Scenariokaarten

Bij de Volksbank heeft men daarom de 80 pagina's crisisdocumentatie teruggebracht tot een pocketboekje en 8 scenariokaarten. Deze scenariokaarten zijn in 10 minuten te lezen en geven houvast voor het crisisproces in bepaalde soorten crisisscenario's. Zo bestaat er een scenariokaart voor als er een locatie uitvalt, maar ook één voor een cybersecurity-incident. Met het boekje en de kaarten kan het crisisteam snel aan de slag. Kloof tussen strategisch beleid en actie gedicht!

Tekststrategie

Marian Stoppelenburg geeft trainingen in tekststrategie en zij gaf het publiek een ander hulpmiddel om de kloof te dichten. Als je wilt dat iemand actie onderneemt, dan is het belangrijk om je boodschap helder over te brengen. Informatiebeveiligers produceren soms lange teksten om uit te leggen wat een medewerker wel of niet mag en welk gedrag er wordt verwacht. Veel medewerkers negeren deze teksten omdat ze het saai vinden of het niet begrijpen. Het verbeteren van saaie, langdradige teksten met lange zinnen en jargon zit 'm niet in het voorkomen van taalfouten. Wil je dat de boodschap overkomt, dan moet je eerst goed bedenken wat je wilt vertellen en wat je wilt dat de lezer gaat doen. Een goede tekststrategie helpt je om een pakkende tekst te produceren. Een goede tekst vraagt dan ook om een goede voorbereiding. Hiervoor kun je een eenvoudig stappenplan volgen. Wanneer je deze stappen volgt, is de kans dat je bereikt wat je wilt veel groter. De deelnemers aan de avond kregen allemaal een template mee waarmee ze hun eigen teksten kunnen aanpakken.

De derde brug om de kloof te dichten stond in het kader van de organisatorische positie van de CISO. Max Webber van Fontys Hogescholen nam de groep mee in een interactieve sessie waarbij het publiek kon stemmen over onderwerpen die te maken hebben met de plaats van de CISO in de organisatie (hoort het dichter bij een bestuur of zit het goed in de IT-afdeling?) en waarom we allemaal de organisatorisch lastig positionering accepteren? Wat is de beste plaats in de organisatie voor een CISO om alle vlakken uit het negenvlaksmodel te kunnen beïnvloeden?

Het negenvlaksmodel is een handig hulpmiddel om je taken als informatiebeveiliger in kaart te brengen. Wanneer samenwerking stroef verloopt of als je de indruk hebt dat de boodschap niet wordt opgevolgd, dan zou het best kunnen liggen aan de kloof tussen de verbindingen van de vlakken in het model. De Maesbruggen-thema-avonden geven handvatten om deze kloven te overbruggen. Kom jij de volgende keer ook?

Referenties

(1) R. Maes. Informatiemanagement in kaart gebracht. Maandblad voor Accountancy & Bedrijfseconomie (MAB), november 2003. Beschikbaar op: https://www.scribd.com/document/49144171/Informatie-management-in-kaart-gebracht.

Theo Sinnema is security project manager bij Schiphol en algemeen bestuurslid bij Cyberworkplace. Theo is te bereiken via t.sinnema@cyberworkplace.tech.

Amerikaanse en Nederlandse jongeren worden cyberheroes in Rotterdam

Een bijzonder programma, dat was het. Een groep van 10 jonge Amerikanen, uit achterstandswijken en indianenreservaten in de staat New Mexico, waren in maart een week te gast in Nederland om mee te doen aan het Cyberheroesprogramma. Dit op uitnodiging van het Rotterdamse Cyberworkplace en met ondersteuning van de Amerikaanse ambassade. Waarom? Om in Nederland te zien dat hacken ook ethisch kan en om jong talent enthousiast te maken voor een carrière in de cybersecurity.

IB4 Cyberheroes_Opmaak 1 09-07-19 13:17 Pagina 9

Op 18 maart kwamen de Amerikaanse jongeren aan in Rotterdam en startte het programma bij de Cyberworkplace in het centrum van de stad. De jongeren kenden de Cyberworkplace, een stichting die zich inzet om jongeren om te scholen tot cybersecurityspecialisten, via haar Amerikaanse partner Cultivating Coders. Bij deze partner hadden zij al meerdere intensieve programmeercursussen gevolgd. Van Nederland wisten ze nog weinig, maar dat hackers hier niet vervolgd worden was wel bekend

"Op dit moment loopt Nederland echt voorop in de partnerschappen met hackers. Nederlandse jongeren zetten hun kennis in om echte cybercrimezaken op te lossen en veiligheidsoplossingen te ontwikkelen. Dit gebeurt nergens anders ter wereld. Ik hoop dat wij - terug in de VS - ook echte heldendaden kunnen gaan verrichten", aldus één van de deelnemers voorafgaand aan het Cyberheroesprogramma. Voor vrijwel alle jongeren was de trip naar Rotterdam de eerste buitenlandse ervaring. "Maar 30 procent van de Amerikanen heeft een paspoort", kregen ze van de Amerikaanse ambassade te horen. "Het feit dat jullie hier alleen al zijn, maakt dat jullie een ervaring rijker zijn dan de meeste Amerikanen."

Veiligere digitale wereld

In de Cyberworkplace leerden de jongeren websites en systemen te beschermen, leerden ze hoe ze digitaal onderzoek kunnen doen en hoe ze codes kunnen kraken. De Amerikaanse talenten zagen van dichtbij hoe ethische hackers in Nederland bijdragen aan een veiligere, digitale wereld. Bekende hackers, werkgevers in IT-security en zelfs de politie hebben bijgedragen bij aan het Cyberheroesprogramma.
Met gerenommeerde sprekers zoals Phil Zimmerman, Oscar Koeroo en Melanie Rieback hebben de jongeren extra kennis vergaard over onderwerpen als cryptografie, penetratietesten en zeker niet onbelangrijk: ethiek. De handen konden uit de mouwen met een 'lockpicking challenge' en het team high tech crime van de politie heeft acte de présence gegeven om inzage te geven hoe er binnen Nederland wordt gewerkt om cybercriminelen net dát stapje voor te zijn. Ook de excursie binnen de Rotterdamse haven met de zeehavenpolitie was een bijzondere ervaring voor de jongeren. De laatste 2 dagen hebben de jongeren een bezoek gebracht aan de Blokhuispoort (historische gevangenis in het centrum van Leeuwarden) waar in samenwerking met Hacklab Friesland een succesvolle en leerzame 'capture the flag challenge' is georganiseerd - onder belangstelling van de lokale pers.

Easter egg

Naast deze leerzame activiteiten was er tijd ingeruimd voor een meet-up met de Amerikaanse ambassadeur Pete Hoekstra in zijn residentie in Den Haag. Er zijn een aantal foto's gemaakt in de residentie waarbij de jongeren zelfs een tot op heden niet ontdekte 'easter egg' mee naar binnen hebben genomen…
Het Cyberheroesprogramma heeft een diepe indruk gemaakt op de Amerikanen. Jong hacktalent wordt in de Verenigde Staten amper gestimuleerd. Zeker na de laatste presidentsverkiezingen hebben hackers daar een slechte reputatie. In Nederland is dat inmiddels anders. In plaats van jongeren te ontmoedigen worden hackers steeds vaker aangemoedigd om lastige veiligheidsproblemen voor het bedrijfsleven en de overheid op te lossen. Alleen al in de Cyberworkplace worden ieder jaar meerdere matches tussen jongeren en opdrachtgevers gemaakt. Ethisch hacken is in opmars.

Door de Amerikaanse jongeren te koppelen aan Nederlandse jongeren - die wekelijks bij Cyberworkplace bezig zijn de 21e eeuwse vaardigheden binnen het IT/cyberwerkveld te versterken - ontstonden er interessante interacties. Amerikaanse jongeren hoorden dat in Nederland hackers samenwerken met de politie. Of dat gemeenten en bedrijven zich vrijwillig laten hacken om daarmee eigen kwetsbaarheden boven tafel te krijgen. "In Amerika zouden agenten en gemeenten ons nooit vertrouwen, daar moeten we echt nog wat zendingswerk doen."

Cyber Peace Corps

Een hack- en wellicht cultuurschok rijker zijn de jongeren weer terug in New Mexico. Maar hoe gaat het nu verder? Alle deelnemers hebben aangegeven dat ze, geïnspireerd door het bezoek aan Nederland, cybersecurityspecialist willen worden. En de samenwerking gaat nog verder. Er worden nu plannen gemaakt om het eerste hacklab in de Navajo community op te richten. Ook de samenwerking met de talenten uit Rotterdam wordt vervolgd. Geïnspireerd door John F. Kennedy's Peace Corps zien de jongeren internationale heldendaden in het cyberdomein ook wel zitten. Zo zijn de eerste plannen voor een Nederlands-Amerikaans Cyber Peace Corps al gelanceerd.

Melchior Aelmans is senior systems engineer bij Juniper Networks.
Hij is bereikbaar via: maelmans@juniper.net.

Is de routetabel wel veilig?

IB4 Routetabel_Opmaak 1 09-07-19 13:27 Pagina 11

De opkomst van Software Defined Wide Area Networks (SD-WAN) met internet als fysieke netwerkinfrastructuur (underlay) ten opzichte van de traditionele 'private' Multiprotocol Label Switching-netwerken (MPLS) heeft een behoorlijke impact op de veiligheid van ons externe netwerkverkeer. De meest gebruikte internetprotocollen zijn niet 'secure by design' en dat geldt zeker voor het Border Gateway Protocol (BGP).

Dit 'two napkin'-protocol (1) voor het routeren van dataverkeer tussen netwerken staat aan de basis van het internet. Het werd enkele decennia geleden ontwikkeld voor een klein aantal netwerken om gegevens met elkaar uit te wisselen. Elk van deze netwerken in handen van één entiteit kreeg een Autonomous System Number (ASN) toegewezen. Tegenwoordig delen de vijf Regional Internet Registries (RIR) de AS-nummers uit: AFRINIC, ARIN, APNIC, LACNIC of RIPE NCC. Ook krijgen organisaties vanuit de RIR publieke IP-adressen tot hun beschikking.

Twee routers die door middel van BGP een verbinding tot stand hebben gebracht voor het uitwisselen van routinginformatie worden 'peers' genoemd. Dergelijke peers wisselen onderling routeringsinformatie uit via BGP-sessies die via TCP lopen. Nadat de BGP-sessie is opgezet, kunnen de routers de routing table, een lijst met netwerkroutes waar ze toegang tot hebben, weergeven (adverteren) en deze evalueren om de kortste route te vinden. Anno 1989 kenden de mensen die op deze netwerken actief waren elkaar. Er was geen noodzaak om maatregelen te nemen om de betrouwbaarheid van de informatie ontvangen van 'de ander' te toetsen. Men kon vrijelijk gebruikmaken van elkaars netwerken om informatie uit te wisselen tussen de verschillende organisaties op het internet.

Kwetsbaarheden

In 2019 voldoet BGP nog steeds redelijk goed voor haar basistaak: de routering van internetverkeer organiseren. Maar informatie-uitwisseling via internet wordt steeds veelomvattender en kritischer en toegang tot het dataverkeer biedt kwaadwillenden vele extra aanvalsmogelijkheden. Protocollen die worden gebruikt om informatie uit te wisselen (al dan niet afhankelijk van de wijze van implementatie) bevatten veelal 'man in the middle'-kwetsbaarheden. Goed vertrouwen volstaat niet langer als uitgangspunt om elkaars netwerken open te stellen voor het forwarden van internetverkeer.

Zoals eerder aangegeven ontvangen ASN-houders (ISP's en enterprises) publieke IP-adressen van een regionaal internetregister (RIR). Dit is echter geen garantie dat zij de enige partij is die deze IP-adressen kan gebruiken. Iedereen met een netwerk dat gebruikmaakt van het BGP kan deze IP-adressen - al dan niet opzettelijk - naar andere netwerken adverteren. Dus zelfs als deze IP-adressen aan een organisatie zijn toegekend, kunnen anderen die nog altijd gebruiken. En erger nog: op deze manier kun je je voordoen als een andere partij. BGP is hierdoor vatbaar voor misbruik door cybercriminelen. Dat kwam de afgelopen jaren pijnlijk aan het licht in de vorm van BGP-hijacks.

BGP-hijack

Onder een hijack wordt de bekendmaking van routes via BGP aan derden zonder de toestemming van de bronhouder, de rechtmatige gebruiker van de prefixes, verstaan. Dit hijacken, of kapen, gebeurt volgens RIPE NCC bijna dagelijks. Hijacks kunnen op wereldwijde schaal plaatsvinden (verspreid naar alle netwerken) of beperkt (slechts één of sommige netwerken). Daarnaast is er een verschil tussen toevallige of opzettelijke hijacks van IP-adressen. De aard van de hijack is over het algemeen goed te achterhalen door te kijken naar parameters zoals duur, herhaling, mogelijke doelen en de grootte van gekaapte adresblokken.

Er zijn voorbeelden te over van hijacks en het fenomeen is als dusdanig ook niet nieuw. Een bekend geval vond circa

tien jaar geleden plaats. Een nationaal telecombedrijf begon toen met het adverteren van de YouTube-IP-adressen in een poging om een specifieke dienst in dat land te blokkeren. Door een configuratiefout en het feit dat de upstream transit provider het bedrijf toestond om deze IP-reeks te adverteren gaf die het door aan de rest van het internet. Daarmee werd een hoop dataverkeer omgeleid. Omdat geen van de organisaties de juiste filters gebruikte, resulteerde een 'simpele' wijziging van de routering per ongeluk in een wereldwijde BGP-hijack.

Een meer recent voorval is de kaping van IP-adressen van DNS-servers van Amazon. Hierbij was sprake van een gerichte aanval. De kapers leidden hierdoor MyEtherWallet-verkeer om via een namaakportaal, zodat ze cryptomunten konden buitmaken. Dit had eenvoudig kunnen worden voorkomen als de betrokken netwerken gebruik hadden gemaakt van de juiste filters.

Tegenmaatregelen

In maart van dit jaar maakte de RIPE-gemeenschap een voorstel openbaar (2), waarin het aangeeft BGP-hijacking als een beleidsschending te zien, zelfs als beide partijen zich buiten de RIPE NCC-serviceregio bevinden. In het voorstel vraagt de RIR externe partijen om hijacks te melden en details van de kapingen door te geven, zoals 'getroffen netwerken', 'ASN van overtreders', 'hijacked prefixes' en 'duur'. Als dit gebeurd is, bepaalt RIPE NCC samen met een aantal wereldwijde experts, of de gemelde BGP-hijacks beleidsovertredingen vormen. De vermoedelijke hijacker ontvangt een rapport met een deskundig oordeel over de zaak.

Een belangrijke vraag is wat ASN-houders kunnen doen om hun routeringstabellen veiliger te maken en zo BGP-hijacks te voorkomen. Traditioneel worden firewalls en IDS/IPS-systemen als eerste beschermingslaag ingezet om het aan internet gekoppelde netwerk te beveiligen. Het BGP-protocol functioneert traditioneel echter buiten deze beschermingslaag, omdat het netwerk anders niet bekend zou zijn bij de rest van het internet. Kwaadwillenden kunnen daardoor ongestoord communiceren met de BGP-diensten van de netwerkrouters. Om te voorkomen dat reeds bekende ongeldige bronnen de BGP-diensten op de routers kunnen bereiken of dat routeringsbeslissingen worden genomen op basis van valse informatie, is het aan te bevelen om routing security toe te passen.

Routing security

Routing security wordt toegepast op de 'BGP-sprekende' routers die de rand van een DFZ-netwerk (default-free zone) vormen. Ze accepteren routes via BGP-sessies met klanten, transitproviders en collega's. Ze kondigen ook routes aan die afkomstig zijn van het eigen netwerk en van de netwerken van klanten. Een route-advertentie bestaat onder andere uit een combinatie van prefix, prefixlengte, oorspronkelijk AS en AS-pad. Beveiliging op dit niveau heeft tot doel het aantal mogelijk ongeldige aankondigingen die een netwerk accepteert te verminderen door ongeldige routeaankondigingen actief af te wijzen en door ervoor te zorgen dat alleen de eigenaar zelf de juiste prefixes kan aankondigen.

Door de juiste maatregelen te nemen op de BGP-edge routers kan worden voorkomen dat het netwerk van de AS een ongeldige prefix bereikt. Daardoor wordt het onmogelijk om volledige tweerichtingscommunicatie tot stand te brengen en kunnen bedreigingen zich veel lastiger verspreiden. De eerste stap om routing security toe te passen, is het gebruik van basisfilters. We bespreken hieronder de belangrijkste filters om 'foute' routes uit te sluiten.

Wijs bogon ASN af

Een BGP-routeaankondiging bevat een veld, het zogenaamde AS-pad, dat bestaat uit de AS-nummers van alle netwerken die de routeadvertentie verspreiden om de bestemming te bereiken, het oorspronkelijke autonome systeemnummer. De AS-paden in de routetabel worden automatisch aangemaakt wanneer elk netwerk dat een routeadvertentie propageert zijn eigen autonome systeemnummer aan het pad toevoegt. Tot slot is het mogelijk om handmatig een AS-nummer voor te bereiden om de routebeslissingen te beïnvloeden.

