iB

INFORMATIEBEVEILIGING

jaargang 18 - 2018

#4

Interview: Crisismanagement borgen in organisatie

Wie is de meest gezochte informatiebeveiliger?

Cybersecurity hoort niet thuis in de directiekamer

Elk implementatietraject heeft zijn security aspecten in zich!

SPRONG IN HET DIEPE

De beste manier om iets te leren, is door het gewoon te gaan doen, zeggen ze. Om die reden, en omdat het voor de andere redactieleden niet goed uitkwam, had ik de eer om het hoofdredacteurschap voor deze editie op me te nemen. Ik moet eerlijk bekennen dat ik dat als kersvers redactielid best spannend vond, maar het feit dat er weer een blad voor u ligt geeft aan dat het allemaal goed gegaan is. Het heeft zeker geholpen dat het PvIB een professioneel team heeft, dat alles regelt rondom vormgeving, drukken, logistieke zaken en weet ik veel wat er allemaal komt kijken bij het leveren van zo'n blad.
Nu de redactie recentelijk versterkt is met maar liefst drie nieuwe leden (en een aantal kandidaten nog in de pijplijn zitten) heeft Bart van Staveren ons laten weten terug te treden uit de redactie. We danken Bart hartelijk voor zijn bijdrage aan het tot stand komen van het blad iB in de afgelopen jaren. Bart, geniet van je pensioen, en als je iets interessants meemaakt, mag je daar uiteraard een artikel over aanleveren.

Uiteraard is er geen blad zonder schrijvers van artikelen. Ook voor deze editie hebben we mensen bereid gevonden om hun kennis en mening te delen door interessante artikelen.
Sandra Kagie ging met Esther Huijser in gesprek over de uitdagingen rondom Business Continuity Management en crisismanagement en Robert Metsemakers geeft zijn visie op het schrijven van security risk scenarios. Nicole van Deursen geeft haar analyse van vacatures voor informatiebeveiligers, Peter van Deutekom schrijft over het belang van security bij implementatietrajecten en The Attributer vraagt zich af of wij klaar zijn voor 'the quantum revolution in secure communications'. In de serie Bestuur in Beeld is het dit keer de eer aan Erwin Bosma om zich aan u voor te stellen.

Hoewel de spannende datum van 25 mei achter ons ligt, laten de AVG en privacy ons maar niet los. Maarten Hartsuijker schrijft over een interessante uitdaging die de AVG met zich meebrengt, Rachel Marbus geeft wederom met een scherpe blik een nuchtere kijk op privacy en in de vaste column van Berry wordt de angst om gegevens te delen gerelativeerd.

Het mag duidelijk zijn dat ook deze editie weer genoeg stof bevat om in te verdiepen en om over na te denken. Dank aan alle auteurs! Aan u als lezer: veel leesplezier. Dat deze editie u mag inspireren en motiveren tot het schrijven van een eigen artikel.

Hugo Leisink

In dit nummer

Voorwoord - **3**
Organisaties worstelen met AVG-identificatie - **4**
Column Privacy – Privacyhaat - **7**
Interview: Crisismanagement borgen in organisatie - **8**
Het bestuur in beeld – Erwin Bosma - **11**
Wie is de meest gezochte informatiebeveiliger? - **12**
Lessons learned bij het schrijven van security riskscenario's - **18**
Ouderlijk toezicht … op je ouders…. - **21**
Cybersecurity hoort niet thuis in de directiekamer - **22**
Column The Attributer - Quantum Ready - **25**
Elk implementatietraject heeft zijn security aspecten in zich! - **26**
Achter het Nieuws - **28**
Column Berry - Een nieuwe bril - **31**

ORGANISATIES WORSTELEN MET AVG-IDENTIFICATIE

Eerste ervaringen inzageverzoeken

Het kan niemand ontgaan zijn. Op 25 mei trad de AVG in werking. Binnen de nieuwe privacywet is de regie die wij zelf op onze eigen privacy kunnen voeren flink verbeterd. Zo is er binnen de nieuwe wet meer aandacht voor de rechten van het individu. Maar hoe weet je als organisatie zeker dat degene die een recht probeert uit te oefenen ook daadwerkelijk de betrokkene is? En of je de opgevraagde data niet aan de verkeerde geeft? Een aantal ingediende inzage-verzoeken laat zien dat de controle of de indiener van een inzageverzoek ook daadwerkelijk de betrokkene is, nog zeer verschillend wordt uitgevoerd.

Op het moment dat je als organisatie een directe relatie met je klant hebt, is identificatie erg eenvoudig

Organisaties die in Nederland erg veel van je weten (en die data dus extra goed moeten beschermen!) zijn natuurlijk de telecomproviders en de banken.

Telecomproviders hebben op elk moment van de dag dat jij je telefoon bij je hebt toegang tot gegevens over waar jij je online en op straat bevindt. Je stamkroeg, supermarkt, bedtijden, reispatronen en bezochte locaties, die je wellicht graag voor je houdt, zijn voor hen geen geheim.

Banken weten op basis van je uitgavenpatroon erg veel over je. Dit geldt in mindere mate ook voor de Payment Service Providers (PSP's) die online aankopen afhandelen. Deze groep bedrijven is minstens zo interessant als je eigen bank. Want hoewel wij onze aankoop bijvoorbeeld bij bol.com doen, verstrekken wij onze persoonsgegevens onafhankelijk aan deze tussenpersoon. Deze organisaties positioneren zich veelal als een onafhankelijke verantwoordelijke. Dit scheelt natuurlijk een hoop verwerkersovereenkomsten richting de webshops. En het geeft de PSP's meteen de ruimte om de transactiegegevens voor eigen doeleinden in te zetten. En wie gaat er bij het iDeal scherm nou kijken naar de privacyvoorwaarden van de online kassa? Maar aangezien de PSP's zich als verantwoordelijke opstellen, geldt natuurlijk ook dat je er als consument rechtstreeks een inzageverzoek mag doen. De identificatiestap binnen zo'n inzageverzoek is dan, gezien de indirecte relatie die je met de partij hebt, extra interessant.

Identificatie

Op het moment dat je als organisatie een directe relatie met je klant hebt, is identificatie erg eenvoudig. Een aanvraagformulier achter de inlogpagina is voldoende. De klant logt dan in met hetzelfde account als waarmee hij diensten afneemt en bewijst daarmee dat de aanvraag authentiek is. In de praktijk verwijzen ook deze organisaties voor inzageverzoeken regelmatig naar een privacypagina en wordt het inzageverzoek vervolgens per post of mail bij de privacy officer ingediend. Vervolgens stuurt het grootste deel van de organisaties het verzoek om een kopie van een identiteitsbewijs, op basis waarvan ze bepalen of jij echt degene bent die jij voordoet te zijn.

Een kopie ID als identificatie

Een kopie van een identificatiebewijs zegt helaas niets over de identiteit van de aanvrager als het origineel niet gelijktijdig op echtheid wordt gecontroleerd. Bij het kopiëren van een paspoort of rijbewijs gaan alle echtheidskenmerken verloren. En het aanpassen van een naam en geboortedatum op een digitale scan is natuurlijk eenvoudig.

Geen passende identificatie

Het resultaat is dat de meeste organisaties geen passende identificatie uitvoeren, waardoor de kans bestaat dat de wijze van identificatie binnen het AVG-inzagerecht tot identiteitsdiefstal en een datalek leidt.

Wat zegt de toezichthouder

De Autoriteit Persoonsgegevens schreef eerder over legitimeren:
"Het vragen om legitimatie heeft alleen zin wanneer de medewerker de echtheid en geldigheid van het identiteitsdocument controleert. Wanneer een medewerker zonder deugdelijke controle een vals of vervalst document als 'bewijs' accepteert, neemt het risico

Maarten Hartsuijker is consultant en ethisch hacker bij Classity en helpt organisaties in de volle breedte met informatiebeveiliging (en privacy). Maarten is tevens redacteur bij het PvIB. Maarten is bereikbaar via www.classity.nl.

De eerste ervaringen met de identificatie na een inzageverzoek tonen vaak hoe het niet moet

op identiteitsfraude en andere vormen van criminaliteit juist toe. Een deugdelijke controle kan alleen plaatsvinden aan de hand van een origineel document, niet een kopie; daarop zijn beschadigingen of vervalsingen vaak niet meer te zien."(1)

Men geeft op de website echter wisselende signalen af door betrokkenen te informeren dat het mogelijk is dat organisaties als onderdeel van een inzageverzoek om een kopie-id kunnen vragen. Op de 'recht op inzage' pagina staat dit als volgt omschreven:

"Voordat de organisatie uw inzageverzoek in behandeling neemt, kan de organisatie controleren wie u bent. De organisatie kan u vragen om uw identiteitsbewijs te laten zien of om een kopie daarvan op te sturen."(2)

Voor organisaties die worstelen met het bepalen van een passende wijze om een aanvrager van een inzageverzoek te identificeren, zou het goed zijn als er op de website eenduidige informatie wordt verstrekt.

Zoekcriteria

Om een overzicht van de over een individu verwerkte persoonsgegevens te maken, zullen organisaties hun systemen moeten raadplegen. Ook hier liggen een aantal risico's op de loer. Een aantal organisaties gaf aan gegevens op te zullen gaan zoeken aan de hand van het e-mailadres waarmee het inzageverzoek werd ingediend. Nadat er werd aangegeven dat dit een ander adres is dan het e-mailadres waarmee webshopbestellingen worden geplaatst, werd in sommige gevallen verzocht om de in het verleden gebruikte adressen te verstrekken. Op dat moment is het belangrijk om voor elk van de adressen zeker te weten dat deze ook daadwerkelijk bij de betrokkene hoort. Dit is complex op het moment dat een adres niet meer in het bezit van de betrokkene is, omdat deze bijvoorbeeld van provider is veranderd. Tijdens één aanvraag werd dit opgelost door te vragen om aan te geven tot welke datum een adres ongeveer in bezit was geweest. Dit zou dan in de selectie worden meegenomen.

Hoe identificeer je een betrokkene passend?

De eerste ervaringen met hoe organisaties de betrokkene achter het inzageverzoek identificeren laten regelmatig zien hoe het niet moet. Maar hoe identificeer je de aanvrager dan wel goed? Je kunt hiervoor bijvoorbeeld de middelen gebruiken waarmee een betrokkene zich eerder identificeerde (of dat nou zijn echte identiteit was of een alias, is eigenlijk niet relevant). Heeft de betrokkene toegang tot een 'Mijn-omgeving'? Dan verloopt de aanvraag bij voorkeur via het portaal. Is er een transactie verricht? Dan kun je verzoeken om vanaf hetzelfde rekeningnummer een eurocent over te maken, die je daarna weer storneert. Ben je bekend met het huisadres, e-mailadres of 06-nummer van de betrokkene? Dan zou je twee van deze middelen ter identificatie kunnen gebruiken (geeft minder zekerheid aangezien dit 'bezit' van eigenaar kan wisselen). Heeft je organisatie fysieke vestigingen? Dan is identificatie op locatie natuurlijk ook een optie. Mits het personeel getraind is om een identificatiebewijs op echtheid te controleren. Van de breed geadopteerde gewoonte om naar een kopie-id te vragen moeten we in elk geval afstappen. Deze geeft evenveel zekerheid over de identiteit van de aanvrager als een kopie van het verzendlabel van de Margriet. Het dient daardoor geen doel en werkt de onnodige verwerking van bijzondere persoonsgegevens in de hand. Niet elke aanvrager zal immers zijn foto en BSN verwijderen of de gegevens in de Machine Readable Zone over het hoofd zien.

Hoe identificeert jouw organisatie de betrokkenen bij een inzageverzoek

Heb jij binnen jouw organisatie een goede manier ontwikkeld om betrokkenen bij een inzageverzoek passend te identificeren? En wil je deze delen met andere PVIB-ers? Post dan je bijdrage binnen de PVIB LinkedIn-groep(3).

Referenties

(1) http://wetten.overheid.nl/BWBR0033181/2012-07-12
(2) https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-inzage
(3) https://www.linkedin.com/groups/133202

PRIVACYHAAT

15 juni 2018 in Breda Vandaag: 'Fuck de nieuwe privacywetgeving, gefeliciteerd geslaagde kanjers!'. Het betreft een column waarin mevrouw Babs Verstrepen fulmineert over de nieuwe privacywet. Dat die ervoor zorgt dat je niet eens meer iemands naam in de krant mag zetten om hem of haar te feliciteren. Dat alles is uiteraard te wijten aan "dat 'lullige wetje' van die privacyknakkers". Haar woorden, niet de mijne. Dat je al jaar en dag niet zomaar iemands naam in de krant mag zetten (u weet wel, hiervoor hadden we de Wbp en daarvoor de WPR), is mevrouw Babs even vergeten. Of ze heeft het nooit geweten.

