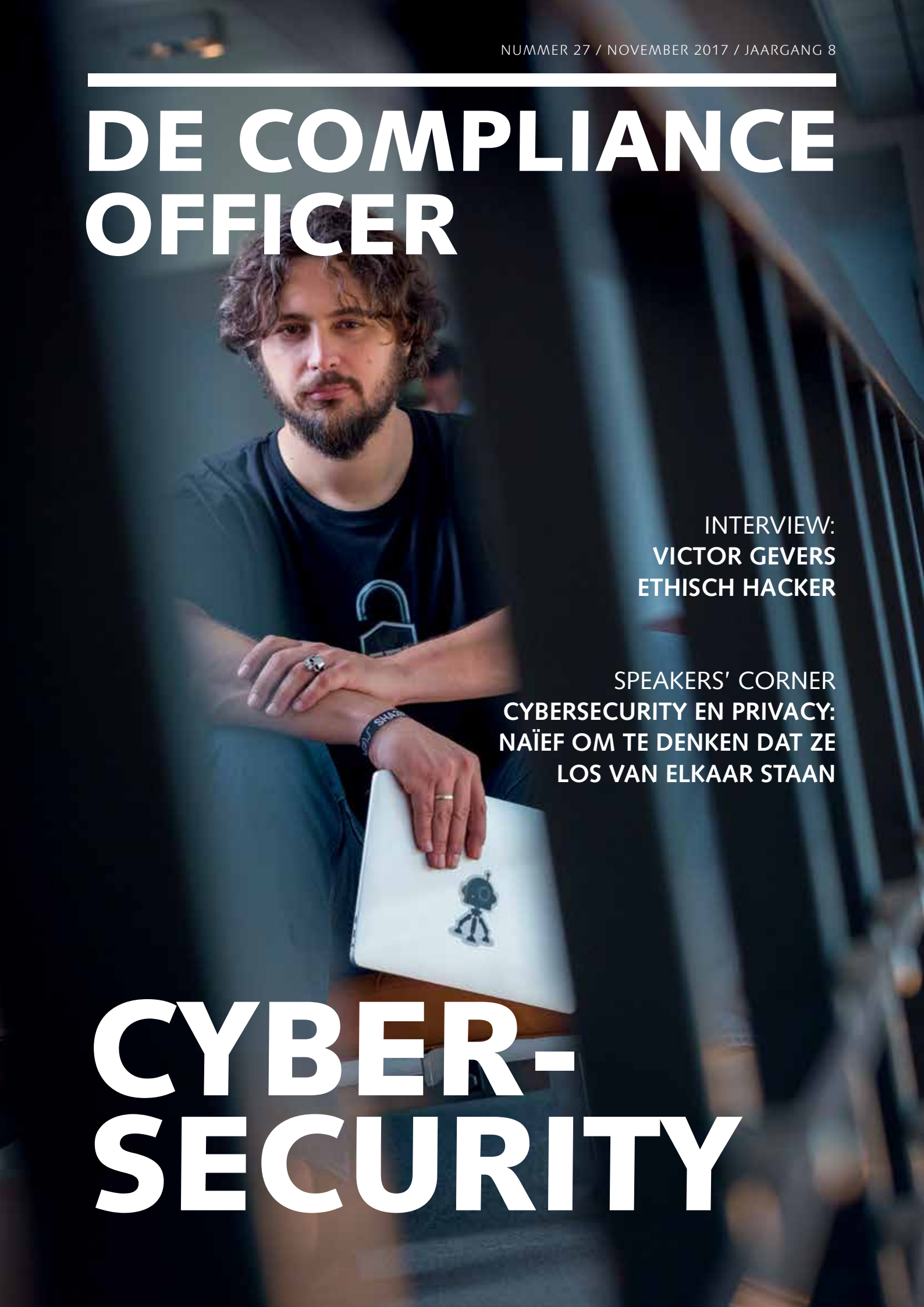
NUMMER 27 / NOVEMBER 2017 / JAARGANG 8

# DE COMPLIANCE OFFICER



INTERVIEW:
**VICTOR GEVERS**
**ETHISCH HACKER**

SPEAKERS' CORNER
**CYBERSECURITY EN PRIVACY: NAÏEF OM TE DENKEN DAT ZE LOS VAN ELKAAR STAAN**

# CYBER-SECURITY

## COLOFON

De Compliance Officer is het vakblad voor compliance officers en andere betrokkenen bij het complianceproces. De doelgroep bestaat uit compliance officers, bestuurders, toezichthouders, secretarissen van de vennootschap en bedrijfsjuristen die betrokken zijn bij het uitvoeren van compliancetaken.

**REDACTIE:**
Sharon Karsten (bureauredactie)
en Cora Wielenga (eindredactie)
Tel 088 99 88 100 E-mail:
redactie@complianceofficer.nl
**AAN DEZE EDITIE WERKTEN VERDER MEE:** Paolo Bouman, Jan-Jan Lowijs, Joost Montens, Roderick Noordhoek, Nicole Vreeman, Thai-Ha Vu
**FOTOGRAFIE:** Wilco van Dijen
**VORMGEVING:** Tangram Studio
**DRUK:** Platform P, Rotterdam
**UITGEVER:** Nederlands Compliance Instituut, Postbus 5111, Capelle aan den IJssel

Nieuwsfeiten, ingezonden artikelen en personeelsmutaties kunt u per e-mail doorgeven aan redactie@complianceofficer.nl.

Het abonnement is gratis voor de doelgroep. Abonnees buiten de doelgroep: € 50 per jaar.

Oplage 3.400 exemplaren
ISSN 1878-7991

# INHOUD

# NIET EEN KWESTIE VAN OF, MAAR VAN WANNEER

*"Cybercrime is mogelijk de fietsendiefstal van de toekomst"* kopte het AD de afgelopen zomer naar aanleiding van een uitspraak van procureur-generaal Gerrit van der Burg. Je hoeft namelijk niet meer een supernerd te zijn om in te kunnen breken op een computer of een netwerk. Het schijnt zo te zijn dat u en ik gewoon 'remote acces tool' software kunnen downloaden waarmee we op andere computers kunnen inbreken. Naast dat het gemakkelijker is geworden om digitaal in te breken, kan een cybercrimineel met een druk op de knop gemakkelijk vele slachtoffers maken. Ik kan me daarom voorstellen dat cybercrime inderdaad wordt aangeduid als de fietsendiefstal van de toekomst. Dan wordt cybercrime iets wat ons allemaal een keer overkomt. Bij mij is het al twee keer voorgekomen dat een fiets van mij gestolen werd. Ik weet niet hoe dat bij u zit?

Deze ontwikkelingen zijn verontrustend. En zeker wanneer ik lees dat het OM het niet lukt om officieren van justitie met verstand van cybercrime aan te stellen. Ze zijn nu overgegaan, bij gebrek aan specialistische instroom, om de huidige officieren op te leiden in cybercrime, omdat de verwachting is dat binnen vijf jaar meer dan 50% van de criminaliteit te maken heeft met computers. Ik vermoed dat we met de vervolging van cybercriminelen achter de feiten aan blijven lopen. IT-bedrijven en ethical hackers zouden ons moeten kunnen helpen hierin. Vroeger bestond bij mij nog het beeld dat met name de grote bedrijven wel in staat zouden zijn om zich te beschermen tegen computercriminelen, al dan niet zelfstandig. Dat bleek naïef. De cryptoworm WannaCry die in mei veel bedrijven wereldwijd schaadde en natuurlijk de ransomware die in juni dit jaar organisaties als APM Terminals, TNT en MSD voor een deel stil legde. En in september bleek dat Deloitte slachtoffer is geweest van een hack, terwijl Deloitte zich profileert als cybercrime-expert. Wie lukt het nog wel om zich goed te beschermen?

Ik besef dat zowel grote als kleine organisaties kwetsbaar zijn voor cybercrime-aanvallen en dat het onmogelijk is om je daar 100% tegen te wapenen. Natuurlijk blijft investeren in bewustwording van mensen belangrijk. Maar omdat cybercriminelen steeds slimmere aanpakken kiezen en er maar één 'foute klik' voor nodig is, ligt daar niet de oplossing. Wat je wel kunt en moet doen, is zorgen dat er een plan ligt om de continuïteit te waarborgen door ervan uit te gaan dat het je organisatie een keer zal overkomen. Het is niet een kwestie van *of*, maar *wanneer*. En een belangrijke stap bij het waarborgen van continuïteit is eenvoudig: zorg dat je back ups op orde zijn. Want zelfs na betaling van 'losgeld' krijg je niet altijd je bestanden weer terug.