Naast de openbare AS-nummers, die door de RIR's zijn toegekend, zijn er privé AS-nummers die voor verschillende doeleinden kunnen worden gebruikt (zoals privé peering met netwerken die geen RIR-gebonden AS-nummer nodig hebben). Vroeger waren alle AS-nummers 16-bits (van 0 tot 65.535), maar tegenwoordig worden ook 32-bit nummers universeel ondersteund. De verschillende soorten autonome systeemnummers zijn:

- 0: gereserveerd;
- 1 tot en met 64.495: openbare AS-nummers;
- 64.496 tot en met 64.511: voorbehouden voor gebruik in documentatie;

IB4 Routetabel_Opmaak 1 09-07-19 13:27 Pagina 13

- 64.512 tot en met 65.534: privé AS-nummers voor intern gebruik binnen een netwerk;
- 65.535: gereserveerd;
- 4.200.000.000.000 tot en met 4.294.967.294: 32-bits privé AS-nummers.

Privé AS-nummers worden vaak gebruikt voor netwerken die niet beschikken over een publiek autonoom systeemnummer dat door een RIR is toegekend om een BGP-sessie met een upstream-netwerk op te zetten. Hier kunnen gemakkelijk fouten ontstaan. Privé AS-nummers kunnen per ongeluk in een voor het publiek zichtbaar AS-pad lekken. Of soms typt een netwerkoperator het AS-nummer verkeerd waardoor het pad vervuild raakt. Zowel privé AS-nummers als foutieve prefixes worden 'bogons' genoemd, verwijzend naar het woord 'bogus' (onzin). Daarom is het belangrijk om route-advertenties, die een privé of gereserveerd autonoom systeemnummer bevatten, af te wijzen.

Wijs bogon prefixes af

Een bogon prefix mag niet zichtbaar zijn in de wereldwijde routeringstabel, aangezien deze prefixes bedoeld zijn voor intern gebruik (RFC 1918), testnetwerken (RFC 4737), multicast, en andere interne doeleinden. Deze prefixes mogen dus nooit worden geaccepteerd of geadverteerd in de DFZ.

Wijs lange prefixes af

De wereldwijde routeringstabel in de DFZ groeit nog elke dag, omdat steeds meer netwerken steeds meer prefixen aankondigen. In principe is het geen probleem om routes van welke lengte dan ook aan te kondigen - technisch gezien werkt zelfs een /32-route (voor een enkel IPv4-adres). Een ongecontroleerde groei van de routeringstabel is echter niet duurzaam (bereken maar eens hoeveel groter de DFZ zou zijn als alle IPv4-ruimte als een /32 zou worden aangekondigd). Veel netwerken zijn dan ook begonnen met filteren op prefixlengte. Het algemene uitgangspunt is dat een aankondiging zal vervallen als een aangekondigde prefix /25 of langer is (een subnet van 128 IPv4-adressen of minder). Deze filter zorgt ervoor dat alle /28 en /32 routes niet in de routing information base (RIB) terechtkomen. Hetzelfde geldt voor IPv6 waar een grens van /48 kan worden aangehouden.

We hebben eerder gezien dat elk netwerk op de route automatisch een AS-pad opbouwt en een eigen AS-nummer toevoegt aan de voorkant van het AS-pad van de geadverteerde route. In de praktijk, aangezien BGP standaard het kortste AS-pad zoekt, hebben de meeste actieve routes die een netwerk gebruikt een AS-pad van slechts 16 AS-nummers. Soms kan een pad wat langer zijn en dan is er natuurlijk een handmatig AS-pad (als een verkeerstechnische maatregel) waardoor langere paden in de tabel te zien zijn. Maar in het algemeen kan een AS-pad dat langer is dan een tiental AS-nummers als nutteloos worden beschouwd.

De meest voorkomende reden voor extreem lange AS-paden zijn handmatige ingrepen in de routering. Het gebruik van twee tot drie keer het eigen ASN in een 'prepend' is, indien nodig, een goede manier om verkeersstromen te beïnvloeden. Meer dan dat wordt als zinloos beschouwd. Kijkend naar de DFZ zijn er enkele prefixes met een AS-padlengte van ongeveer 40 AS-nummers waarvan ten zeerste betwijfeld wordt of dat nuttig is. Laten we een veilige marge nemen en alles met een AS-pad van meer dan 50 beschouwen als nutteloos. Die kunnen worden weggefilterd uit de beveiligde routeringstabel.

Wijs routes van Tier-1 netwerken en grote netwerken van ASN's af

De grootste netwerken ter wereld (bekend als Tier-1) kopen nooit transit van elkaar of van kleinere (Tier-2) netwerken. Het zou bijvoorbeeld heel vreemd zijn als een klant of collega-ISP routes zou sturen die AS2914 (NTT) of AS1299 (Telia) in hun AS-pad hebben. Daarom is het goed AS-padfilters in te stellen, die routes weigeren die de AS-nummers van de 'grote namen' in zich hebben. Daaronder vallen ook sommige andere zeer grote netwerken zoals Facebook, Google, Microsoft en Cloudflare.

Het gebruik van de hierboven beschreven filters biedt bescherming tegen het accepteren van routes die andere organisaties of ISP's per ongeluk doorsturen (lekken genaamd).

RPKI

De volgende stap om tot een veilige routing table te komen, is om ervoor te zorgen dat rechtmatige resource houders hun eigen route advertentie statement vastleggen. Oftewel: een ROA (Route Origin Authorisations) creëren en het Resource Public Key Infrastructure (RPKI)-systeem in staat stellen om de ontvangen en de geadverteerde routes te

IB4 Routetabel_Opmaak 1 09-07-19 13:27 Pagina 14

verifiëren. RPKI is een door de gemeenschap ondersteund kader waaraan alle RIR's, diverse software developers en prominente routerfabrikanten deelnemen. RPKI biedt de mogelijkheid tot 'BGP origin validation'. De vraag die het probeert te beantwoorden is: is deze specifieke routeaankondiging geautoriseerd door de rechtmatige eigenaar van de address space?

Opgemerkt moet worden dat RPKI niet het volledige AS-pad valideert. Het geeft aan of het oorspronkelijke AS die specifieke prefix mag adverteren. Op dit moment is er nog geen goede manier om het volledige AS-pad te valideren. Wel wordt er in de IETF gewerkt aan een mechanisme om dit probleem op te lossen (3)(4).

Origin Validation stelt netwerkoperatoren in staat om statements af te geven over de BGP routeaankondigingen die cryptografisch kunnen worden gevalideerd met de prefixes die zij ontvangen hebben. Deze statements worden ROA genoemd. Een ROA geeft aan welke AS bevoegd is om een bepaalde prefix van een IP-adres te adverteren. Bovendien kan het de maximale lengte van de prefix bepalen. Andere netwerkbeheerders kunnen hierop hun routeringsbeslissingen baseren.

Het gebruik van RPKI vereist actie op twee onderdelen:

1. De legitieme houder van een IP-prefix creëert een certificaat, of ROA, waarin staat van welke AS'en de prefixes zullen worden geadverteerd (afkomst) en de maximaal toegestane prefixlengte. Alleen de eigenaar van de IP-adrestoewijzing kan een ROA maken voor deze toewijzing (dit is betrouwbaarder dan andere beschikbare gegevens).

2. Andere netwerkoperatoren kunnen hun routeringsbeleid instellen op basis van de RPKI-validiteit van routeaankondigingen bij het vergelijken met de ROA's die zijn aangemaakt. Dit zijn de routing policies die uiteindelijk ongeldige aankondigingen zouden afwijzen.

Het creëren van ROA's voor de IP adress space binnen het autonomous system betekent dat andere netwerken nog steeds in staat zullen zijn om een poging te doen de IP prefixes te kapen. De netwerken die RPKI geïmplementeerd hebben zullen deze kapingen vervolgens echter weigeren.

Het RPKI-systeem maakt gebruik van een validator met een database van ROA's (Route Origin Authorisations) die een router in staat stellen om de ontvangen routes te controleren. Als de route volgens de database ongeldig is, wordt die niet in de routeringstabel geïnstalleerd. Door het ondertekenen van hun eigen routes en het controleren van de ontvangen routes kunnen de deelnemers dus bijdragen aan een veilige routeringstabel. De verificatie van alle ontvangen routes op ongeldige vermeldingen zorgt er bovendien voor dat die niet worden doorgegeven aan andere ISP's, internetknooppunten en klanten.

Een aantal (grote) operators zoals Cloudflare, AT&T, Fusix Networks, Coloclue en Atom86 heeft RPKI reeds binnen hun netwerk geïmplementeerd en wijzen actief ongeldige routes af. Op het internet zijn uitgebreide handleidingen te vinden waarin wordt uitgelegd hoe RPKI binnen het netwerk kan worden toegepast. Op de websites van RIR's valt hier ook een hoop informatie over te vinden. Verder bieden de meeste netwerkleveranciers op hun website informatie over het configureren van hun routers aan.

Deze aanpak kan vragen opwerpen over het ontbreken van een deel van de routeringstabel. Het actief afwijzen van routes met RPKI zorgt ervoor dat op dit moment ongeveer 0,79 procent (eigen berekening) van het internet in de tabel ontbreekt. Dat komt op een paar duizend routes neer. De vraag is echter waarom iemand überhaupt gebruik zou willen maken van deze ongeldige routes. Zeker gezien de potentiële schade die deze routes zouden kunnen opleveren is het niet verstandig om hiermee een gok te wagen. Het devies is om te beginnen met de installatie van een validator, het verifiëren van de routes die door routers worden ontvangen en het actief afwijzen van ongeldige vermeldingen om zaken als BGP-hijacking buiten de deur te houden. Het risico dat hierdoor schade ontstaat, wordt namelijk alleen maar reëler naarmate steeds meer netwerkverkeer al dan niet via SD-WAN via het publieke internet verloopt.

Referenties

(1) www.computerhistory.org/atchm/the-two-napkin-protocol/.
(2) www.ripe.net/participate/policies/proposals/2019-03.
(3) www.datatracker.ietf.org/doc/draft-ietf-grow-rpki-as-cones/ .
(4) www.tools.ietf.org/html/draft-azimov-sidrops-aspa-verification-01.

IB4 Column Rachel_Opmaak 1 11-07-19 15:10 Pagina 15

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

#Doeslief tegen de FG

"Ik ben FG en in mijn organisatie zie ik een gegevensverwerking waarvan ik denk dat die in strijd met de wet is, maar als ik ze daarop wijs, dan doen ze niets. Heeft u advies over wat ik dan kan doen?" Ik adviseerde de jonge mijnheer om – als het echt de spuigaten uitloopt – gewoon de gegevensverwerking stil te laten leggen. Hij keek me met grote vragende ogen aan en stamelde vervolgens: "Oh … mag ik dat dan doen als FG?" Mocht je het je echt nog afvragen, het antwoord is: DRIEWERF JA!

De AVG is alweer een tijdje onderweg en de terugkerende thematiek op congressen, waar ik spreek, is 'de rol van de functionaris gegevensbescherming' - en dan alle verschillende facetten ervan. De wet en ook de richtlijnen van de toezichthouders bieden enige houvast over waar allemaal aan voldaan zou moeten zijn als je een FG in huis hebt, maar de praktijk is toch vaak erg weerbarstig. Zo vertelde de dame die de FG-hotline van de Autoriteit Persoonsgegevens bemenst mij dat de telefoon roodgloeiend staat met FG's die het in de praktijk even niet meer zien zitten of het gewoonweg niet meer weten.

Dat kan aan de organisatie liggen waarin de FG moet werken, het gebrek aan competentie van de FG zelf of de moeilijke spagaat die je ervaart op het moment dat de baas je loon betaalt, maar je wel vervelende maatregelen moet nemen en je dat vervolgens kwalijk wordt genomen. En denk nu niet dat dit alleen in kleine organisaties voorkomt of organisaties die het niet zo nauw nemen met de wet en wel een klein risicootje lusten. Ook ik merk in mijn eigen organisatie dat er moeite is met mijn rol als interne en onafhankelijke toezichthouder. Op juist die spannende momenten moet je wel heel sterk in je schoenen staan om je rol goed te kunnen blijven vervullen.

Ik suggereerde onlangs aan een zaal vol met medevakgenoten dat het misschien ook gewoonweg eens tijd zou worden om niet alleen de functionaris goed op te leiden, maar ook de organisatie zelf. Het is natuurlijk ook best heel lastig om iemand in dienst te hebben die je geen instructies mag geven over zijn taken en die het je best wel eens heel lastig kan maken als het niet goed gaat met de privacy van de personen waarvoor je de verantwoordelijkheid draagt. Begrijp me niet verkeerd, een FG is er niet voor bedoeld om het een organisatie lastig te maken, maar zo wordt het wel vaak ervaren.

Ach, en misschien moeten we met zijn allen ook eens een beetje aansluiting zoeken bij Sire en de #doeslief en iets vaker stilstaan bij het feit dat we allemaal mensen zijn die zo goed mogelijk ons werk willen doen. Want eerlijk is eerlijk: zolang er advocaten worden ingehuurd om rapporten van die interne toezichthouder onderuit te halen, aangekaarte issues worden afgedaan met "Maar er is toch nog helemaal niet echt iets enorm misgegaan?" en AP overstelpt wordt met radeloze functionarissen, dan doen we toch nog iets heel erg fout en dat geeft geen comfortabel beeld voor de privacy van heel veel Nederlanders.

Rachel

Rodger Lukken is zakelijk adviseur bij Heilbron.
Rodger is bereikbaar via rodger.lukken@heilbron.nl.

Cybercriminaliteit: ver-van-mijn-bed-show tótdat je er zelf wakker van ligt

Cybercrimininaliteit kan iedereen overkomen. Het risico is groter dan je misschien denkt. De (financiële) gevolgen kunnen schrikbarend zijn. Het is dan ineens geen ver-van-mijn-bed-show meer als het jezelf overkomt. Je wilt dan natuurlijk niet wakker liggen van de enorme gevolgen, toch? Hieronder lees je meer over cybercriminaliteit en waarom het belangrijk is dat je vooraf maatregelen treft.

IB4 Cybercriminal_Opmaak 1 09-07-19 13:58 Pagina 17

Is je organisatie al eens getroffen door cybercriminaliteit? Bijvoorbeeld een aanval op je computersystemen, diefstal van data, chantage met ransomware, virussen of e-fraude. Niet? Prijs je dan gelukkig. Hoewel definities en statistieken variëren staat buiten kijf dat cybercriminaliteit ieder jaar nog steeds toeneemt en momenteel de snelst groeiende criminele activiteit ter wereld is. Het is dus niet zozeer óf je getroffen gaat worden door een cyberincident, maar eerder wanneer.

Het zijn niet alleen criminelen die ervoor zorgen dat vertrouwelijke (persoons)gegevens openbaar kunnen worden. Dit kan ook gebeuren door slordig gebruik van gegevensdragers, het delen van accountinformatie, maar ook door menselijke fouten.

Boete

Voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen uit de EU is de Algemene verordening gegevensbescherming (AVG) van toepassing om te voorkomen dat je als ondernemer hierin een te afwachtende houding aanneemt. De AVG dwingt tot actie en maatregelen. Doe je dit niet dan riskeer je een stevige boete van maximaal 20 miljoen euro of 4% van je wereldwijde omzet!

Ondanks het gebruik van alle vormen van informatiebeveiliging, dataencryptie of van antivirussoftware kan het verlies van één laptop al tot ernstige financiële gevolgen en reputatieschade leiden. Naast de aansprakelijkheid heb je ook te maken met kosten die je moet maken om iedereen te informeren over het dataverlies. Daarnaast kan je ook nog bedrijfsstilstand ervaren.

Vaak denkt men even een back-up terug te zetten. Maar is de back-up wel schoon? De SamSam ransomware is hier een goed voorbeeld van. Doordat het al lang in het systeem zat, is de back-up hiermee inmiddels ook besmet.

Hoe kan je deze kosten afdekken? Dat kan met een goede cyberverzekering. Met zo'n verzekering ontvang je dan niet alleen een financiële tegemoetkoming als er zich een dergelijk evenement voordoet, maar kan je ook terugvallen op een hulplijn die 24/7 bereikbaar is.

Team van specialisten

Met één telefoontje krijg je hierdoor onverplichte toegang tot een team van specialisten. Denk daarbij aan specialisten in technisch forensisch onderzoek, juridisch advies en data recovery. Maar ook ten behoeve van meldingsverplichtingen, reputatiemanagement en communicatie. De goede cyberverzekeringen betalen namelijk ook de kosten van een andere dienstverlener waarvan je gebruikmaakt.

Heb je dit specialisme al in eigen huis? En heb je een plan klaarliggen indien een incident je overkomt? Het gaat dan niet alleen om jouw ICT-responsplan, maar ook om de melding richting Autoriteit Persoonsgegevens (AP) of om de uitvoering van je plan van aanpak met betrekking tot beheersing van mogelijke reputatieschade. De eerste 48 uur zijn namelijk het belangrijkste als je een incident overkomt. Dan zijn de kosten in dat geval nog wellicht bijzaak.

Praktijkvoorbeeld

Het netwerk van een middelgroot advocatenkantoor werd gehackt. Gevoelige klantinformatie was mogelijk in gevaar waaronder een overnamekandidaat van een beursgenoteerde onderneming, een beoogd technologiepatent van een andere beursgenoteerde onderneming, een voorlopige prospectus van een participatiemaatschappij en een aantal lijsten met persoonsgegevens van eisers in een collectieve rechtszaak. Het bedrijf kreeg toen een telefoontje waarin geëist werd om €30.000 te betalen om verkoop van de informatie op de zwarte markt tegen te gaan. Het advocatenkantoor nam contact op met het cyberincident-responsnummer, een cyberincident-manager werd toegewezen en forensische ICT-experts en een juridisch adviseur werden ingeschakeld om het incident aan te pakken.