Mevrouw Babs is het lijdend voorwerp, maar ze is in het geheel niet de enige. Wat wil je dan ook, als je letterlijk doodgegooid wordt met allerhande e-mails en pop-ups en apps met screens, waar je je elke keer bij het openen eerst doorheen moet worstelen (hou eens op daarmee Bijenkorf!) om bij de inhoud te komen. Om nog maar te zwijgen van die reclame op de radio van DAS Rechtsbijstand. Daarin hoor je een meneer steen en been klagen over die vreselijke nieuwe privacywet. Fijne boodschap DAS! En dan zegt een andere meneer dat DAS dat wel even voor je oplost door je een kek lekker nieuw privacystatement te geven. Ik had er als Privacy Officer van gedroomd dat het zo makkelijk was geweest.

In eigen huis komt het ook voor hoor. De hoeveelheid berichten, verzoeken en 'wat dies meer zij' die ik wel niet heb gehad over zaken die door afzenders onder 'de Gee-Dee-Pee-ERRR' geschoven worden, maar die overduidelijk bijzonder weinig te maken hebben met de nieuwe privacywet, zijn niet te tellen. Voor een gedeelte heeft dat echt te maken met het feit dat privacy een lastig vak is en daardoor voor iemand die er niet in gespecialiseerd is, bijzonder moeilijk correct te plaatsen is. En dat geeft ook helemaal niets, daar zijn nu juist de specialisten voor. Maar omdat iedereen er op de één of andere manier mee te maken krijgt, hebben de meesten wel ergens een klok horen luiden en roepen dan navenant. Ik lieg niet mensen; over het implementatieprogramma, dat ik samen met mijn mensen uitvoerde, hadden maar liefst drie verschillende auditors een mening. Vaak ook nog zonder enig inhoudelijk verstand van zaken. Wat tot ontzettend veel ellende en stress heeft geleid. Maar omdat er al zoveel onkunde de wereld in is geslingerd, door zoveel mensen, is bijna alles geloofwaardig geworden. En dat is echt een probleem.

Privacyhaat of privacyafschuifgedrag ("het is een probleem van de privacymensen/wet!") heeft voor een groot gedeelte te maken met onkunde. En dat kun je echt op maar één manier oplossen. Door kunde te geven en anderen mee te nemen in het echte verhaal over privacy. Privacy is het verhaal over autonomie en vrijheid. Een samenleving waarin je kunt zijn wie je bent, je vrij bent om beslissingen te nemen en je het recht hebt om bepaalde zaken bij je te houden en te delen (of niet) met wie jij dat wilt. In januari 2001 begon ik met mijn eerste privacybaan aan de Technische Universiteit van Eindhoven. En in bijna 20 jaar tijd is mijn privacyliefde alleen maar groter geworden. Ik ga de komende 20 jaar nog meer mijn best doen om kunde te brengen en liefde te verspreiden. Dat is nog steeds het enige medicijn tegen haat.

Mr. Rachel Marbus
@rachelmarbus op Twitter

INTERVIEW

CRISISMANAGEMENT BORGEN IN ORGANISATIE

Kwestie van testen, trainen, onderhouden en verbeteren

"Business Continuity Management (BCM) is binnen Geldservice Nederland (GSN) geen papieren tijger. Ons Business Continuity Plan (BCP) is niet een boekje dat op de kast staat of in een la ligt. Integendeel, BCM is voor ons een continu proces van testen, trainen, onderhouden en verbeteren."

Zo trapt Esther Huijser, hoofd Risk, Security en Compliance van GSN, ons gesprek af. Een gesprek waarin het borgen van BCM/crisismanagement in een organisatie centraal staat. Om haar BCP actueel te houden, vindt GSN het testen en oefenen van wat op papier is gezet heel belangrijk. "Met zo'n oefening pakken we dan ook meerdere keren per jaar uit", zegt Esther. "Je moet voelen wat een crisissituatie inhoudt. Wat de gevolgen zijn van een genomen beslissing. Alleen droog oefenen heeft wat ons betreft geen zin. Papier is geduldig, maar de praktijk is weerbarstig. En daarom testen we meerdere keren per jaar of dat wat we op papier hebben gezet in de praktijk werkt."
In die oefeningen komen dreigingen die spelen in het 'fysieke domein' steeds vaker samen met dreigingen in het cyberdomein. In het geval van GSN kunnen scenario's bijvoorbeeld betrekking hebben op brandstichting, het plegen van een overval, maar ook op een cyberaanval. "Oefeningen zijn binnen GSN ingebed in het proces, in de organisatie", benadrukt Huijser. De wereld om ons heen verandert zo snel. Dat vraagt volgens haar van een organisatie dat je 'resilient' (red. veerkrachtig) bent. "Dit betekent dat je als moderne organisatie continu moet werken aan je improvisatietalent. En dat is anno 2018 écht een ander proces dan pakweg zeven à acht jaar geleden", concludeert Huijser.

'Een BCP is nooit af'

Jacques Mortiers, manager IT bij GSN, sluit zich volledig aan bij zijn collega. "De snelheid waarmee ontwikkelingen elkaar opvolgen, maakt dat je als organisatie BCM en daarmee crisismanagement als een continu proces moet beschouwen. Een Business Continuity Plan is dus nooit af", benadrukt hij. Voor GSN verandert de wereld momenteel volgens beiden wel heel snel. Vanaf volgend jaar is het bedrijf, dat in 2011 door de drie Nederlandse grootbanken (ABN AMRO, ING en Rabobank) werd opgericht, namelijk eigenaar van álle stort- en geldautomaten van deze banken. Dat worden dan uniforme, zogenoemde 'witte' automaten. GSN zorgt al sinds 2011 voor het verwerken en distribueren van het contante geld en het beheer en onderhoud van de stort- en geldautomaten voor haar aandeelhouders (de drie genoemde grootbanken). Vanuit die samenwerking is de intentie ontstaan om het eigenaarschap van alle geldautomaten en de achterliggende processen van de deelnemende banken in Nederland onder te brengen bij GSN. Eén partij, zo denken de banken, kan contant geld beter toegankelijk, beschikbaar, veilig en betaalbaar houden in tijden van afnemend gebruik van contant geld en toenemend geweld tegen geldautomaten, dan drie afzonderlijke partijen. "Een ontwikkeling die ervoor zorgt dat we, nog meer dan voorheen, een belangrijke schakel in de samenleving vormen. Dit als onderdeel van de kritische financiële infrastructuur. We hebben dadelijk niet drie klanten, onze aandeelhouders, maar 17 miljoen klanten", aldus Mortiers. Huijser: "We worden steeds meer een regiepartij, ook in het IT-domein. Dat betekent dat we ook wat BCM betreft niet alleen plannen voor onszelf, onze eigen panden, moeten maken en testen. Maar dat we ook in de keten, en in de nieuwe situatie zelfs, Nederland-breed moeten denken als het gaat om het minimaliseren van de impact van een crisis, calamiteit of andere verstoring van onze dagelijkse processen."

'Het begint bij cultuur'

Maar hoe krijgt GSN haar medewerkers en haar ketenpartners nu zover om hierin mee te gaan? Wat maakt dat binnen GSN het oefenen van crisisscenario's serieus wordt genomen? "Het begint bij cultuur", stelt Huijser. "Wanneer een medewerker van ons een afwijking van het gewone, hoe klein ook, constateert, wordt dit gemeld bij onze digitale BHV, zoals wij dat noemen. Dat kan een phishing mail zijn, een vreemde vraag die telefonisch binnenkomt of bijvoorbeeld een vorm van afwijkend gedrag in de buurt van één van onze gebouwen." "En deze meldingen worden vervolgens altijd serieus genomen. Ook al is iemand de honderdste die de melding doet. We hameren erop, dat onze medewerkers de oren en ogen van de organisatie zijn. Dat ze ertoe doen en dat we in hun belang veiligheid hoog in het vaandel hebben staan. We zijn met andere woorden een High Reliability Organization." "Elke afwijking, hoe klein ook, kan de opmaat zijn tot een situatie die uit de hand loopt",

Sandra Kagie is freelance tekstschrijver/journalist. Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst en taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'informatiebeveiliging'. Haar website is www.sanscriptproducties.nl en op Twitter is zij actief als @SanSanscript.

benadrukt ook Mortiers. "Reden waarom we elke melding serieus nemen. En reden ook voor ons om zo nu en dan zelf een 'foute mail' te versturen aan medewerkers. We monitoren dan hoeveel meldingen er binnenkomen en deze resultaten communiceren we vervolgens ook weer terug naar de mensen." Tot zijn tevredenheid kan Mortiers melden dat het responsepercentage wat dit betreft binnen GSN behoorlijk hoog ligt. Dat medewerkers binnen GSN zo doordrongen zijn van het feit dat melden moet, heeft volgens beiden zeker ook te maken met de aanwezigheid van 'cash centers' binnen de organisatie. "Dat zijn natuurlijk bij uitstek plekken waar het omgaan met allerhande veiligheidsprotocollen ingebakken is. Het hebben van een BCP is voor GSN alleen al daarom altijd een no-brainer geweest", aldus Huijser. "Maar, ik durf te zeggen dat het veiligheidsdenken in het DNA zit van al onze mensen. Iedereen is zich bewust van het belang hiervan voor de continuïteit van onze organisatie."

Durf keuzes te maken

De belangrijkste tip die beiden andere organisaties willen meegeven in het kader van BCM is: 'durf keuzes te maken'. "Business as usual is echt iets anders dan een crisis. Je kunt niet alles redundant uitvoeren. Alleen al vanuit het kostenaspect is dit onmogelijk. Dwing jezelf dus zaken af te bakenen. Kijk naar de meest belangrijke processen in je bedrijfsvoering. En bepaal wat nodig is om de continuïteit daarvan te garanderen." Vervolgens is het wat Huijser en Mortiers betreft een kwestie van 'train as you fight'. Table top oefeningen en dilemma spelvormen zijn wat hen betreft niet voldoende. Het gaat om het echte werk, bijvoorbeeld 'red teaming'. Bij deze levensechte oefeningen wordt echt iedereen betrokken. "Niet alleen vaste mensen, maar ook ingeleend personeel en ketenpartners", aldus Huijser. "Wat heeft het immers voor zin om een uitwijk te testen, zonder dat je het bedrijf erbij betrekt dat voor jou als uitwijklocatie fungeert. Je wilt toch weten hoe lang zij nodig hebben om binnen hun processen, jouw processen in te passen", geeft ze als voorbeeld.

Scenario-testen

Zo heeft GSN bijvoorbeeld onlangs nog het scenario getest waarin het cash center in Weesp plat lag. Dit door een grote brand. Een voorbeeld van een scenario dat samen met hulpdiensten is bedacht en uitgevoerd. "Alles moet zo levensecht mogelijk zijn. Alleen dan weet je daadwerkelijk hoe je als organisatie in een stress-situatie functioneert." Zo'n scenario-oefening wordt vervolgens geëvalueerd met alle betrokkenen. "Niet om mensen af te rekenen, maar om ervan te leren", benadrukt Huijser. "Resultaten zullen dus nooit terugkomen in een beoordelingsgesprek van medewerkers. En, fouten maken mag. Als je er maar van leert." Een ander voorbeeld van een recente scenario-oefening binnen GSN betrof een zaak van een informatielek. De oefening was opgezet rond een vergadering van het Crisis Management Team (CMT). De laptop en tas van de voorzitter van de vergadering waren weggehaald en tijdens de vergadering belde de zogenaamde afperser. "Hij heeft de werkelijke spanning gevoeld", stelt Huijser. Dit om aan te geven hoe realistisch de oefeningen zijn. Durven stretchen als organisatie is in haar ogen heel belangrijk. Een goed voorbeeld hiervan is bijvoorbeeld communicatiemiddelen wegnemen. "Dan komen mensen echt in een creatieve modus, omdat er een beroep wordt gedaan op hun flexibiliteit en improvisatievermogen. En dat vermogen wil je uiteindelijk naar boven brengen."

Gevolg geven aan oefenresultaten

Uiteindelijk moet er met de resultaten van een oefening natuurlijk iets worden gedaan, stellen beide leden van het CMT van Geldservice Nederland tot slot. Dat betekent dat het management van een organisatie bereid moet zijn budget vrij te maken, om leerpunten die uit een oefening naar voren komen ook daadwerkelijk aan te pakken. Gebeurt dat niet, dan zullen medewerkers op hun beurt in oefeningen niet meer het achterste van hun tong laten zien. "De doodsteek voor realistisch oefenen en daarmee het einde van een actueel BCP", waarschuwt Huijser.

Toetsingskaders voor risicobeheersing

GeldserviceNederland heeft haar Business Continuity Management beleid gebaseerd op NEN-EN-ISO 22301 en op het Toetsingskader Business Continuity Management Financiële Kerninfrastructuur (FKI). DNB en de Autoriteit Financiële Markten (AFM) hanteren dit Toetsingskader in het toezicht op de naleving van de normen door de instellingen van de FKI.
Voor verschillende instellingen gelden verschillende continuïteitseisen. Instellingen die niet onder een bepaalde wet of regelgeving vallen, kunnen deze wel als leidraad gebruiken voor hun risicobeheersing. Op de website van de DNB zijn verschillende voorbeelden van deze toetsingskaders te vinden: www.dnb.nl/betalingsverkeer/overige-taken/bcm-en-crisismanagement/index.jsp

ERWIN BOSMA

De eer is aan mij dit keer, zo heb ik begrepen, om iets te vertellen over mezelf, mijn werk en mijn functie binnen het PvIB. En om mijn gedachten te laten gaan over de vereniging en de ontwikkelingen binnen informatiebeveiliging.