Is de compliance officer nu eigenlijk verantwoordelijk om cybercrime te bestrijden? Bij sommige organisaties zal dat inderdaad het geval zijn. Bij de kleinere organisaties zien we dat de compliance officer cybercrime 'erbij krijgt'. Bij de grotere organisaties is er meestal meer ruimte om specialistische afdelingen in te richten. Wij zijn er geen voorstander van dat de compliance officer ook de digitale criminaliteit onder zijn hoede krijgt. Het bestrijden van cybercrime is een vak apart. Maar enige basiskennis is wel op zijn plaats. Dat is dan ook onze insteek van dit themanummer. Veel leesplezier.

Cora Wielenga

VICTOR GEVERS:

# "INTERNETVEILIGHEID HEEFT NIETS MET TECHNIEK TE MAKEN MAAR ALLES MET MENSEN"

*Victor Gevers* is ethisch hacker. Al negentien jaar. In zijn eentje waarschuwde hij meer dan vijfduizend organisaties voor lekken in hun softwaresystemen. Als hobby, of beter gezegd, als missie naast zijn fulltime baan. Nog geen twee jaar geleden richtte hij, samen met Vincent Toms, de vrijwilligersorganisatie GDI.Foundation op. Inmiddels heeft dit 'Rode Kruis voor het internet' al honderdzesentwintig duizend bedrijven attent gemaakt op hun kwetsbaarheid voor datadiefstal, virussen, ransomware en andere digitale ellende. Paolo Bouman skypt met Victor, die net de openingsspeech heeft gehouden op een conferentie van security bedrijf Nixu Corporation in Helsinki.

**VAN HOBBY HACKER NAAR VEELGEVRAAGDE AUTORITEIT IN CYBER SECURITY. WAAR IS DIT OOIT BEGONNEN?** "Het spelen met computers begon op mijn zesde en op mijn twaalfde schreef ik mijn eerste scripts. Serieus werd het toen ik voor mijn eerste werkgever, een non-profitorganisatie, een webserver inrichtte. Die werd direct na de live-gang gehackt en gewist. Daarmee was drie weken werk in één klap weg. Daar baalde ik enorm van. Vooral omdat het mijn eigen schuld was. Ik wist natuurlijk wel dat je software kon hacken, maar was nog me nog onvoldoende bewust dat dit gevaar ook via internet dreigde."

**DAT GAF HET STARTSCHOT OM ZELF TE GAAN HACKEN?** "Ja, het leek me super cool om stiekem, naast mijn werk, lekken in computers op te sporen en te melden. Zodat anderen niet zou overkomen wat mij was gebeurd. Dat was in 1997, Windows 95 was net uitgebracht. Daarin stond netwerksharing standaard aan. Ik liet daar een script op los en kreeg zo alle computers te zien bij wie dit niet was uitgezet. Daar kon ik zo naar binnen. Nu maken alle Nederlanders een aantal dezelfde directories, zoals 'Belastingdienst', 'Foto's' en er staat ook altijd ergens een cv. Daarin vond ik dan de contactgegevens, zodat ik een mailtje kon sturen met de mededeling dat de pc open stond, met een screenshot van het cv erbij plus instructies hoe de pc dicht te zetten."

**WAS DAT LEGAAL?** "Nee, het was computervredebreuk, ook al deed ik het met de beste bedoelingen. Ik deed het anoniem, ook omdat ik niet wist hoe mijn werkgever hier tegenaan zou kijken. Toen kreeg ik een reactie van iemand die ik had gewaarschuwd en die bleek zich echt rot geschrokken. Niet zozeer van het feit dat zijn pc voor iedereen openstond, maar van het feit dat ik, een anonieme indringer, in zijn computer was geweest. Toen besefte ik dat het niet zo handig was om anoniem te hacken. In 1998 begon ik het daarom onder mijn eigen naam te doen. Daar ging ik mee door tot in 2016, zo deed ik in mijn eentje vijfduizend driehonderdzeven meldingen als ethisch hacker."

**MAAKT HET WOORD ETHISCH HET WÉL LEGAAL?** "Het woord ethisch verwijst naar een standaard binnen de softwareontwikkeling genaamd responsible disclosure. Dit zijn richtlijnen die aangeven hoe je een lek in software verantwoord meldt, zoals: alleen aan de maker en niet aan de hele wereld. Die praktijk gaf een eerste aanzet om te laten zien dat hacken op een maatschappelijk verantwoorde manier mogelijk is, ook al is het computervredebreuk. Het duurde nog wel even voordat ook in Nederland responsible disclosure werd gezien als een toegestane manier van hacken, maar eind 2013 kwam het NCSC (Nationaal Cyber Security Centrum) met een leidraad hiervoor. Daar kwam veel commentaar op, zowel vanuit hackers als vanuit de security branche, maar ik was er blij mee want het was

een begin. Voor hackers zijn deze ontwikkelingen enorm belangrijk, want je grootste zorg is dat je op een zekere dag wordt opgepakt."

**WAT WAS JOUW EERSTE RESPONSIBLE DISCLOSURE?** "Dat was bij mijn videotheek. Daar stond een terminal waarmee de klanten titels konden opzoeken in hun UNIX-systeem. Het toetsenbord was deels afgedekt maar de Ctrl- en de F1-toets kon je indrukken. Met bepaalde toetsencombinaties kon ik daarmee in hun systeem komen, ik had daar bijvoorbeeld mijn eigen credits kunnen verhogen. Dus ik meldde dit en zij zegden toe dit op te lossen. Drie maanden later was er nog niets gedaan. Toen heb ik op een drukke vrijdagavond hun mainframe maar even herstart. Hierdoor konden ze een half uur lang, ook bij de kassa, niet in hun systeem."

**IK DENK DAT ZE LIEVER HADDEN GEHAD DAT JIJ JE CREDITS HAD VERHOOGD.** "Dat is stelen, dat zou ik nooit doen. Dit zou ik trouwens ook nooit meer doen, het was eigenlijk niet heel erg responsible."

**HOE GA JE DAN NU OM MET BEDRIJVEN DIE GEEN MAATREGELEN NEMEN NA EEN RESPONSIBLE DISCLOSURE?** "Vroeger zag ik dat als hun fout, nu zie ik het als een tekortkoming aan onze kant. Wellicht hebben we dan de urgentie niet duidelijk genoeg gecommuniceerd. Dan mail ik nog een keer naar mensen hoger in de organisatie of naar hun beveiligers. Maar tegenwoordig, met aanvallen van ransomware en dergelijke, is iedereen wakker en worden vrijwel alle responsible disclosures goed opgevolgd. In sommige landen gebeurt het niet om politieke redenen. Ook dan doen we niets vervelends, we treden er ook niet mee naar buiten. Dat doen we wel als een organisatie zelf naar buiten komt en liegt. Het bedrijf Cloudpets maakt knuffelberen waarmee kinderen met ouders in het buitenland, vaak militairen, kunnen communiceren. Begin dit jaar maakte de Australische journalist Troy Hunt bekend dat dit speelgoed lek was en er twee miljoen ingesproken berichten op straat lagen. Toen kwam CloudPets naar buiten met het bericht dat ze dit voor het eerst hoorden en het snel zouden verhelpen. Maar wij hadden dat bedrijf daarvoor al negen(!) keer gewaarschuwd. Toen hebben wij onze versie – met de bewijzen erbij – met de media gedeeld. Door hun liegen en lakse handelen speelden ze zich in de kijker van de California Attorney General die nu stappen tegen CloudPets onderneemt."

**DEZE RESPONSIBLE DISCLOSURE DEED JE VANUIT GDI.FOUNDATION, DE NON-PROFITORGANISATIE DIE JE SAMEN MET VINCENT TOMS OPRICHTTE. VERTEL EENS WAT MEER OVER DEZE CLUB.**
"Ik wilde niet langer alleen werken en zocht naar een professionelere manier om internet veiliger te maken, met een duidelijke afzender en een hogere meldingscapaciteit. Dat werd GDI.Foundation. Onze eerste activiteit na oprichting op 1 januari 2016 was Project 366. Daarin gingen we kijken hoeveel responsible disclosures we in alle dagen van 2016 zouden kunnen realiseren. Het werden dagen van vijftien uur, in wat in totaal leidde tot zeshonderd negentig responsible disclosures. Onlangs analyseerde een journalist onze cijfers van 2017 en hij kwam op een resultaat van honderdzesentwintig duizend meldingen wereldwijd waarvan er honderdvijfentwintig duizend zijn opgelost. Dat is dus een gigantische toename! Dat kan omdat we nu dertien vaste leden en drieëntwintig vrijwilligers over de hele wereld hebben en talloze incidentele online helpers die ons inmiddels kennen. In de pers zijn we wel 'het Rode Kruis van internet' genoemd. Die naam klopt wel, we leggen een noodverbandje en gaan weer verder."