Daarnaast is er een callcenter opgezet waar men terecht kon voor vragen en er werd een pr-deskundige ingeschakeld om de impact op de reputatieschade te beperken. De totale kosten van dit incident kwamen uit op circa €295.000,-.

Regel dus vooraf goede bijstand en zorg dat je niet te laat handelt.

IB4 Nicole_Opmaak 1 09-07-19 14:08 Pagina 18

Nicole van Deursen is onderzoeker en redactielid van iB-Magazine. Dit artikel is geschreven op persoonlijke titel. Zij is bereikbaar via nicolevdeursen@hotmail.com.

Communicatie en informatiebeveiliging

Communicatieve vaardigheden zijn de meest gevraagde competenties in vacatures voor informatiebeveiligers. Toch besteden de meeste opleidingen en certificeringen maar weinig aandacht aan dit onderwerp. Kennis van communicatie is belangrijk voor informatiebeveiligers en dit gaat verder dan de trucjes voor interpersoonlijke communicatie zoals luisteren-samenvatten-doorvragen (LSD). Vaak heb je als ib'er te maken met het overtuigen en activeren van groepen mensen. Kennis van communicatie- en marketingmodellen kan je hierbij helpen.

In dit artikel bespreek ik 3 communicatiethema's:
1. Hoe mensen leren
2. De context waarin communicatie plaatsvindt
3. Hoe mensen beïnvloed worden

Hoe mensen leren

Veel security awareness programma's bieden trainingen en e-learningmodules aan. Critici van deze aanpak stellen dat dit soort trainingen niet tot gedragsverandering leiden en dat het inhoudelijk vooral gaat over wat de CISO wil vertellen en niet wat de mensen nodig hebben in hun dagelijks werk. De verklaring hiervoor wordt soms in verband gebracht met Blooms taxonomy voor niveaus van leerdoelen (1) . Veel ib-trainingen gaan niet verder dan het tweede of derde niveau van Bloom en leiden daardoor niet tot het niveau dat eindgebruikers nodig hebben om te kunnen koppelen aan hun digitale vaardigheden.

Een ander punt om rekening mee te houden is de leerstijl. Diverse onderzoeken concluderen dat de meeste mensen een voorkeur hebben voor een leermethode die een combinatie is van kijken, luisteren, lezen en doen. Awarenessprogramma's zouden daarom een combinatie van deze leerstijlen moeten aanbieden.

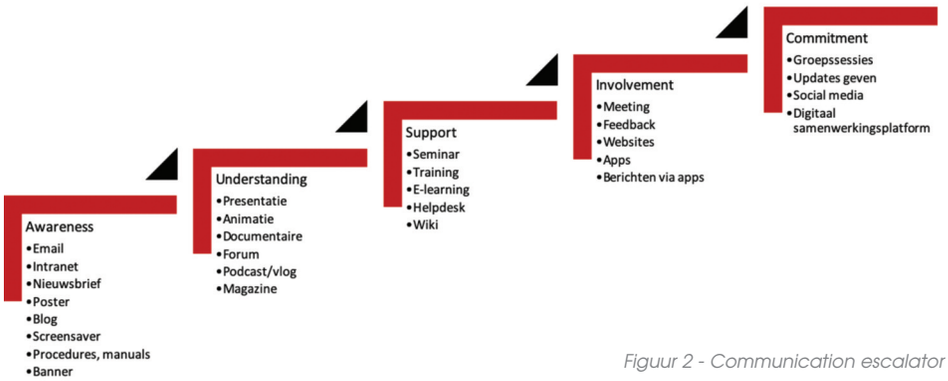
De context waarin communicatie plaatsvindt

De interne communicatie over ib-onderwerpen is sterk gerelateerd aan de cultuur en structuur van een organisatie.

Figuur 1 - Blooms taxonomy van leerdoelen.

Bijvoorbeeld in een machine-organisatie (2) is de communicatie vaak formeel en gestructureerd. In zo'n organisatie zijn er meestal veel handboeken. Een klassieke top-down-aanpak van ib met een beleid, procedurehandboek en audits past vaak goed in deze organisatie. Anders is het in een ondernemende organisatie, zoals bijvoorbeeld een startup. Daar is de communicatie vaak direct, horizontaal en informeel. In deze organisatie kun je als ib'er beter niet met een directieve communicatiestijl en allerlei voorschriften aankomen.
Wanneer gedragsverandering een doel van je communicatie-activiteiten is, biedt het model van de communication escalator

IB4 Nicole_Opmaak 1 09-07-19 14:08 Pagina 19



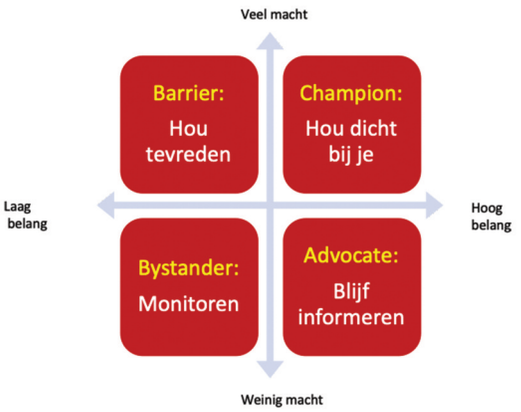
Figuur 2 - Communication escalator (aangepast origineel van Quirke).

van Quirke (3) een handvat. Het model beschrijft de doelen en middelen voor interne communicatie in een organisatie. Hoe hoger op de trap, hoe groter de beoogde gedragsverandering zal zijn. In het model is te zien dat awareness op de onderste trede ligt en dat voor echte verandering je moet streven naar commitment van je doelgroepen met ib-onderwerpen.

Soms kun je doelgroepen ook indirect beïnvloeden. Bijvoorbeeld door samen te werken met belangrijke spelers in de organisatie. Er zijn vaak mensen te vinden die invloed hebben. Niet door hun plaats in de hiërarchie, maar door hun sociale positie binnen een groep. Deze mensen kunnen je succes als ib'er positief, maar ook negatief beïnvloeden. Het kan je helpen om goede relaties met deze personen te onderhouden en ze in te zetten in je communicatieplannen. Een hulpmiddel om inzicht te krijgen wie deze personen zijn is bijvoorbeeld een stakeholderanalyse. Je kunt hiervoor een diagram tekenen met belangrijke personen en hun relatieve macht en belangen die zij hebben bij informatiebeveiliging. Op basis hiervan kun je een communicatieplan opstellen.

Hoe mensen beïnvloed worden

Marketing is een wetenschap dat zich richt op het begrijpen waar een klant behoefte aan heeft en welke benadering het beste past om die behoefte te vervullen. In de praktijk wordt die vaak ingevuld door activiteiten die het koopgedrag van klanten beïnvloeden. Eén van de oudste marketingmodellen die beschrijft hoe mensen worden beïnvloed tot het uitvoeren van een handeling (iets kopen) is het AIDA- model. AIDA staat voor 'Attention' (aandacht trekken door bijvoorbeeld te schreeuwen "Lekkere appels"), 'Interest' ("Vers van de boom"), 'Desire' ("Proef maar, kijk eens hoe anderen smullen") en 'Action' (je bent om en koopt).
Moderne marketingmodellen gaan echter verder. Kopen is niet meer het doel: de ervaring na het kopen is net zo belangrijk. Tegenwoordig vertrouwen mensen vooral op de F-factor (Facebook, friends, family, followers). Klanten worden gezien als vrienden van een merk en hun verhalen op social media en



Figuur 3 - Stakeholderdiagram.

voorbeeldgedrag is van grote waarde voor de perceptie over een product of dienst. Vooraanstaande marketing geleerden hebben een nieuwe variant op AIDA bedacht: de 5 A's (4). Deze staan voor: 'Aware' (I know it), 'Appeal' (I like it), 'Ask' (I am convinced), 'Act' (I buy it) en 'Advocate' (I recommend it). Dit model kan ook helpen om ib-programma's een stap verder te krijgen. Awareness is de eerste stap, maar waar je naar toe wilt is dat mensen elkaar het goede voorbeeld geven, daarover schrijven op social media en elkaar beïnvloeden.
Een ander beïnvloedingsmodel is het Elaboration Likelihood Model (ELM). Het model beschrijft dat er twee routes zijn om mensen te beïnvloeden. De centrale route is de logische, bewuste en bedachtzame route. In deze route denken (elaboration) mensen langer na over een boodschap die ze ontvangen. Dit doen ze alleen als ze interesse hebben in het onderwerp. Hoe langer de elaboratie, hoe groter de beïnvloeding op attitude en gedrag. De tweede route, de perifere route, vindt plaats als mensen geen zin, geen tijd, of te veel afleiding hebben. Ze beschouwen de boodschap slechts oppervlakkig en denken er niet over na. In deze route zijn mensen niet over te halen door goede argumenten, maar de aandacht kan wel getrokken worden oppervlakkige zaken zoals de populariteit van een spreker

IB4 Nicole_Opmaak 1 09-07-19 14:08 Pagina 20

of een mooi design, met een kortdurende beïnvloeding tot gevolg. Elaboratie wordt versterkt door herhaling van communicatie (maar niet te veel, anders gaat het voor mensen de perifere route in), interesse in de boodschap, goede concentratie en goede (persoonlijke) argumenten. Indien het publiek bij voorbaat al niet geïnteresseerd is in je boodschap, zorg dan voor een goede presentatie. Dit zorgt in ieder geval voor een tijdelijk, hoewel fragiel, effect.

Cognitieve dissonantie is een derde theorie voor beïnvloeding. Het is het ongemakkelijke gevoel dat je krijgt als je weet dat iets niet goed voor je is, maar het toch doet (bijvoorbeeld roken en drinken of de update uitstellen). Mensen praten dit gedrag vaak goed door tegenargumenten te gebruiken ("Na de update werkt die ene app niet meer") of door extra argumenten toe te voegen aan hun gedrag ("Het installeren van de update duurt te lang en ik moet nu iets afmaken"). Je kunt op diverse manieren omgaan met dit soort redenaties. Je kunt er bijvoorbeeld voor zorgen dat ze nieuwe overtuigingen krijgen door te laten zien wat de gevolgen zijn (hoe makkelijk het is om toegang te krijgen tot iemands computer), door ze nieuwe informatie te geven (handige oplossingen die ze nog niet kenden, zoals een wachtwoordmanagementprogramma), of door het belang van hun argumenten weg te nemen (door geforceerde beveiligingsinstellingen).

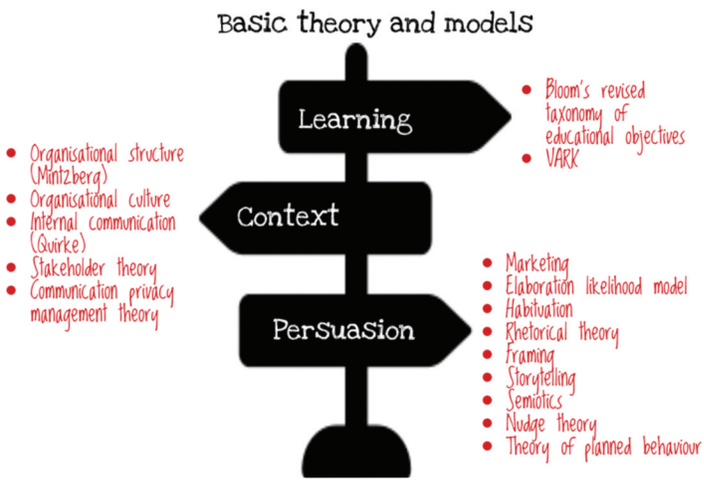
De laatste theorie die ik hier wil aanstippen is 'nudging'. Nudges zijn kleine aanpassingen in de omgeving van een gebruiker om de gewenste gedragskeuze te stimuleren (niet om af te dwingen). De meest bekende is waarschijnlijk de geschilderde vlieg in de urinoirs op Schiphol. Het schijnt dat mannen daar automatisch op mikken, waardoor ze minder naast de pot plassen. Nudges worden ook vaak toegepast in de ICT, zowel door criminelen als door beveiligingsspecialisten. Mensen zijn geneigd om op iets te klikken dat interessant lijkt, waardoor ze ongemerkt software kunnen installeren. Maar een metertje dat de sterkte van een wachtwoord laat zien bij het instellen is ook een nudge. Andere vormen zijn de vooraf aangekruiste privacycheckboxen en settings bij apps of websites, zoals de instelling of je wel of niet een nieuwsbrief wil ontvangen. Als daar standaard de meest veilige opties staan ingesteld, gaan mensen ze niet zo snel veranderen in de minder veilige opties.

Conclusie

Kennis van communicatietheorie kan ons helpen om betere beslissingen te maken over ib-awareness programma's. Enkele lessen om te onthouden zijn:

1. Pas je soort trainingen aan het niveau van je leerdoelen aan.
2. Gebruik bij training en voorlichting een mix van spraak, schrift, beeld en doen.
3. Kies een communicatiestijl die past bij de organisatiestructuur.
4. Maak gebruik van informele stakeholders en influencers.
5. Berichten moeten relevant zijn en herhaald worden.
6. Informatie moet passen bij wat men al weet en denkt.
7. Overtuiging heeft vertrouwen en geruststelling nodig.
8. De meest veilige beslissing moet makkelijk te maken zijn.
9. De sterkste beïnvloeding komt van de sociale groep waarin iemand zich bevindt.
10. Awareness is slechts een eerste stap en niet een doel. Streef je gedragsverandering en beïnvloeding na, dan moet de lat veel hoger liggen.

Het overzicht in dit artikel is bij lange na niet compleet. Er zijn meer relevante modellen binnen deze thema's, zoals te zien is in figuur 4. Bovendien is nog een vierde thema: overtuigen door middel van beeld, verhalen, retoriek, personal branding en symboliek. Wil je meer weten of meer lezen? Neem gerust contact met me op.



Figuur 4 Basis communicatie theorie en modellen (5).

Referenties:

1. B. S. Bloom and D. R. Krathwohl, Taxonomy of educational objectives: The classification of educational goals. New York, NY, USA, 1956.
2. Zie de typologieen van Mintzerg: H. Mintzberg, Mintzberg on management. New York, NY, USA: The Free Press, 1989.
3. B. Quirke, Making the connections: using internal communication to turn strategy into action., 2nd edition. London and New York: Routledge, 2017.
4. P. Kotler, H. Kartajaya, and I. Setiawan, Marketing 4.0: Moving from traditional to digital. Hoboken, New Jersey: John Wiley & Sons, 2017.
5. Uit: N. van Deursen, Visual communication for cybersecurity: beyond awareness to advocacy. River Publishers, juli 2019 (in productie).

IB3 new Column Attributer_Opmaak 1 09-07-19 14:10 Pagina 21

Governed

In the previous blog article (Conflicted, April 2019) The Attributer examined the potential conflict between the decisions made by autonomous systems and those made by their human operators. The case study was the alleged failure of the MCAS (1) system on the Boeing 737 Max and the part it may have played in two recent crashes of this aircraft. We draw our information for this article from a BBC News website article published on 17 May 2019 and accessed on that same date (2).

SABSA Thinking is based on systems thinking (3). Everything is a system or a system of systems. All that differs from one system to another is the definition of scope. This civil aviation case study clearly exemplifies the importance of system scope. We call the in-scope system the 'system of interest' or SOI (4).
Let's begin with the SOI scope as the 737 Max. However, we soon recognise there's more: the flight crew and the actions they took, their experience, their training, the systems that support their training, the resources available to them for incident management, their interaction with ground staff and air traffic controllers, the design of the MCAS sub-system, the flight testing, and the testing and certification of the aircraft.

The SOI scope must also include the manufacturer and its supply chain companies; industry regulators; independent safety auditors and inspectors and shareholders of all the commercial interests, including Boeing shareholders. Within such a complex SOI conflicts of interests are easily created, unless the governance lifecycle is well-constructed for independent oversight and honestly executed.

Every stage of an aircraft's complex lifecycle must be governed to assure compliance with standards of quality and safety that guarantee the safety of passengers, crew, and any other third parties on the ground where a plane might crash. The ultimate governance hierarchy is the regulating body in any industry that is regulated – in this case the FAA (5) in the US. They are responsible for certifying aircraft manufactured by Boeing.
The FAA is a relatively small government agency when compared with the corporate might of Boeing. The company employs more than 135,000 people, making it the main pool of expertise for engineers and auditors with the knowledge and skills to certify a complex aircraft. One of the goals of architecture work is to identify and resolve conflicts that might arise under these circumstances.
In fact, the FAA outsources 90% of its certification work to Boeing. The company is self-certifying in so many ways that it carries the burden of managing the significant challenges of intra- and inter-domain systemic risks and their unintended consequences. Independent oversight is the central challenge that they face, whilst simultaneously protecting their commercial interests and trading in a competitive marketplace.

Taking this scope analysis a stage further, we can see that the entire global civil aviation industry is the real scope of the SOI here, not just the 737 Max and its MCAS software. Boeing developed the 737 Max as a timely response to the Airbus A320. Its development and delivery required overcoming the serious technical difficulties of mounting larger engines on a re-engineered wing design.
At 1st January 2019 Boeing had an order book for more than 4,500 of the 737 Max, which tells you how right they were in their judgement of the market demand. The 737 family is the bestselling aircraft in the history of civil aviation (6). However, there are many industry commentators pointing to weak governance as the underlying cause of the failures. Perhaps some SABSA Thinking would help them.