Laat ik beginnen met mezelf. Ik ben 55 jaar, studeerde Lucht en Ruimtevaarttechniek in Delft en ben sinds 2001 werkzaam in de informatiebeveiliging, bij verschillende multinationals. Nu werk ik als Information Security Officer bij Athlon Car Lease in Almere.

Sinds 2011 ben ik als bestuurssecretaris actief binnen het PvIB. Ik heb daarvoor gekozen, omdat ik merk dat het me veel voldoening geeft om te zien wat we als vrijwilligersorganisatie jaar na jaar neerzetten en ik het fijn vindt om daar een steentje aan bij te dragen. Daarnaast merk ik dat mijn contacten met peers, die ik ontmoet tijdens de diverse bijeenkomsten en waar ik graag ideeën en ervaringen mee uitwissel, bestendiger worden dankzij mijn rol binnen de PvIB. Dat vind ik een groot voordeel van het actief lid zijn binnen de vereniging, of dat nou binnen het bestuur is of binnen één van de commissies, werkgroepen of de redactie van iB Magazine.

Als ik kijk naar de ontwikkelingen binnen ons vakgebied de laatste jaren, valt me vooral op dat organisaties, naast het nemen van preventieve maatregelen op het gebied van informatiebeveiliging, zich ook steeds meer realiseren dat je alsnog slachtoffer kan worden van een aanval die je bedrijfsprocessen ernstig hindert of zelfs lamlegt, hoe goed je je maatregelen ook hebt geïmplementeerd. En dat je er dus op voorbereid moet zijn om de gevolgen van zo'n aanval zoveel mogelijk te beperken en/of de eventuele schade zo snel mogelijk te repareren. Dit vergt veelal andere competenties binnen een organisatie, die – als het goed is - ook nog eens niet gebruikt zullen worden. Hoewel de actualiteit een andere toekomst schetst.

Voorbeelden van grootschalige aanvallen op informatiebeveiliging komen wereldwijd voor en volgen elkaar steeds vaker op, zo lijkt het. Denk aan de cyber-attacks door State-sponsored groeperingen op Oekraïne, Singapore (tijdens de topontmoeting tussen de Amerikaanse president Trump en de Noord-Koreaanse leider Kim Jong-Un) en Nederland (DDoS aanvallen op banken en overheid). Maar het lijkt ook alsof we zulke aanvallen steeds normaler gaan vinden. En wat mij beangstigt is, dat dit soort situaties, ondanks de vele genomen maatregelen op wereldniveau, feitelijk niet te voorkomen zijn. En dat als een staat echt kwaad wil, dit een ontwrichtende werking kan hebben, die uiteindelijk niet of slechts gedeeltelijk te voorkomen is.

Om dit relaas een beetje luchtig te houden, even terug naar het PvIB en de toekomst die ik voor het platform zie. Ik heb er alle vertrouwen in dat we onze hoofdtaken over vijf jaar nog steeds zullen uitvoeren. We hebben een koers ingezet die we blijven volgen. Ons doel is om mensen uit de branche op een laagdrempelige manier bij elkaar te brengen. Maar we willen wel meer leden actief betrekken in (betrokken krijgen bij!) het delen van hun kennis en ervaring. Om dat te bereiken zijn we (bestuur samen met de commissies) nu bezig initiatieven te ontwikkelen om kleinere opdrachten open te stellen voor leden die zich daarvoor willen inzetten. Enerzijds omdat we merken dat niet iedereen zich voor langere tijd kan of wil vrijmaken voor vrijwilligerswerk, terwijl we anderzijds wel willen dat het PvIB een vrijwilligersvereniging blijft, omdat dat ook grotendeels onze identiteit en de sfeer binnen de vereniging bepaalt.

Erwin Bosma
secretarispvib@gmail.com

WIE IS DE MEEST GEZOCHTE INFORMATIEBEVEILIGER?

Diverse experts waarschuwen voor een tekort aan specialisten in cybersecurity. In dit artikel wordt samengevat welke experts werkgevers zoeken en de stijl waarin vacatures zijn geschreven. De gebruikte methode was een content analyse van 52 vacatures op vacature-websites.

Het blijkt dat in de meerderheid van de vacatures niet eenduidig wordt gecommuniceerd welke kennis de werkgever zoekt. Veel vacatures bevatten taakomschrijvingen die onbegrijpelijk zijn en competentie-eisen die onrealistisch en onoprecht zijn. De conclusie is dat de stijl waarin vacatures zijn opgesteld, kan leiden tot een mismatch van gestelde eisen en potentiele kandidaten. Bovendien kan de stijl een negatieve invloed hebben op het enthousiasme van geschikte kandidaten om te solliciteren.

Inleiding

De Cyber Security Raad luidde recentelijk de noodklok over het dreigende tekort aan cybersecurityspecialisten in Nederland (1). Er wordt inmiddels al jaren over dit onderwerp gesproken, gewaarschuwd en geadviseerd (2) (3). Diverse mogelijke oorzaken en oplossingen zijn reeds beschreven, waaronder de aansluiting van onderwijs met de vraag van werkgevers, het aantrekken van meer jonge arbeidskrachten en vrouwen, of het veranderen van werkprocessen in organisaties.

Rapporten over dit onderwerp worden doorgaans geschreven vanuit de vraag hoe opleidingsinstituten het curriculum kunnen verbeteren om aan te sluiten bij de vraag van werkgevers. Voor dat doel hebben diverse onderzoekers al vaker analyses van vacatures uitgevoerd om de eisen van werkgevers te beschrijven, en voor dit artikel was dat ook één van de doelstellingen. Daarnaast is voor dit artikel ook gekeken naar de stijl waarin vacatures zijn opgesteld. Er is weinig onderzoek beschikbaar over de stijl waarin informatiebeveiligingsvacatures zijn geschreven en of die stijl invloed zou kunnen hebben op het aantal reacties van geschikte kandidaten. Zouden werkgevers hun vraag kunnen aanpassen om betere kandidaten te vinden, in plaats van kandidaten te vragen om bij de vacatures te passen? Hoe presenteert de werkgever zich door de schrijfstijl van de vacature? Is het aantrekkelijk en realistisch voor een kandidaat om te solliciteren?

Analysemethode

Voor de analyse zijn op de websites van Indeed.nl en Intermediair.nl de zoektermen 'informatiebeveiliging', 'cybersecurity' en 'IT security' ingevoerd op vrijdag 13 april 2018. In totaal zijn 52 vacatures in Nederland beoordeeld die op die datum gepubliceerd stonden. Dit zijn niet alle vacatures van dat moment, maar met dit aantal kan een snelle indruk worden verkregen.

De vacatures zijn geprint en de teksten zijn handmatig gecodeerd, zonder software voor content analyse. Deze methode van het coderen van content in vacatures om de eisen van werkgevers te achterhalen, wordt frequent gebruikt in onderzoeken naar vacatureteksten (4) (5) (6).

In de teksten is gezocht naar woorden en zinnen die verwijzen naar de volgende variabelen:

1. functietitel
2. competenties
3. taakomschrijving
4. beloning (in cijfers en in voorwaarden)

Om de stijl van de vacatures te beoordelen, is gebruik gemaakt van een aangepaste versie van de 'Critical Discourse Analysis' methode van Wall, Stahl & Salam (7). Deze methode identificeert dominante patronen in communicatie-uitingen door te testen op overtredingen van waarden, zoals bijvoorbeeld begrijpelijkheid, waarheid, legitimiteit of oprechtheid.

Voor het doel van dit artikel zijn vacatureteksten beoordeeld op:

1. Begrijpelijkheid (de tekst is eenduidig en begrijpelijk). Een onbegrijpelijke tekst kan leiden tot verwarring en onzekerheid bij de kandidaat om te solliciteren.
2. Oprechtheid (de tekst is feitelijk juist, eerlijk en weerspiegelt wat de auteur bedoelt). Wanneer een werkgever een verkeerd beeld voorhoudt, solliciteert de kandidaat op een andere baan dan geadverteerd. De werkgever lijkt dan onbetrouwbaar.
3. Realiteit (de eisen zijn haalbaar en bestaan ook). Wanneer onrealistische eisen worden gesteld, ontstaat er een mismatch tussen kandidaat en vacature.
4. Enthousiasmerendheid (de baan en werkgever worden positief beschreven). De stijl en inhoud van de tekst kan een kandidaat enthousiast maken of juist laten afknappen.

Resultaten

Functietitels

Onder de 52 vacatures zijn 36 unieke functietitels geteld (figuur 1). Een aantal van die functietitels zijn varianten op groepen van functies zoals adviseur, officer of specialist. Sommige titels zijn niet begrijpelijk, bijvoorbeeld 'IT Wizard'. Een diversiteit aan functietitels en onbegrijpelijke titels maken het lastig zoeken voor een kandidaat en verduidelijken niet wie de werkgever zoekt. Een kandidaat die online zoekt naar een bepaalde functietitel, kan hierdoor vacatures mislopen.

Een vacature heeft als titel:' IT Architect-Cybersecurity'. In de tekst wordt verder gesproken over 'IT Solution Engineer'. De titel zal de interesse wekken van architecten, terwijl de werkgever een engineer zoekt, wat de oprechtheid van de werkgever in twijfel trekt.

Vooropleiding en certificeringen

De meest gevraagde vooropleiding is HBO of WO. Dit is opvallend omdat een HBO opleiding en wetenschappelijk onderwijs verschillende opleidingsdoelstellingen hebben. Het komt in 48 procent van de vacatures voor dat totaal verschillende opleidingen of certificeringen worden gevraagd op een manier alsof ze uitwisselbaar zijn (bijvoorbeeld 'bachelor of master'). Wanneer een werkgever MBO, HBO of WO vraagt en deze opleidingen allemaal geschikt vindt, dan komt dat op de kandidaat niet oprecht over: krijgt een MBO opgeleide dan hetzelfde werk te doen als een HBO opgeleide? En ook hetzelfde salaris?

Dr. Nicole van Deursen werkt als onderzoeker en consultant. Zij analyseert graag ontwikkelingen en trends rondom informatiebeveiliging. Op dit moment voert ze voor The Hague Security Delta een onderzoek uit naar de eisen in vacatures in het bredere veiligheidsdomein. Nicole is bereikbaar via nicole-ib@rujanima.com

Figuur 1 - Overzicht gevonden functietitels

CISM gecertificeerde personen worden iets vaker gevraagd dan CISA gecertificeerde, maar vaak beschrijft de werkgever dat ze tevreden zijn met óf CISSP óf CISM óf CISA. Hierdoor komt de tekst onoprecht over, omdat deze opleidingen verschillend zijn en andere doelgroepen aanspreken. Een ander voorbeeld van onoprechtheid is, dat een werkgever schrijft dat een universitaire opleiding inwisselbaar is voor certificaten: `academische vooropleiding of CISSP of CISA of CISM'.

Regelmatig worden lijstjes met mogelijke certificaten genoemd en wordt geëist dat de kandidaat één of twee van die certificaten bezit. Deze certificaten kosten veel geld en inspanning van de kandidaat. Ze onderscheiden zich van elkaar en ondersteunen verschillende specialisten in verschillende carrières. Een werkgever die ze op één hoop gooit en het prima vindt, zolang de kandidaat maar een certificaat heeft, komt niet oprecht over. Enkele voorbeeldteksten uit vacatures zijn:

- `CIPP/e, CDPO, CISSP, CISM, CISA of CEH'
- `CISSP, CISA, ISO 27001 CEH of CISM'
- `CISM, CISSP, CISO, ISMS foundation'
- `interesse om CISSP(-associate) en/of CEH, GCIA, GMON, GCIH of OSCP te behalen of je bent reeds gecertificeerd'
- `Certificering in Information Security, Internal Auditing, Regulatory Compliance, Engineering , ISA Certified Automation Professional en bij voorkeur een GICSP certificaat. CISSP- en/of CISA-certificering is een pré`

In de helft van de vacatures wordt gevraagd om kandidaten met een CISSP certificaat. Opvallend is dat regelmatig gevraagd wordt naar een CISPP of CISM certificaat bij kandidaten met twee tot vijf jaar werkervaring. Volgens de website van certificerende instantie (ICS) kun je daar alleen voor in aanmerking komen wanneer je meer dan vijf jaar betaalde werkervaring hebt. Deze combinatie van eisen is dus niet realistisch.