**WORDEN RESPONSIBLE DISCLOSURES BELOOND DOOR DE BEDRIJVEN DIE JE WAARSCHUWT?**
"Tegenwoordig bestaan er bug bounties waarmee je bij sommige programma's flink geld kunt verdienen. Zeer succesvolle Nederlandse bedrijven als HackerOne en Zerocopter bieden open en gesloten platforms waar softwareontwikkelaars hun producten kunnen aanbieden en waar hackers dan de gaten in mogen zien te vinden. Wie wat vindt en dit volgens de regels meldt, wordt beloond. Wij zoeken de gaten in reeds draaiende software. Dat wordt zelden beloond, maar daar doen we het ook niet voor. We doen het voor een veiliger internet. Maar met meer geld kunnen we opschalen. We laten ook iedereen zien wat we doen, zodat anderen ons werk kunnen kopiëren."

**WAAR LEEF JE VAN?** "Bij ons krijgt niemand een salaris, er zijn alleen onkostenvergoedingen. Soms ontvangen we giften en binnenkort krijgen we een ANBI-status waardoor bedrijven ons werk belastingaftrekbaar kunnen steunen. Ik leef van mijn fulltime baan als innovatiemanager bij de overheid en doe dit ernaast. Dus mijn nachten zijn soms heel kort, zeker als er aandacht vragende operaties lopen. Mijn familie en vrienden kennen mij als iemand die vaak

een laptop op schoot heeft. Dat moet nu maar even zo zijn, want ik wil deze stichting goed van de grond helpen trekken. Straks mag een jongere generatie het overnemen, zij vinden dit heel gaaf."

**WELKE CASE GAF JE HET MEESTE VOLDOENING?** "Case 35 uit januari dit jaar. Een Frans onderzoeksinstituut naar leukemie was na een ransomware-aanval op open MongoDB alle onderzoeksgegevens kwijtgeraakt. Het ging om welke behandelmethoden hadden gewerkt en welke niet. Er zijn dus kinderen overleden bij het vergaren van deze kennis! En die kennis was weg. Wij zijn daar naar toe gegaan en hebben er drie dagen zitten sleutelen. Deels door puur geluk en deels doordat het om ouderwetse harddisks ging, lukte het op de derde dag de data terug te halen. Niet eerder voelde ik zo'n enorme druk om een operatie te laten slagen."

**EN OOK IN DIT GEVAL, GEEN BELONING?** "Nee, reiskostenvergoeding, maar dat is prima. Ik denk trouwens dat in dit geval de artsen en onderzoekers te erg van slag waren om daar überhaupt aan te kunnen denken. Maar ons werk is zeker waardevol. Soms letterlijk. Zo hebben we hele wasstraten met computersystemen voor bitcoin mining gewaarschuwd dat ze openstonden voor het internet. De beheerder had het voorbeeldwachtwoord uit de handleiding overgenomen. Een handleiding die je via Google kunt vinden! Bij nader onderzoek bleek hij niet de enige. Iemand rekende voor me uit dat alle systemen die ik zo aantrof in totaal een miljoen dollar per dag genereerde. En ik kon daar zo bij. Ik ontdekte dat de meeste van de Chinese overheid waren. Ik waarschuwde hen en ze werden dichtgezet. Verder hoor je niks. Ik had het wel leuk gevonden om een brief te krijgen waarin staat dat GDI.Foundation een prima club is die altijd welkom is in China."

**HOE STAAT HET NU MET DE (JURIDISCHE) VEILIGHEID VAN HACKERS?** "In Amerika heeft men een probleem met de term responsible disclosure, daar heeft men het over Coordinated Vulnerability Disclosure en daar is een officiële standaard ISO/IEC 29147:2014 voor opgesteld. Hierdoor krijgen securityonderzoekers en ethische hackers een kader aangeboden waarbinnen zij legaal zwakheden in systemen mogen melden. Ook is er een wet voorgesteld die hackers met goede bedoelingen vrijwaart van aansprakelijkheid en vervolging. Dat is echt een enorme verschuiving en daar hebben hackers wereldwijd enorm aan bijgedragen. Als die wet doorgaat, streeft de VS Nederland voorbij. Maar in Senegal staat op hacken nog de doodstraf. Wij gaan naar allerlei internationale bijeenkomsten over cyber security. Dan leg ik uit wat wij doen en dan vraag ik aan de aanwezige politici: hoe kan ik dit straffeloos doen in jullie land?"

**HOE VEILIG OF WEERBAAR ZIJN NEDERLANDSE BEDRIJVEN?** "De overheid en grote bedrijven hebben veel gedaan aan de eigen systemen, maar het mkb blijft ver achter. De diensten die worden aangeboden zijn duur en onoverzichtelijk. Ik vind dan ook niet dat het mkb daarop mag worden afgerekend, maar dat zij steun van de overheid zou moeten krijgen. Verder hebben we het NCSC dat waakt over kritische infrastructuur. Dan denk je: dat is mooi, dan zijn alle belangrijke zaken gedekt. Maar dat valt dus vies tegen; ziekenhuizen bijvoorbeeld, vallen daar niet onder. Het NCSC-verzorgingsgebied is heel erg beperkt."

DE OVERHEID EN GROTE BEDRIJVEN HEBBEN VEEL GEDAAN AAN DE EIGEN SYSTEMEN MAAR HET MKB BLIJFT VER ACHTER.

**DENK JE DAT DE ONVEILIGHEID TOENEEMT DOOR ONTWIKKELINGEN ALS INTERNET OF THINGS EN BIOTECH?** "Absoluut, door Internet of things gaan we terug in de tijd. Er komen nu producten op de markt met een beveiliging zo slecht als tien jaar geleden. Als die apparaten straks worden overgenomen door bijvoorbeeld een Mirai Botnet en gaan samenwerken, dan kunnen er hele netwerken omvallen. En dat, omdat er zo nodig een webserver in een Siemens wasmachine moet zitten. Voor biotech geldt dat er, als proef, al pacemakers zijn gehackt. Als dit doorgaat worden er binnenkort mensen omgelegd of krijg je als patiënt bericht dat je losgeld moet betalen. Ik vrees dat dit eerst moet gebeuren voordat er maatregelen worden genomen."

**WAT ADVISEER JE BEDRIJVEN WAARVAN DE COMPUTERS ZIJN GEGIJZELD VOOR LOSGELD?** "Niet betalen. Om drie redenen. Je houdt zo de industrie in stand. Je kunt er zeker van zijn dat ze terugkomen. En, als je betaalt beken je schuld. Vanaf 25 mei 2018 gaat de Europese privacyverordening in: de Algemene Verordening Gegevensbescherming (AVG), ofwel General Data Protection Regulation (GDPR). Deze nieuwe wet legt boetes op tot 4% van de jaaromzet aan bedrijven die de gegevensbeschermingsregels overtreden. Dit biedt criminelen de kans om bedrijven met datalekken flink af te persen. Ik denk dan ook dat de GDPR meer ellende zal veroorzaken dan oplossen. Ik heb hier met ambtenaren en politici over gesproken en die gaven toe dit aspect over het hoofd te hebben gezien."

**WAAR ZITTEN DE KWETSBAARHEDEN BIJ BEDRIJVEN EN DUS OOK: WAT KAN EEN ORGANISATIE DOEN OM TE VOORKOMEN DAT ER EEN HACK PLAATSVINDT?** "Heel veel Windows-netwerken zijn nog niet gesegmenteerd. Ze hebben wel een firewall, maar als een enkele pc niet is gepatcht, dan kunnen ze allemaal worden geïnfecteerd met ransomware, zoals NotPetya en WannaCry. Tijdens de aanval van deze virussen begin dit jaar was ik gevraagd om een aantal Britse organisaties te adviseren en mijn advies moest zijn: richt het maar opnieuw in. Dat betekent dat alle computers een paar uur uit moeten. Dat is heftig. In Nederland speelde dit bij een van de drie distributiecentra voor supermarkten. Ook daar moesten de computers uit. Dat betekende dat supermarkten in bepaalde delen van het land vier dagen niet konden worden bevoorraad. Wat ik dan ook niet begrijp, is dat we eindgebruikers een Windowscomputer geven waar men op linkjes kan klikken. Dat is vragen om phishing. MijnOverheid stuurt nooit een link mee in haar berichten. Mensen vinden dat irritant maar we doen dat om mensen te leren zelf naar een portal te gaan en daar in te loggen. Zodat je weet wat je doet. Mijn boodschap is ook altijd dat internetveiligheid niets met techniek te maken heeft, maar alles met mensen."

**HEB JE TIPS VOOR COMPLIANCE OFFICERS ALS HET GAAT OM CYBER SECURITY?** "Kijk of je de officiële ISO-standaard voor Coordinated Vulnerability Disclosure kunt toepassen en zorg dat je zelf de spelregels opstelt voor ethische hackers die kwetsbaarheden willen melden en zet die op je site. Wil jouw bedrijf oefenen hoe dit in de praktijk werkt, dan kunnen ze een beroep op ons doen. Verder verwijs ik graag naar de factsheets op de website van het NCSC. Daar vind je richtlijnen vanuit de overheid en ook voorbeeldteksten. Tot slot vind je de actuele adviezen van de overheid op Alert Online."