The Attributer

References

(1) Maneuvering Characteristics Augmentation System.
(2) https://www.bbc.co.uk/news/resources/idt-sh/boeing_two_deadly_crashes.
(3) Enterprise Security Architecture: A Business-Driven Approach. 2005. Sherwood, Clark and Lynas. Chapter 5.
(4) As defined in ISO 42010: Systems and software engineering – Architecture Description.
(5) FAA: Federal Aviation Authority.
(6) http://www.b737.org.uk/sales.htm.

IB4 André Koot_Opmaak 1 09-07-19 14:14 Pagina 22

André Koot is consultant bij Nixu.
Hij is bereikbaar via andre.koot@nixu.com.

Een kijkje over de grens

Open grenzen, dat was een belangrijke missie van de EU. Open grenzen om de economische ontwikkeling van de lidstaten te versnellen. Dat heeft de lidstaten geen windeieren gelegd. De economische ontwikkeling maakt onderlinge samenwerking over de grenzen heen veel eenvoudiger door het afschaffen van tariefmuren en door het vrije verkeer van mensen en goederen mogelijk te maken.

IB4 André Koot_Opmaak 1 09-07-19 14:14 Pagina 23

Als je het geluk hebt om binnen het Schengengebied te blijven, dan ben je het concept 'grens' eigenlijk allang vergeten. Ook in de virtuele wereld merken we niets van grenzen. Wij versturen vanaf het begin van het internettijdperk pakketjes met data heen en weer en dankzij het TCP-protocol hoeven we ons geen zorgen te maken. Het pakketje komt wel aan. Maar juist op dit gebied blijken er toch forse grenzen te bestaan. Dankzij de wet- en regelgeving op het gebied van informatiebescherming, en dan met name op het gebied van privacybescherming, is er feitelijk niet zonder meer sprake van vrij dataverkeer. Er is sinds vorig jaar binnen Europa weliswaar één GDPR, maar elke lidstaat heeft die moeten omzetten in eigen wetgeving.

Virtuele grenzen

Op het gebied van informatiebeveiliging is er geen eenduidigheid die vrij verkeer op een transparante manier mogelijk maakt. Europese regelgeving ontbreekt en ook toezichthouders richten zich op de eigen landelijke wetten en regels. Daar waar in de fysieke wereld samenwerking en ketencontracten binnen de EU prima samengaan en daar waar organisaties uit de verschillende lidstaten over elkaars grenzen heen producten en diensten kunnen afzetten, leveren de virtuele grenzen grote problemen op. Kijk maar naar de volgende casus.

Eigen regels

De Nederlandse overheid wil diensten van een cloud service provider (CSP) aanbesteden, maar die CSP moet dan voldoen aan de vigerende wet- en regelgeving. In casu de AVG en BIO (Baseline Informatiebeveiliging Overheid, voorheen de BIR, Baseline Informatiebeveiliging Rijksdienst). Bij voorkeur moet die CSP ook ISO27001 gecertificeerd zijn en een ISAE3402-verklaring hebben. Een volstrekt logische set eisen. Maar wel een set eisen waar een CSP uit bijvoorbeeld de Tsjechische republiek niet aan kan voldoen: die kent namelijk de BIO niet en als die CSP al ISO27K gecertificeerd is, dan zegt dat eigenlijk alleen dat er een ISMS bestaat, niet of die partij ook BIO-compliant is. Of dat dan ook resulteert in de noodzakelijke passende beveiligingsmaatregelen voor clouddiensten ten behoeve van de Nederlandse overheid, is daar niet zomaar uit af te leiden. Oftewel: door het stellen van de betreffende eisen zou je, met een beetje een kritische blik, kunnen stellen dat de Nederlandse overheid het buitenlandse partijen onmogelijk maakt om aan de Nederlandse overheid clouddiensten te leveren. Marktbescherming. En dat geldt natuurlijk niet alleen voor de Nederlandse overheid, maar dat geldt voor alle lidstaten. Iedere staat heeft een eigen setje regels, waarmee feitelijk de buitenlandse concurrentie wordt buitengesloten.
Een tweede obstakel in de internationalisering: voor de verdere groei van digitalisering is de toenemende eis van toezichthouders om permanent in staat te zijn de betrouwbaarheid van geautomatiseerde verwerkingen te kunnen vaststellen. Waar een bank 10 jaar geleden de primaire processen nog volledig in eigen hand had en de systemen in eigen rekencentra draaiden, is de transitie naar uitbesteding hedentendage in volle gang. En daar waar overheden nog strikte eigen reguleringen hanteren, maken financiële instellingen al op grote schaal en wereldwijd gebruik van CSP's. Zij kennen geen grenzen meer. Waar vroeger de auditors ter plekke konden meekijken, is dat nu niet meer haalbaar. In de cloud bestaat dat niet meer. Over de landsgrenzen heen kan een toezichthouder ook niet in de cloud kijken, terwijl de financiële instellingen daar wel op grote schaal aanwezig zijn.

In control

Beide problemen hebben te maken met de noodzaak van een cloud service provider om aan te kunnen tonen 'in control' te zijn op het gebied van security. Maar zowel de afzonderlijke lidstaten als de afzonderlijke toezichthouders schermen hun eigen zeggenschap af. De landsgrenzen beperken daarmee voor CSP's nog steeds de mogelijkheid om over grenzen diensten aan te kunnen bieden. Dat gaat in tegen het gedachtengoed van de EU, namelijk het wegnemen van handelsbarrières. Het wegnemen van deze 'in control'-barrières is dan ook de belangrijkste drijfveer achter het EU-SEC-programma. Het EU-SEC-programma is onderdeel van het Horizon2020-innovatieprogramma van de Europese Commissie. In 2016 heeft de Commissie een com-

IB4 André Koot_Opmaak 1 09-07-19 14:14 Pagina 24

petitie georganiseerd voor projecten op het gebied van certificering voor producten en diensten. De doelstelling van dit project is te identificeren wat de verschillen zijn, maar vooral de overeenkomsten tussen de wetten en regels van de verschillende lidstaten.

Certificeringsraamwerk voor clouddiensten

De Cloud Security Alliance heeft samen met 8 andere partijen (onder andere Nixu) een consortium opgericht om binnen het Horizon2020-programma een certificeringsraamwerk voor clouddiensten te ontwikkelen. Na de gunning van de innovatieopdracht aan het consortium is het project in 2017 begonnen met de eerste van 7 deelprojecten, namelijk de requirementsanalyse. Namens Nixu was ik de programmamanager voor deze eerste track. Daarbij werden de security- en privacyeisen alsmede eisen op het gebied van auditing, multi-party recognition en continuous auditing geïnventariseerd. Als basisraamwerk is gebruik gemaakt van de Cloud Controls Matrix (de 'CCM') van de Cloud Security Alliance (CSA).

Op basis van de geïnventariseerde requirements is een control framework met een control architectuur opgezet en zijn tools (door)ontwikkeld om de audits te kunnen faciliteren. Het control framework bevat onder meer verschillende soorten auditmethoden voor bijvoorbeeld ISO27K-achtige certificeringen en voor ISAE3402-achtige certificeringen.

Er waren al geautomatiseerde hulpmiddelen van bijvoorbeeld de CSA (STARWatch) en het Fraunhofer Institut (Clouditor). Vanuit het ontwikkelde raamwerk zijn de tools uitgebreid en binnen de EU SEC-auditaanpak werden de requirements, beheersmaatregelen en tools goed op elkaar afgestemd. Zo werden voor de Continuous Auditing certificeringsfaciliteiten meerdere nieuwe audit-API's gespecificeerd, waardoor auditors in staat zijn om continu de verwerking van CSP's te monitoren en auditen.

Op dit moment is het programma de pilot audits aan het afwerken. Vanuit de doelstelling zijn twee pilotprogramma's ontwikkeld. Het eerste programma richt zich op het uitvoeren van audits conform de multi-party recognition (MPR)-methode. Het tweede programma toetst de continuous auditing-aanpak.

MPR betekent dat voor het uitvoeren van audits of certificeringen gebruik kan worden gemaakt van al aanwezige audits en certificeringen en dat over de grenzen heen de eisen aan auditors afgestemd zijn. Hierdoor wordt hergebruik van al uitgevoerde rapportages en cerificeringen mogelijk gemaakt. Het MPR-programma bestond uit 4 pilots. De resultaten van deze 4 pilots zijn zeer bemoedigend. De EU-SEC-methode blijkt goed bruikbaar en levert toegevoegde waarde, onder meer doordat er door hergebruik van al aanwezige rapporten en bewijsstukken tot 80% minder controlehandelingen hoeven plaats te vinden. De belangrijkste randvoorwaarde is wel dat een CSP die in aanmerking wil komen voor een EU-SEC-audit zelf volwassen is op het gebied van security. Bij de pilots hadden alle CSP's een ISO2700-certificering.

Continuous Auditing houdt in dat een Cloud Service Provider aan de Cloud Service Consumer permanent inzicht kan (laten) verschaffen in het niveau van dienstverlening door de CSP en ook in het niveau van beveiliging: geautomatiseerde tools kunnen gebruik maken van API's om de CSP direct te bevragen. De resultaten van de Continuous Auditing pilot zijn momenteel nog niet in detail bekend.

Allemaal mooi en aardig, maar wat heb ik eraan? Dat hangt een beetje af van je rol. Feit is dat vrijwel elke organisatie al gebruik maakt van clouddiensten. Feit is ook dat er onduidelijkheid bestaat over de stand van zaken op het gebied van compliance en governance. Dus misschien is het niet nu relevant, maar voor de volgende doelgroepen zien we al wel toepassingsmogelijkheden:

- Als je clouddiensten aanbiedt, of als je cloud service provider bent en op een meer efficiënte manier wilt aantonen in control te zijn, dan zou je de relevante informatie van het project door kunnen nemen. Omdat EU-SEC nog in de innovatieprojectfase verkeert, is het nog geen formeel geadopteerde standaard. Maar we verwachten wel dat de EU en de lidstaten het zullen overnemen. Dat betekent dat je als aanbieder van diensten daarop voorbereid kunt zijn door gebruik te maken van deze kennis.
- Als je als klantorganisatie diensten wilt uitbesteden is kennisnemen van de informatie ook waardevol. Voor aanbesteding van clouddiensten is op dit moment toepassen van de CAIQ-methode van de CSA al bruikbaar, maar voor het inrichten van beheersmaatregelen biedt EU-SEC aanvullende handvatten.
- Als auditor is EU-SEC ook een waardevol hulpmiddel. De auditrequirements en de aanpak is volkomen in lijn met de vigerende standaarden en de aanvulling met tools (voor met name cloudomgevingen) is een bruikbare innovatie.

Op de projectsite www.sec-cert.eu/eu-sec/project-outcome zijn de volgende documenten te vinden:

- requirementsanalyses;
- methodes en architecturen;
- beschrijvingen van tools en aanpak;
- auditrapporten van de pilotaudits.

Mocht je inhoudelijk meer willen weten, aarzel niet om contact op te nemen.

Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligingsexpert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

20 manieren om je security-carrière te blokkeren

Meer dan goed gedrag (dat je nalaat) bepaalt slecht gedrag (dat je wél doet) het gebrek aan succes in je loopbaan. Marshall Goldsmith behandelt in zijn boek *What got you here, won't get you there* twintig gedragingen die jouw medewerkers helemaal gek maken. En waardoor het succes van je loopbaan stopt.

20 habits to avoid

1. **Winning too much**
2. **Adding too much value**
3. **Passing judgment**
4. **Making destructive comments**
5. **Starting with No, But or However**
6. **Telling the world how smart we are**
7. **Speaking when angry**
8. **Negativity or 'Let me explain why it won't work'**
9. **Withholding information**
10. **Failing to give proper recognition**
11. **Claiming credit that we don't deserve**
12. **Making excuses**
13. **Clinging to the past**
14. **Playing favorites**
15. **Refusing to express regret**
16. **Not listening**
17. **Failing to express gratitude**
18. **Punishing the messenger**
19. **Passing the buck**
20. **An excessive need to be 'me'**

Door je eigen foute gedragingen aan te vinken, is het een bruikbare 'to-stop-list'. Je kunt de lijst ook invullen voor een collega die men moeilijk of lastig vindt om mee samen te werken. Zo is het te verbeteren gedrag nauwkeuriger te benoemen dan te zeggen: "Je moet je gedrag echt veranderen hoor!" En door de slechte gewoonte(s) op een verantwoorde manier te melden, is het mogelijk jullie samenwerking te verbeteren. Goldsmith behandelt ook handige manieren voor geven en ontvangen van feedback (bij hem: feedforward). Dit helpt wanneer je het aandurft de lijst over jou te laten invullen door iemand die je zakelijk of privé kent. Of door al je collega's tegelijk in een 360°-beoordeling.

De tabel geeft de lijst van de 20 gewoontes die Goldsmith in zijn boek behandelt. Aan de hand van de tabel hiernaast geef ik een korte toelichting.

Twintig uitdagingen in interpersoonlijk gedrag

1. **Te veel winnen.** De gevoelde noodzaak om ten koste van alles en in alle situaties te willen winnen. Te veel willen winnen ligt ten grondslag aan bijna elk ander gedragsprobleem. Als we informatie achterhouden (zie 9), is dat om onszelf een voorsprong te geven. Als we favorieten spelen (zie 14), is dat om bondgenoten te winnen en 'onze kant' een voordeel te geven.
2. **Te veel waarde toevoegen.** Het overweldigende verlangen je eigen inbreng toe te voegen aan elke discussie. Wanneer iemand met een idee naar je toekomt, klop je hem niet op de schouder, maar zeg je: "Goed idee, maar het is beter als je het op deze manier doet." Nu heb je het idee misschien met 5% verbeterd, maar zijn commitment om het uit te voeren met 50% verminderd. Zijn idee is nu jouw idee – en de bedenker is er minder enthousiast over. Hoe hoger je komt in een organisatie, des te meer je andere mensen winnaars moet maken en des te minder je zelf steeds moet willen winnen.
3. **Beoordelingen geven.** De behoefte om anderen te beoordelen en onze eigen normen aan hen op te leggen. Met een mening in een normale zakelijke discussie mogen mensen het eens of oneens zijn, maar het is niet gepast om een oordeel te geven wanneer we mensen specifiek vragen om hun mening over ons te geven.

IB5 Blog Robert_Opmaak 1 11-07-19 15:12 Pagina 27

Mensen houden er niet van om bekritiseerd te worden, op welke indirecte wijze ook. Door je oordeel te vellen, jaag je mensen weg en weerhoud je jezelf van groter succes. Het geeft je alleen zekerheid dat deze mensen je niet opnieuw zullen helpen. Je mag geen enkele behulpzame opmerking van een collega, vriend of familielid beoordelen. Wat je er ook van denkt, houd dat voor jezelf, vraag door wat ze bedoelen en zeg 'dankjewel'.

4. **Destructieve opmerkingen maken.** Onnodig sarcastische en bijtende opmerkingen maken waarvan we denken dat ze scherp en geestig zijn. Destructieve opmerkingen zijn het snijdende sarcasme dat we uitspreken met of zonder intentie, maar met geen ander effect dan mensen neerhalen, ze verwonden of ons als superieur laten gelden. Ze zijn anders dan opmerkingen die te veel waarde toevoegen (zie 2), omdat deze hier alleen pijn toevoegen. Het is irrelevant of een destructieve opmerking waar is. De vraag is: is dit het waard om gezegd te worden? Dat is het vrijwel nooit.
5. **Zinnen beginnen met 'nee', 'maar' of 'echter'.** Overmatig gebruik van deze negatieve kwalificaties die in het geheim zeggen: "Ik heb gelijk, jij niet." Wanneer je een zin begint met 'nee', 'maar' of 'echter', maakt het niet uit hoe vriendelijk je toon is. De boodschap aan de ander is: "U hebt ongelijk." Daarna kan er niets productiefs gebeuren. En gebruik ook nooit het dubbelzinnige: "Dat klopt, echter ..." of "Ja, maar ..."
6. **De wereld vertellen hoe slim we zijn.** De noodzaak mensen te laten zien dat we slimmer zijn dan zij denken dat we zijn. Wat averechts werkt, is de bewondering van mensen willen winnen door hen te laten weten dat we minstens zo slim, of nog slimmer zijn dan zij. Slim zijn trekt mensen aan, maar zelf verkondigen hoe slim je bent, stoot mensen af. Zie ook 5.
7. **Spreken wanneer je boos bent.** Emotionele uitbarstingen zijn niet het meest betrouwbare leiderschapsinstrument. Wanneer je boos wordt, ben je meestal onbeheerst en als je jezelf niet beheerst, zijn mensen moeilijk te leiden. Je denkt dat je je temperament beheerst en dat je spontane woede kunt gebruiken om mensen te motiveren, maar het is moeilijk te voorspellen hoe mensen op jouw woede reageren. Woede is zelden de schuld van iemand anders. Het is een fout die alleen de onze is. Tel tot tien (of hoger indien nodig) om rustig te worden.
8. **Negativiteit of zeggen "Laat me jou vertellen waarom dat niet werkt."** De noodzaak om onze negatieve gedachten te delen, zelfs als ons daar niet om werd gevraagd. LMJVWDNW is een unieke fout omdat het pure negativiteit is, maar die vermomd is als 'behulpzaam zijn'.
9. **Informatie achterhouden.** De weigering informatie te delen om zo een voordeel boven anderen te behouden. Informatie is macht en dat maakt achterhouden nog extremer en irritanter. Opzettelijk achterhouden van informatie verwijdert waarde. Je ziet het bij mensen die elke vraag beantwoorden met een tegenvraag. Ze geloven dat iets onthullen hen op achterstand plaatst. Achterhouden bereikt zelden het gewenste effect. Je krijgt geen voorsprong en consoliderende kracht, maar kweekt wantrouwen. Tegen jou. Slecht zijn in informatie delen is iets anders dan moedwillig achterhouden. Maar voor de omgeving is het hetzelfde. Stop dus met achterhouden en deel je informatie.
10. **Niet de juiste erkenning geven.** Het onvermogen om lof en beloning aan andere personen te geven. Als je de bijdrage van iemand aan een teamsucces niet erkent, zaai je onrecht en behandel je mensen oneerlijk. Je berooft mensen van de emotionele winst van succes. Zonder erkenning kunnen ze niet 'afsluiten' en dat moet iedereen met elke interpersoonlijke transactie doen. Succesvolle presteerders worden geweldige leiders als ze leren de focus te verschuiven: van zichzelf naar anderen.
11. **Onverdiend krediet claimen.** De vervelendste manier om onze bijdrage aan enig succes te overschatten. Onverdiend krediet claimen voegt belediging toe aan het letsel ontstaan door de 'vergeten' erkenning (zie 10). Wanneer een collega de eer steelt voor een succes dat jij hebt gemaakt, is dat de interpersoonlijke misdaad op de werkplek die de meeste irritatie opwekt. Vraag je dus bij elke gebeurtenis af of het op enige manier mogelijk is dat iemand anders het krediet verdient voor 'jouw' prestatie. Zo ja (dat is meestal zo), bevestig dit dan.
12. **Uitvluchten zoeken.** De behoefte om ons vervelende gedrag te presenteren als een gegeven ("Ik ben nu eenmaal zo"), zodat mensen ons dat gedrag vergeven. Zodra je volwassen bent, kan niets wat andere mensen zeggen of doen nog een excuus zijn voor fouten die jij maakt. Als je stopt met smoesjes zoeken, kun je beter worden in bijna alles wat je wilt.