Een gecertificeerde ethical hacker (CEH) wordt vaker gevraagd dan een persoon met certificaten gerelateerd aan kennis over privacywetgeving. Dit is bijzonder, omdat in 22 van de vacatures staat dat de kandidaat iets met privacy (beleid) gaat doen, en in slechts drie vacatures staat iets over het daadwerkelijk vinden van beveiligingsmazen in een netwerk of technisch onderzoek doen naar kwetsbaarheden.

Er zijn twee werkgevers die een onrealistisch beeld hebben van ISO 27001. Een van deze biedt "Eventuele training tot omscholing voor en naar de norm ISO 27001." De ISO 27001 is echter niet van toepassing op een persoon. Een `training tot omscholing' is ook niet begrijpelijk. Er is nog een tweede werkgever die hoopt dat de kandidaat ISO 27001 gecertificeerd is en die dat op één hoop gooit in de lijst gewenste certificeringen `CISM, CISA, ISO 27001, CEH of CISM'.

De top 5 van meest gevraagde certificaten is:

1. CISSP
2. CISM
3. CISA
4. CEH
5. CIPP/e

Kennis en competenties

De gewenste inhoudelijke kennis wordt in weinig vacatures concreet beschreven. Er wordt vaak gevraagd om kennis van de ISO 2700x serie (52 procent van de vacatures). In een derde van de vacatures wordt

de CISSP certificering in combinatie met kennis van ISO 2700x gevraagd. Een goede beheersing van de Engelse taal wordt in 15 van de 52 vacatures expliciet als eis genoemd.

Het komt ook voor dat werkgevers de vacature zo opstellen, dat het lijkt alsof ze met iedereen blij zullen zijn. Wat voor kandidaat zoekt de werkgever die het volgende schrijft: "je bent een kei in tenminste één van de volgende onderwerpen:

- ICT infrastructuur
- Beheerprocessen
- Applicatiebeveiliging
- Business continuity management
- Privacy
- Adviseren
- Inschatten welke effecten de maatregelen zullen hebben'

Maakt het voor deze werkgever echt niet uit in welke van deze onderwerpen de kandidaat gespecialiseerd is? Een privacy jurist zou kunnen solliciteren, maar ook een IT beheerder. En wellicht maakt iemand die niets weet van deze onderwerpen, maar heel goed kan adviseren, ook een kans.

De vraag naar technische competenties loopt uiteen. Het is niet altijd duidelijk voor de lezer wat de specifieke competentie moet zijn. Vacatures beschrijven bijvoorbeeld dat het werk inhoudt: "adviseren over technische beveiligingsmaatregelen". Deze omschrijving is vaag, omdat technische maatregelen voor een werkplek met een bepaald besturingssysteem een ander soort kennis vereisen dan technische maatregelen in een datacenter.

Vacatures staan vol met paraplu-begrippen zoals: 'technische beveiligingsmaatregelen', 'infrastructuur', 'architectuur' of 'secure ontwikkelen'. Slechts incidenteel wordt concreet aangegeven met welke besturingssystemen of applicaties wordt gewerkt of welke soort systemen beveiligd moeten worden.

De top 10 van meeste gevraagde technische competenties is:

1. Technische beveiligingsmaatregelen
2. Infrastructuur
3. Security architectuur
4. Secure software ontwikkeling
5. Applicatie security
6. Netwerken
7. Vulnerability management
8. Incident response
9. Beheer
10. IAM

Uit de tientallen vacatures is een grotere hoeveelheid gewenste 'soft skills' geteld dan gewenste concrete technische kennis. Het lijkt daardoor alsof er veel waarde wordt gehecht aan competenties, wellicht zelfs meer dan aan specialistische kennis. De ideale kandidaat is vooral communicatief vaardig (67 procent), analytisch (30 procent), overtuigend (27 procent), zelfstandig (23 procent) en kan goed samenwerken (21 procent).

De vraag naar zeer ervaren mensen lijkt zeldzaam. Slechts één vacature vraagt specifiek naar iemand met meer dan 10 jaar ervaring. De meest gevraagde persoon is nét geen starter meer en heeft drie tot vijf jaar ervaring. Daarnaast zijn er veel werkgevers die het vaag houden met termen als 'ruime ervaring', 'meerdere jaren' of 'ervaring'. In 35 van de 52 vacatures wordt gevraagd om werkervaring rond de vijf jaar of minder. In Nederland is een grote groep ervaren werknemers die niet enthousiast zullen worden om te solliciteren naar functies die bedoeld zijn voor het begin van een carrière.

Werkzaamheden

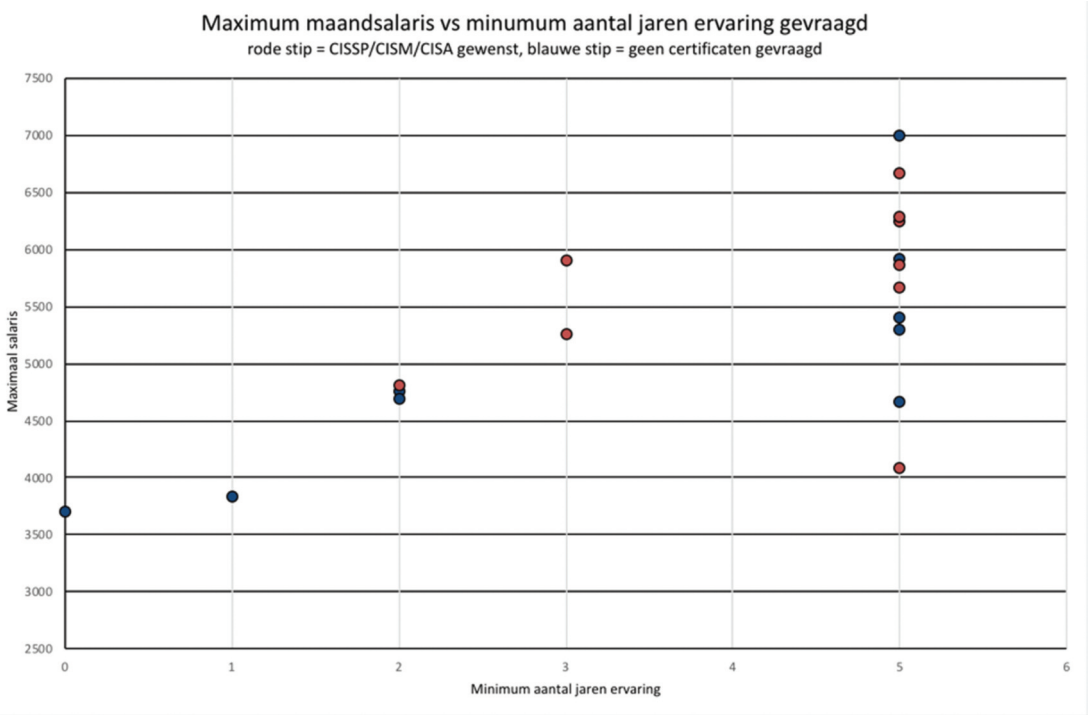
In de vacatures is gezocht naar werkwoorden (doe-woorden) gecombineerd met inhoudelijke vaktermen die beschrijven welke werkzaamheden de kandidaat gaat verrichten. Het valt op dat er vaak werkwoorden staan waarbij geen meetbare resultaatverplichting te bedenken valt, bijvoorbeeld: toezien op, bewaken, bijdragen aan, ondersteunen, stimuleren, enzovoorts. Het is niet bij alle vacatures duidelijk wat precies het doe-gedeelte van dergelijke werkwoorden is. Waarop beoordeel je een persoon die 'bijdraagt aan'? De meest gezochte kandidaten gaan vooral adviseren (62 procent van de vacatures). De adviezen moeten gaan over een diversiteit aan gebieden (er wordt advies verwacht over in totaal 33 verschillende onderwerpen), maar voornamelijk over maatregelen, incidenten, verbeteringen en informatiebeveiliging. Een ander werkwoord dat veel wordt gebruikt, is 'uitvoeren'. Dit gaat vooral om risico-analyses, audits en (privacy) impact assessments.

Bij de vaktermen is 'beleid' het meest frequent gebruikte woord. Het komt voor in combinatie met 30 verschillende werkwoorden. Beleid moet worden opgesteld, gerapporteerd, uitgebouwd, uitgedragen, gemaakt, vertaald, geschreven, actueel gehouden, vormgegeven en zo voort, er moet sturing aan gegeven worden of men moet zich ermee bezighouden.

De meeste vacatures lijken zich vooral te richten op werkzaamheden die het aantoonbaar maken, dat er (zoals enkele werkgevers ook eerlijk beschrijven) 'een goed verhaal voor de directie' is en dat men 'zich bezig houdt met' informatiebeveiliging.

De taakomschrijvingen bevatten veel onbegrijpelijke taken, bijvoorbeeld:

- 'in staat stellen om te begrijpen' (hoe meet je of het is gelukt om iemand in staat te stellen?)
- 'zorgdragen voor governance' (gaat de kandidaat de organisatie zelf besturen? Wat is governance eigenlijk?)
- 'zorgdragen voor incidenten' (gaat de kandidaat zorgen dat er incidenten komen?)
- 'toetsen van audits' (een audit is een soort toets, dus toetsen van de toets?)
- 'streven naar oplossing' (streven naar of daadwerkelijk oplossen?)
- 'op niveau brengen' (hoe meet je dat?)



Figuur 2 - Salaris vs minimum aantal jaren gevraagde werkervaring

- o 'loodsen naar bewust accepteren' (hoe meet je het resultaat van loodsen?)
- o 'procedures ontsluiten' (zijn de procedures dan verstopt?)
- o 'optreden als manager' (betekent dat doen alsof je manager bent?)
- o 'kaders inbedden' (meestal bed je iets in binnen een kader)

Een vacature beschrijft dat men een manager zoekt die het informatiebeveiligingsbeleid maakt en een bijdrage levert aan de ontwikkeling van dat beleid. Gaat deze persoon dan alleen iets bijdragen of daadwerkelijk de leiding nemen over het beleid schrijven? Bovendien gaat, volgens deze vacature, de kandidaat ook het netwerk inrichten volgens specificaties en apparatuur configureren. Deze functiebeschrijving klinkt niet oprecht en is ook niet realistisch. Een van de vacatures springt er uit wat betreft onoprecht taalgebruik; hier gaat de kandidaat 'ondersteunen bij een verhaal voor het bestuur'. Daar wordt informatiebeveiliging dus tot 'verhaal' gereduceerd.... In een andere vacature wordt het doel van de functie beschreven als: 'door de inzet van (bedrijfsnaam) hoeven opdrachtgevers zich geen zorgen te maken over de risico's van de digitale wereld'. Deze uitspraak is twijfelachtig: elke organisatie zou zich altijd zorgen moeten maken over risico's. 100 Procent veilig bestaat niet en de verantwoordelijkheid kan zeker niet worden overgedragen aan een consultant.

Top 5 taken uit vacatures:

1. Adviseren maatregelen
2. Uitvoeren risicoanalyse
3. Uitvoeren audits
4. Identificeren risico's
5. Toezichthouden op beleidsnaleving

Beloning

Informatiebeveiliging wordt volgens 27 procent van de vacatures beloond met een 'marktconform' salaris, afhankelijk van ervaring en (een enkele keer) leeftijd (figuur 2).

Soms staat in een vacature het maximale maandsalaris genoemd. Van die vacatures is het gemiddelde maandsalaris van een persoon met vijf jaar werkervaring €5.736. Opvallend is dat de gepubliceerde salarissen bij vijf jaar werkervaring steeds meer uiteen gaan lopen en het verschil bijna €3.000 per maand kan zijn. De best betaalde vacatures zijn te vinden in de ICT dienstverlening, transport en maritieme sectoren. Er is een verschil te zien in gevraagde vooropleiding en geboden salaris bij vijf jaar werkervaring. Functies waar tenminste een wetenschappelijke vooropleiding wordt gevraagd, bieden bij vijf jaar ervaring een maandsalaris van gemiddeld €5.839, dat is bijna €800 per maand meer dan bij vacatures waar HBO als vooropleiding wordt gevraagd. Ook zijn de salarissen voor CISSP/CISA/CISM gecertificeerden doorgaans iets hoger.

Veel werkgevers besteden in de vacaturetekst aandacht aan de secundaire arbeidsvoorwaarden en arbeidsomstandigheden. Opleidingsmogelijkheden zijn standaard, daarmee adverteren bijna alle werkgevers. De laptop en smartphone worden ook vaak vermeld alsof het een beloning is (en dus niet hoort bij de standaarduitrusting om het werk te kunnen uitvoeren). In een enkel geval wordt in de vacaturetekst de paragraaf over wat de werkgever biedt, nog aangevuld met zaken als een proeftijd van twee jaar (de vraag is of kandidaten dat als een beloning zien?), optie op verlenging, of uitzicht op een vaste aanstelling.