**KUN JE OOK EEN LEUK BOEK AANRADEN OVER DEZE MATERIE?** "Ja, van Chris van 't Hof: het boek Helpende Hackers of Helpful Hackers. Gratis in het Nederlands en Engels als ePub te downloaden van zijn site www.cvth.nl, maar ook als gedrukte uitgave te koop."

**HEB OF HAD JIJ OOK EEN VOORBEELDFIGUUR?** "Nee, maar de tekst uit Spiderman 'with great power comes great responsibility' vond ik geweldig. Maar dat was vroeger. Ik heb lang geleden mijn masker afgelegd. Op mijn lezing vandaag gaf ik als reden dat het slecht pizza eten is met een bivakmuts op. Een omgekeerd aangetrokken hoodie is veel beter: uit de capuchon kun je popcorn eten terwijl je doorwerkt."

WITH GREAT POWER COMES GREAT RESPONSIBILITY.

# CYBERSECURITY


Equifax zegt u waarschijnlijk niet zo veel. Het bedrijf bestaat sinds 1899, maar haar bestaan was mij onbekend totdat ik hier een huis kocht. Zonder mijn medeweten of instemming legde Equifax een dossier aan over mijn financiële kredietwaardigheid. Equifax is namelijk een *consumer credit reporting agency*. Het verzamelt en verstrekt financiële gegevens van zo'n acht honderd miljoen consumenten wereldwijd. En laatst werden van zo'n honderd drieëntveertig miljoen consumenten hun persoonlijke gegevens gestolen. Waaronder de mijne. Hackers wisten in te breken in het computersysteem van Equifax, doordat het bedrijf basale computerbeveiliging niet op orde had.

Dit voorbeeld alleen al verdient een hele column, maar dit is niet hét computer gerelateerde risico waar u – compliance professionals – het meest wakker over zou moeten liggen. Ik denk dat het risico voor ons van een heel andere kant komt: onze baan bestaat namelijk niet lang meer.[1]
Kort gezegd zit dat namelijk zo. Allereerst staat computertechnologie op het punt van wasdom om een groot deel van uw huidige werk sneller, beter en goedkoper uit te voeren. Daarnaast toont de investeringsgroei in compliance startups aan dat investeerders hierin ook brood zien.[2]

De technologie om zonder menselijke input zinvolle verbanden te leggen uit een immens grote hoeveelheid 'vrije tekst' (wetteksten, documenten, tijdschriften, nieuwsartikelen, whatsapp-berichtjes, noem maar op) bestaat al. Waar u en ik jaren over doen, maken computers dit eigen in milliseconden. Daarnaast worden computers steeds beter om realistische interactie te hebben met mensen. Zowel in tekst als in alle twaalf meest gesproken talen. Dit alles wordt mogelijk gemaakt door een nog altijd stabiele groei van reken- en opslagcapaciteit. Jaar op jaar op jaar.

Machinelearning, datamining, artificial intelligence (AI), blockchain: als deze termen u helemaal niets zeggen, dan raad ik aan daaraan iets te doen. Als u hier alles al vanaf weet, weet u ook dat de soep niet zo heet gegeten wordt als hij opgediend wordt. In alle berichtgeving lees ik momenteel nog veel kretologie en hyperbool, maar een gewaarschuwd mens telt voor twee.

Groetjes,
Joost

*Joost Montens werkt voor AstraZeneca, een innovatief biofarmaceutisch bedrijf. Sinds februari 2015 woont en werkt hij in de Verenigde Staten. In deze column bericht hij over zijn compliance-ervaringen en bevindingen.*

1 The Future of Employment, How Susceptible are Jobs to Computerisation?, Oxford, Frey (2013).

2 RegTech Startup trends, CBInsights (2017).

# CYBERSECURITY EN PRIVACY: NAÏEF OM TE DENKEN DAT ZE LOS VAN ELKAAR STAAN

NICOLE VREEMAN EN JAN-JAN LOWIJS

**Vanaf 25 mei 2018 zal de nieuwe Europese privacyregelgeving, de Algemene Verordening Gegevensbescherming (AVG)[1] van toepassing zijn en gehandhaafd worden door de Autoriteit Persoonsgegevens (AP). Dit brengt allerlei veranderingen met zich mee voor organisaties aangaande de manier waarop ze met persoonsgegevens om (mogen) gaan.**

*Security*, de beveiliging van data en informatie, is een belangrijk onderdeel binnen het privacylandschap. Hoe dient een organisatie de persoonsgegevens die worden verwerkt te beveiligen? Wat zegt de AVG hierover? Beveiliging van persoonsgegevens kan al snel twee derde van de inspanning innemen bij het adresseren van het onderwerp privacy. Wij geven in dit artikel *food for thought* om mee te nemen in zowel privacy als (cyber)security-aanpassingen die u ongetwijfeld in de komende maanden zal (dienen te) nemen binnen uw organisatie.

## WAT ZEGT DE NIEUWE WET OVER HET BEVEILIGEN VAN PERSOONSGEGEVENS?

Voordat u deze paragraaf overslaat omdat u denkt 'wij verwerken geen persoonsgegevens', even terug naar de basis: wat wordt er verstaan onder het begrip 'persoonsgegevens'? Een persoonsgegeven is informatie die direct of indirect herleidbaar is naar een natuurlijke persoon. Indirect wil zeggen dat de informatie in combinatie met andere informatie (onverminderd of deze in uw bezit is) te herleiden is tot een persoon. Persoonsgegevens zijn dus in ieder geval de gegevens die u heeft over uw medewerkers, de paspoortkopieën, uw klantenbestand, uw distributielijsten, enzovoort. Maar het gaat veel verder. Gegevens van zakelijke contactpersonen (naam, zakelijk e-mailadres) bij klanten en leveranciers zijn ook persoonsgegevens.

Technische gegevens zoals we die kennen uit computernetwerken, zoals inlognamen, wie wanneer heeft ingelogd en wachtwoorden zijn persoonsgegevens en in bepaalde gevallen kunnen zelfs IP-adressen dat zijn. En als laatste voorbeeld: als u een vloot met voer-, vaar- en/of vliegtuigen beheert en u kent zowel de locatie daarvan als diegenen die bestuurder of passagiers zijn, dan zijn die locatiegegevens persoonsgegevens van deze personen.

1 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). In het Engels wordt de AVG aangeduid als de *General Data Protection Regulation* (GDPR).

ALS U HET VERTROUWEN VAN UW KLANTEN WILT, WEES DAN OPEN OVER HOE U MET DATA OMGAAT EN PERSOONSGEGEVENS BEVEILIGT.

# UW ORGANISATIE VERWERKT DUS PERSOONS-GEGEVENS.

Deze gegevens dient u te beveiligen. Daarbij is het plaatsen van een firewall in uw computernetwerk om onbevoegden buiten te houden en het verplicht maken van een wachtwoord met minimaal zes tekens niet meer toereikend. Het huidige securitytijdperk vraagt om maatregelen die zorgen dat data wordt beschermd, maar die bovendien helpen detecteren wanneer een bedreiging zich aandient, om hierop te kunnen reageren en om de normale status te kunnen herstellen. Om dit te kunnen bewerkstellingen is allereerst een risicoanalyse nodig die de waarschijnlijkheid en ernst van de risico's in kaart brengt, gevolgd door identificatie van alle mogelijke beveiligingsmaatregelen. Na een risico-kostenafweging mondt dit uit in de daadwerkelijk te nemen beveiligingsmaatregelen.
In deze analyse dient u de risico's op inbreuk op de rechten en vrijheden van natuurlijke personen centraal te stellen. Daarnaast kunt u uiteraard de financiële risico's, reputatie-risico's of andere risico's die uw organisatie raken, meenemen in de analyse, maar het opnemen van de impact van beveiligingsincidenten op personen mag niet achterwege blijven.

Gedeelde smart is halve smart – niet alleen de verwerkingsverantwoordelijke is verantwoordelijk voor de beveiliging van de persoonsgegevens, maar de verwerker ook![2] Dit is een verandering ten opzichte van de oude (huidige) wetgeving. In de praktijk is dit van belang, omdat organisaties dus kunnen samenwerken om de beveiliging van de persoonsgegevens die ze uitwisselen op orde te hebben: het is immers hun beider verantwoordelijkheid en ze kunnen er beide op worden aangesproken door de toezichthouder. In de AVG wordt een aantal manieren aangedragen waarop persoonsgegevens beveiligd kunnen worden, waaronder de mogelijkheid encryptie toe te passen of te pseudonimiseren.