13. **Vasthouden aan het verleden.** De noodzaak om de schuld te verleggen van onszelf naar gebeurtenissen en mensen uit ons verleden. Een variant op 'iedereen' de schuld geven (zie 19). Mensen die zich vastklampen aan het verleden overtuigen zichzelf dat ze zijn zoals ze zijn en niet zullen veranderen. Ze gebruiken het ook om iets positiefs over zichzelf te benadrukken ten koste van iemand anders. Zeg niet: "Piet was vergeten om zus en zo, maar gelukkig kon ik ..." Stop met anderen de schuld te geven van gevolgen van keuzes die jij zelf hebt gemaakt. En zeg nooit: "Toen ik zo oud was als jij ..."
14. **Bepaalde personen (je favorieten) beter behandelen omdat ze jou leuk vinden en niet omdat ze beter presteren.** Niet inzien dat we daarmee iemand anders of de rest van het team oneerlijk behandelen. De eerste stap is erkennen dat we allemaal de neiging hebben om (zoals in beoordelingsgesprekken) mensen te bevoordelen die vóór ons zijn, ook al willen we dat eigenlijk niet. Wees objectief.
15. **Weigeren om spijt te betuigen.** Het onvermogen om verantwoordelijkheid te nemen voor onze (verkeerde) acties, ons ongelijk toe te geven, of te herkennen hoe onze acties andere personen beïnvloeden. Aanbieden van excuses is niet 'de wedstrijd verliezen'. Alle angsten die ons dwingen om geen spijt te betuigen - de angst om te verliezen, toe te geven dat we fout zijn, afzien van controle - worden gewist door een verontschuldiging. Als je al je kaarten in handen van iemand anders legt, zal die persoon je beter behandelen dan wanneer je ze voor jezelf houdt. Geef toe dat je schuld hebt, vraag om verontschuldiging en smeek om hulp. En zeg niet: "Het spijt me dat ik te laat ben, maar er stond een grote file", maar stop na "Het spijt me."
16. **Niet luisteren.** De meest passief-agressieve vorm van gebrek aan respect voor collega's. Niet luisteren is stil en onzichtbaar. Je kunt niet luisteren omdat je verveeld of afgeleid bent of zit te formuleren wat je zelf gaat zeg-

IB5 Blog Robert_Opmaak 1 11-07-19 15:12 Pagina 29

Verantwoordelijkheid afschuiven is de behoefte om iedereen de schuld te geven, behalve jezelf

gen en niemand zal het weten. Maar wanneer je extreem ongeduld vertoont, merken ze het. Slecht luisteren kan gebeuren omdat je denkt dat je al weet wat je gaat horen of dat jouw geest zo snel werkt dat je elke boodschap kunt begrijpen door de blanco's zelf in te vullen. Stop met denken: `volgende!` en zeg het niet hardop. Medewerkers accepteren respectloos gedrag niet meer, maar gaan ze bij je weg.

17. **Geen dankbaarheid tonen.** De meest elementaire vorm van slechte manieren. `Bedankt' zeg je als je niets leuks te zeggen hebt. Het irriteert de persoon die het hoort nooit. Je kunt iemand tijdens een project bedanken en aan het eind nogmaals, maar uitgebreider. Daar worden ze niet kwaad over. Luisteren naar mensen, zowel positieve als negatieve feedback, een suggestie of een vaag idee: het maakt je nooit dommer. Je leert altijd meer of niets, maar nooit minder, dus bedank ze altijd voor hun hulp. Zeg nooit "Ik ben in de war" wanneer iemand iets suggereert omdat dat oneerlijk is. Je zegt eigenlijk "Jij bent in de war" dus "Jij hebt het fout." Dankbaarheid is geen beperkte, kostbare hulpbron. Het is zo overvloedig als lucht. We ademen het in, maar vergeten uit te ademen. Door 'bedankt' te zeggen, blijven mensen met je praten. Als je niet zegt: `dank u wel', stoppen ze ermee.
18. **De boodschapper straffen.** De misleide noodzaak om de onschuldige persoon aan te vallen die ons gewoonlijk alleen maar probeert te helpen. Dit is niet alleen de onrechtvaardige represaille tegen een klokkenluider of de boze tirade als iemand iets zegt dat we niet graag horen. Het zijn ook kleine reacties (minachtend snuiven) die we maken als we gehinderd worden door teleurstellingen. Zoals een secretaresse die zegt dat ze geen afspraak met de directie voor je heeft kunnen maken. Als iemand meldt dat een project niet start of een contract niet wordt getekend, ga dan niet schelden of vloeken, maar vraag: wat ging er fout? Zo kan iedereen (!) die aanwezig is in de vergadering ervan leren.
19. **Verantwoordelijkheid afschuiven.** De behoefte om iedereen de schuld te geven, behalve jezelf. De donkere keerzijde van onterecht krediet claimen. Hier zadelen we anderen ten onrechte op met de schaamte van ons falen. Niemand verwacht dat we altijd gelijk hebben, maar als we het mis hebben, verwachten ze zeker dat we het toegeven. Een fout maken geeft de kans te laten zien wat voor soort persoon, leider of collega we zijn. Hoe je je eigen fouten toegeeft, maakt een grotere indruk dan hoe je geniet van je successen.
20. **Een buitensporige behoefte om `jezelf' te zijn.** Onze fouten tot deugden verheffen omdat ze zogenaamd zijn wie we `als authentiek persoon' zijn. Dit is één van de moeilijkste obstakels om je gedrag op lange termijn te verbeteren. Want alles wat anders is, lijkt voor jou onecht, een trucje of een rol spelen. Wanneer je merkt dat je weerstand biedt tegen verandering omdat je vasthoudt aan een valse notie van je `ik', heeft Goldsmith goed nieuws voor je. Het gaat niet om jou, maar over wat andere mensen van je denken. En dát kun je veranderen. Succes met jouw to-stop-list, ik ben bezig met de mijne.

Referenties

(1) Uit: M. Goldsmith, 2007. What Got You Here Won't Get You There: How Successful People Become Even More Successful. Hachette Books.

Chris de Vries, redacteur iB-Magazine. Je reactie op dit artikel kan je sturen naar IBmagazine@pvib.nl.
Fotografie: Daisy de Pater.

Security Bootcamp 2019

Op 13 maart kwamen uit het hele land zo'n 750 informatiebeveiligingsspecialisten bij elkaar in de Van Nelle-fabriek Rotterdam voor het SecureLink cybersecuritycongres. Onder het thema 'Better together' werd er door verschillende sprekers een lans gebroken om niet alleen 'de eigen zaak' te beveiligen, maar door samenwerking het ook uit te breiden tot de 'buren'.

IB4 Securitybootcamp_Opmaak 1 11-07-19 16:57 Pagina 31

Naast de techneuten kwamen ook Richard van Hooijdonk (trendwatcher & futurist) en neurowetenschapper Erik Schoppen aan het woord. Een gemêleerd gezelschap met rijke inzichten dat leidde tot een gevarieerd dagprogramma.

KEYNOTESPREKER

Richard van Hooijdonk
(trendwatcher & futurist)

Wat denkt deze futuroloog met betrekking tot de nabije toekomst? Richard heeft al 2 chips bij zichzelf laten implanteren en overdenkt ook nog om een hersenchip te laten plaatsen. Dat signaleert ons inziens een bijzonder hoog vertrouwen in de toekomstige technologie.

Als belangrijkste trends ziet Richard:

- De slimme stadsinfrastructuur: lichtsystemen met camera's, wegen met wegsensoren.
- Zelfrijdende auto's: met aandacht voor hackingsrisico's via het entertainmentsysteem.
- Robots: zoals implantaten plaatsende robotten in de zorg.
- Drones: met onder andere gezichtsherkenning, tactische sensoren, breedbeeld camera's.
- De 'bullet train': met snelheden van 1.900 km/uur in plaats van nu nog 900 km/uur.
- De hersenchip: aansturing van drones in geval van handicaps en dementie.

Er speelt angst voor wat achter de technologie schuilgaat. Dit leidt tot onder andere de Europese regelgeving in wording opdat enkel gecontroleerde algoritmes ingezet en 'not explaining algorithms' verboden gaan worden.

De zorgtechnologie gaat volgens Richard een spannende tijd tegemoet. Bij elk bedrijf gaat het in toenemende mate over data & algoritmes en elk bedrijf verandert daarmee in een technologiebedrijf. En als je ermee rekening houdt dat de modernste computer al 10,5 miljoen kansberekeningen aan kan, dan moet de mens leren samen te werken met computers. Zijn bijbehorende metafoor: een ('duivels') dans van de mens met de computer.

De mens voert elke dag dezelfde, aangeleerde processen uit. Deze tijd vereist echter een continue dagelijkse aanpassing/verandering en dat gaat over de 'mindset'. Het 'uncomfortable excited' geraken en het afleren van wat wij geleerd hadden.

De vereiste vaardigheden:

- passie;
- nieuwsgierigheid;
- aanpassingskracht;
- het kunnen stoppen als het mislukt;
- samenwerking (het thema van dit congres).

De bijbehorende uitdagingen:

- een ecosysteem werkend met andere culturen en mensen;
- ethische normen (hoe houd je elkaar gelukkig?).

Kinderen van nu moeten we opleiden met filosofie, antropologie, psychologie en sociologie, zodat zij morgen de uitleggevers kunnen zijn.

Richards visie: bedrijven van nu zoeken bewust naar een managementkoppel. Die moet bestaan uit een de ervaren oudere (die het nu goed begrijpt) en de jonge, gekke gast van circa 24-27 jaar die de toekomst aanvoelt. Over 10 jaar besturen zij de wereld. Zij staan bekend als de omega (Ω)-generatie.

Richard van Hooijdonk besloot zijn presentatie met een schets van de 3 menstypen die er zijn:

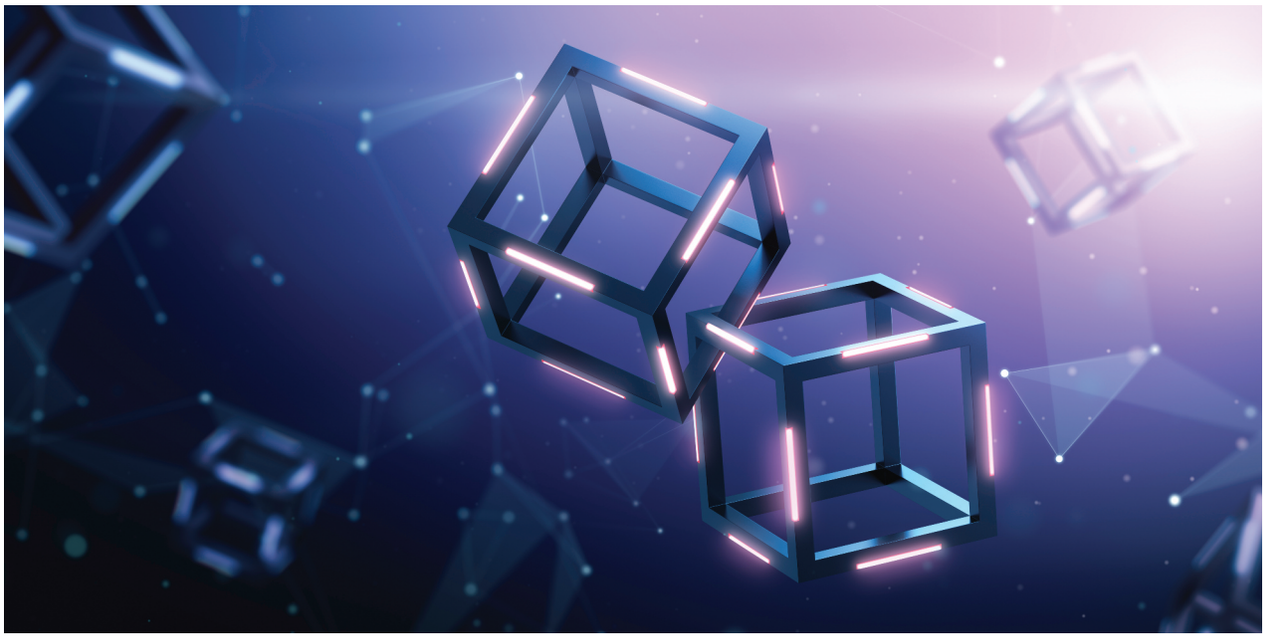
1. De zwarte beer: het afwijzende type (overheid: 50%; zorg: 70%).
2. De bruine beer: het niet willen aanpassen, maar er wel toe te stimuleren type.
3. De witte of blauwe beer: het geïnspireerde, gepassioneerde type dat los wil.

Zijn advies: met een witte beren team 1 dag vrije tijd doorbrengen en allerlei trendsetters bezoeken. Terugkomen met ideeën en budget van de eigen organisatie vragen. Bij afwijzing: wegwezen bij deze dinosauriërs. Daar is geen toekomst voor. In één zin door hem samengevat: "Meer anarchie is nodig op de werkplek."

IB4 Securitybootcamp_Opmaak 1 11-07-19 16:58 Pagina 32

INTERVIEW MET

Lucien Barink



Cryptshare is een internationaal opererend Duits bedrijf dat zich heeft toegelegd op het beveiligen van de inhoud van 'e-mails' en het kunnen laten toevoegen van grote bestandsbijlagen. Zij beschouwen zichzelf als vervanger van Shadow IT-oplossingen, zoals onder andere WeTransfer & Dropbox. Met 4 miljoen gebruikers in circa 20 landen (waaronder 2.000+ medewerkers ondernemingen) hebben zij zich sinds het jaar 2000 (oprichting door Dominik Lehr) als een belangrijke speler kunnen positioneren. Wij spraken met de algemeen directeur Lucien Barink.

Waar lopen jullie tegen aan bij de uitwisseling en beveiliging van gevoelige gegevens?
"Dat de gebruikers variëren van de zorgsector, de lokale overheid en de industrie. Opvallend is de bescherming van de data binnen de eigen veiligheidsomgeving, maar zodra deze informatie opgepakt wordt (bijvoorbeeld in de communicatie naar derden toe) geschiedt dit als een soort 'ansichtkaart'. Een enveloppe valt binnen het postgeheim (de Postwet), maar een ansichtkaart is door iedereen te lezen.

De 'e-mail'-methodiek (SMTP) beveiligt niet: er is sprake van niet-gestructureerde data en het gemak staat voorop. Vandaar dat vele datalekken opduiken. Het zijn organisaties met specifieke doelstellingen (zoals Amnesty International) die vooroplopen met de beveiliging van hun data en communicatie: zij zijn diegene die als eerste het nut van beveiliging zien."

Welke fouten komen veel voor?
"Er zijn twee fouten die veel voorkomen, te weten:
1. Een technische fout – SMTP beschermt niet (de 'ansichtkaart').
2. De verkeerde adressering – de meest voorkomende fout.

De noodzaak is te werken aan de wijze waarop data de beschermde veiligheidsomgeving verlaat en gecommuniceerd wordt. Dat zorgt er dan voor dat de 'man-in-the-middle'-aanval bemoeilijkt/verhinderd wordt.

Er is in het recente verleden een wildwest geweest op de markt met oplossingen, zoals Surfnet, Gemnet (lokale overheid), Zorgnet en SUNET. Echter, deze oplossingen werken binnen de eigen, aangesloten groep. Alternatieve, nieuwe oplossingen adresseren iedereen."

Hoe positioneert Cryptshare zich met betrekking tot ketenveiligheid en het MKB?
"Zij leveren aan ondernemingen bestaande uit de enkele medewerker tot organisaties met zo'n 30.000 medewerkers. Voor de kleine gebruiker (< 25 personeelsleden) bestaat er de cloudoplossing. Met deze oplossing verzorgt Cryptshare de verwerkingsovereenkomst.