Werkgevers proberen zich vaak enthousiasmerend te presenteren door een beschrijving van de werkplek en de sfeer op kantoor. De moderne werkplekken zijn duurzaam, technisch hoogstaand, innovatief, flexibel of thuis. Veel organisaties zorgen daarnaast voor je eten en drinken: ze serveren lekkere (Italiaanse) koffie, 'brain food' of elke dag vers fruit. Er is ook aandacht voor 'mindfullness'. De informatiebeveiliger krijgt een personal trainer, balans, een sportschool, geluksmomenten, of massages. Sociaal zijn de meeste werkgevers ook: er is een bruin café, er zijn kantoorborrels (ook op donderdag), strandfeesten, sportdagen, informele etentjes, weekendjes weg, 'buddies' en bedrijfsuitjes. En dat alles met enthousiaste collega's, die hun kennis delen met humor en die dagelijks staan te springen om hun steentje bij te dragen. De kans bestaat dat kandidaten die graag werk en privé gescheiden willen houden, afknappen op dit soort zaken.

92 Procent van de onderzochte vacatures bevindt zich in de Randstad. Kandidaten die niet van reistijd houden, moeten zich dus in de Randstad vestigen, tenzij de werkgever het toestaat om structureel vanuit huis te werken. Thuiswerken wordt in enkele vacatures wel als mogelijkheid genoemd, maar meestal met de toegevoegde nuance 'in overleg' of 'flexibel'. Verhuisregelingen worden nergens vermeld.

Enkele vacatures beschrijven het doel van het werk (zingeving). Deze zingeving kan wellicht verkeerd geïnterpreteerd worden, met name wanneer de nadruk ligt op het tevreden houden van toezichthouders, klanten of directie. Er wordt in die gevallen beschreven, dat het doel van de functie te maken heeft met 'beleid hebben', 'in control zijn' of iets met 'de business in staat stellen'. Aan de positieve kant zijn er diverse werkgevers die wel het maatschappelijk en persoonlijk belang van het werk benadrukken:

- 'werken waar je elke dag een bijdrage levert aan een duurzame en veilige wereld'
- 'hoofd bieden aan cybercrime'
- 'nog slimmer worden dan cybercriminelen'
- 'persoonsgegevens en onderzoeksdata beschermen'

Conclusie

Deze analyse heeft een aantal argumenten opgeleverd om te stellen dat het gebrek aan goede kandidaten iets te maken kan hebben met onduidelijke en demotiverende vacatureteksten. De meest gevraagde informatiebeveiliger is een jonge alles-of-iets-kunner met een maakt-niet-uit-wat-certificaat voor een doe-maar-een-functietiteltje. De stijl waarin vacatures zijn geschreven, komt over alsof sommige werkgevers zich laten leiden door dagelijkse problemen en blij zijn met elk iemand die er zit om iets te doen.

Informatiebeveiliging is een heel breed vakgebied met daarbinnen diverse specialisaties. Er zijn veel vacatures, maar de kandidaat moet over allerlei denkbare competenties tegelijk beschikken en het takenpakket is omvangrijk. De taakomschrijvingen bestaan vaak uit diverse activiteiten die bij meerdere functies lijken te horen. Ook de beloning is ondoorzichtig en uiteenlopend. De diversiteit aan eisen en wensen maakt het lastig solliciteren voor specialisten. Tenslotte kan een lange lijst met gevraagde certificaten intimiderend overkomen, ook omdat de bijbehorende opleidingen en examens veel geld kosten en een grote inspanning vereisen van de kandidaat.

Aanbevelingen

Om de vacatures op te vullen, zou het kunnen helpen, wanneer de werkgever gerichter communiceert naar welke kennis en competenties wordt gezocht. Wanneer tijdens het opstellen van een vacature blijkt, dat er een lange lijst aan eisen en wensen ontstaat, dan loont het wellicht de moeite om terug naar de tekentafel te gaan en te heroverwegen wat de organisatie nu echt nodig heeft of om de functie te splitsen. Zelfs indien dit betekent, dat eerst een adviseur moet worden ingehuurd om te ondersteunen bij het inrichten van de security organisatie, loont het op de lange termijn. Wanneer kandidaten terecht komen in een organisatie met een duidelijk plan en een heldere structuur voor informatiebeveiliging, zullen ze beter kunnen presteren en niet na een kort dienstverband alweer vertrekken.

Functietitels en taakbeschrijvingen moeten duidelijk zijn. Kandidaten die online naar vacatures zoeken, geven zoekopdrachten met concrete taal en zoeken doorgaans niet op termen als 'wizard' of 'een verhaal maken'. Ook zouden de functietitel en de gevraagde certificaten een relatie moeten hebben met de taakomschrijving.

Tenslotte komt de organisatie professioneler over, wanneer het duidelijk is dat men begrijpt dat het doel van de werkzaamheden groter is dan alleen te zorgen voor het voldoen aan wet- en regelgeving en het geruststellen van de directie. Hoopgevend zijn die werkgevers die benadrukken hoe belangrijk en maatschappelijk relevant het vakgebied is. Dit is niet om een enkel systeem te beveiligen, of om de toezichthouders tevreden te stellen, maar veel persoonlijker. Informatiebeveiliging gaat om het beschermen van onze eigen persoonsgegevens, innovatie in Nederland en onze vrijheid en maatschappij in het algemeen tegen digitale aanvallen door middel van samenwerken en kennis delen.

Referenties

(1) https://bit.ly/2Jr4uP7
(2) https://www.wodc.nl/binaries/2486-volledige-tekst_tcm28-73679.pdf
(3) https://bit.ly/2kNQOiY
(4) Messum, D., Wilkes, L., Peters, K., & Jackson, D. (2016). Content analysis of vacancy advertisements for employability skills: Challenges and opportunities for informing curriculum development. Journal of Teaching and Learning for Graduate Employability, 6 (1), 72-86.
(5) Ahmed, F., Capritz, L.F., Bouktif S., & Campbell, P. (2012). Soft skills requirements in software development jobs: A cross-cultural empirical study. Journal of Systems and Information Technology, 14(1), 58–81.
(6) Ahsan, K., Ho, M., & Khan, S. (2013). Recruiting project managers: A comparative analysis of competencies and recruitment signals from job advertisements. Project Management Journal, 44(5), 36–54.
(7) https://bit.ly/2kP88Ek

LESSONS LEARNED BIJ HET SCHRIJVEN VAN SECURITY RISK SCENARIOS

Tussen 2000 en 2005 ging ik bijna wekelijks naar de Sneak Preview in bioscoop Cinecitta in Tilburg. Je gaat dan naar de bioscoop tegen gereduceerd tarief, maar weet niet welke film er op het scherm komt. Dat kan tot grote tegenvallers leiden (de 'Zoutmannen van Tibet' was een persoonlijk dieptepunt), maar ook tot aangename verrassingen, zoals de eerste keer 'There is Something About Mary' in een uitverkochte zaal vol hardop lachende en joelende mensen. Dat was een Gezamenlijke Positieve Ervaring, waar ik in een volgende column meer over zal schrijven.

Acteur Sylvester Stallone sprak meer dan 200 verschillende filmproducers in Hollywood. Er zijn er niet zóveel gevestigd, dus naar sommige producers ging hij vaker dan één keer. Van elk gesprek leerde hij iets en daarmee kon hij zijn presentatie en elevator pitch steeds verder verbeteren, maar telkens zonder het beoogde succes. Totdat hij door het kijken naar een bokswedstrijd op TV het idee kreeg voor de eerste Rocky film. Hij schreef de hele nacht door aan zijn eerste filmscenario en de volgende dag lukte het hem eindelijk om dit uitgewerkte idee te verkopen, zodat het daarna verfilmd kon gaan worden. Met een hoofdrol voor zichzelf, waar al die eerdere bezoeken voor waren bedoeld.

Scenario denken

Bij het woord scenario denk ik dus zelf meteen aan een filmdraaiboek. Dat draaiboek bevat niet alleen de dialoog van de film, maar nog veel meer:

- wie spreekt de tekst uit ?(en ook: wie is die acteur, is het

NR	OMSCHRIJVING	J/N
1	Law enforcement has notified you that hosts underlying two of your compute instances were seized from your cloud infra two months ago without your assistance / notification.	
2	A malicious browser extension is modifying the rendered values of stocks on financial websites. When an active day trader is infected, it additionally swaps ticker values to penny stocks and increases quantity of the trade.	
3	Due to a botched CI/CD script, complete source code exposure on production.	
4	The credit card you use to pay for infra SaaS dependencies was just locked down, due to unrelated fraud.	
5	HR typo'd a new employee's email. All onboarding process is going to an unknown email address.	
6	A new marketing employee purchased an email list from a spammer. Your next email campaign contains address honeypots. Massive blacklisting occurs and delivery rates plummet for all email that share MX with marketing.	

Figuur 1 - LET OP: de genoemde informatiebeveiliging voorbeelden vallen niet in alle organisaties uitsluitend binnen het werkgebied van de IT security afdeling.

fluisterend of geschreeuwd, hoe kijkt - of zelfs - voelt de acteur zich daarbij);
- welke attributen zijn daarbij nodig ? (soms zo specifiek als een werpmes of een AK47 machinegeweer, een bepaalde auto of een los paardenhoofd);
- waar speelt het zich af ? (in de bibliotheek, in de auto, in de kerk, een boksschool, op kantoor, in een vliegtuig, op een onzinkbaar cruiseschip);
- wanneer speelt de scène zich af ? (nu of als een flashback in het verleden of wordt er in de film naar de toekomst gereisd).

Zo'n gedetailleerde beschrijving van wat er moet gebeuren, in welke volgorde en door wie (en welke hulpmiddelen ze daarbij nodig hebben) past ook in een security risk scenario. Energiemaatschappij Shell introduceerde ooit scenario denken in Nederland als een succesvolle aanpak in riskmanagement. Zeker wanneer je - net als Stallone - bij elke uitgevoerde test of ieder werkelijk opgetreden security-incident het betreffende risicoscenario aanpast op de nieuwe inzichten en ervaringen, en het zo dus steeds verder verbetert.

1 miljoen omschrijving

Verder heeft elk filmdraaiboek een korte samenvatting. Daarin staat kort, maar zeer aansprekend, waarover het gaat. In filmland spreekt men daarom ook wel over de "1 miljoen omschrijving". Het is een bijzondere vorm van de bekende `elevator pitch', waarmee mensen zich voorstellen bij sollicitaties en speeddating. Het is namelijk een beschrijving in één zin van een nieuw te maken film, waar een geldschieter meteen iets in ziet en jou daarom een miljoen betaalt, als je alsjeblieft voor hem/haar het scenario wilt uitschrijven. Bijvoorbeeld: `Jaws, maar dan met hondsdolle apen en Meryl Streep als jager' (al zou ik deze film zelf niet willen zien, ook niet tegen gereduceerd tarief). De eerste versie van het scenario zal dan later eventueel nog door andere (betere, succesvollere) scenarioschrijvers verder verfijnd en verbeterd worden, en daarna wordt pas besloten of een producer de film ook echt gaat draaien. Maar je miljoen heb jij dan voor je idee al binnen. Ook bij security risk scenarios kun je voorin het document een korte, geldschieters aansprekende beschrijving maken van iets dat technisch fout kan gaan in de IT, of van een mogelijke cybercrime- aanval, of van een ongelukkige samenloop van omstandigheden door fouten of vergissingen van eigen personeel. Er bestaat een twitter-website `badthingsdaily' (1), die veel van deze voorbeelden opsomt (figuur 1). Tijdens mijn eerste bezoek bevatte deze site 130 voorbeelden. Voortdurend voegen bezoekers daar via Twitter nog gevallen aan toe. Het zijn allemaal korte zinnen die in een tweet passen, maar ze vormen wel inspiratie om na te denken over scenario's voor in theorie mogelijke, toekomstige, onprettige security-situaties.