## ENCRYPTIE, PSEUDONIMISERING EN ANONIMISERING

"Onze data is allemaal geanonimiseerd, dus de AVG is niet op ons van toepassing" – lees toch nog even verder. Data die eens persoonsgegevens waren, zijn bijna nooit anoniem. Data wordt als anoniem gekwalificeerd indien geen enkele mogelijkheid bestaat waarop die data herleid kan worden naar een bepaald persoon. Alleen het weggooien van het identificerende deel van de persoonsgegevens (naam, mogelijk geboortedatum, et cetera) is daarvoor niet voldoende. Vaak blijven er genoeg unieke kenmerken over in de data die het mogelijk maken om deze weer te herleiden naar een bepaalde individu. En de paradox is: hoe beter we worden in data-analyse, door het inzetten van technieken als *machine learning* en kunstmatige intelligentie, hoe lastiger het is om persoonsgegevens anoniem te maken; we worden simpelweg te goed in dit herleiden van 'anonieme' data naar een specifiek persoon.

De AVG is expliciet wél van toepassing op gepseudonimiseerde data[3]. Pseudonimisering is een vorm van encryptie, waarbij de identificeerbare delen van de persoonsgegevens worden omgezet in artificiële *identifiers*, zogenaamde pseudoniemen. Het doel is om de 'persoon' uit persoonsgegevens te halen. Hierdoor wordt de resulterende data binnen beperkte context anoniem. Buiten die context is identificatie echter nog steeds mogelijk. Dat voor identificatie externe informatie nodig is, doet niet ter zake; alle puzzelstukjes zijn er nog, ze liggen alleen niet allemaal meer bij elkaar. Simpeler gesteld: de persoonsgegevens zijn versleuteld maar de sleutel bestaat nog. De originele persoonsgegevens zijn dus te achterhalen. De AVG beschouwt pseudonimisering als een geschikte vorm van beveiliging, maar niet als middel om onder de AVG uit te komen.

2 Onder **verwerkingsverantwoordelijke** wordt verstaan de organisatie die bepaalt wat er met de persoonsgegevens gebeurt en op welke wijze deze worden verwerkt. De **verwerker** (voorheen: bewerker) verwerkt de gegevens enkel en alleen in opdracht van de verwerkingsverantwoordelijke.

3 De definitie die de AVG geeft van pseudonimisering is "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld".

Gepseudonimiseerde persoonsgegevens zijn geschikt voor een groot scala aan analytische activiteiten, onderzoeksprojecten en voor statistische doeleinden. Omdat niet alle informatie meer in zijn originele vorm zichtbaar is, vermindert het risico van misbruik in geval van een datalek. De AVG roemt de voordelen van persoonsgegevens die gepseudonimiseerd zijn en lijkt organisaties daarom een duwtje te geven in de richting van pseudonimiseren om zo het niveau van beveiliging te verhogen.

Bij juiste toepassing kan pseudonimisatie meer mogelijkheden voor gebruik van de persoonsgegevens die u in huis heeft met zich meebrengen, dan wanneer dezelfde persoonsgegevens niet gepseudonimiseerd zouden zijn. Onthoud echter, dat de overgebleven data niet anoniem is geworden!

**MELDEN VAN EEN DATALEK**

Een andere maatregel die verband houdt met beveiliging van persoonsgegevens is dat een datalek gemeld dient te worden. Vanaf 1 januari 2016 is in Nederland de Wet meldplicht datalekken van toepassing. Met de AVG wordt deze meldplicht Europa-breed ingevoerd. Een datalek dient binnen 72 uur te worden gemeld aan de toezichthouder en eventueel aan degenen op wie de persoonsgegevens betrekking hebben (na een afweging omtrent de melding). Zijn de persoonsgegevens beveiligd door bijvoorbeeld pseudonimisering, dan kan de afweging of het datalek gemeld dient te worden aan de AP en aan betrokkenen wellicht eerder leiden tot het niet hoeven melden. Uit de meldplicht vloeit bovendien een procedureplicht voort. Dat betekent dat uw organisatie een overzicht dient bij te houden van alle datalekken. Dus ook van de datalekken die na uw afweging niet meldingsplichtig waren en niet gemeld zijn.

Als u in de telecombranche werkzaam bent, dan is deze meldplicht voor u niet nieuw. Onder de ePrivacy-richtlijn, die is omgezet in onze Telecommunicatiewet, bestond een dergelijke meldplicht al voor telecomproviders.

De meldplicht zorgt voor transparantie met betrekking tot hacks, datalekken en zelfs zwakke plekken in fysieke beveiliging. Hier kunnen andere organisaties lessen uit trekken en op hun beurt de security weer verhogen. De organisatie waar de inbreuk op de beveiliging plaatsvond, kan hier ook een positieve draai aan geven door het onderzoek te delen. Denk aan de vliegtuigbranche, waar al jaren elk ongeval wordt onderzocht om lering uit te trekken voor volgende vluchten.

Wanneer een datalek uw organisatie treft – *wanneer* en niet *als*, want het zal u eens overkomen – dan is melden niet uw eerste taak. Het datalek of de hack tegengaan is het eerste wat u doet. Roep het crisisteam bijeen, spoor indringers op en houd ze tegen, ga na wat de schade is en wat er dient te gebeuren om terug te keren naar de normale status. Onderdeel van deze response is natuurlijk het op tijd melden van het datalek, maar het datalek direct bestrijden en in kaart brengen wat de schade is, is ook zeer van belang.

Neem het proces omtrent een datalek op in uw *security incident response-plan*. Wanneer u dan een oefening houdt – u houdt oefeningen, toch? – waarbij datalekken aan bod komt, dan is de procedure bij iedereen bekend.

**HOE NEEMT U BOVENSTAANDE MEE IN UW ORGANISATIE?**

Dient u nu op stel en sprong alle persoonsgegevens die uw organisatie verwerkt, te pseudonimiseren? Dient u uw crisisplan te herschrijven, zodat datalekken centraal komen te staan? Of alle servers op slot te doen en te stoppen met de verwerking van persoonsgegevens? Nee, natuurlijk niet, dat zou een overtrokken reactie zijn.

Wat u wél kunt doen, is zorgen dat u inzicht heeft in de persoonsgegevens die u verwerkt, zodat er geschikte beveiligingsmaatregelen genomen kunnen worden, zowel op de persoonsgegevens zelf (encryptie) als op de systemen, het pand en de mensen. Dat betekent het regelmatig uitvoeren van risicoanalyses. Zo kunt u *security breaches* (inbreuken op uw beveiliging) voorkomen, opsporen en er adequaat op reageren. Zorg er ook voor dat het melden van datalekken in procedures is vastgelegd in uw organisatie.

Als u het vertrouwen van uw klanten wilt, wees dan open over hoe uw organisatie met data omgaat en ook hoe zij persoonsgegevens beveiligt. Dat is een basis van een sterk merk.

**N.L.K. (Nicole) Vreeman (CIPP/E) werkt bij Deloitte Risk Advisory in het Privacy Services team. Ze adviseert organisaties over hoe ze met hun data om kunnen gaan. J.J. (Jan-Jan) Lowijs (CIPP/E, CISSP) werkt bij Deloitte Risk Advisory in het Privacy Services team. Hij heeft ruim twaalf jaar werkervaring op het gebied van cybersecurity en privacy.**

GERRIE DE JONGE:

# "INTERNET LIJKT ZO ONGEVAARLIJK ALS EEN KEUKENTRAPJE"

*Gerrie de Jonge* is IT-directeur van PostNL Pakketten en Logistiek en daarnaast als CISO (chief information security officer) verantwoordelijk voor de cybersecurity van heel PostNL. Een jaar geleden bracht zijn CEO, Herna Verhagen, een advies uit aan de BV Nederland om deze vorm van veiligheid net zo serieus te nemen als onze dijken. Paolo Bouman vraagt hem hoe hij binnen PostNL waakt over digitale droge voeten.

**GERRIE, WIL JE EERST KORT IETS VERTELLEN OVER JOUW ACHTERGROND?** "Ik werk nu vijfentwintig jaar in de IT. Ik ben wiskundige en heb daarnaast een master in logistiek management. Vlak na de privatisering begon ik bij de toenmalige PTT in het management trainee programma. Eerst een paar jaar zelf software ontwikkelen, daarna vooral erover praten. Vervolgens werkte ik acht jaar bij andere bedrijven, onder andere in Canada, om in 2004 terug te keren naar PostNL. Daar vervulde ik diverse senior IT-rollen, introduceerde de virtuele werkplek en ontwikkelde en implementeerde de cloudstrategie. Drie jaar geleden werd ik gevraagd om IT-directeur bij Pakketten te worden, afgelopen juli kwam Logistiek daar bij."