De grote(re) ondernemingen wensen vaak de oplossing geplaatst binnen de eigen infrastructuur als een SaaS-oplos-

IB4 Securitybootcamp_Opmaak 1 11-07-19 16:58 Pagina 33

sing (‘on premise’). Daarmee staat het achter de eigen bedrijfsfirewall en is het geheel de zaak van de klant. Daarbij wordt ook regelmatig een koppeling gezocht met andere applicaties, bijvoorbeeld:

- een ziekenhuis informatiesysteem;
- een document managementsysteem binnen de advocatuur of;
- een beveiligd maatwerksysteem voor personentransport.

Ten aanzien van de typefouten (adresseringsfouten) werkt de synchrone encryptie gekoppeld aan de ‘2 factor’-authenticatie. Uitgangspunt is daarbij, zoals bekend, het gedeelde geheim: de 2e e-mail of een sms. Dat laatste via de sms-‘gateway’, dat gebruik maakt van een 2e kanaal.”

Wat zijn de nieuwe ontwikkelingen?

“In de komende maand komt Quick Technology op de markt waarbij in plaats van de ‘2 factor’- authenticatie per afzonderlijke e-mail slechts één keer een authenticatie noodzakelijk is voor een dan permanent ingestelde veilige communicatiebus. Deze oplossing is nog niet eerder toegepast en een patentaanvraag loopt. De essentie is dat 100% van alle communicatie (al of niet met gevoelige data) verloopt via het veilige kanaal zonder dat extra handelingen vereist zijn. Het oplossen van dit probleem via de data-leak-prevention (dlp) kan leiden tot ‘false positives’.

Door iedereen binnen de eigen wereld aan te sluiten op de Quickstatus creëer je dus eigenlijk een omgekeerde firewall. De toegestane buitenwereld kan veilig binnenkomen en data kan op veilige wijze naar buiten toe worden gecommuniceerd (getransporteerd).”

Welke belangrijke sectorontwikkelingen vallen op?

“De wetgever heeft recent (met name door de AVG/GDPR) de vraag en de verantwoordelijkheid opgerekt. Bedrijven constateren meer en meer dat zelfs via hacking van hun mailverkeer Intellectueel Eigendom (IE) in gevaar komt. Een recente casus leerde verlies van gevoelige data naar China.

Er is sprake van een inhaalactie waarbij het bedrijfsculturele aspect binnen een onderneming het handelsaspect ontmoet. Zo was en is het bij delen van het bank- en verzekeringswezen de regel dat geen enkele USB-poort is toegestaan.

Maar ook verschillen in landsculturen spelen een rol. In Nederland zijn er 20.881 gemelde datalekken (bron: Autoriteit Persoonsgegevens), terwijl in België dit beperkt bleef tot 442 meldingen (bron: Emerce). De indruk bestaat soms dat 25 mei voor België slechts een startpunt was. Natuurlijk kan het zijn dat Nederland zo hoog mogelijke cijfers wil hebben met het oog op de fte-bezetting bij de verantwoordelijke autoriteiten of dat wij in Nederland veel volgzamer en het beste jongetje van de klas willen zijn.

Anderzijds kan je ook wijzen op de aanwezigheid van het grote internetknooppunt in Amsterdam (1 van de 3 op de wereld), de hoge acceptatiegraad van het internet en dat velen Nederland zien als ‘stepping stone’ voor Europa. Feit is dat Nederland veel sterker internationaal actief (handelend) is.

Ook het perspectief speelt een rol. Organisaties kijken er anders tegen aan dan de particulier, de burger. Gevoelige informatie over bijvoorbeeld huiselijke geweld of vermeende pedofilie kan op persoonlijk niveau veel ernstiger consequenties hebben (veroordeling voordat er zelfs maar een toetsing, laat staan een proces, is geweest) dan het verlies van 1.000 digitale dossiers.

De vraag of je iets te verbergen hebt kan misschien dan ook beter omgezet worden in de vraag: heb je iets te delen? Gedeelde informatie legt vervolgens bij de ontvanger een grote verantwoordelijkheid op om er veilig mee om te gaan. Dus de beslissing om die informatie op de eigen server te plaatsen of te plaatsen in de cloud (grote ondernemingen) is hun keuze en hun verantwoordelijkheid. Cryptshare borgt het transport van de informatie, niet de wijze van opslag (tenzij bij de kleinere ondernemingen de cloudoplossing is aangeboden). De ontvanger heeft feitelijk dus een gedelegeerde verantwoordelijkheid. Essentie is dus dat er vertrouwen in de ontvangende partij moet bestaan om informatie te delen.”

Hoe is het keymanagement geregeld?

“Door middel van synchrone encryptie. Er bestaat geen ‘keystore’ en de bescherming bestaat uit de verschillende datalagen welke existeren, zoals:

- inbraak detectie (achter de firewall van haar klant);
- het anonimiseren van de bestandsnamen;
- het anonimiseren van de foldernamen;
- de AES 256-bit encryptie.

Wat is het bedrijfsmodel?

“Cryptshare levert nooit aan de eindgebruiker, maar altijd indirect via partners als SecureLink. Zij bieden namelijk een point solution waarbij het noodzakelijk is dat hun partners dat inbedden in de context van diens respectievelijke klantsystemen.”

KEYNOTESPREKER

Erik Schoppen

Met veel belangstelling hadden wij uitgekeken naar de presentatie van Erik Schoppen, werkzaam bij de Rijksuniversiteit Groningen en onderzoeker in de neurowetenschappen. Zijn thema was 'Cybersecurity en de zwakste schakel – de mens'. Emoties en vertrouwen in organisaties komen voort uit de mentale en fysische eigenschappen van de mens. Onze mentale gesteldheid bepaalt onze emoties en empathie (of het ontbreken daarvan). De fysische gesteldheid bepaalt de mate waarin de maatschappij impact op en macht over ons heeft. De mentale gesteldheid leidt tot een houdbare en prosociale positionering en dat leidt weer tot vertrouwen en gedragsverandering in de fysische gesteldheid.

Echter daar waar cybersecurity over technologie gaat, behandelt de neurowetenschap de zwakste schakel daarbinnen, te weten: de mens. Binnen 150 milliseconden kan de mens al een beslissing nemen welke voor zijn organisatie verkeerd kan uitpakken, want zijn gedrag is voornamelijk onbewust spiegelgedrag.

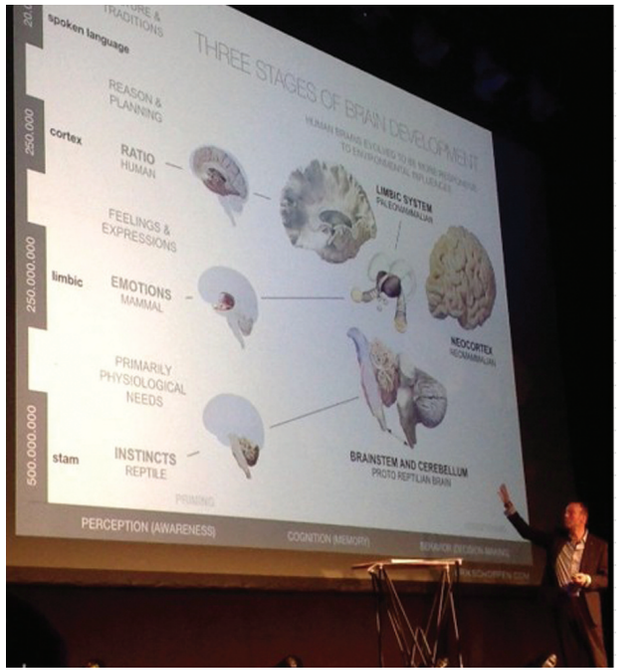
De neurowetenschappen bestudeert twee kernthema's:

1. De informatievoorziening (bereikbaarheid van informatie voor onze hersenen).
2. De competentie (de betrouwbaarheid van het informatiesysteem).

Erik Schoppen presenteerde een schema van hersenontwikkeling en de betekenis ervan in ons denken. Zo bestaat het oudste deel van onze hersenen (de hersenstam en het cerebellum) al meer dan 0,5 miljard jaar. Dit is het instinctmatig (reptielen) brein. Functies: voornamelijk fysiologische behoeftebevrediging. Van de circa 85 miljard neuronen in ons hersenen zit 50% in dit deel, gericht op onbewuste fijnmotorische aansturing. Een ¼ miljard jaar geleden ontwikkelde zich het limbisch (mammal) systeem, waardoor gevoelens en expressies tot stand kwamen. Pas zo'n 9 miljoen jaar geleden ontwikkelde zich de buitenste hersenschors (neocortex) waarmee ook redeneren en plannen mogelijk was.

De hersenontwikkeling doorliep hiermee dus 3 fases. De gesproken taal (ongeveer 20.000 jaar terug) en de geschreven taal (ongeveer 5.000 jaar terug) - en daarmee cultuur en traditie - kwamen daaruit voort. Omdat de neocortex het limbisch systeem opgevolgd heeft, volgt zij dus ook het limbisch systeem en rationaliseert de cortex achteraf de door het limbisch systeem genomen beslissing.

Hackers maken daarvan gebruik. Zij weten – als 'psychologen' die zij (b)lijken te zijn – dat de mens angst en pijn wil vermijden, streeft naar genot en gevoelig is voor autoriteit alsook vriendelijkheid. De mens in noodsituatie zal snel en zonder lang na te denken reageren. De hacker trekt dus aandacht, biedt een direct uitvoerbare opdracht aan waaraan een direct voordeel gekoppeld is, waar weinig inspanning voor nodig is en sociale status gewonnen kan worden. De hersenen zijn met name voor dat laatste gevoelig, omdat dit de kans verhoogt op beter voedsel en nageslacht.



Three stages of brain development.

Naast deze hersenontwikkeling heeft zich in de loop der tijd het vertrouwen ontwikkeld en wel langs navolgende lijn:

- zelfvertrouwen (persoonlijk);
- sociale wederkerigheid (team vertrouwen);
- organisatie vertrouwen (meerdere teams samengevoegd bijvoorbeeld tot een bedrijf);
- systeemvertrouwen (men kent elkaar niet, maar vertrouwt op het systeem);

From brain trust to trust systems.

IB4 Securitybootcamp_Opmaak 1 11-07-19 16:58 Pagina 35

Schema: wat doet je iemand vertrouwen?

- sociaaleconomisch vertrouwen (verbindingen op maatschappelijke schaal).

Deze hyperverbondenheid doet de emotionele kwetsbaarheid toenemen. Ons brein is daarbij achtergebleven. Daarnaast zien wij een toename van lerende systemen die niet alleen ons gedrag registreren, maar ook daarop gaan reageren. Zij raken ons. Dit gaat zelfs zo ver dat (door de ontwikkeling van) kunstmatige neurale netwerken, die continue ons gedrag monitoren steeds beter in staat zijn ons gedrag te voorspellen en (deels onbewust) te sturen. Erik Schoppen spreekt dan ook uit dat 'neurofacing' (implantaten die rechtstreeks communiceren via onze hersenen) binnen enkele decennia toegankelijk zijn voor een breed publiek. Hierdoor verleggen we een deel van ons evolutionaire biologisch vertrouwen naar digitaal vertrouwen op basis van kunstmatige intelligentie. We vertrouwen steeds meer op onze virtual assistent (of digital agent).

Vervolgens ging hij in op wat je iemand doet vertrouwen en dat is wanneer informatie met het gevoel wordt verbonden. Bovenstaand schema verduidelijkt dat:

In de hersenen zijn onder andere twee stoffen aanwezig te weten: dopamine en epinephrine (adrenaline). Het eerste stimuleert impulsief zoekgedrag ('gain novelty seeker': benaderen, impulsief, risico), het tweede beschermend, terughoudend gedrag ('pain safety keeper': voorkomen, beschermen, vechten, vluchten of stilstaan).

Het proces dat hackers proberen te benutten werkt als volgt: lok een positief emotioneel antwoord uit, dat produceert de beloning in de vorm van dopamine en dat leidt tot de actie met vorming van adrenaline. Hetzelfde proces dat plaatsvindt indien iemand reageert op het opflikkerend lampje van de mobiele telefoon. Op dit moment is mobielgebruik wereldwijd de grootste (mentale) verslaving.

Erik Schoppen vat één en ander als volgt samen: de motivatie en beloning leidt tot de behoefte om verder te gaan (keer op keer). Ons gedrag wordt emotioneel aangedreven en wordt ondersteund door onze empathie (dat wil zeggen: denken, voelen en gedragen als een ander, maakt ons blij). Dit wordt veroorzaakt door de spiegelneuronen en vertaalt zich in het elkaar imiteren als sociale wezens. Wie gaat niet gapen als een ander gaapt?

Als uitsmijter attendeert Erik Schoppen de aanwezigen erop dat wij allen attent moeten zijn op:

- Hoe competent is het systeem en waar komt de informatie vandaan?
- Hoe werken de mensen binnen het systeem en wat is de cultuur van de organisatie?
- Kijk nadrukkelijk uit voor de geautomatiseerde routines, dat zijn de grote schadeberokkenaars.

INTERVIEW MET

Erik Schoppen

In aansluiting op de presentatie spraken wij met Erik Schoppen. Wij hoopten handreikingen te krijgen hoe wij als mens ons kunnen wapenen tegen de door de hacker gecreëerde verleidingen.

Mensen neigen tot routinegedrag en de hacker bereidt zich goed voor en houdt dus rekening met dat routinegedrag. De perfecte misdaad is dat de gehackte medewerker niet bewust is van de schade die hij veroorzaakt. Voorbeeld van een hackingtechniek is het zogenaamd verliezen van een USB-stick, welke na 'vondst' door derden gewoon in gebruik wordt genomen. Het probleem is dat mensen regels vervelend vinden (ze zijn vaak belemmerend) en daardoor ook de veiligheidsinstructies negeren.

Om hackers voor te blijven zal de toekomst ons de digitale assistent bren-

IB4 Securitybootcamp_Opmaak 1 11-07-19 16:58 Pagina 36

gen. Deze spoort afwijkingen in patronen op en legt die aan de gebruiker voor ter beoordeling. Het probleem is dat het brein een trucje leert en dat voortdurend herhaalt. Ook een kind leert op eenzelfde wijze, waardoor handelingen geautomatiseerd worden. Hierdoor kan ons brein efficiënter werken. Daarom is gedragsverandering ook zo moeilijk. Deze geautomatiseerde handelingen afleren is alleen mogelijk door nieuwe handelingen aan te leren – die na verloop van tijd de oudere handelingen vervangen. Voor organisaties is dit meestal te duur en te tijdrovend. Als ze het zorgvuldig zouden willen oppakken dan moeten zij kostbare 'sandboxes' creëren waarin fouten gemaakt mogen worden.

De technologische ontwikkelingen gaan echter nu zo snel dat wij ook de lange termijn consequenties niet meer kunnen overzien. Vroeger had je de tijd om beschouwelijk te zijn, nu niet meer. Binnen een jaar moet je innovaties volgen op straffe van marktverlies. Als er fouten zitten in de innovaties (in de apps) dan worden deze aangepakt op basis van 'management by failure'. Sandboxes zijn te duur, kosten tijd en geven geen garantie, waardoor ook onze privacy in gevaar komt, omdat gevoelige informatie op straat komt te liggen. En hierdoor verliezen gebruikers weer vertrouwen in (alweer) nieuwe systemen.

Denk ook aan nieuwe abonnement- en betaalsystemen, waardoor 'betaalpijn' verdwijnt. Dit is een belangrijk evolutionair signaal dat je brein attendeert dat je mogelijk risico kan oplopen. Maar de verleidingen zijn nu domweg te aantrekkelijk, omdat ze altijd bereikbaar zijn. Wij proberen wel door middel van protocollen zaken te veranderen rondom ons brein, maar ons brein verandert niet. Ook al verwachten wij dat implantaten veel in deze kunnen betekenen, wij weten nog te weinig van het brein af om nu de resultaten of consequenties te overzien.

Wat we wel weten is dat ons brein gelimiteerd is in nieuwe informatie opnemen. Het brein beschermt je door te filteren en alvast vooruit te kijken. Bijvoorbeeld naar het weekend op vrijdagmiddag. Hierdoor verslapt de aandacht op het werk – want je brein kan zich maar op een ding tegelijkertijd focussen. Dat is ook de reden dat het ideale moment voor hackers de vrijdagmiddag is. Nog snel even dat ene mailtje wegwerken. Ook al omringen wij ons met technologie, de mens blijft even kwetsbaar als een miljoen jaar geleden.

Wij stelden dan ook de vraag of er iets te doen zou zijn om het veiliger te maken. Erik Schoppen gaf aan dat dit de vorm zou moeten krijgen van tweede muren, maar dit werkt niet echt. Het vertraagt slechts. De techniek moet ons gaan beschermen. Mogelijk dat wij als beveiligingsspecialisten vooroplopen, omdat wij ons bewuster zijn van de risico's.

Eén van de risico's is de haast waarmee wij leven en onthaasten is nu niet meer mogelijk. Dan zou je in een andere, duurdere wereld leven. Mensen vinden het fijn direct inzicht (via apps) te hebben in hun hebben en houden en om behaalde voordelen met anderen te vergelijken.

Er is wel sprake van een soort tegenbeweging van bewust levende mensen (voorbeeld 'slow food'). Het is echter een dure manier van leven: je betaalt echt meer en je moet je de luxe kunnen veroorloven. Per slot van rekening is dopamine de 'motor van de economie' volgens Erik Schoppen.