Security risk scenarios

Een mogelijke aanpak in stappen om deze badstuff-gevallen te gebruiken voor het opstellen van je eigen security risk scenarios is de volgende:

1. Bekijk of je de op de website `badstuff' genoemde situatie echt begrijpt en deze dus kort (in één zin of elevator pitch) kunt

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

uitleggen aan degene die voor de oplossing moet gaan betalen. Vaak is dat iemand met minder technische security-kennis dan jijzelf. Kort en bondig formuleren is daarbij goed, maar doe het niet té kort (met afkortingen en jargon), zodat het begrijpelijk blijft.
2. Overweeg telkens of het risico werkelijk kan optreden bij jouw organisatie, of dat je enige zaken in de omschrijving moet aanpassen. Bijvoorbeeld W2-formulieren in de USA komen in Nederland niet voor, dus ze kunnen ook niet (voor alle medewerkers van je organisatie) na een misleidend telefoontje van een social engineer door een medewerker naar het zogenaamde 'nieuwe' gmail adres van de Belastingdienst worden opgestuurd. Maar met andere formulieren of gegevens (zoals een fiscale jaaropgaaf in PDF) kan zoiets in theorie hier natuurlijk wél gebeuren. Met "in theorie" bedoel ik het bestaan van een bruto risico, dus voorafgaand aan alle genomen beheersmaatregelen en security awareness acties. Als die getroffen maatregelen en acties nog niet voldoende zijn, bestaat er nog steeds een netto risico dat het issue optreedt en tot schade leidt.
3. Bepaal per situatie van de lijst of je een oplossing weet, of slechts een beetje, of helemaal niet. In het laatste geval: het voorbeeld verder bestuderen en er verder op doorvragen bij anderen, bijvoorbeeld collega bedrijven en organisaties in dezelfde sector. Kijk daarbij ook al naar de volgende vraag: misschien is de situatie wel op te lossen, maar kun jij of je security afdeling het niet alleen en is hulp van andere afdelingen in de organisatie noodzakelijk.
4. Bekijk bij punt 3 in elk geval of je het als security professional zelf of met alleen je collega's van de security afdeling kunt oplossen. In veel security situaties is er namelijk voor een oplossing ook communicatie naar alle medewerkers nodig, of een door de directie vastgesteld beleidsdocument dat, bijvoorbeeld, stelt dat managers geen zakelijke laptop mee mogen nemen naar bepaalde landen waar de douane inzage vraagt in de opgeslagen gegevens en daarom vrijgave van de encryptiesleutels afdwingt.
5. Op basis van de eerdere antwoorden is een datum in te schatten hoe lang het (nog) duurt om al die oplossingen en werkafspraken uit te zoeken. En ze tegelijkertijd leesbaar, voor gebruikers begrijpelijk en daarmee toepasbaar in spannende crisissituaties te documenteren in security risk scenarios.
6. Als je per situatie een: '1 miljoen vraag' (of een lager bedrag) bedenkt, kun je daarmee naar je budgethouder stappen. De risico's waarvoor je budget krijgt, zijn de aangewezen kandidaten om als eerste uit te gaan werken.

Er bestaat na al die stappen een lijst met uit te werken security risk scenarios. Je weet echter niet vooraf welk risico of dreiging als eerste zal optreden. Kies daarom volkomen willekeurig de volgorde van uitwerken van de scenario's en maak een planning waarin de scenario's snel genoeg 'allemaal' klaar zijn. Een beetje structuur kan echter wel, want sommige risico's hebben een lage frequentie, maar kunnen bij optreden wel tot een grote schade leiden.

Sommige andere risico's hebben per geval niet zo'n grote schade, maar kunnen wel vaak of zelfs op meerdere plaatsen tegelijk optreden. Ik zou beginnen met de groep 'vaak en grote schade', vervolgens met 'vaak en kleinere schade', dan 'zelden en grote schade' en daarna pas met 'zelden en kleinere schade'. Die laatste groep is natuurlijk relatief klein, want hiervoor is het sowieso moeilijk om de interesse van de geldschieters/budgetverstrekkers te wekken. Zodra de eerste versie van het risicoscenario beschikbaar is, kun je deze in een 'tabletop exercise' door een groep deskundigen laten lezen om hun tips en commentaar te verzamelen. Bijvoorbeeld alle draaiboekauteurs zelf, maar dan allemaal samen, zodat ze van elkaars fouten en ervaring kunnen leren. Een goede aanpak is om dit in een fysieke vergadering te doen (ouderwets, ik weet het), waarbij één persoon het draaiboek hardop voorleest, zodat de rest kan reageren; instemmend of met verbeteringen. In het algemeen stimuleert en motiveert het de originele auteur meer, wanneer daarbij complimenten worden gegeven, zoals "dat is een goed idee, dat ga ik in mijn draaiboeken ook zo doen!".

Daarna volgt nog een periode die nodig is om het draaiboek te oefenen in één of meerdere security tests. Het scenario kan zo ook goed voorspellen of de situatie (het beschreven risico) werkelijk optreedt, zoals genoemd bij 'badstuff' en dan kun je het handboek in het echt toepassen. Tijdens het oplossen van een (security) crisis is het altijd een goed idee als iemand het overzicht over alle genomen besluiten en uitgevoerde acties en hun resultaten bewaart en dat allemaal voor het nageslacht vastlegt in een logboek. In dat logboek staat dan als aan het eind de crisis zo goed mogelijk is opgelost, ook waardevolle informatie om het betreffende draaiboek (riskscenario) te verbeteren. Door het te vereenvoudigen, te versnellen, aan te vullen met telefoonnummers, andere of meer acteurs/rollen of betere attributen op te nemen enzovoort.

Crisisdraaiboek op papier

Een filmscenario wordt niet meer aangepast nadat de film eenmaal is geproduceerd. Maar een risico scenario kan je altijd blijven verbeteren en actualiseren. Afdrukken van een crisisdraaiboek op papier of lokaal opgeslagen kopieën lijken ouderwets, in deze tijd van "we zijn in de wolken met onze cloudoplossingen". Maar soms treedt het security-risk in kwestie uitgerekend op als het netwerk of de internetverbinding niet beschikbaar is, of de centrale documentatie-server is omgevallen (of omgeduwd door een saboteur). En dan is het fijn dat tijdens de securitycrisis het draaiboek, met de noodzakelijke rollen, functionarissen en hun telefoonnummers tòch beschikbaar is. Ondanks de aangestoken brand in het rekencentrum, de bezetting van het kantoor met gijzeling van medewerkers, of de langdurige DDOS-aanval op de website en de thuiswerk-servers.

Referentie

https://twitter.com/badthingsdaily - Met dank aan @Edwin Tump die mij op deze site wees.

OUDERLIJK TOEZICHT... OP JE OUDERS...

Ouderlijk toezicht op het gebruik van ... mobieltjes, internet, sociale media, alles eigenlijk, van uw kinderen lijkt belangrijker dan ooit. De gevaren nemen alleen maar toe, toch? Kinderen zijn steeds jonger op social media te vinden en weten zo veel sneller dan voorheen allerlei omwegen om de gewone 'parental control' heen. En steeds meer, steeds geraffineerdere kwaadwillenden ook. Op de kleintjes letten, het is ingewikkeld…

Maar wat dacht u van: op de grootjes letten? Waar we voorheen nog alleen van doen hadden met redelijk eenvoudig in de hand te houden types (simpel verbieden hielp al wat, voor straf geen zakgeld ook, of een rijbewijs als je tot je 18e niet rookt), hebben we nu daarnaast nog eens van doen met lui die op veel terreinen volwassener zijn of waren dan wij. We gingen (gaan?) nog bij ze langs voor hun levenservaring, als we zelf onzeker zijn… Inderdaad, ik bedoel uw ouders. Hopelijk hebt u ze nog.
Maar het genoegen is niet onverdeeld. Ze zijn immers langzamerhand toch online gegaan, of ze zijn dat al langer, maar beginnen allengs wat van hun geestelijke scherpte te verliezen. Waarmee ze eigenlijk onder ons ouderlijk toezicht zouden moeten komen te staan, ook voor wat betreft hun online gedrag. Voor je het weet, doen ze online alles wat ze ons verboden hadden. Daar moeten we wat aan doen…
Hetgeen direct de vraag opwerpt: Hoe dan? Ze zijn tenslotte in enige, misschien afnemende mate maar toch of nog volledig, handelingsbekwaam. Maar niet snel genoeg meer van geest om de gevaren van online zijn te kunnen vatten of bijhouden. Als een kind een heel groot deel van het internetverkeer (ik bedoel geen kattenvideo's) wil ontdekken, kan dat nog wel worden verboden of is dat een prima aanleiding voor een lesje over wat wel en niet kan, online en IRL. Maar als degenen die ú hebben geleerd over de bloemetjes en de bijtjes juist daarover helemaal los gaan op het Internet … lew! En hoe komt u daarachter, en kunt u er iets van zeggen, en hoe gaat u zo'n gesprek aan? Hetzelfde geldt – snel even over naar minder gênante zaken – voor goksites of trol-gedrag.
Niet noodzakelijkerwijs verboden voor een volwassene, maar waar loopt het uit de hand? Zeker als we daarbij ook nog moeten inschatten of sprake is van teruglopende zelfredzaamheid of geestelijke weerbaarheid, en waar de grenzen van kunnen, willen en mogen ingrijpen zouden kunnen liggen. De (U)AVG heeft wel ondergrenzen voor ouderlijke toestemming over toegang tot gegevensvragende diensten aan kinderen, maar aan de andere kant van het spectrum is niks geregeld.
Ja, als je dood bent, dan is duidelijk: je data (ook die op social media) vallen onmiddellijk de overheid toe en ook familie heeft er geen bevoegdheid meer over. Door verwrongen interpretatie van wat obscure wetsartikelen, duidelijk tegen redelijke morele en ethische verwachtingen van nabestaanden in (nabestaanden - de biologische/fysieke en/of social media-naasten?).
Voor bankrekeningen en zorg zijn er wel allang praktische regels en protocollen, zodat kinderen (zelf hopelijk volwassen) langzaam de wettelijke vertegenwoordiging en voogdijschap inglijden.
Maar zoals duidelijk is: het online gedrag van steeds meer geestelijk hulpbehoevende ouderen is nog vogelvrij; tegen henzelf of tegen kwaadwillenden in bescherming nemen is niet iets dat op de agenda staat. Vrijheid en kwaliteit van leven kunnen elkaar zo weleens flink in de wielen rijden…
En dat willen we als informatie'beveiligers' in de brede zin die we willen zijn, toch voorkomen.
Dus zouden we niet eens voogdijschapsregels moeten gaan regelen voor het online gedrag van onze ouders? En hoe zouden die regels eruit moeten zien? En hoe kunnen ze worden afgedwongen (om misbruik tegen te gaan) …?
We horen zeer graag van u.

Ir. drs. J. van der Vlugt CISA CRISC, jvdvlugt@xs4all.nl

CYBERSECURITY HOORT NIET THUIS IN DE DIRECTIEKAMER

Hoewel cybersecurity belangrijk is, wil het helaas niet voor iedere organisatie lukken om dit onderwerp tot een succes te maken. Bij veel organisaties is cybersecurity beperkt tot vooral technische maatregelen. Securityspecialisten die het onderwerp onder de aandacht willen brengen van directieleden, ervaren vaak genoeg desinteresse of zelfs tegenwerking. De reden hiervoor is dat naar mijn idee het onderwerp verkeerd aangepakt wordt. Dit artikel beschrijft wat er fout gaat en hoe het onderwerp op de juiste manier in de directiekamer kan worden geïntroduceerd.

Een organisatie die goed omgaat met bedrijfsinformatie heeft daarvoor een informatiemanager

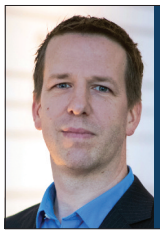
Informatie als productiefactor

In economische wetenschappen wordt gesproken over verschillende productiefactoren: natuur, arbeid en kapitaal. In de praktijk betekent dat grondstoffen en machines om producten mee te fabriceren, middelen om een dienst aan te bieden, grondstoffen om een product mee te maken, personeel voor geestelijke en fysieke arbeid en financiële middelen om dit alles te bekostigen. Voor al deze zaken geldt, dat als je ze volledig wegneemt, een organisatie een groot probleem heeft. Kans op faillissement is dan zeker aanwezig. Daarom hebben organisaties vaak een manager aangesteld om alles rondom zo'n onderdeel te organiseren. Een manager voor productie, logistiek, voorraad, ICT, et cetera, een P&O manager voor de medewerkers en een CFO voor de financiën.

Maar hoe zit het eigenlijk met 'informatie'? Organisaties maken er veel gebruik van en zijn er ook vaak van afhankelijk. Natuurlijk gebruikten organisaties vroeger ook informatie, maar zonder een computer kost het verwerken van informatie veel meer tijd en moeite. Door de komst van de computer is het gebruik van informatie geëxplodeerd. Maar wat nu als alle informatie binnen een organisatie wordt weggenomen? De e-mailserver, de fileserver, de boekhouding, het CRM-systeem, de personeelsdossiers, alles leeg of weg. Heeft een organisatie dan niet ook een groot probleem? Is kans op faillissement dan niet ook aanwezig? We kunnen dus eigenlijk wel stellen dat, gezien de omvang van het gebruik van informatie en de afhankelijkheid daarvan voor veel organisaties, informatie een op zichzelf staande productiefactor is. Maar wie managet al die bedrijfsinformatie? Een organisatie die goed omgaat met bedrijfsinformatie heeft daarvoor een informatiemanager. Maar neemt uw organisatie het vak van informatiemanagement wel serieus?