**BEHALVE IT DIRECTEUR VAN POSTNL PAKKETTEN EN LOGISTIEK BEN JE OOK CISO VAN HEEL POSTNL. DAT IS EEN ONGEBRUIKELIJKE COMBINATIE VAN ROLLEN. LEG EENS UIT.**
"Dit besluit kwam voort uit een rationaliseringsslag waarbij we het CIO-office hebben opgeheven. De taken hierin brachten we onder bij de IT-board en zo kwam security en privacy bij mij terecht. Deze combinatie van IT-directeur en CISO vindt men vaak vreemd vanuit de redenering: cybersecurity is toch niet iets dat je er even bij doet. Wij zien dat anders, wij zeggen: wij vinden security zo belangrijk dat we het bij een IT-directeur onderbrengen. En verder doe ik het er natuurlijk niet even bij, ik heb mijn security officers. Ik ken geen ander bedrijf dat het zo heeft georganiseerd, maar beluister om me heen dat traditionele CISO's soms moeite hebben om binnen hun eigen bedrijf te worden gehoord. Dat probleem heb ik niet, ik moet tenslotte ook over mijn eigen 'IT-winkel' waken."

**WAT DOE JE, ALS IT-DIRECTEUR EN ALS CISO?**
"Pakketten en Logistiek is de snelst groeiende poot van PostNL. Als IT-directeur van deze divisie ben ik vooral bezig om vanuit IT de voorwaarden te creëren waaronder we kunnen blijven groeien door de systemen duurzaam en schaalbaar te maken. Als CISO probeer ik aan de technische kant onze detectiemogelijkheden te verbeteren, denk aan DDoS-beveiliging van onze website, het inzetten van tooling om systeemlogs te controleren op abnormaal systeemgedrag en tooling die meet welke informatie het bedrijf verlaat en dus ook of je een lek hebt. Aan de preventiekant doen we veel door onze mensen het inzicht, de verantwoordelijkheden en de middelen te bieden om veilig te werken. Dat gaat van uitleggen wat een goed wachtwoord is tot medewerkers leren hacken. Ook vragen we zogenaamde social engineers regelmatig om te proberen bij ons in te breken. En omdat we steeds nieuwe producten bedenken moeten ook nieuwe systemen worden ontwikkeld. In het ontwerpen, programmeren en testen van die nieuwe systemen ben je ook voortdurend bezig met veiligheid."

**ZIJN DE MEDEWERKERS ZICH VOLDOENDE BEWUST VAN HET BELANG VAN CYBERSECURITY?**
"Door onze aandacht hiervoor durf ik te stellen dat de awareness bij ons meer dan gemiddeld is. Als ik de aftrap geef van een awarenesstraining haal ik altijd een onderzoek aan dat is gedaan naar gepercipieerd en feitelijk persoonlijk gevaar. Het vliegtuig staat op nummer één als ons grootste gepercipieerde gevaar terwijl het keukentrapje feitelijk ons grootste gevaar is. En daar stappen we elke dag weer onbezorgd op. Diezelfde houding geldt ook voor ons cybergedrag. Elke dag gaan we weer het web op met

ELKE DAG GAAN WE WEER HET WEB OP MET SOFTWARE WAARVAN WE NIET WETEN OF DIE LAATSTE UPDATES HEEFT, MET IDENTITEITEN DIE MAKKELIJK TE KRAKEN ZIJN, EN LATEN WE VAN ALLES ACHTER.

software waarvan we niet weten of die laatste updates heeft, met identiteiten die makkelijk te kraken zijn, en laten we van alles achter."

**WAT IS JOUW ROL TEN OPZICHTE VAN DE FUNCTIONARIS GEGEVENSBESCHERMING BIJ POSTNL?** "Bij ons heet deze functionaris chief privacy officer. Deze functie kom je meestal tegen bij afdelingen als Legal, Compliance of Audit. Wij hebben ervoor gekozen om dit onder mijn verantwoordelijkheid als CISO te laten vallen. We doen dit onder het motto 'privacy en security zijn broertje en zusje'. Je kunt zaken heel secure doen, maar tegelijkertijd de wet overtreden, bijvoorbeeld omdat je gegevens te lang bewaart. Andersom heb je heel veel security nodig om de privacy te borgen. Daarom hebben wij het over broertje en zusje waarbij security de grote broer is. Ik heb drie privacy officers in mijn afdeling, volbloed ervaringsdeskundigen die over het hele bedrijf de bestaande en nieuwe processen monitoren op gegevensbescherming."

**JE ZEI EERDER DAT HET INTERNE BEWUSTZIJN MET BETREKKING TOT CYBERSECURITY BIJ POSTNL MEER DAN GEMIDDELD IS. GELDT DAT OOK VOOR HET BEWUSTZIJN MET BETREKKING TOT PRIVACY?** "Ook daarin speelt het voordeel dat wij security en privacy hand in hand laten gaan, want beide zaken lijken veel op elkaar en voor beide moet je ongeveer dezelfde programma's draaien. Daar zit veel synergie in. We hebben een netwerk van dertig ambassadeurs opgericht die binnen hun afdeling als extra taak hebben om op security en privacy te letten. Zij geven onder onze supervisie ook voorlichting, werken oplossingsgericht en dragen zo bij aan de awareness en effectieve aantoonbaarheid van de naleving van de regelgeving."

**BINNEN IT VERBINDEN JULLIE SECURITY EN PRIVACY MAAR COMPLIANCE IS WEL APART GEORGANISEERD. WAAROM?** "Op die manier kunnen de mensen van security en privacy hun rol van ambassadeur het beste vormgeven zonder in de rol van politieagent terecht te komen. Zij kunnen zich meer richten op het uitdragen van kennis en het verbeteren van het vakmanschap. En ze krijgen zo ook meer kans om kwetsbaarheden te zien. Daarna is het aan medewerkers van compliance en aan de auditors om te controleren of we het goed genoeg doen."

**IS POSTNL AL AVG-PROOF?** "We zijn goed op weg dat te worden. Al anderhalf jaar geleden stelden we een chief privacy officer aan om kwartier te gaan maken. Hij begon met het vergroten van de awareness met speciale programma's, het maken van impactanalyses en het inventariseren van gegevensstromen. Ook heeft hij onze bestaande relaties met belangrijke stakeholders zoals bijvoorbeeld de Autoriteit Persoonsgegevens en de Consumentenbond verder verdiept, zodat zij weten wat wij doen en waarom. Inmiddels loopt er een programma waarmee we kunnen checken of we voldoen aan normen van de AVG. Daar is soms de nodige discussie over vanwege de veelal open normen en het nieuwe risico gebaseerde karakter van de AVG. Want wanneer en hoe stel je vast of je compliant bent? Het gaat ons erom dat we tenminste een compleet beeld hebben van de gegevensstromen waarin persoonsgegevens zijn verwerkt, weten hoe en waarom we dat doen en of ze passend beschermd zijn. Dat proces staat

op de rit maar we moeten bij een groot bedrijf als het onze altijd scherp blijven of dat complete beeld nog steeds klopt."

**POSTNL VERZAMELT GEGEVENS OVER AFZENDERS EN GEADRESSEERDEN. BEZORGT JE DAT HOOFDBREKENS ALS CISO?** "Niet echt. Voor het verzamelen van gegevens moet een rechtmatige grondslag bestaan en die hebben we. Adressen hebben we nodig voor de uitoefening van onze dienstverlening. Maar er gelden wel regels en die respecteren we. Sommige andere diensten roepen nog wel eens vragen op, zoals onze zakelijke datadiensten, maar die blijven altijd binnen de geldende wettelijke of zelfregulerende kaders. Verder bemoeien we ons niet met de inhoud van wat we bezorgen vanwege het briefgeheim, maar ook omdat we dat niet willen weten. Maar voor een mogelijke retour is het vanuit klantbeleving wel wenselijk dat we het adres van de afzender weten en dus ook enige tijd bewaren. En als het gaat om een zending van bijvoorbeeld een vakbond of politieke partij gelden weer scherpere regels, want die informatie kan worden gezien als bijzonder persoonsgegeven. PostNL profileert zich al tweehonderd jaar als de hoeder van het briefgeheim. Die missie nemen we heel serieus, ook als het gaat om pakketten."

**WAT IS JOUW ROL BIJ DATALEKKEN?** "Dat is de taak van de chief privacy officer. Hij beoordeelt incidenten en meldt het datalek indien nodig bij de Autoriteit Persoonsgegevens. Ook starten we altijd direct een onderzoek waarbij de chief privacy officer betrokken blijft als crisiscoördinator. We hebben dit een paar keer aan de hand gehad en dit valt ook niet altijd met interne controls te voorkomen. Soms komt het omdat een systeem verkeerd is geconfigureerd, waardoor het tijdelijk open stond. Soms meldt een medewerker dat hij iets kwijt is, zoals een USB-stick of een laptop of dat er per ongeluk een bestand aan de verkeerde ontvanger is verzonden. En soms word je daar door een externe bron op gewezen, een ethisch hacker bijvoorbeeld. Dan komt het er op aan zo snel mogelijk te reageren, bijvoorbeeld door alle mogelijk getroffenen te informeren. Iets wat met onze omvang natuurlijk een flinke klus kan zijn."