De bescherming door 'machine learning' is een mogelijkheid, maar vereist nog (menselijke) input. De beste wijze van bescherming: houd de meest kwetsbare systemen buiten mensenhanden en bouw muren in van intelligente zelflerende systemen die problemen signaleren en voorleggen aan de specialisten. Verder moet de leverancier zijn product beter beschermen en niet de eindgebruiker opzadelen met zijn problematiek. De mens als zwakste schakel krijgt altijd de schuld, echter omdat het brein niet denkt als een computer en niet kan omgaan met systeemproblemen, is dit een onredelijk uitgangspunt.

"Wat je nodig hebt zijn goede design thinkers en interface designers", zegt Erik Schoppen. Privacy by design is daar een voorbeeld van. Voorkom dat je mogelijkheden in het systeem aanbiedt aan gebruikers die dat niet horen te zien. Informatie en interactiemogelijkheden moeten alleen worden getoond als het nodig is.

Toekomstig zal software tot ontwikkeling komen door machine coding. Er is voldoende gebruikersdata beschikbaar om dit mogelijk te maken. Gebruikersdata komt bijvoorbeeld uit onverwachte hoeken, niet alleen door mobiele telefoons (die alles loggen), maar bijvoorbeeld ook vanuit intelligente tandenborstels. Dit zijn inmiddels identificatiemiddelen met trackingsystemen, want wereldwijd mag de data worden uitgelezen. Je moet je afvragen of je dit als bedrijf ethisch verantwoord vindt.

In een land als China zal dit op minder problemen stuiten. Zij zijn gewend dat de staat al veel weet. Daar is ook een WeChatapp gekoppeld aan een socialcreditsysteem. De acceptatie zal zo hoog zijn, omdat de staat daar ook welvaart tegenover stelt.

Maar laten wij realistisch zijn, ook in Nederland kijkt de overheid mee. Wij krijgen er alleen niets voor terug. Ten aanzien van dit privacyvraagstuk bezitten wij twee keuzes, te weten:

- Wij delen niets
- Wij delen wat we willen, maar stellen kritische vragen over de toegepaste protocollen en met wie de informatie wordt gedeeld

Weet dat hackers ondernemers zijn. Voor hen is hacken gewoon business en zijn het bedrijven met werknemers. En deze ondernemingen werken ook met garanties, zoals vastgelegd in hun terms of use. Het 'niet betalen'-advies van de overheid is dan ook niet vrij van naïviteit.

Deze aanvullende, waardevolle inzichten leidt tot onze aanbeveling presentaties, onderzoeken en publicaties van Erik Schoppen (onder andere columns in Management Team) te volgen.

IB4-Bestuur in Beeld_Opmaak 1 09-07-19 15:10 Pagina 37

KELVIN RORIVE

"Ik heb een passie voor techniek, security, organisatie en politiek. Deze combinatie is erg leuk, omdat ik daarmee altijd op het kruispunt van techniek en business werkzaamheden verricht op het gebied van security. Ik heb uiteenlopende functies gedaan over de as van security: programmeur, IT-architect, beleidsmaker, programmamanager, IT-auditor, lijnmanager en nu chapter lead security bij de Rabobank. Deze laatste functie is geïnspireerd op het Spotify-organisatiemodel, waarbij de chapter verantwoordelijk is voor het garanderen van expertise en ontwikkeling over teams heen van een thema. In mijn geval is dat security. Mijn team bestaat momenteel uit 30 medewerkers die allemaal security in hun taakpakket hebben zitten, maar het is niet hun primaire verantwoordelijkheid.

Ik ben getrouwd met Susan, heb twee prachtige dochters van 16 en 14 jaar en woon in het mooie en centraal gelegen Zeist. Mijn vrije tijd besteed ik grotendeels aan het PvIB. Ik ben voorzitter van de activiteitencommissie en jurylid van de Joop Bautz Information Security Award (JBISA). Super leuk om met enthousiaste vrijwilligers te werken die allemaal worstelen om tijd vrij te maken om een mooi evenement te organiseren. Maar de kick, plezier en passie voor het vak maakt toch elke keer weer dat we een mooi evenement kunnen neerzetten.

Ooit ben ik aangesloten bij het PvIB, omdat ik vakgenoten zocht om mee te sparren. Bij mijn vorige werkgever was ik de enige die met hart en ziel ging voor security. Dat is me zo goed bevallen dat ik al snel actief werd. Sindsdien (nu 18 jaar) is het een perfecte thuisbasis om samen met mijn securityvakgenoten aan de ontwikkeling van het vakgebied (en aan mezelf) te werken.

De grote verandering die ik zie in ons vakgebied is de komst van de cloud. Dit bestaat al jaren, maar je merkt nu echt de effecten voor organisaties. De ene organisatie zit nog in de weerstand, omdat beheersing van security controls uitdagend is, terwijl andere organisaties agressief naar de cloud gaan. Die leidt tot nieuwe businessmodellen en verschuiving van expertise. Dit is gerelateerd aan het onderwerp shadow IT, wat voor organisaties een steeds grotere zorg wordt. Zowel vanuit privacy- als vanuit security-oogpunt. De uitdaging met shadow IT is dat grenzen van IT verantwoordelijkheid steeds vager worden, terwijl de aansprakelijkheid niet verandert. Een mooi voorbeeld waarbij techniek en organisatie heel dichtbij elkaar staan.

Ik durf wel te stellen dat het hebben van het PvIB van levensbelang is voor Nederland. Zonder goede samenwerking en kennisdeling zou onze gemeenschappelijke kennis lang niet op het niveau zijn zoals het nu is. Dat zal het PvIB de komende 5 jaar moeten blijven stimuleren met lezingen, het vakblad en door middel van publicaties. Ook moet het PvIB vernieuwingen omarmen. Ik denk vooral dat de vernieuwing zit in het faciliteren van de leden met moderne technologieën die het samenwerken en kennisdelen vereenvoudigen en nog leuker maken. Ik zal de komende maanden veranderingen implementeren op de website. Alle leden kunnen dan digitaal in- en uitchecken bij evenementen en ze hebben altijd een actueel, online overzicht van de behaalde PE-punten.

IB4 Marcel Spruijt_Opmaak 1 11-07-19 15:15 Pagina 38

Marcel Spruit is lector Cyber Security & Safety aan de Haagse Hogeschool.
Hij is te bereiken via m.e.m.spruit@hhs.nl.

Masteropleiding Technische Cybersecurity gebaseerd op PvIB-beroepsprofiel

Er is wereldwijd een toenemend tekort aan goed opgeleide en ervaren informatiebeveiligers. Om daarop te anticiperen zijn voor informatiebeveiliging meer volwaardige opleidingsmogelijkheden nodig. Bovendien is meer harmonisatie van bestaande en nieuwe informatiebeveiligingsopleidingen gewenst om beter door te kunnen stromen naar vervolgopleidingen en deelopleidingen aan andere opleidingsinstellingen te kunnen volgen. In dit artikel delen we de ervaringen met het opzetten van een geaccrediteerde masterstudie in de informatiebeveiliging, gebaseerd op een gestandaardiseerd PvIB-beroepsprofiel en het onderliggende Europese e-Competence Framework.

IB4 Marcel Spruijt_Opmaak 1 11-07-19 15:15 Pagina 39

Organisaties verwerken steeds meer digitale gegevens en zijn daar de afgelopen decennia steeds afhankelijker van geworden. Deze gegevens moeten dan ook goed beschermd worden en dat vraagt om voldoende goed opgeleide en ervaren informatiebeveiligers (1)(2). Daar is echter een toenemend tekort aan (3)(4). Blijkbaar worden er minder informatiebeveiligers opgeleid dan er nodig zijn.

Er zijn veel opleidingsmogelijkheden op het gebied van informatiebeveiliging, maar het betreft vooral relatief korte cursussen. Er zijn beduidend minder mogelijkheden om in het middelbaar of hoger onderwijs een volwaardige studie op het gebied van informatiebeveiliging te volgen. In het hoger onderwijs in Nederland waren er in 2018 slechts twintig studies, deels deeltijd, deels voltijd (5). Bovendien is er weinig consensus over welke competenties informatiebeveiligers zouden moeten bezitten (6). Met name door dat laatste zijn de bestaande opleidingen onderling slecht vergelijkbaar en kost het doorstromen, of het volgen van deelopleidingen aan andere opleidingsinstellingen, grote moeite. Bovendien is het werkgevers niet duidelijk welke afgestudeerden het beste op hun vacatures passen, terwijl afgestudeerden moeilijk kunnen aangeven op welk niveau ze zitten.

In reactie hierop heeft het PvIB, samen met een groep bekende organisaties, gestandaardiseerde beroepsprofielen op het gebied van informatiebeveiliging opgesteld (7)(8). Deze profielen specificeren de competenties die een informatiebeveiliger zou moeten bezitten. Voor het uitwerken daarvan wordt gebruik gemaakt van het Europese e-Competence Framework (9).

Het is de vraag in hoeverre het mogelijk en haalbaar is om een geharmoniseerde opleiding op het gebied van informatiebeveiliging te ontwikkelen, op basis van een gestandaardiseerd PvIB-beroepsprofiel en met gebruikmaking van het onderliggende Europese e-Competence Framework (e-CF).

Beroepsprofielen

Om meer helderheid te krijgen over de eisen die organisaties stellen aan de informatiebeveiligers die ze aan willen nemen, heeft het PvIB, samen met een groep bekende organisaties, het project Qualification of Information Security (QIS) opgezet. Dit project heeft gewerkt aan het formuleren van een beperkt aantal generieke beroepen binnen het domein informatiebeveiliging. Ieder van deze generieke beroepen is beschreven in een gestandaardiseerd beroepsprofiel (8). Een beroepsprofiel beschrijft de competenties die een informatiebeveiliger zou moeten bezitten. Een competentie is het vermogen om bepaalde kennis en vaardigheden toe te passen om taken en functies succesvol uit te voeren in een bepaalde rol of positie (9)(10)(11)(12). Een competentie kan uitgewerkt worden in kennis- en vaardigheidselementen. De e-competenties zijn uitgewerkt in e-CF, versie 3.0 (9). De algemene competenties heeft de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen.

Competenties, alsook de kennis- en vaardigheidselementen, kunnen op een competentieniveau, lopend van 1 tot 5, beheerst worden. De niveaus zijn door het PvIB beschreven (8). Kort door de bocht kunnen we stellen dat de niveaus globaal overeenkomen met een bepaald denk- en werkniveau, te weten:

1. basisniveau;
2. mbo-niveau;
3. hbo-niveau;
4. masterniveau;
5. phD-niveau.

Door de betrokkenheid van een groot aantal vertegenwoordigers van allerlei sectoren en geledingen en uitgebreide reviewrondes kunnen de PvIB-beroepsprofielen rekenen op een breed draagvlak bij informatiebeveiligers, werkgevers in de publieke en private sector en onderwijsinstellingen. De beroepsprofielen kunnen gebruikt worden voor een nog te realiseren systeem voor certificatie en registratie van informatiebeveiligers.

Masteropleiding

De hiervoor genoemde gestandaardiseerde beroepsprofielen bevatten competenties die verder zijn uitgewerkt in kennis- en vaardigheidselementen. Elke beoefenaar van een in een beroepsprofiel gespecificeerd beroep moet de in het profiel genoemde competenties beheersen voor het uitoefenen van zijn of haar werk. Dit betekent dat de betreffende persoon de vereiste competenties moet kunnen verwerven, bijvoorbeeld door het volgen van een daarop gerichte opleiding.

Een informatiebeveiligingsopleiding kan worden ontworpen op basis van de competenties die in een informatiebeveiligingsprofiel worden vermeld. De daarin genoemde e-competenties zijn in het e-CF uitgewerkt in kennis- en

vaardigheidselementen. De algemene competenties heeft de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen. Het detailniveau van de kennis- en vaardigheidselementen is een compromis tussen de nauwkeurigheid die vereist is voor standaardisatie en de flexibiliteit die in opleidingen voor de betreffende kennis en vaardigheden nodig is.

De kennis- en vaardigheidselementen die zo zijn bepaald, kunnen direct worden gebruikt als leerdoelen voor een opleiding. Op basis van de gespecificeerde kennis- en vaardigheidselementen kunnen docenten hun lesmateriaal ontwikkelen.

Dat deze aanpak werkt, konden we aantonen met de ontwikkeling van een technisch georiënteerde Master of Science-opleiding op het gebied van informatiebeveiliging. Deze masteropleiding werd ontwikkeld voor de Cyber Security Academy en de Haagse Hogeschool. Beide instellingen ontvangen al geruime tijd signalen dat een technisch georiënteerde masteropleiding op het gebied van informatiebeveiliging c.q. cybersecurity in de Haagse regio zeer welkom zou zijn. De nieuwe opleiding is tweejarig en parttime (60 ECTS) en is Master Cyber Security Engineering gedoopt. De opleiding is in 2018 door de NVAO geaccrediteerd en is 1 februari 2019 gestart. Als toelatingseis geldt een bachelor in informatica, informatiebeveiliging of cybersecurity, plus minimaal twee jaar relevante werkervaring.

Voor het ontwikkelen van de opleiding hebben we eerst het meest relevante beroepsprofiel gekozen, namelijk ICT-security specialist 3 (8). De volgende competenties zijn in dit profiel gespecificeerd:

- A7: volgen van technologische ontwikkelingen, competentieniveau 4;
- B4: oplossingen implementeren, competentieniveau 4;
- E3: risicomanagement, competentieniveau 3;
- E8: informatiebeveiligingsmanagement, competentieniveau 3;
- G3: communicatie en overtuigingskracht, competentieniveau 2;
- G4: onderzoek, competentieniveau 4;
- G7: analytisch vermogen, competentieniveau 4;
- G8: integriteit, competentieniveau 2.

Dat de competentie 'integriteit' op niveau 2 staat, betekent niet dat de beroepsbeoefenaar beperkt integer hoeft te zijn, maar dat deze 'slechts' de uitgangspunten en regels voor integer gedrag kent en kan verklaren en daarnaar kan handelen.

Elk van de gespecificeerde competenties is verder uitgewerkt in kennis- en vaardigheidselementen. De e-competenties zijn met behulp van het e-CF uitgewerkt in kennis- en vaardigheidselementen. We gebruikten hiervoor versie 3.0. Deze versie hebben we inhoudelijk enigszins aan moeten passen, omdat we inconsistenties en onvolledigheden tegenkwamen en deze vervolgens als voorschrijvende standaard gebruikt. De algemene competenties zijn met behulp van de uitwerking van de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen. Deze uitwerking kon onverkort gebruikt worden.

De kennis- en vaardigheidselementen zijn vervolgens gedefinieerd als de leerdoelen. Dit resulteerde in een complete lijst met leerdoelen voor de opleiding. Vanzelfsprekend staat het elke opleidingsinstelling vrij om extra leerdoelen toe te voegen of bepaalde kennis en vaardigheden verder uit te diepen dan nodig is volgens het beroepsprofiel. Zo hebben we in deze opleiding bijvoorbeeld de onderzoekscomponent extra zwaar ingevuld en extra tijd ingeruimd voor het toepassen van kennis en vaardigheden op het gebied van cybersecuritytechniek in specifieke typen organisaties.

De tweede stap was het ontwerpen van een opleidingsstructuur. Daarbij is gekozen voor een indeling in drie semesters met ieder drie modules, en een vierde en laatste semester voor het thesisonderzoek. In elke module loopt een individueel project of een groepsproject, zodat er voldoende ruimte is om aan vaardigheden te werken. De inhoud van de semesters is in het kort:

1. Conceptualisatie van cyberbeveiliging. Dit semester is een beknopte inleiding in allerlei relevante aspecten, zoals menselijke factor, management, wetgeving en ethiek. Bovendien worden de onderdelen ICT en ICT-beveiliging opgefrist en op masterniveau gebracht.
2. Bouwstenen voor cyberbeveiliging. In dit semester duiken de studenten diep in de techniek van de ICT-beveiliging.
3. Cyberbeveiliging in sectoren en trends. In dit semester wordt de kennis uit de vorige semesters toegepast op specifieke typen organisaties. Verder worden de nieuwste technische trends op het gebied van ICT-beveiliging behandeld.

IB4 Marcel Spruijt_Opmaak 1 11-07-19 15:15 Pagina 41

Op het gebied van informatiebeveiliging zijn meer volwaardige geharmoniseerde opleidingsmogelijkheden nodig

4. Onderzoek. Elke student moet individueel een wetenschappelijk onderzoeksproject doen en een masterscriptie schrijven.

De derde stap was het verdelen van de leerdoelen over de modules, zodanig dat alle modules (behalve de thesismodule) ongeveer dezelfde omvang zouden hebben en iedere module een logisch en samenhangend geheel zou vormen.

Ten slotte konden voor iedere module de docenten op basis van de aan hun toegewezen leerdoelen hun lesmateriaal ontwikkelen.

De op deze manier ontwikkelde opleiding voldoet qua competenties (kennis en vaardigheden) volledig aan het onderliggende PvIB-beroepsprofiel. Ook andere onderwijsinstellingen kunnen de PvIB-beroepsprofielen gebruiken om nieuwe opleidingen te ontwikkelen of bestaande opleidingen aan te passen. We zijn niet bang voor een `eenheidsworst', omdat opleidingsinstellingen binnen de opleiding voldoende ruimte hebben om leerdoelen toe te voegen, binnen de leerdoelen accenten te plaatsen en te werken met verschillende onderwijsvormen. Maar dankzij de gemeenschappelijke basis zijn verschillende opleidingen op basis van hetzelfde beroepsprofiel gelijkwaardig en kunnen ze effectiever worden geaccrediteerd. Bovendien kunnen vervolgopleidingen makkelijker aansluitend worden gemaakt en zijn deelopleidingen van andere opleidingsinstellingen (bijvoorbeeld minoren) makkelijker in te passen.