De positie van de informatiemanager

Zoals ik eerder heb beschreven (artikel 'Zicht en grip op informatie', iB2), is zicht en grip op informatie een belangrijke voorwaarde voor zicht en grip op informatiebeveiliging. Het beheren van informatie binnen een organisatie kost dusdanig veel tijd dat daarvoor het beste een aparte manager kan worden aangesteld. Echter, veel organisaties die een informatiemanager hebben aangesteld, plaatsen deze functie onder de ICT-manager. Dit is een totaal verkeerde positie. Voor de argumentatie hiertoe nemen we personeel als voorbeeld. Waar het kunnen bieden van een dienst of het leveren van producten het doel is, zijn medewerkers een middel. Waar het kunnen laten werken van de medewerkers het doel is, zijn bedrijfspanden en werkplekken het middel. Voor de medewerkers hebben organisaties meestal een P&O-manager en voor de panden en de werkplekken een manager facilitaire zaken. Als je zou voorstellen om de P&O-manager onder de manager facilitaire zaken te plaatsen, vind je denk ik niet veel medestanders. De manager voor het doel en die voor het middel horen voor een goede balans tussen vraag en aanbod naast elkaar te staan, niet boven of onder de ander. Maar hoe zit het op ICT-gebied? Waar het verwerken van informatie het



Hugo Leisink is Specialist in Informatiebeveiliging en Privacy (CIPP/E) en werkzaam bij het Ministerie van Justitie en Veiligheid. Hugo is bereikbaar via hugo.leisink@ncsc.nl. Vanaf deze uitgave maakt Hugo onderdeel uit van de redactie van dit magazine.

	Personeel	Informatie
Doel	P&O-manager	Informatiemanager
Middel	Manager facilitair	ICT-manager

doel is, is ICT het middel. ICT bestaat binnen een organisatie bij de gratie van de behoefte om informatie te verwerken. Organisaties die dit onderwerp serieus nemen, hebben voor het organiseren van alle bedrijfsinformatie een informatiemanager aangesteld. Voor het beheren van alle ICT-middelen hebben de meeste organisaties een ICT-manager. Waar het mis gaat, is dat zij vaak de manager die het doel managet, plaatsen onder de manager die de middelen daartoe managet. Waar deze constructie voor personeelszaken dus bijzonder vreemd zou zijn, is het voor informatie blijkbaar wel acceptabel. Om ook hier een gezonde balans tussen vraag en aanbod te krijgen en de organisatie te kunnen laten groeien in haar volwassenheid in de omgang met bedrijfsinformatie, dienen deze managers naast elkaar te staan.

Informatie als onderwerp in de directiekamer

Informatie zien als een aparte productiefactor en daar binnen de organisatie op een goede manier mee omgaan, is een belangrijke eerste stap om informatiebeveiliging tot een succes te maken binnen een organisatie. Ga met directieleden het gesprek aan over bedrijfsinformatie en het belang van sommige bedrijfsinformatie voor de organisatie. Laat directieleden inzien dat informatie gezien de omvang, de afhankelijkheid en alle ontwikkelingen op dat vlak echt een productiefactor is. Laat directieleden zelf tot de conclusie komen dat sommige informatie het waard is om goed te beveiligen. Het is beter om het onderwerp zo aan te pakken dat de directieleden informatiebeveiliging bij de CISO komen halen, dan dat de CISO dit onderwerp moet brengen.
Informatie als productiefactor, de noodzaak om belangrijke informatie te beveiligen en de middelen die daarvoor nodig zijn, is het enige dat binnen de directiekamer besproken hoeft te worden.
Informatiebeveiliging zelf is namelijk vooral een tactisch en operationeel onderwerp. Het is alleen een strategisch onderwerp als een organisatie informatiebeveiliging als concurrentiepositie wil gebruiken, maar dat laten we voor nu buiten beschouwing. Ik denk dat het niet efficiënt is om informatiebeveiliging te bespreken in een één-op-één gesprek tussen de CISO en een directielid. Wat naar mijn idee een betere aanpak is, is om 'informatie' als onderwerp te gebruiken. Betrek bij dat onderwerp daarom ook de informatiemanager, de ICT-manager en de privacy officer. Op die manier kan er beter zicht en grip verkregen worden op deze productiefactor in brede zin. Beveiliging is namelijk minder efficiënt als je er niet de noodzaak, de technische middelen en de privacy-zaken bij betrekt.
Ik gebruik in dit artikel bewust 'informatiebeveiliging' in plaats van 'cybersecurity'. De term 'cyber' is namelijk een erg ruim begrip en daardoor eigenlijk nietszeggend. Wil je het onderwerp makkelijk bespreekbaar kunnen maken met collega's die niet goed inhoudelijk bekend zijn met dat onderwerp, dan kan het mogelijk beter zijn om duidelijk te benoemen wat het is: het beveiligen van (bedrijfs)informatie, dus informatiebeveiliging. Ik doe hiermee geen poging om het woord 'cybersecurity' uit te bannen. Als voor jouw organisatie deze wat hippere term beter werkt dan de oude, misschien wat stoffige, term 'informatiebeveiliging', dan is dat prima. Wat ik hier alleen mee wil zeggen, is dat je je goed moet realiseren dat managers vaak geen techneuten zijn en ze dus mogelijk onvoldoende zicht hebben op de hele ICT-wereld. Door duidelijk aan te geven waar je het over hebt en wat je van ze verlangt, loop je minder kans dat de directie geen interesse zal tonen in het onderwerp.

Om informatiebeveiliging tot een succes te kunnen maken, is het belangrijk om het onderwerp op een juiste manier binnen de directiekamer te introduceren

Samenvattend

Om informatiebeveiliging tot een succes te kunnen maken, is het belangrijk om het onderwerp op een juiste manier binnen de directiekamer te introduceren. Beperk je daarbij tot de strategische zaken, namelijk informatie als productiefactor, de waarde van informatie voor de organisatie en de noodzaak om sommige informatie te beveiligen. Bespreek de strategische zaken rondom informatie, zoals beheer, de beveiliging, privacy, et cetera, in een gesprek met de informatiemanager, de ICT-manager en de privacy officer. Laat al deze functies direct onder de directie vallen om de invulling ervan zo efficiënt mogelijk te kunnen maken.

QUANTUM READY

Are you ready for the quantum revolution in secure communications? OK, so you're not ready! But don't panic, it's still a long time coming. However, it is useful to be cognizant with the latest cryptographic developments and to get a glimpse of what is coming over the horizon. These developments will change the way we do things in the future. There are some interesting issues that you will need to address to make practical use of the new cryptographic technologies. This article will give you an overview of all that.

There are two main applications of quantum physics in the world of cyber security: breaking current cryptography to render it useless; and creating a key exchange protocol that is provably unbreakable. So, the universe and its laws take away something with one hand whilst giving something even better with the other hand. Or does it? We shall see.

Today's computers based on transistor architecture have limits on computational power: heat dissipation, packing density in 2- and 3-dimensional structures and clock speed. If the cryptographic key space is large enough, data is secure against brute force attacks, (but beware, there are other attack methods and encryption does not solve all security problems).

The Noble prize winning theoretical physicist and mathematician, Richard Feynman, first floated the idea of a quantum computer in around 1982. Quantum computer architecture avoids these limitations by providing massive parallelism at the physical level. There are algorithms (such as one by Peter Shor in 1994) that can leverage this property allowing an entire cryptographic key space to be searched (almost) instantaneously. Key length becomes irrelevant, provided that you can build a quantum computer with sufficient 'qubits' – something still not technically possible but experts predict that in future it will be. Let's assume the experts are right and that quantum computing is a threat to all modern cryptographic systems. To our rescue comes quantum cryptography. The concept is based on a fundamental law of physics: if you inspect a quantum state to measure it, you cannot avoid changing the state. Alice and Bob exchange information bit-encoded as quantum particles in a stream of single photons. Eve (the eavesdropper) can look at the stream and measure its bits, but will leave a trail that is detectable. Only when Alice and Bob find they have and tamper-free stream will they use it for secure communications. The exchanges are generically known as quantum key distribution protocols (QKD).
The history of cryptology is one of new emerging cryptographically secure methods (meaning beyond current technical resources), only to be followed by new cryptanalytic methods to break them. So it goes on. It turns out to be 'too difficult' at present to produce a stream of true single photons required for QKD. In practice a stream of attenuated time-gap laser pulses is used, each pulse having a Poisson-distributed probability of containing less than one photon of energy. Some pulses will contain no photons, some one, and some will be multi-photon. This enables an attack scenario known as 'photon number splitting' (PNS). Let's just say it's complicated, but Eve can exploit this without disturbing the quantum states. Whoops! Next up comes the 'decoy state' approach. Using randomly chosen, multiple intensity levels at the transmitter's source, (one signal state and several decoy states), the photon number statistics vary throughout the channel. At the end of the transmission Alice announces publicly which intensity level has been used for each qubit. This defeats the PNS attack. No channel is error free, and error rates increase with distance. To be successful Eve would need to maintain the expected bit error rate (BER) at the receiver's end (Bob). She cannot achieve this with multiple photon statistics. If Alice and Bob monitor all the BERs they will detect an attack by Eve. Phew!

And so it will go on. Thrust and parry. However, the Attributer wants to draw attention to something that seems to be ignored with the present direction of cryptographic research into QKD. One of the classical attack methods on any security system is to disable it so that the users are forced to move to another capability to maintain business continuity. If Eve were to flood the photon channel and mount a denial of service (DoS) attack, what will Alice and Bob do then? As always in SABSA thinking, security architecture must be a holistic, end-to-end approach. The most secure techniques will never help us if there are other attack routes for our adversaries.

And another thing: what about all that data currently encrypted with today's crypto technology? Once the quantum computer is available, any data collected today with expectations of long security life will fall immediately. Be careful what you commit to public collection for future harvesting in the post-quantum era.

The Attributer

ELK IMPLEMENTATIETRAJECT HEEFT ZIJN SECURITY ASPECTEN IN ZICH!

Of het nu gaat om de verbouwing van een woning of, zakelijk gezien, het implementeren van een kritische verandering in een bedrijf, zoals een nieuw softwaresysteem, je zult het eerst moeten plannen en organiseren om het tijdens de verandering te controleren, zodat alle risico's vooraf geëlimineerd worden.

Plannen en organiseren gaat vaak op 'gevoel', er gaat tijdens de verandering gegarandeerd veel mis, bijvoorbeeld door communicatie over meerdere onveilige kanalen (mail, telefoon, chat), en het afbreukrisico is groot. Er zijn veel risico's mee gemoeid. Het levert veel stress op en kost uiteindelijk veel geld. En hoe zorg je er nu voor dat het veilig is wat je gaat doen?

Of het nu gaat om het upgraden van programmatuur, de migratie van data of het installeren van technische componenten, het zijn tijdrovende processen waarin vele groepen mensen acties moeten leveren en waarbij we regelmatig worden geconfronteerd met onverwachte en onaangename verrassingen, ook op securitygebied. Liever zouden we 'in controle blijven' en de situatie volledig in de hand hebben.

Een terugblik op de werkwijze; wat werkte niet?

Veel bedrijven kozen er in de jaren 90 voor om planning en organisatie van veranderingen vast te leggen in tekstverwerking of spreadsheetpakketten, waarbij beveiliging een groot gemis is! In een tekstverwerking pakket zag je vaak een geheel van verschillende hoofdstukken. Activiteiten, betrokkenen, het communicatieprotocol en vele andere onderdelen werden in hoofdstukken ondergebracht. Dit bleek niet werkbaar, omdat het totale overzicht ontbrak en sturing op verandering daardoor niet mogelijk was.

Ook in een spreadsheetpakket liepen we tegen de grenzen van het pakket aan, omdat de hoeveelheid taken, afhankelijkheden en betrokkenen al snel te groot werd. Inzicht en overzicht ontbraken. Niet verwonderlijk, want de genoemde programma's zijn perfect als tekstverwerker of spreadsheet, maar zijn geen implementatie softwarepakketten die specifiek gericht zijn op het gecontroleerd implementeren en het elimineren van risico's.

De grootste gevaren bij het gebruik van spreadsheets en tekstverwerkers zijn:

- qua beveiliging is er weinig tot niets te regelen, wat zeker met de nieuwe GDPR wetgeving grote gevolgen kan hebben;
- geen logging, je kan niet aantonen waar het mis gaat of beter kan;
- bij hergebruik kan je niet snel starten en moet je hopen dat de template niet corrupt is;
- mensen worden niet aangestuurd en communicatie gaat over verschillende kanalen met als gevolg:
  - projecten lopen uit vanwege het missen van een stap in het stappenplan: de afbakening van taken is onduidelijk;
  - geen alarmering;
  - Toewijzing van menselijke resources door planning, elk bedrijf heeft met ad hoc zaken te maken, die zijn niet te vangen in een spreadsheet of tekstverwerker. Dit heeft zijn weerslag op de doorloop van projecten.

De oplossing, wat werkt wel!

Dit wetende is het verstandig om je te oriënteren op een geautomatiseerd stappenplan, dat je daadwerkelijk werk uit handen neemt. En dat ervoor zorgt dat je bij implementaties volledig veilig en secure in regie bent.

Werken in een afgeschermde omgeving is daarom belangrijk en naast de betere beveiliging zijn de voordelen die je dan voor jezelf creëert:

- Dat je daarna een stappenplan hebt dat altijd consistent en overzichtelijk is. Je ziet meteen wat de totale doorlooptijd is en wat de impact is voor de business, want alles kan dan automatisch doorgerekend worden. Je kan hierdoor gaan sturen en begeleiden in plaats van brandjes blussen.
- Noodzaak is wel dat de programmatuur zodanig beveiligd is, dat alleen de mensen die geautoriseerd zijn toegang hebben. Er zijn te veel voorbeelden van documenten die onbedoeld zijn gaan zwerven of waarin per ongeluk ongezien een wijziging heeft plaatsgevonden. Dit kan desastreuze gevolgen hebben in een project en risico's van datalekken liggen hier op de loer.