**WAAR HEBBEN JULLIE VOORAL LAST VAN?** "Van phishing. En dan niet zozeer intern, want daar trainen we onze collega's op. We versturen bijvoorbeeld regelmatig zelf intern phishing mails rond om te zien of men erop klikt. Waar wij vooral last van hebben is misbruik van onze 'trusted brand name'. Mensen ontvangen mailtjes met het bericht dat er een pakketje voor ze klaarstaat met het verzoek even te klikken om aan te geven wanneer het wordt opgehaald. In oktober 2014 haalden we het achtuurjournaal met een e-mailgolf die zogenaamd uit onze naam was verstuurd en ransomware bevatte. Heel veel mensen hadden daar op geklikt, want met ons aantal klanten zijn er heel veel potentiële slachtoffers. Daar hebben we heel veel werk aan gehad. Je moet je klanten informeren, je callcenter opschalen en samenwerken met de autoriteiten. Het kost je dus flink geld terwijl het niets met ons te maken heeft. We doen dan ook altijd aangifte, soms met een succesvol vervolg. Inmiddels is onze incidentenrespons zeer geolied georganiseerd, maar de phishing mailtjes worden helaas ook steeds beter."

**IN DEZE COMPLIANCE OFFICER VERBAAST ETHISCH HACKER VICTOR GEVERS ZICH OVER HET FEIT DAT ER NOG MET LINKS WORDT GEWERKT.** "Ik sprak Victor in het kader van het cybersecurityadvies van Herna Verhagen en hij heeft zeker een punt. Ik wil dit ook veranderen, maar dat gaat langzaam want onze klanten zijn het gewend. Wij zijn lid van de Veilige E-mail Coalitie die nieuwe standaarden ontwikkelt waarmee valse e-mails gemakkelijker kunnen worden herkend en tegengehouden. Maar ik zou eigenlijk willen overgaan op in-app-verkeer. Apps kun je beter afschermen. Ook de webshops waarvoor wij werken moeten dan stoppen met links in hun mailverkeer. We moeten mensen zelf naar hun site laten gaan om daar in te loggen, net zoals Mijnoverheid.nl dat doet."

**WAT ZIE JE ALS DE GROOTSTE CYBERBEDREIGING?** "Dan denk ik aan SCADA/ICS-systemen die worden gebruikt in de vitale procesindustrie zoals energiecentrales, raffinaderijen, waterzuivering en stormvloedkeringen. Deze systemen zijn niet zozeer ontworpen met oog op security, maar worden meer en meer verbonden met een intern netwerk en indirect ook met internet. Aanvallen hierop hebben direct impact op de fysieke wereld. Ook wij werken met deze systemen. Het stilvallen ervan is bij ons niet direct levensbedreigend, maar wel het laatste wat je wilt."

# DIGITAL TRUST CENTER: CYBERSECURITY WAARBORGT DE NEDERLANDSE DIGITALE ECONOMISCHE GROEI

THAI-HA VU

CYBERCRIME GROEIT AL JAREN EXPONENTIEEL EN VORMT HIERDOOR EEN GROTE BEDREIGING VOOR DE NEDERLANDSE ECONOMIE. VERTROUWEN IN DE DIGITALE WERELD IS VEREIST EN VERGT EEN GOEDE DIGITALE WEERBAARHEID VAN ONDERNEMINGEN. DE MINISTER VAN ECONOMISCHE ZAKEN MAAKTE IN EEN KAMERBRIEF D.D. 23 SEPTEMBER 2017 BEKEND DAT HET KABINET IN 2018 INVESTEERT IN DE OPRICHTING VAN HET DIGITAL TRUST CENTER (DTC).

Cybersecurity is de basis voor de kansrijke Nederlandse digitale economie, voor het vertrouwen van de consument in betrouwbare diensten en producten. Eveneens biedt het mogelijkheden om risico's van de processen van ondernemers te mitigeren. Vanwege het belang van onze economie, de Nederlandse economie, mogen zowel consumenten als ondernemingen bepaalde veiligheidswaarborgen verwachten vanuit de overheid. De minister van Economische Zaken gaf gehoor aan deze behoefte en maakte mede namens de staatssecretaris van Veiligheid en Justitie in een Kamerbrief de oprichting van het Digital Trust Center (DTC) bekend. In totaal maakt het ministerie € 26 miljoen beschikbaar voor het aanpakken van cyberspionage en -sabotage, de bestrijding van cybercrime en het oprichten van het DTC.

Door digitalisering ondervinden ondernemingen voordelen voor de export van kennis, producten en diensten. Ook kan digitalisering benut worden om de productiviteit te vergroten en de dienstverlening te verbeteren. Voorwaarde hierbij is dat ondernemingen een goede digitale weerbaarheid hebben. En dat er voldoende aandacht moet zijn voor cybersecurity. Dit betekent dat er inspanningen en investeringen door de ondernemingen gedaan moeten worden om de cybersecurity voor de organisatie te verbeteren. Pas wanneer de cybersecuritycirkel rond is, kunnen de economische kansen van digitalisering volledig door ondernemingen worden benut.

Mkb-bedrijven zijn het meest kwetsbaar voor cybercrime vanwege onvoldoende kennis over beveiliging en risico's. De mkb-bedrijven hebben behoefte aan actuele en heldere informatie, maar hebben ook baat bij objectieve adviezen over welke adequate maatregelen zij zouden moeten nemen. In het kader van de digitale veiligheid, is het voor deze bedrijven goed nieuws dat in 2018 het DTC wordt opgericht.

Bij het DTC kunnen ondernemingen terecht om meldingen te maken van cybercrime, maar ook voor vragen en advies. Om te komen tot een goede en gerichte informatiedeling en objectieve advisering aan ondernemingen, is een goede samenwerking tussen de overheid en het bedrijfsleven noodzakelijk. Het DTC zal ondernemingen ondersteunen om cyberweerbaar te zijn, met als gevolg dat de kennis-(economie) van Nederland niet weglekt.

In de Kamerbrief is aangegeven dat een basisniveau van digitale veiligheid en een goede informatie-uitwisseling tussen publieke en private organisaties van belang is.

Momenteel zijn enkel de Rijksoverheid en organisaties uit de vitale infrastructuur (water, energie en telecombedrijven) de doelgroepen met wie het Nationaal Cyber Security Centrum (NCSC) informatie uitwisselt. Dit betekent dat een heel groot deel van het bedrijfsleven geen toegang krijgt tot de kennis en kunde van het NCSC.
Het kabinet zal het DTC dusdanig vormgeven, dat zij dezelfde rol krijgt als het NCSC. Echter zal het DTC een andere doelgroep gaan bedienen. Het DTC zal generieke informatie uitwisselen over dreigingen en zal tevens adviseren en hulp verlenen bij incidenten. Het advies over o.a. maatregelen wordt zowel op algemeen als operationeel niveau gegeven. De ondersteuning die het DTC biedt zal afhankelijk zijn van het niveau van de vraag en zal daarom meer maatwerk moeten worden. Dat zal een uitdaging zijn, aangezien het DTC een grote doelgroep gaat bedienen, terwijl het NCSC een afgebakende groep organisaties binnen de overheid en vitale infrastructuur ondersteunt.

Het DTC zal ogenschijnlijk samenwerkingsverbanden aangaan. Het is de bedoeling dat intermediaire organisaties aanhaken en dat zij een natuurlijk en vertrouwd eerste aanspreekpunt zijn voor de bij hun aangesloten bedrijven. Dit kan worden ingericht op regionaal, sectoraal of op brancheniveau van bedrijven. Daarnaast dient er een digitaal platform te worden ontwikkeld, zodat bedrijven geholpen worden die (nog) niet zijn aangesloten bij een intermediaire organisatie.

De oprichting van het DTC is een blijk van bewustzijn van de gevolgen die digitalisering met zich meebrengt. Deze investering in vorm van kennisverwerving, kennisontwikkeling en kennisdeling is cruciaal om de Nederlandse digitale economie veiliger te maken. Dit voor ondernemers, maar ook voor het vertrouwen van de consument.

PAS WANNEER DE CYBERSECURITY-CIRKEL ROND IS, KUNNEN DE ECONOMISCHE KANSEN VAN DIGITALISERING VOLLEDIG DOOR ONDERNEMINGEN WORDEN BENUT.

# FR.UDE F.LM FESTIV .L 2017

RODERICK NOORDHOEK

OP VIJF EN ZES OKTOBER JL. WERD IN HET PRACHTIGE EYE FILMMUSEUM HET JAARLIJKS TERUGKERENDE FRAUDE FILM FESTIVAL (FFF) GEORGANISEERD. HOEWEL OP DE EERSTE DAG ALLEEN GENODIGDEN AANWEZIG MOGEN ZIJN (VEELAL OP UITNODIGING VAN SPONSOREN), STAAT HET FESTIVAL OP DE TWEEDE DAG OPEN VOOR HET PUBLIEK.

De opzet van het FFF is dat er binnen een tijdsbestek van ongeveer anderhalf uur een fraudethema wordt besproken door middel van een introductie, een film, en daarna een Q&A-sessie met de maker van de film en eventueel met specialisten op het betreffende thema. Het is dus door het vertonen van films dat het FFF aandacht probeert te geven aan het onderwerp fraude. Daarvoor sluit het FFF zich aan bij een uitspraak van Jean-Luc Godard (Franse filmregisseur en scenarist): "*Cinema is the most beautiful fraud in the world.*" Met deze paradoxale uitspraak, zeker gezien de doelstelling van het FFF, wist het FFF dit jaar zo'n dertienhonderd mensen te trekken.

Een belangrijk thema van het FFF was cybersecurity; een onderwerp dat in het verlengde van fraude ligt. Omdat dit ook het thema is van deze editie van de Compliance Officer, volgde ik een drietal inhoudelijke sessies (zonder film) die wellicht goed inzicht kunnen geven in cybersecurity in de toekomst.

Ik bevond mij de hele middag in het, tegenover het EYE gelegen A Lab. In dit voormalig Shell-laboratorium komen start-ups, technologiebedrijven, app-ontwikkelaars en andere creatievelingen op het gebied van media en technologie samen. In de A Lab-sessies werd – in afwijking op de rest van het programma – meer de focus gelegd op discussie en werden er alleen korte video's ter inspiratie vertoond. Tijdens deze sessies werd er gezamenlijk een blik op de toekomst geworpen, noem het 'crowdsourcing'.

De drie sessie die werden gegeven hadden de namen: 'Kan blockchain fraude uitbannen?', 'De verleiding', en 'The future of fraud'.

Hoewel de eerste sessie qua titel breder leek te zijn in opzet, werd toch vooral het onderwerp cryptovaluta behandeld. Op zich een interessant onderwerp als het gaat over fraude. Een voorspelling die werd gedaan, is dat wanneer er cryptovaluta ontworpen worden die alleen op vooraf te bepalen plekken uitgegeven kunnen worden (bijvoorbeeld een 'zorgcrypto' of 'verzekeringscrypto'), er minder fraude gepleegd kan worden. Misschien dat zo ooit het persoonsgebonden budget ook daadwerkelijk persoonsgebonden wordt?

Toch was er veel scepsis in de zaal toen de vraag werd gesteld: 'Kan blockchain fraude uitbannen?'. Dit heeft mede te maken met de onzekerheid over hoe deze technologie zich gaat ontwikkelen. Volgens de moderator van deze sessie is dat vergelijkbaar met het internetprotocol, voordat het wereldwijde web bestond. Het was toen al veelbelovend, maar had de steun van de massa nodig om het potentieel te kunnen definiëren.

Daarna volgde 'De Verleiding' waar in Lagerhuis opstelling twee tegenstrijdige gedachtes binnen het brein van een wethouder (in het eerste dilemma) en een douanier (in het tweede dilemma) werden nagebootst. Achteraf bleken er 'mollen' mee te discussiëren die het debat in een bepaalde richting wilde sturen. Zo leerde de deelnemers dat één gedachtegang onder druk de mens kan corrumperen.

Als laatste onderdeel van die middag kwam 'The future of fraud' aan bod. Onder begeleiding van Andrea Wiegman, fulltime trendwatcher bij de FIOD, mochten de deelnemers zich wanen in 2050 en fraude in de toekomst beschrijven. Voorafgaand kregen wij een goede inleiding op SciFi (wetenschappelijk onderbouwde fictie) en hoe vaak SciFi op termijn werkelijkheid wordt. Wiegman gaf hierbij aan dat de grote 'technerds der aarde' zich door deze films laten inspireren. Een wellicht aansprekend voorbeeld is het enorme scherm uit de film 'Minority Report'; het scherm bestaat inmiddels echt. Of het gebruik van hologrammen, wat voor het eerst voorkwam in Star Wars, maar nu realiteit is.
Na de motiverende woorden van de moderator over SciFi-denken als strategische tool, gingen de deelnemers in teams aan de slag om 'the next big thing' op het gebied van fraude in 2050 te voorspellen. Met alleen een aantal steekwoorden als off-grid, data deserts, crypto, DNA technology, en quantum computing, kwamen de meest bizarre scenario's naar voren.

JEAN-LUC GODARD:

## "CINEMA IS THE MOST BEAUTIFUL FRAUD IN THE WORLD."

Als we de deelnemers mogen geloven, dan leven burgers in 2050 als nomaden (e-citizenship), is er één privaat bedrijf dat oppermachtig wordt en meer weet dan de mens (singularity[1]), heeft men de mogelijkheid om DNA via de blockchain te verhandelen en kan men daarmee een persoonlijkheid kopen (DNA technology). Een vrij heftig vooruitzicht zo op de vrijdagmiddag.

Uiteindelijk bleek het moeilijk om te voorspellen op welke wijze hiermee gefraudeerd zou kunnen gaan worden. Wat wel te verwachten is, is dat vormen van fraude en cybercrime in de toekomst steeds persoonlijker worden.

1 De moeite waard om te 'googlen'.

# OPLEIDING PRIVACY OFFICER

28, 29 NOVEMBER 2017

De Opleiding Privacy Officer geeft u in twee dagen een overzicht van diverse actuele (wettelijke) privacyonderwerpen. Tijdens de opleiding wordt onder meer aandacht besteed aan: de taken van de privacy officer, het ontwikkelen en implementeren van een privacyprogramma, het uitvoeren en interpreteren van een risicoanalyse, en het monitoren van privacygevoelige processen, producten of diensten.

De Opleiding Privacy Officer heeft als doel de deelnemers inzicht te verschaffen in de meest actuele ontwikkelingen die voor de uitoefening van de functie van privacy officer van belang zijn.

De gerichte benadering en de kleine setting van deze opleiding biedt u voldoende gelegenheid tot interactie met de docenten en de andere deelnemers.

Wilt u meer informatie over de opleiding Privacy Officer? U kunt altijd Martin Vente contacten via 088 - 99 88 100 of via vente@compliance-instituut.nl

## COMPLIANCE-AGENDA

| | |
|---|---|
| 07 NOVEMBER | Masterclass Zorgplicht |
| 21 NOVEMBER | Compliance & Integriteit voor HR-professionals |
| 21 NOVEMBER | VBIN Update Compliance |
| 28, 29 NOVEMBER | Opleiding Privacy Officer |
| 14 DECEMBER | Nationaal Compliance Congres |

**2018**

| | |
|---|---|
| 01 FEBRUARI | Leergang Compliance Officer in de Zorg |
| 14 FEBRUARI | Leergang Compliance Professional |
| 14 FEBRUARI | Leergang Compliance Officer |
| 08 MAART | Leergang Compliance Officer Pro |
| 22 MAART | Introductie Compliance |
| 04 APRIL | Opleiding Privacy Officer |
| 05 APRIL | Leergang Bestrijding witwassen en terrorismefinanciering |
| 12 APRIL | Leergang Dutch Caribbean |

NATIONALE COMPLIANCE AWARD

# NOMINEER NU VOOR DE NATIONALE COMPLIANCE AWARD 2017

**Kent u iemand die:**
- **baanbrekend werk heeft verricht op het terrein van compliance en integriteit;**
- **grote mate van collegialiteit en bereidheid tot samenwerking heeft getoond;**
- **sectorbreed actief betrokken is bij kennisoverdracht;**
- **innoverende ideeën heeft;**
- **regelmatig publiceert op het terrein van compliance en integriteit;**
- **voorstellen heeft ontwikkeld die bijdragen tot verhoging van efficiency en kwaliteit van compliance?**

NOMINEER HEM/HAAR DAN VOOR DE NATIONALE COMPLIANCE AWARD 2017 EN ONTVANG HET JAARBOEK COMPLIANCE 2018 ALS DANK.
U HEEFT NOG TOT 30 NOVEMBER A.S.

Nomineren gaat via onze website:
compliance-instituut.nl/over-ons/compliance-award-2
Hier vindt u tevens aanvullende informatie over de Compliance Award.

**VOOR DE NOMINATIE VRAGEN WE MINIMAAL DE VOLGENDE GEGEVENS:**
- Naam genomineerde
- Beroep
- Functie
- Motivatie van tenminste tweehonderdvijftig woorden
- NAW-gegevens aandrager

De nominatie moet zowel naar ons als naar Notariskantoor Van der Hammen worden verstuurd. Dit gebeurt automatisch; zodra u op de button ‘Nomineren’ klikt, verschijnt er een e-mailbericht welke geadresseerd is aan Notariskantoor Van der Hammen en aan ons.

# NCC

## NATIONAAL COMPLIANCE CONGRES

14 DECEMBER 2017

COMPLIANCE-INSTITUUT.NL/NCC