Conclusie

Op het gebied van informatiebeveiliging zijn meer volwaardige geharmoniseerde opleidingsmogelijkheden nodig. In dit artikel hebben we aan de hand van de ontwikkeling van de Master Cyber Security Engineering, op basis van het beroepsprofiel ICT-securityspecialist 3, laten zien dat het mogelijk en haalbaar is om een geaccrediteerde informatiebeveiligingsopleiding te ontwikkelen op basis van een PvIB-beroepsprofiel. Dit resulteert in een opleiding die qua competenties volledig voldoet aan het onderliggende beroepsprofiel en daarmee geharmoniseerd is met andere opleidingen die op hetzelfde beroepsprofiel gebaseerd zijn.

We hebben geconstateerd dat standaard competentieuitwerkingen zoals het e-CF, zij het inhoudelijk enigszins aangepast en als voorschrijvende standaard gebruikt, en de uitwerking van de PvIB-werkgroep Kwalificatie van informatiebeveiligers goed bruikbaar zijn voor het uitwerken van competenties tot leerdoelen.

Referenties

(1) Munnichs, G., Kouw, M. & Kool, L. (2017). Een nooit gelopen race. Rathenau Instituut.

(2) Smith, S.S. (2017). Internet Crime Report. FBI.

(3) Van Lakerveld, J.A., e.a. (2014). Arbeidsmarkt voor Cyber Security Professionals. PLATO.

(4) Morgan, S. (2017). Cybersecurity Job Reports, 2017 Edition. Herjavec.

(5) Van Noord, F. & Barthel, J.P. (2019). Inventarisatie van erkende cybersecurityopleidingen in Nederland. Informatiebeveiliging, 3.

(6) Spruit, M. & Van Noord, F. (2011). Onderzoek naar kwalificatie en certificatie van informatiebeveiligers. CPNI.NL.

(7) Van Noord, F. & Spruit, M. (2014). Informatiebeveiligers definiëren hun kwalificatiestelsel op basis van e-CF. Informatiebeveiliging, 4, 24-26.

(8) Spruit M. & Van Noord, F. (2017). Beroepsprofielen Informatiebeveiliging 2.0. PvIB.

(9) CEN (2014). CEN Workshop Agreement CWA 16234:2014 Part 1, European e-Competence Framework 3.0 - Part 1: A common European Framework for ICT Professionals in all industry sectors. CEN.

(10) Delamare Le Deist, F. & Winterton, J. (2005). What is competence? Human Resource Development International, 1, 27-46.

(11) M. Mulder, T. Weigel & K. Collins, "The concept of competence concept in the development of vocational education and training in selected EU member states. A critical analysis", Journal of Vocational Education and Training, nr. 1, 2006, pag. 65-85.

(12) Winterton, J., Delamare Le Deist, F. & Stringfellow, E. (2006). Typology of knowledge, skills and competences: clarification of the concept and prototype, Office for Official Publications of the European Communities.

IB4 Erwin Haasnoot_Opmaak 1 09-07-19 15:28 Pagina 42

Erwin Haasnoot is software engineer bij Ubiqu Access B.V en promovendus onder de Data Science groep aan de Universiteit van Twente. Hij is te bereiken via erwin@ubiqu.com.

Refactor de factoren

Sterke authenticatiemethodes zijn een vereiste als je online iets van belang wilt doen. Zij kunnen bestaan uit één of meerdere factoren. Dit laatste staat bekend als 'Multi-Factor Authenticatie' (MFA). Factoren kunnen dingen zijn die je weet (zoals wachtwoorden), hebt (zoals smartcards) of bent (biometriën zoals vingerafdrukken). We noemen dit het '3 Factoren van Authenticatie'-model (3FA-model). Dit model is naar mijn mening niet volledig en zal herzien moeten worden.

IB4 Erwin Haasnoot_Opmaak 1 09-07-19 15:28 Pagina 43

Het authenticatiespel bestaat uit het bewijzen van jouw identiteitsclaim: de claim wie jij bent. Als we de slogan mogen geloven dan is dat makkelijk. We kunnen simpelweg bewijzen wie we zijn door wie we zijn. De twee andere type factoren zijn helemaal niet nodig. Echter, 'zijn'-factoren zijn niet wat ze zeggen dat ze zijn.

'Zijn'-factoren worden ook omschreven als 'inherente'-factoren. Ik ben niet mijn vingerafdruk, maar misschien is mijn vingerafdruk wel inherent aan mij. Het probleem is dat iets wat je weet, hebt en wat inherent aan je is niet zo lekker klinkt als het origineel. Alsof de neefjes van Oom Donald opeens Kwik, Kwek en Piet zouden heten.

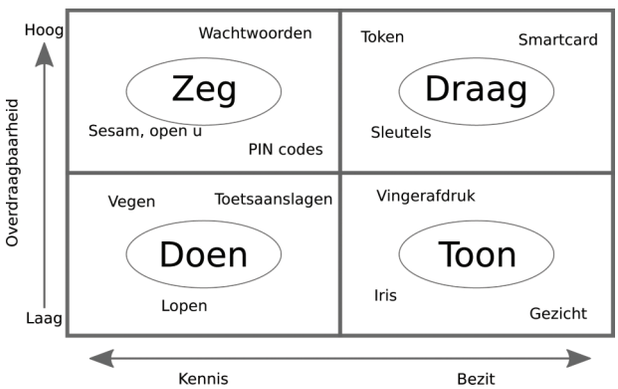
Sterke MFA-methodes

Belangrijker is dat 'zijn'-factoren een onterechte stimulans in status krijgen van deze versimpelde blik op authenticatie. Wij kennen over het algemeen de problemen met wachtwoorden en smartcards, maar biometriën hebben even grote problemen. Alleen door op een intelligente manier factoren samen te voegen kunnen we sterke MFA-methodes bouwen.

Er is verder nog een onofficiële categorie factoren in opmars die bekend staan als dingen die je doet. Creditcardverwerkers voorkomen fraude door onder andere te kijken naar waar en wanneer transacties worden uitgevoerd. Dezelfde principes worden nu door vele websites toegepast. Wanneer je inlogt op een nieuwe computer, dan moet je deze sessie ook nog valideren via een email die je toegestuurd wordt. In deze categorie schaar ik ook de manier waarop je tikt en veegt op je smartphone en andere soortgelijke 'touch/keystroke dynamics' (KD). Full disclosure: dit is het onderwerp van mijn promotieonderzoek.
In het 3FA-model vallen 'doe'-factoren in een niemandsland tussen dingen die je bent en weet. Bijvoorbeeld, de manier waarop je veegt is afhankelijk van de lengte van je vingers, maar ook van hoe goed je bent met je smartphone - ook wel bekend als 'procedurele kennis'.

2DA-model

We hebben dus een model nodig waar 1) geen enkele factor boven een andere factor staat en 2) 'doe'-factoren



netjes geïntegreerd worden. Hierbij presenteer ik het '2 Dimensies van Authenticatie'-model (2DA-model), dat dit precies doet.
'Zijn'-factoren zijn beter uit te leggen als 'heb'-factoren, in mijn optiek. Ik ben niet mijn vingerafdruk, maar ik heb er wel één (of 10). De eerste dimensie is daarom die van wat je weet versus wat je hebt, oftewel kennis versus bezit. Dit komt ook door de intuïtieve lakmoesproef heen: "Ik heb een vingerafdruk" en "Ik heb een smartcard" tegenover "Ik weet mijn wachtwoord", "Ik weet waar ik ben" en "Ik weet hoe ik mijn smartphone moet gebruiken."

Overdraagbaarheid

De tweede dimensie, overdraagbaarheid, volgt hier op een natuurlijke manier uit. Het grootste onderscheid wat je kan maken tussen het hebben van een smartcard en een vingerafdruk - en het weten van een wachtwoord en mijn manier van smartphonegebruik - is dat mijn vingerafdruk en manier van smartphonegebruik niet makkelijk overdraagbaar zijn.
Alle kwadranten in dit model beschrijven nu een nieuwe categorie van factoren. Ze maken onderscheid tussen de dingen die je draagt (zoals smartcards) toont, (zoals vingerafdrukken), doet (zoals swipes op smartphone) en zegt (zoals je wachtwoord aan je computer). Dit kan een eerste stap zijn in de introductie van het 2DA-model waarvan ik hopelijk duidelijk heb gemaakt dat het op een intuïtieve manier een aantal problemen oplost die in het 3FA-model voorkomen.

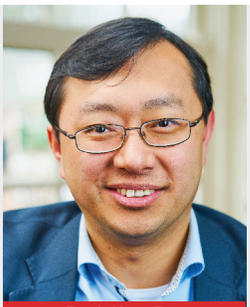
IB4 AHN_Opmaak 1 11-07-19 15:21 Pagina 44

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.

Bitcoin: to be or not to be?

De bitcoin is weer in het nieuws. Op 17 juni tikte de bitcoin een waarde van €8.375,92 aan. Daarmee toont deze munt zijn jojokwaliteit, want in december 2018 was de waarde gezakt naar €2.962,50. De totaalwaarde bedraagt inmiddels dan ook $ 163 miljard. Daartegenover staat de piekwaarde van eind 2017 van €15.151,37 per stuk. De vraag is: zal de bitcoin een serieuze munt worden of blijft zij een speelbal van sentimenten, zoals Facebooks plannen voor een eigen munt? De afgeleide vraag is: verliezen staten en banken hun monopolie als geld creërende instituties?



Fook Hwa Tan

Het lijkt erop dat de bitcoin en andere cryptocurrency een blijvertje gaan zijn

Fook Hwa Tan

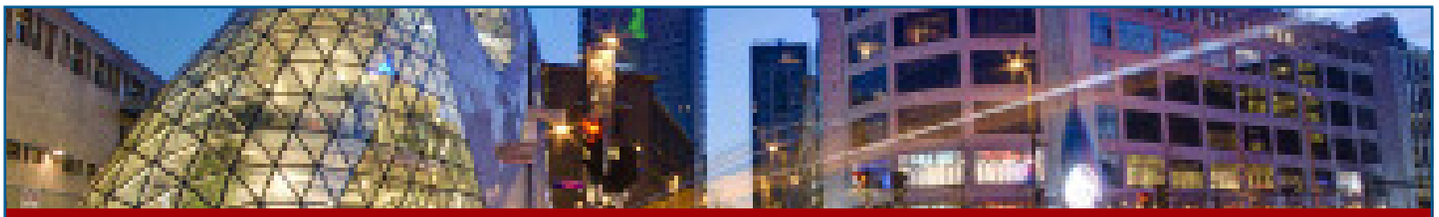
We hebben het al jaren over cryptocurrency - en voornamelijk over bitcoins. Na de val van de koers het afgelopen jaar zie je de adoptie ook vertragen. Toch geloof ik niet dat bitcoins helemaal zullen verdwijnen. Ook zien we andere cryptocurrencies ontstaan. Waarom zullen cryptocurrencies blijven?

De hype is inmiddels wel een beetje voorbij, maar daardoor zie je wel dat er steeds meer serieuzere toepassingen ontstaan met minder grote koersfluctuaties. Ook institutionele investeerders zijn langzaam geïnteresseerd in de potentie van cryptocurrency. Serieuze cryptocurrency exchanges beginnen langzaam opgezet te worden met nog meer focus op informatiebeveiliging. Ondanks de inherente beveiliging van cryptocurrency - door het gebruik van blockchaintechnologie - is ook duidelijk geworden dat er meer komt kijken dan alleen de techniek. Het gaat ook om de processen en de mens. In Europa is nu ook een nieuwe speler bezig om zich voor te bereiden op een veilige en snelle manier van handelen van cryptocurrency gericht op de Europese markt.

Daarnaast zien we ook de eerste tekenen dat grote multinationals zoals Facebook zich bezig willen gaan houden met cryptocurrency. Dit lijkt op een verdere adoptie, waarbij grote partijen gebruik willen gaan maken van de mogelijkheden van deze technologie. Ook onze Belastingdienst laat bijvoorbeeld al jaren toe onze cryptocurrency bij onze belastingaangifte op te geven.

Als laatste zijn er geluiden dat de banken en toezichthouders naar de regulering willen gaan kijken voor deze opkomende markt. Het is niet meer iets wat mogelijk voorbij zal gaan. Het vormt - naast de reguliere valuta - wel degelijk een alternatief voor veel consumenten. Dat betekent dat het ook invloed gaat krijgen op reguliere valuta, wat regulering in de toekomst noodzakelijk maakt. Hoe? Dat moet dan nog uitgezocht worden.

Hogere adoptie, minder hype en mogelijke regulering lijken erop te duiden dat de bitcoin en andere cryptocurrency een blijvertje gaan zijn. Voor ons als securityprofessionals is het dan ook van groot belang om up-to-date te blijven als het gaat om de achterliggende technologie en te weten hoe we het gebruik ervan veiliger kunnen maken.



IDENTITY MANAGEMENT & ACCESS CONTROL TRAINING

Leer in 4 dagen hoe u Identity Management en Access Control succesvol kunt implementeren in úw organisatie!

Gezien het toenemende belang van beheersing, risk en compliance krijgt identiteiten- en autorisatiebeheer steeds meer de aandacht. In veel organisaties zijn inmiddels Identity & Access Management trajecten gestart, helaas vaak met onvoldoende succes. In deze 4-daagse training Identity Management & Access Control van IMF Academy worden alle aspecten van een IAM traject zodanig belicht dat de kans op een succesvolle implementatie aanzienlijk toeneemt.

Deze training is tevens beschikbaar als 9-delige schriftelijke cursus, met de mogelijkheid deze online te bestuderen via digital learning. Kijk voor meer informatie op:

WWW.IMF-ONLINE.COM/PARTNER/PVIB

In-company

Al onze opleidingen kunnen wij ook in-company (en op maat) voor u verzorgen.

Korting voor PvIB leden

PvIB-leden ontvangen EUR 200,- korting op alle IT security opleidingen van IMF. Vermeld uw lidmaatschapsnummer bij uw inschrijving en de korting wordt meteen verrekend!

IMF Academy

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
Maarten Hartsuijker
Lilian Knippenberg
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 2019 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

creative commons

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

IB4 new Column Berry_Opmaak 1 09-07-19 15:36 Pagina 47

Het is allemaal nep

Het is al een aantal jaren geleden, dat geef ik wel toe, maar er was een tijd dat je je spullen gewoon in winkels kocht. Een winkel is een gebouw waarin spullen liggen die je als consument kunt kopen. Vroeger had je heel veel winkels: schoenenwinkels, warenhuizen (met allerlei verschillende producten), elektronicawinkels en ga zo maar door. Je liep dan zo'n winkel in, pakte een product uit de schappen, je bekeek het aan alle kanten, soms paste je het en als je helemaal happy was dan pakte je je portemonnee.

Natuurlijk kon je ook een tv kopen in een winkel. Die nam je gewoon mee, want een 19 inch toestel was vroeger al best groot. Natuurlijk kon het voorkomen dat je huiswaarts langs een etalage liep waarin je toevallig jouw nieuwe aanwinst zag staan - alleen dan met een heel anders prijskaartje. Soms liep je fluitend verder, maar het kon ook voorkomen dat de bui iets minder positief werd. Tja, shit happens en je nam je verlies als een man.

Op een bepaald moment waren de vliegvakanties aan het opkomen en vakantievierend Nederland zwermde over de hele wereld uit en nam (vaak stiekem) de mooiste shirts mee uit verre oorden. Ook sportschoenen waren zeer in trek, want waarom zou je die spullen laten liggen als ze in Nederland minimaal 5 keer duurder zijn? Dat die kleding puur nep was dat mocht de pret natuurlijk niet drukken.

Als we dan de laatste stap maken naar vandaag de dag dan is de situatie nog veel schrijnender geworden. We komen nu bij Aliexpres en andere websites waar we een plaatje zien van een product en die daar kunnen bestellen voor bedragen die veel en veel lager zijn dan bij de westerse winkels. Een iPhone 10 voor nog geen 100 euro is natuurlijk geen geld. In de winkelmand maar. Een horlogebandje voor je horloge voor 1 euro? Dat klink beter dan de 79 euro die Apple vraagt. Eigenlijk weet je het al als je het in je winkelmand gooit. En ja, het klopt: het is gewoon namaak. Zelfs van de iPhone wist je het en als je merkt dat de telefoon op Android werkt, dan weet je dat je teveel betaald hebt. Dan zal de Rolls Royce op Aliexpress (echt waar) ook wel niet echt zijn.

Moeten we ons daar over opwinden of weten we gewoon dat we genept worden? Als ik op Marktplaats een product koop dat eigenlijk te voordelig geprijsd is dan vraag je er toch eigenlijk om genept te worden? Als je een brief krijgt van je bank dat je je inloggegevens even moet invoeren dan weet je zo langzamerhand toch wel dat je genept wordt? Eigenlijk is er in al die jaren niet veel veranderd.

Berry

Project1_Opmaak 1 09-07-19 15:53 Pagina 1

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

NIEUW IN ONS PORTFOLIO:

Leer in twee dagen de basisconcepten van het dark web, Tor en Blockchain.

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 cursussen en Masterclasses aan. Denk hierbij aan cursussen als Identity and Access Management, Social Engineering of de Masterclass Business Resilience.
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