Denk hierbij aan https://www.noordhollandsdagblad.nl/-zaanstreek/burgemeester-zaanstad-doet-aangifte-van-lekken-documenten-cultuurcluster en dat is maar een simpel voorbeeld. De keren dat dit heden nog voorkomt, is onvoorstelbaar.

Bij elk implementatietraject is een goede communicatie het hart van de implementatie. Het is de bedoeling dat het hart gecontroleerd en veilig alle processtappen van een implementatietraject aanstuurt. Tijdens het traject is het cruciaal dat communicatie actueel inzicht en overzicht blijft geven van activiteiten, verantwoordelijkheden, afhankelijkheden, tijden, afdelingen en medewerkers.

Daar liggen de uitdagingen in het implementatieproces dat je moet stroomlijnen wil je `in controle' zijn. Als manager wil je je bezighouden met je eigenlijke werk, en meer aandacht geven aan de mens zelf. Security issues mogen je niet afleiden van de normale implementatie problematiek. Mobile toegang geeft veel voordelen, maar brengt wel security vraagstukken met zich mee.

De laatste stap, mobiele toegang

Vroeger was het alleen maar mogelijk om medewerkers een terugkoppeling te geven omtrent hun activiteiten en de voortgang te volgen door middel van de desktop of laptop.

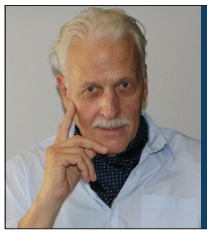
Tegenwoordig wil je ongeacht waar je bent, dus ook vanaf huis of een andere locatie, de voortgang kunnen volgen en niet direct gebonden zijn aan een desktop of laptop. Je wilt je eigen activiteiten te kunnen afmelden via elk mobiel device zonder gebruik te hoeven te maken van e-mail of sms, maar wel beveiligd!

Alleen, hoe ga je om met de beveiligingsaspecten? Want alles wat zich extern bevindt, draagt een groter risico met zich mee. Medewerkers moeten de mogelijkheid krijgen om eigen activiteiten kunnen afmelden, maar niet die van een ander. Het is dus noodzakelijk om strikt persoonsgebonden te werken. En ervoor te zorgen dat de informatie die wordt gedeeld, beperkt is en wordt afgeschermd van ongewenste ogen. Ook persoonsgebonden informatie, zoals een mobiel nummer en e-mailadressen, mogen niet gedeeld kunnen worden via het internet.

Een implementatie is een serieuze business. Er mag niets fout gaan, want er is veel geld mee gemoeid. Dreigende datalekken en security vraagstukken moeten goed geregeld worden, omdat het grote imagoschade kan veroorzaken.

Het is dus werkelijk van groot belang dat de beveiliging op alle fronten goed is geregeld, want uiteindelijk verzamelen we activiteiten die van belang zijn voor een organisatie en haar business. Dit mag simpelweg niet op straat terecht komen.

Het is belangrijk om stap voor stap te bouwen aan een succesvolle en veilige implementatie, waarbij vooraf alle risico's worden geëlimineerd.



Peter van Deutekom is Implementatiespecialist bij Mirada BV. Peter is bereikbaar via info@time-it.org.

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.

AVG EN BASELINES

Ongetwijfeld heeft u als security professional de afgelopen periode diverse verwerkersovereenkomsten (DPA's) voorbij zien komen ter beoordeling van de door de verwerkende instantie toegepaste informatie beveiligingsmaatregelen in het kader van de AVG (GDPR). Veel verwerkers schermen met hun ISO 27001 certificaat, of stellen dat zij conform BIR werken, of de NEN 7510 als uitgangspunt hanteren. Maar hoeveel zekerheid geeft dat? Is het toepassen van een baseline (BIR, BIG, BIWA, IBI, BIC, NEN 7510) inderdaad voldoende als zekerheid naar de 'eigenaar' van de persoonsgegevens, en vooral naar de 'data subjecten'? Onze redacteuren geven hun visie op het verschijnsel 'baseline' als zekerheidstelling voor de AVG.


Maarten Hartsuijker


Lex Dunn


Hugo Leisink


Fook Hwa Tan

Maarten Hartsuijker

Als beveiligingsspecialist maak ik graag gebruik van frameworks en standaarden. En natuurlijk gebruik ook ik veelvuldig de onderdelen uit de ISO 27000 series. Het geeft houvast, een vaste structuur en het helpt organisaties om onderling (al helpen de vele afsplitsingen niet) '1 taal' te spreken. Organisaties die nog moeten starten met informatiebeveiliging kunnen er heel snel een grote sprong mee vooruit maken. Zicht krijgen op de onderwerpen die er toe doen. En daar vervolgens invulling aan geven. Maar zijn ISO27001 gecertificeerde organisaties dan veiliger? Nee, zeer zeker niet. Ik kom tijdens audits en pentesten continu gecertificeerde omgevingen tegen die zo lek zijn als het spreekwoordelijke mandje. Voor velen is een certificaat richting klanten een must geworden en een doel op zich. De 27001 'beheersingsactiviteiten' (nog snel even laten bekrachtigen door het MT voor de auditor komt) worden uitgevoerd voor het certificaat. En risico's worden vakkundig weggeredeneerd. Een risicoanalyse wordt vaker gemaakt om te verantwoorden waarom je niet aan een kwetsbaarheid gaat doen, dan om een kwetsbaarheid op de juiste manier te verhelpen. Feitelijke veiligheid is helaas op zo'n moment ondergeschikt aan de verkoopwaarde van ISO27001 gecertificeerd zijn. Het meest fascinerende van de "je moet ISO 27001 gecertificeerd zijn mafia" is naar mijn idee dat van alle organisaties die een certificaat als eis stellen, vrijwel niemand zelf het certificaat heeft. En veel krachtiger kan de beperkte waarde ervan niet uitgedrukt worden.

Lex Dunn

Bij het voorbereiden op de AVG zullen bedrijven en organisaties die een security baseline hanteren, een klein voordeel hebben gehad, immers zij hadden al een standaard set security maatregelen beschikbaar (al of niet geïmplementeerd). Maar is het hebben van een baseline of certificaat een garantie voor de 'data subjecten', dat er zorgvuldig met hun persoonlijke informatie wordt omgegaan? Nee, zeker niet. Net zo goed als het feit dat iemand een rijbewijs heeft, nog niet betekent dat hij goed kan rijden, zegt een ISO 27001 certificaat ook niets over de zekerheid voor klanten/medewerkers ten aanzien van hun persoonsgegevens. In de haast om vóór 25 mei alles op orde te krijgen, is vaak zo'n baseline of certificaat als eis opgenomen in de 'Data Processing Agreements', zonder verder in te gaan op de risico's die een bepaalde verwerking van persoonsgegevens door derden met zich mee brengt. Daarbij hebben veel opstellers van de DPA zich onvoldoende gerealiseerd dat een ISO 27001 certificaat ook nog een Statement of Applicability heeft, dat aangeeft waarop het Information Security Management System van toepassing is, en welke maatregelen daarbij wel en welke niet zijn geselecteerd. Kortom, een baseline of certificaat kan wel helpen om sneller inzicht te krijgen in de toegepaste beveiligingsmaatregelen, maar het is zeker geen garantie dat er geen datalekken zullen optreden.

Hugo Leisink

De enige manier om de betrokkenen zekerheid te geven over wat er met hun informatie gebeurt, is door open en eerlijk te zijn. Of, om in AVG-termen te spreken, door transparant te zijn. Aangeven dat je een baseline voor de beveiliging toepast, is daar uiteraard niet voldoende voor. Want wat houdt 'toepassen' dan precies in? Vol trots je ISO 27001 certificaat op je website zetten is leuk, maar als organisaties echt zeker zijn over hun informatiebeveiliging, dan doen ze dat bijvoorbeeld ook met hun 'Verklaring van Toepasselijkheid' (Statement of Applicability). En dan wel één zoals beschreven in ISO 27001, dus met rechtvaardiging van opnemen of uitsluiten van controls en status van implementatie. Het bekende lijstje met controls en slechts een vinkje in een 'Van toepassing'-kolom, zoals dat nu vaak wordt toegestuurd, is nietszeggend. Daarnaast vind ik dat organisaties die puur vasthouden aan hun sectorale baseline, niet goed bezig zijn. Zoals de naam al aangeeft, biedt een baseline slechts een basis aan informatiebeveiliging. Goede informatiebeveiliging is risicogestuurd en dus gebaseerd op een gedegen risicoanalyse. Dus weg met de baselines en allemaal aan de risicoanalyse op basis van, bijvoorbeeld, ISO 27002, met eventueel per sector een paar specifieke aanvullende maatregelen.

Fook Hwa Tan

De 25 mei 2018 is inmiddels een tijdje gepasseerd. Nieuws over handhaving in Nederland is nog erg rustig. Betekent dit, dat je niets hoeft te doen? Ik hoop het niet. In de afgelopen jaren zijn in verschillende sectoren baselines opgezet om organisaties te helpen een stukje veiliger te worden. Deze baselines zijn vaak gebaseerd of gerelateerd aan de ISO27001 norm. Veel organisaties zijn voor de AVG druk bezig geweest met deze baselines, maar let wel op dat dit baselines zijn. Oftewel, dit is basis 'hygiëne'. Als je adequaat zou willen beveiligen, dan moet je toch goed nagedacht hebben over welke risico's je loopt en additionele maatregelen nemen bovenop de baseline!

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Tom Bakker
Lex Dunn
Maarten Hartsuijker
Hugo Leisink
Rachel Marbus
Fook Hwa Tan
Rick van Dijk

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

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

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

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

ISSN 1569-1063

EEN NIEUWE BRIL

Begin juni was ik even bij de opticien om voor mijn vakantie een nieuwe bril te laten aanmeten. Ik ben niet kieskeurig dus had al vrij snel een nieuwe bril. Bij het uitschrijven van de bestelling kwamen we bij de prijs en ik wist niet of ik 'ouderen'korting kreeg, 'mooi weer' korting of hoe we het ook allemaal noemen. Nee, ik kreeg een tweede bril gratis! Over het algemeen red ik me uitstekend met één bril, en het dragen van twee brillen tegelijk lijkt mij niet praktisch. Maar ik kon geen korting krijgen op de ene bril, dus toen heb ik toch die tweede voor 'erbij' genomen. Ik vertel dit, om aan te geven dat ik op dat moment al niet meer zo blij was als toen ik binnenliep die ochtend. Bij de tweede poging van het uitschrijven van de bestelling, dit keer voor twee brillen, vroeg de winkeljuffrouw of ze mijn e-mailadres mocht noteren. Ik legde haar vriendelijk uit, dat ik geen behoefte had aan alle opticienaanbiedingen. Dus schrapte ze zuchtend het e-mailadres dat zij al had. Of ze dan wel mijn adres mocht hebben? Ik krabde mij op het achterhoofd en vroeg haar of ze die niet allang had. Hierop kreeg ik een uitgebreide uiteenzetting over de Europese Privacy Verordening (EPV). Nu weet ik niets van brillen, maar wel redelijk veel over de EPV, en ik had de indruk dat de dame tegenover mij in een vergelijkbare positie zat, maar dat zij redelijk veel over brillen weet. Voor de grap zei ik, dat ik graag wilde dat ze die ook schrapte. Ik zag haar gezicht roder worden. Ze vroeg of ik dat meende, waarop ik bevestigend antwoordde. "Als ik uw adres verwijder, dan kan ik uw brillen niet registreren en kan de koop niet doorgaan", reageerde de brillenjuffrouw geagiteerd. Plagend vroeg ik haar wat een bril met mijn adres te maken had. Daar had ze geen antwoord op, behalve dan dat ze dit moest vragen van het hoofdkantoor. Ik vroeg haar wat er in het script stond als ik weigerde mijn adres te laten registreren. "Dat antwoord staat er niet in meneer." Ik vertelde haar dat ik een grapje maakte en dat ze het adres natuurlijk wel mocht, en ze deed een dappere poging om te glimlachen. Ik nam afscheid en had buiten spijt dat ik het meisje zo had geplaagd. Wij maken ons druk om een adres bij de opticien en Facebook komt ermee weg de data van 10-tallen miljoenen mensen te hebben gelekt. Wij willen niet dat een e-mailadres wordt vastgelegd, terwijl er in 2017 10.000 meldingen van datalekken waren bij de autoriteit Datalekken. Overigens: 10.000 gemelde lekken, de niet gemelde zouden weleens een veelvoud kunnen zijn. Gemeenten lekken zoveel dat ze het al niet meer melden. Daar maak ik mij zorgen om…
De juffrouw van de brillen vind ik niet spannend, vind het niet zo'n probleem dat men weet dat ik twee brillen van het huismerk in huis heb.

Berry

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

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

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers