iB

INFORMATIEBEVEILIGING

jaargang 18 - 2018

#2

Interview met Lex Borger en Kas Clark

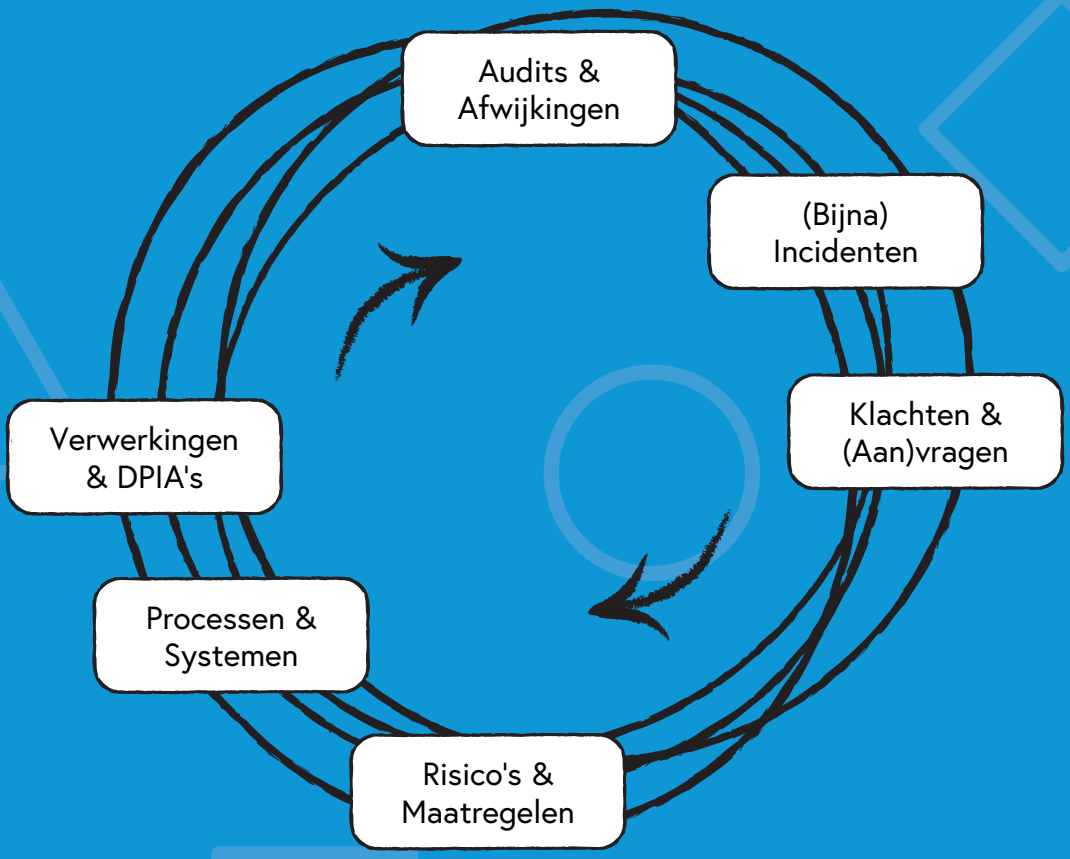
Omgaan met medische behandelplannen

Global agenda for cyber capacity building

Zicht en grip op informatie

De meest complete Privacy / AVG / GDPR Software

smile



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

Start nu gratis! Kijk snel op: privacysuite.eu

VERS BLOED

Alweer de tweede keer dat ik dit voorwoord mag schrijven (ook in iB2 van 2017 was het voorwoord van mijn hand). Tom heeft al uitgelegd dat we, sinds het vertrek van Lex Borger als hoofdredacteur, deze rol afwisselen tussen de zittende redactieleden. Met zes redactieleden zou dat theoretisch geen probleem moeten zijn met zes nummers iB, maar de praktijk is (zoals gebruikelijk) weerbarstiger. Op dit moment weten we nog niet wie u als auteur van het voorwoord van iB3 (en dus hoofdredacteur voor dat nummer) gaat aantreffen. Wel is duidelijk dat er mutaties in de samenstelling van de redactie zullen plaatsvinden. Vandaar dat ik vanaf deze plaats een dringende oproep aan alle PvIB-leden wil doen. Heeft u interesse om toe te treden tot de redactieraad, laat dan van u horen via IBmagazine@pvib.nl. Vers bloed is bijzonder welkom, mede vanwege de veranderingen die Tom al beschreef in het voorwoord bij iB1. Als u een of meerdere artikelen wilt schrijven, bent u natuurlijk ook van harte welkom!
In dit nummer blikken Lex Borger en Kas Clark terug op hun tijd als respectievelijk hoofdredacteur en redacteur van iB. Ook gaan zij in op de veranderingen van publiceren op papier, dat gepaard gaat met harde deadlines (i.v.m. capaciteit bij opmaker en drukker), naar het online publiceren wat vaker en sneller en op elk gewenst moment kan plaatsvinden. Achter de schermen zijn vele vrijwilligers binnen PvIB bezig met deze verandering, waarbij de PvIB website een cruciale rol zal spelen.
Naast de gebruikelijke columns van Berry, de Attributer en natuurlijk Rachel Marbus (aan wie we sinds het vorige nummer natuurlijk allemaal wat vaker denken ;-), kunt u (onder andere) het derde deel van het drieluik over "Cyberveilig gedrag" van Inge Wetzer lezen.
Tot slot nog een opmerking over artikelen (of voorstellen van artikelen) die we regelmatig ontvangen die, al dan niet subtiel, bepaalde producten of diensten beschrijven. Natuurlijk willen wij onze lezers graag op de hoogte brengen van nieuwe ontwikkelingen, maar het moet geen reclame worden. Als een artikel het betreffende product of dienst in perspectief plaatst en vergelijkt met andere, dan kunnen we (soms met wat redactionele aanpassingen) meestal tot plaatsing overgaan. Natuurlijk is adverteren in iB altijd mogelijk, maar dat gaat buiten de redactie om.

Veel leesplezier!
Lex Dunn

In dit nummer

INTERVIEW

Lex Borger en Kas Clark over hun afscheid van iB magazine:

‘WE LATEN ONS GRAAG VERRASSEN DOOR ONZE OPVOLGERS’

Het was toch wel even wennen begin februari. Voor het eerst sinds jaren viel het iB magazine bij Lex Borger op de mat zónder dat hij wist welke artikelen erin stonden. ‘Eerste iB magazine van het redactieteam, nu zonder mij. Goed gedaan!’, tweette de kersverse voormalig hoofdredacteur van het magazine dat u nu leest. Om vervolgens direct het blad op te pakken en te gaan lezen.

"Hoe anders was dat de afgelopen jaren", blikt Lex terug. "Als het magazine in de bus viel, legde ik het eerst even weg. Ergens in een hoekje. Ik kende de inhoud immers al. Misschien wel iets te goed…", zegt hij glimlachend. "Nu laat ik me weer graag verrassen."

Vierenvijftig uitgaven van iB magazine verschenen in de afgelopen zeven jaar onder de verantwoordelijkheid van Lex als hoofdredacteur. En ook daarvoor was hij al zo'n vier jaar lid van de redactie. iB magazine was voor hem een 'way of life' geworden.
De ervaring echt verrast te worden door ons magazine heeft Kas Clark, ruim vier jaar lid van de redactie, de laatste jaren ook niet meer. Maar binnenkort zal dat ook voor hem veranderen. Kas draagt het redactiestokje namelijk over aan een collega van het Nationaal Cyber Security Centrum (NCSC). Om vervolgens zelf een nieuw avontuur in Amerika te beginnen. Waar hij hoopt op de hoogte te kunnen blijven van het werk van zijn voormalig redactiecollega's. En dan vooral via de online versie van het magazine.

Fysiek magazine en/of online?

Die laatste vaststelling brengt ons meteen op het eerste onderwerp dat we graag met deze oude rotten in het vak willen bespreken. iB magazine is nog altijd een blad in de vorm van een fysieke uitgave. "Nog wel", zegt Lex. En dat zal volgens hem nog wel even zo blijven. "De steeds weer terugkerende uitgave-cyclus van het blad biedt structuur. Een stok achter de deur. Zou je kiezen voor alleen online, dan ben je die vastigheid als redactie kwijt. Online wordt het allemaal wat vrijblijvender. Deadlines zijn geen deadlines meer. Want je kunt immers altijd publiceren."
"Online ben je dus veel dynamischer", haakt Kas in. Een conclusie die Lex onderstreept. "Een artikel hoeft niet helemaal af te zijn voor je online tot publicatie overgaat", geeft hij aan. "Je kunt immers updates, nieuwe meningen en invalshoeken blijven toevoegen." De online ontwikkeling van het magazine is daarom, wat de voormalig hoofdredacteur betreft, zeker een onderwerp dat bij de huidige redactie hoog op de agenda zou moeten blijven staan. En dat is ook het geval, zo weet hij. Waar je online volgens beide heren echter voor moet waken, is meegaan in louter 'hypegedrag'. De snelheid waarmee je online kunt acteren, betekent dat alles veel vluchtiger wordt, waarschuwen ze. "Terwijl we er met het magazine juist naar streven om bepaalde onderwerpen van verschillende kanten te belichten. We willen lezers een complete blik op een bepaald onderwerp bieden. Dat is wat mij betreft de meerwaarde van iB magazine", vindt Kas. Online is dat verdiepen van security-onderwerpen volgens beiden wat lastiger, omdat de presentatie dus vluchtiger is, maar ook omdat je moet concurreren met vele sites waar korte nieuwsberichten elkaar in razend tempo opvolgen.

Belangrijkste verandering

Die snelheid qua ontwikkelingen die spelen, is volgens Lex misschien wel de belangrijkste verandering die hij gedurende zijn tijd in de redactieraad heeft meegemaakt. Hij herinnert zich nog een artikel uit zijn begintijd: 'Stuxnet - de zomerhit van 2010'. Een artikel dat hij samen met Maarten Hartsuijker schreef. Voor de uitgave die in november 2010 uitkwam…

Dat zou nu volgens hem niet meer kunnen, zo'n 'uitgestelde publicatie', zoals hij het artikel met terugwerkende kracht noemt. "Kijk alleen maar naar de eerste paar weken van dit jaar. De security-onderwerpen duikelen in het nieuws over elkaar heen." En hij noemt de onthulling van Nieuwsuur en de Volkskrant dat de AIVD minimaal een jaar mee kon kijken met Russische hackers, de DDoS-aanvallen op sites van banken en de Belastingdienst, maar ook de Meltdown- en Spectre-kwetsbaarheden waarmee we het jaar begonnen.
"Moesten we in mijn begintijd nog echt op zoek naar onderwerpen die we konden belichten, nu liggen de onderwerpen voor het oprapen", concludeert Lex. Ook in de reguliere media is security volgens beide heren immers een 'hot topic'. Dat betekent voor iB magazine dat de toegevoegde waarde wat hen betreft steeds

Sandra Kagie is freelance tekstschrijver/journalist. Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & 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.

Stuxnet - de zomerhit van 2010

nadrukkelijker in de echt doorwrochte, complete artikelen zit. "De duiding voor onze lezers. Wat betekenen ontwikkelingen op securityvlak voor hen als professionals in de praktijk. Hoe ervaren zij bepaalde nieuwe regels en wetgeving", vult Kas in. "Ik denk dat we in de belichting daarvan een heel belangrijke rol hebben. "

'Vakgebied is volwassen geworden'

Er is de afgelopen jaren dus heel veel veranderd in securityland. Ontwikkelingen die volgens Lex en Kas misschien nog wel het best zijn samen te vatten met de vaststelling 'dat security definitief zijn intrede heeft gedaan in de boardrooms van bedrijven en organisaties'. "Het vakgebied is volwassen geworden", concluderen ze.
Toch zijn er ook zaken niet of nauwelijks veranderd, geeft Kas aan. "Ter voorbereiding op dit gesprek ben ik eens gaan bladeren in magazines van vijf jaar geleden. Om te zien waar we ons toen zorgen over maakten. En wat opvalt, is dat dit ook grotendeels zaken waren waar we ons nu nog druk om maken. Denk aan het gebrek aan awareness op de werkvloer en de mogelijkheden of onmogelijkheden qua beleid om deze bewustwording te vergroten. Zwakke wachtwoorden zijn nog steeds een ding en er wordt nog altijd massaal geklikt op foute links."

Onderwerpen voor de toekomst

Natuurlijk leggen we beide heren ook de vraag voor welke onderwerpen zij de komende tijd sowieso hopen terug te zien in iB magazine. En wat blijkt, ideeën zijn er voldoende! Zo hoopt Lex dat een onderwerp als API (Application Programming Interface)-security aandacht zal krijgen in één van de komende uitgaven. Want die almachtige achterliggende structuur waardoor programma's onderling kunnen communiceren, blijkt volgens hem steeds vaker misbruikt te worden door kwaadwillenden. "Die structuur moet dus veiliger. En daar zou ik graag meer over lezen", geeft hij aan. Een tweede onderwerp dat hij noemt, is Blockchain, een topic waar natuurlijk al heel veel over geschreven is en wordt. Maar waar Lex speciaal naar uitkijkt, is een artikel over de eerste echt succesvolle praktische toepassing ervan.
Ook hoopt hij dat zijn opvolgers het thema professionalisering van de beroepsgroep zullen blijven belichten. 'De formalisatie van het vakgebied', zoals hij het noemt, is immers bij uitstek een thema waaraan het PvIB wat hem betreft een belangrijke bijdrage heeft geleverd en nog altijd levert. En hij verwijst naar de Whitepaper Beroepsprofielen Informatiebeveiliging, gepubliceerd in mei 2014, gevolgd door een 2.0 versie in januari 2017, waarin de verschillende beroepsprofielen en bijbehorende competenties zijn neergezet. "De basis van een uniform kwalificatiestelsel binnen ons vakgebied dat er absoluut moet komen. Een ontwikkeling die ik via het magazine graag wil blijven volgen."
Om tot slot van dit 'hoofdstuk' te pleiten voor nog wat meer kruisbestuiving tussen de redactie en de commissie Kennis & Innovatie van het PvIB. Een samenwerking die wat Lex betreft zou moeten leiden tot het structureel inbedden van 'innovatie' als thema in iB magazine.

Buzzwords 'graag in samenhang'

Kas op zijn beurt hoopt vooral dat er in de komende uitgaven van het magazine ruimte is voor de belichting van drie ontwikkelingen die wat hem betreft heel nauw met elkaar samenvallen. Te weten: big data, machine learning en cyber threat intelligence. 'Buzzwords' die volgens hem binnen veel organisaties enorme verwachtingen scheppen. "Er worden binnen organisaties massaal potjes geclaimd om hiermee aan de slag te gaan", weet hij.
"Ik zou de buzzwords in samenhang terug willen zien in ons blad. Hoe gaat dit in de praktijk werken? Wanneer we slimme algoritmes loslaten op heel veel data, creëren we dan automatisch slimme intelligence? Ik vraag het me af. De resultaten tot nu toe vallen nog tegen. Ik ben benieuwd naar bijvoorbeeld een thema-uitgave rond artificial intelligence en de werking hiervan in de praktijk. In de komende jaren gaan we de zin en de onzin op dit vlak van elkaar scheiden. Een ontwikkeling die we in ons blad zeker moeten volgen."

Succesnummers

Ideeën genoeg dus van beide heren voor hun opvolgers. Maar wat zijn eigenlijk de uitgaves van iB magazine waar zij met het meeste plezier of misschien wel trots op terug

kijken? Privacy is volgens beiden een thema dat het altijd goed doet. Zo'n themanummer kun je dan ook elk jaar laten terugkomen, geven ze aan. Het is en blijft interessant.

Een uitgave die Kas zich nog heel goed kan herinneren, is er één uit zijn begintijd, rond Shellshock en Heartbleed. "Er speelde toen een levendige discussie rond open source software. Waarin er echt sprake was van verschillende kampen. In het magazine hebben we die discussie bijna filosofisch opgepakt. In de discussie mengden zich namelijk ook niet-security mensen die over security gingen schrijven", herinnert Kas zich. Een interessante ontwikkeling die wat hem betreft leidde tot een memorabele uitgave.

Boodschap voor opvolgers

En nu kijken beide heren dus uit naar nieuwe memorabele en verrassende uitgaves van hun opvolgers. Iets waar ze alle vertrouwen in hebben. De veelheid van meningen en personen binnen de redactie gaat hier volgens hen zeker voor zorgen. Want als ze iets binnen de redactie altijd hebben gewaardeerd, is het wel die diversiteit, die zorgt voor een brede blik op ontwikkelingen die spelen.
Lex: "iB magazine moet wat mij betreft meer zijn dan tromgeroffel. Het draait om dingen die je zelf op professioneel vlak meemaakt, terug willen geven. Jouw kennis en ervaring willen delen met andere professionals. Inhoudelijk moeten we van belang zijn voor de professionele security-community. "

Enkele iconische covers van iB magazine, de keuze van Lex Borger en Kas Clark.

Wetenswaardigheden en foutjes, een compilatie samengesteld door onze oud-hoofdredacteur:

2011-1 – Foto-cover #1: Toen ik hoorde dat het voorstel was dit toetsenbord op iedere uitgave te gebruiken, heb ik ingegrepen en jarenlang voor ieder nummer een unieke cover gezocht.
2011-8 – Mijn favoriete cover, het trojaanse paard (Locatie FAO Schwarz in Forum Shops Las Vegas)
2012-8 – Het leukste interview dat ik heb gehad met Gary McGraw.
2013-7 – De zombie-cover waar we een klacht over kregen: hij was te eng! Het magazine kwam op Halloween uit.
2013-7 – De verantwoorde onthulling die het meest spannend was om te redigeren, omdat ik hem zelf had meegemaakt.
2014-6 en -8 – Voorpagina's: Zoek de verschillen
2015-3 – Wij hadden ze vroeg in beeld: Redsocks interview
2015-3 – Pagina 14: Drukfout in de kop, daar had dus iedereen overheen gelezen…
2015-5 – Voorpagina: Drukfout of opzet? Alleen de redactie weet het zeker

Illustratie: Copyright Hoffmann Cybersecurity B.V.

PSYCHOLOGEN OVER CYBERVEILIG GEDRAG: HANDVATTEN VOOR DE PRAKTIJK

De integrale visie op cybersecurity wint de laatste jaren enorm terrein: veel organisaties zijn er zich van bewust dat cybersecurity een technische, een organisatorische én een menselijke component heeft. Om een stap verder te kunnen zetten in de menskant, combineerde Hoffmann expertise op het gebied van cybersecurity met die van psychologie. Dit resulteert in een vernieuwende aanpak die zich richt op het daadwerkelijke gedrag van medewerkers van een organisatie; wat is ervoor nodig om dat meer cyberveilig te maken? Dit artikel is het laatste van een drieluik dat PVIB hierover publiceert. Het huidige artikel gaat in op de maatregelen die organisaties kunnen nemen om het gedrag van hun medewerkers cyberveiliger te maken. Deze inzichten komen voort uit recente onderzoeken in verschillende typen organisaties. Ze laten zien hoeveel meer mogelijkheden dan alleen awareness-trainingen een organisatie heeft die de menskant van cybersecurity wil aanpakken.

Artikel 3 van Drieluik cyberveilig gedrag

De toenemende aandacht voor de menskant van cybersecurity is een feit. De inzet van gedragskundigen daarbij, blijft echter achter. Tijdens de opkomst van cyberaanvallen was er vooral behoefte om het bewustzijn over de risico's bij werknemers te verhogen. Dit wordt gedaan in velerlei vormen, zoals awareness trainingen, e-learnings of games. Echter, steeds meer blijkt de awareness van medewerkers wel in orde: men wéét wel wat er van hen wordt verwacht (Wetzer, 2017a). Toch blijft het gewenste gedrag achter. In een programma ontwikkeld door psychologen dat zich specifiek richtte op de gedragskant van cybersecurity, werd duidelijk waarom: gedrag bestaat naast awareness uit nog twee factoren: motivatie (wíl iemand het wel?) en gelegenheid (wordt iemand wel in staat gesteld om het te doen?). Het eerste artikel uit dit drieluik gaf inzicht in welke specifieke gedragingen door organisaties onder 'cyberveilig gedrag' worden verstaan. Het is immers belangrijk dat gedrag heel specifiek gedefinieerd wordt. Een breed begrip als 'cyberveilig gedrag' kan immers niet gemeten of veranderd worden (Wetzer, 2017b). Het tweede artikel van dit drieluik (Wetzer, 2018) gaf inzicht in de redenen voor de afwezigheid van gedrag: Wat houdt mensen nou tegen om het gewenste gedrag te vertonen? De inzichten uit die onderzoeken maken het mogelijk om nu de belangrijke vervolgstap te zetten: gegeven dat we weten waarom mensen soms toch niet cyberveilig handelen, wat kunnen organisaties dan aan maatregelen nemen om dat te veranderen?

Cyberveilig gedrag: waarom dóen we het nog niet?

In het vorige artikel uit dit drieluik werd inzicht gegeven in de redenen voor het ontbreken van gedrag. Dit inzicht is ontstaan uit een onderzoek dat een team van psychologen van Hoffmann in 2017 heeft gehouden onder meer dan 100 medewerkers van verschillende organisaties. Het meten waarom gewenst gedrag niet optreedt, gebeurde door middel van diepte-interviews met werknemers uit een bepaalde doelgroep. In deze interviews zoomden de psychologen in op concrete gedragingen die door management of (C)ISO's van de betreffende organisaties waren benoemd als gewenst. De open gesprksstructuur en de gesprekstechnieken van de psychologen leidden tot nieuwe inzichten in het waaróm van het ontbreken van het gewenste gedrag. Een aantal belangrijke conclusies uit dit onderzoek luidden:

- **Het ontbreekt regelmatig aan motivatie of gelegenheid**
  Hoewel awareness programma's zich in grote mate richten op het verhogen van de capaciteit, is het ontbreken van capaciteit vaak niet de oorzaak van waarom medewerkers zich niet cyberveilig gedragen.
- **Risico-inschatting is vaak laag**
  Risico bestaat uit kans (dat het mis gaat) x impact (gevolgen als het mis gaat). De resultaten toonden aan dat veel werknemers maar met één van deze twee rekening houden en de andere bagatelliseren.
- **Vriendelijkheid gaat vaak boven veiligheid**
  Medewerkers zijn soms minder gemotiveerd om zich veilig te gedragen omdat dat voor hen voelt als sociaal onwenselijk (denk aan het weigeren om telefonisch informatie te verstrekken).
- **Als awareness ontbreekt, dan gaat het om een specifiek element**
  Op het moment dat awareness wel de oorzaak is van het ontbreken van gedrag, is het belangrijk om te weten welk specifieke stuk awareness ontbreekt. Zo kan gerichter getraind worden.
- **Gemakzucht verklaart, maar minder dan gedacht**
  Soms speelt gemakzucht wel een rol in het verklaren waarom medewerkers iets niet doen, maar meestal is het niet de enige reden en is het aandeel maar beperkt.

Maatregelen uit de praktijk

Als duidelijk is waaróm mensen iets nu niet doen, kan vervolgens concreet gekeken worden naar maatregelen: Wat kan een organisatie doen om de oorzaak aan te pakken? Inzicht in de oorzaken voor het ontbreken van gewenst gedrag geeft dus handvatten voor gerichte interventies. Aan de hand van de inzichten uit het vorige artikel van dit drieluik, wordt hier besproken welke interventies in de praktijk veel voorkomen.

Sleutelen aan gelegenheid

In het geval dat gelegenheid een ontbrekende factor is, kan een organisatie het gedrag veranderen door de gelegenheid te creëren. De werknemers wílen de gewenste gedragingen immers wel vertonen, maar worden door omstandigheden niet in staat gesteld. Deze omstandigheden veranderen is in deze gevallen de sleutel naar gedragsverandering. In het onderzoek dat Hoffmann

Dr. Inge Wetzer is sociaal psycholoog cybersecurity bij Hoffmann Cybersecurity. Inge is te bereiken via i.wetzer@hoffmannbv.nl

een jaar lang bij uiteenlopende organisaties heeft gedaan, bleek dat de gelegenheidsoplossing voor gedragsverandering vaker dan gedacht het antwoord was. Te denken valt aan het plaatsen van shredders in kantoren om het veilig weggooien van vertrouwelijke documenten te vergemakkelijken, het beschikbaar stellen van afsluitbare kasten om vertrouwelijke documenten veilig op te bergen of het aanbieden van pashouders die aan de wensen van de werknemers voldoen.

Veiliger gedrag door meer realistische risico-inschatting

Een andere reden voor de afwezigheid van veilig gedrag is dat men de neiging heeft om het risico van een incident te laag in te schatten. Dit kan gaan over de kans ("hier kan echt niemand binnen komen") maar ook over de impact ("dan is hier iemand binnen … en dan?"). Wanneer het risico wordt onderschat, is men automatisch minder gemotiveerd om zich veilig te gedragen. Een veel geadviseerde maatregel om de kans inschatting realistischer te maken, is door simpelweg te laten zien hoe eenvoudig sommige handelingen zijn. Dit kan bijvoorbeeld door met een inlooptest te laten zien hoe makkelijk het is om in iemands kantoor te komen zonder te worden aangesproken, of door een nep-phishingmail te versturen die aantoont hoe snel men toch nog op een besmette link klikt. Wanneer niet de kans, maar juist de impact wordt onderschat, zijn weer andere interventies van toepassing. Hier kan bijvoorbeeld gedacht worden aan een crisisoefening, waarin men de consequenties van een bepaald incident uitwerkt. In plaats van dat medewerkers overtuigd worden van de ernst van de gevolgen van een incident, bedenken zij in een dergelijke oefening die gevolgen zelf, wat hun motivatie zal verhogen.

Veilig hoeft niet onvriendelijk: geef handvatten

In het tweede artikel van dit drieluik werd beschreven dat medewerkers soms moeite hebben om zich veilig te gedragen, omdat zij het veilige gedrag als onbeleefd ervaren. In deze gevallen speelt de factor motivatie een belangrijke rol: men is minder gemotiveerd om zich veilig te gedragen, omdat dat een gevoel van onvriendelijkheid met zich meebrengt. Denk aan het sluiten van de deur voor iemands neus, het aanspreken van een onbekende of het niet verstrekken van gevraagde informatie. De interventie om dit veilige gedrag te stimuleren, zou dus moeten aangrijpen op die lage motivatie. Een duidelijk voorbeeld hiervan is dat medewerkers handvatten krijgen om wel het gewenste veilige gedrag te vertonen, zonder dat ze zich onbeleefd voelen. Je kunt bijvoorbeeld bruut de deur voor iemands neus sluiten, maar je kunt ook tegen die persoon zeggen dat het de bedoeling is dat binnen iedereen een pas draagt en vervolgens aanbieden om even met die persoon naar de receptie te lopen. Een groot deel van de veilige gedragingen kan worden omgezet in gastvrijheid, als men eenmaal heeft geleerd hoe dit moet. Het aanspreken van een onbekende klinkt helemaal niet meer onvriendelijk als je vraagt naar wie diegene op zoek is en of je hem kunt helpen.

Lessen uit de psychologie in de praktijk

De toepassing van psychologie in het veld van cybersecurity en een jaar praktijkervaring bij uiteenlopende organisaties heeft geleid tot belangrijke nieuwe inzichten in de 'menskant' van cybersecurity. Op basis van deze inzichten kan inmiddels een volgende stap gezet kan worden in het weerbaar maken van medewerkers. Dit drieluik beschreef deze inzichten en een aantal belangrijke lessen:

Kijk verder dan awareness

Dit artikel laat zien dat er legio maatregelen zijn die kunnen helpen bij het creëren van cyberveilig gedrag. In de tijd dat de cyberdreigingen nog nieuw en onbekend waren, was awareness de belangrijkste stap aan de menskant. Logisch en terecht; om je veilig te kunnen gedragen, moet je eerst weten wat de risico's en de gevaren zijn. Er is alleen een tendens ontstaan, dat men is blijven hangen in het creëren van bewustzijn, terwijl het merendeel van de werknemers inmiddels wel wéét dat men ook in de digitale wereld risico's loopt. Dit artikel focust op het uiteindelijke doel; gedragsverandering. Awareness is daarin een noodzakelijke stap, maar niet voldoende om op zichzelf tot effectieve gedragsverandering te leiden.

Andere maatregelen leiden tot meer structurele gedragsverandering

Een vraag die bij awareness-trainingen (inclusief e-learnings en games) vaak gesteld wordt, is hoe lang het beklijft. Een terechte vraag. Medewerkers worden op een bepaald moment bewust gemaakt van bepaalde risico's en dan heeft dat even veel aandacht. Vervolgens gaat men over tot de orde van de dag en gaan andere factoren zoals tijdsdruk en gemak een rol spelen. De nieuw verworven awareness wordt hierdoor weer naar de achtergrond gedrukt en de impact van de interventie neemt daarmee af. Een interessant gegeven is dat bij andere typen interventies, zoals die gericht zijn op het verhogen van gelegenheid, geen sprake meer is van het beklijven van het nieuwe gedrag. Wanneer gedrag veranderd is, doordat er gesleuteld is aan de gelegenheid, is de verandering permanent. Bijvoorbeeld; er is een tussendeur geplaatst, waardoor men de pas wel bij zich móet dragen, of men heeft geen papierbak op het eigen kantoor meer, dus men moet wel naar de papiercontainers lopen en kan dan net zo makkelijk kiezen voor de beveiligde container als het gevoelige informatie betreft. Omdat het nieuwe gedrag niet leunt op awareness, maar op veranderingen in de omgeving, is de gedragsverandering daarmee structureler en dus stabieler.

Referenties

Wetzer, I. M. (2017a). Voorbij awareness; grip op cyberveilig gedrag. 'InformatieBeveiliging', 17 (3), 24-26.

Wetzer, I. M. (2017b). Cyberveilig gedrag: Meer dan alleen het locken van je beeldscherm. 'InformatieBeveiliging', 17 (6), 4-7.

Wetzer, I. M. (2018). Cyberveilig gedrag: Waarom dóen we het nou niet? 'InformatieBeveiliging', 18 (1), 12-15.

Mr. Rachel Marbus
@rachelmarbus op Twitter

HELP ANDEREN DOOR ONZIN HEEN TE PRIKKEN

De gemiddelde Nederlander gelooft doorgaans wat hem verteld wordt over privacy of veiligheid. Zeker als dat gebeurt op het nieuws. Dat is niet zo gek. De gemiddelde Nederlander heeft niet het arsenaal aan kennis om door privacy,- en securityonwaarheden heen te prikken. En soms levert dat wat telefoontjes op van bezorgde familieleden: "…maar de banken zijn dus niet gehackt zeg je? En is mijn geld wel echt veilig dan? Gaan de automaten geen geld spugen?". Het Rijbroek-incident staat ook niet op zichzelf, een beetje desinformatie en ongeïnformeerde lekenbralpartijen zijn van alle tijden. Aan ons om daar tegen op te treden en mensen van de juiste informatie te voorzien.

Het kan nog erger. Waar het in het voornoemde incident vooral ging over FUD-zaaien met foute informatie, kun je ook de andere kant bespelen. Mensen een vals gevoel van veiligheid en een vals gevoel van privacy geven. Dat is exact waar Facebook op dit moment mee bezig is. Ik weet het, Facebook is laaghangend fruit, maar wacht heel even met oordelen en lees tot het einde door.

De sociale netwerksite promoot Onavo, een (lees: haar)VPN securityapp. Nu heb ik bij mijn familie erin gestampt dat ze een VPN moeten gebruiken om zichzelf en hun data te beschermen als ze het net op gaan. En dat dan met de analogie van de condoom. Ach, u voelt hem wel, nietwaar? Het is voor u en voor mij natuurlijk geen verrassing dat die app alle data doorstuurt naar Facebook. Maar voor de gemiddelde Nederlander wel! De Consumentenbond sprong er meteen bovenop en waarschuwde om de app niet te gebruiken. Dat bericht van de Consumentenbond ebt straks weer weg in de waan van de dag, die app van Onavo zie ik echt niet zomaar verdwijnen.

Nog eentje dan. Het zal u niet ontgaan zijn dat toezichthouders in Europa (zowel privacy toezichthouders als die van mededinging) met verve achter de praktijken van Facebook aangaan. De ene na de andere handhavende actie krijgt het bedrijf op zijn bord. Superirritant natuurlijk en dan vooral voor je reputatie. Facebook is daarom begonnen met een privacy-charmeoffensief. Het mooiste voorbeeld daarvan trof ik pasgeleden op mijn eigen timeline aan. Een post met de boodschap "Je privacy is goed geregeld bij ons. Je gegevens zijn jouw eigendom. We doen niets zonder jouw toestemming." Onder het bericht kon je vragen stellen. Ik vroeg of ze dus de niet-exclusieve licentie op de intellectuele eigendomsrechten hadden laten vervallen uit de voorwaarden? "Super interessante ontwikkeling!", schreef ik er nog bij.

U raadt het wel. Ieders vraag werd netjes beantwoord. De mijne niet natuurlijk. Dus heb ik dat zelf maar even erbij gedaan (een weekje later, ik wilde ze natuurlijk nog wel een kans geven zelf te antwoorden). Enfin. Die niet-exclusieve licentie staat er uiteraard nog steeds in. Ze kunnen je juridisch gezien inderdaad eigenaar noemen, alhoewel dat in Europa een incorrecte term is als het gaat om persoonsgegevens. Alleen is het een sigaar uit eigen doos, want je hebt met het aanvaarden van de voorwaarden die niet-exclusieve licentie gegeven op jouw gegevens. En dus mag Facebook jouw gegevens uitnutten voor eigen gewin. Weg is je privacy. Het is dus echt je reinste onzin. En dan hebben we het nog niet eens gehad over die zogenaamde 'toestemming'. Maar daarover wellicht een andere keer meer. En in de tussentijd blijf ik strijden tegen dit soort onzin en ik hoop u ook.

OMGAAN MET MEDISCHE BEHANDELPLANNEN

Lessons learned voor security actieplannen

Vroeg of laat krijgen we allemaal zelf of voor een dierbare te maken met een medisch behandelplan. Ik bedoel daarmee een combinatie van medicijnen, ingrepen, operaties, diëten en/of fysiotherapie. Als leek op medisch gebied die de behandeling moet ondergaan, is het moeilijk zo'n behandelplan op nut en noodzaak te beoordelen. Voor mezelf heb ik daarbij een vuistregel, die ik graag met u deel.

Wanneer de behandeling als 'werkend' wordt geadviseerd door een ervaren (meestal oudere) arts, accepteer ik dat advies meteen. Immers, deze doctor heeft al jarenlang ervaring met deze aanpak, het is proven technology. Hij heeft die ene ingreep al vaak met succes uitgevoerd en de positieve resultaten van een bepaald dieet al vele malen mogen aanschouwen. Als de man/vrouw met ervaring aangeeft dat iets werkt, dan geloof ik dat dus direct en ben ik ook bereid om het te gaan doen of te ondergaan.

Maar bij een advies van een ervaren arts dat een bepaalde aanpak niet werkt, ben ik voorzichtiger. Want het aantal medische artikelen met onderzoeksresultaten en nieuwe inzichten dat dagelijks in de vakliteratuur verschijnt, zelfs binnen een specialisme, is te groot om bij te houden voor één persoon. De allernieuwste technieken en medicijnen die tegenwoordig op de medische faculteit

Fruit blijft gezond; maar eet geen appel meteen na het tandenpoetsen, om het zojuist gepolijste glazuur enige hersteltijd te gunnen.

worden onderwezen, zijn mogelijk of eigenlijk vrijwel zeker niet bij hem/haar bekend. Maar goed, in een behandelplan staan dan ook vrijwel nooit de zaken opgesomd die niet worden geadviseerd. Een uitzondering daarbij is wanneer de patiënt zelf overstapt van geneesheer A naar geneesheer B. In dat bijzondere geval zal geneesheer B adviseren om meteen te stoppen met de aanpak van A, of bijvoorbeeld de medicijndosering verhogen of verlagen. Dit 'negatieve advies' is dan volkomen logisch, want als de patiënt tevreden was over de werking van aanpak A (en dus indirect ook over doctor A), dan was hij/zij niet geswitcht. En het past bij de uitspraak: "Insanity: doing the same thing over and over again and expecting different results".
Omgekeerd: wanneer een minder ervaren (vaak jongere) arts aangeeft dat een bepaalde aanpak juist niet werkt, geloof ik dat ook meteen. Tijdens zijn/haar relatief recent afgeronde opleiding tot medisch professional heeft hij/zij uitgebreid geleerd van de eerdere fouten van andere artsen. Het briljante idee om je handen met zeep te wassen tussen twee operaties door, was namelijk niet van de eerste dokter ooit, maar is pas later door schade en schande bedacht. Zoals ook de bedenker van het basketbalspel in eerste instantie de bodem van de manden (zie de naam van de sport) had laten zitten. Zodat na elk gescoord punt de bal met een ladder uit de mand gehaald moest worden – maar dat is een heel ander onderwerp. Als zelfs de pas afgestudeerde arts, voorzien van de nieuwste kennis en inzichten en nog geheel bij met het lezen van de medische vakbladen, geen enkel sprankje hoop (meer) ziet in een bepaalde aanpak, dan neem ik dat voor waarheid aan.
Maar wanneer een minder ervaren arts op de proppen komt met een nieuwe effectieve aanpak, therapie, medicijn of dosering, ben ik juist voorzichtig. Voor je het weet, zit je drie keer per dag met je voeten in lauwwarm water naar rustige muziek (André Rieu) te luisteren met een cocktail van 14 medicijnen in je mik, terwijl je (`geaard' en wel) je holistische genezing visualiseert. Ik overdrijf hier natuurlijk een beetje. Ik bedoel dat de kans bestaat dat met goed bedoeld enthousiasme een not-yet-proven technology wordt aanbevolen, die mogelijk ook helemaal niet werkt voor de betreffende patiënt. Dat kost geld en belangrijker nog: tijd. En bij bepaalde ziektes is helaas juist die tijd nauwelijks meer voorhanden.
Een ideale combinatie is daarom voor mij een behandelplan opgesteld door een ervaren arts met daarin een opsomming van positieve adviezen, met daarbij een second opinion van een minder ervaren arts die er de inmiddels achterhaalde, antieke of niet meer optimale onzin uitschrapt. Twintig jaar geleden moest je na een herniaoperatie zes weken plat in bed blijven liggen; nu ga je de volgende dag lopend het ziekenhuis uit. Weliswaar naar de taxistandplaats, dat dan nog wel. Fruit blijft gezond; maar eet geen appel meteen na het tandenpoetsen, om het zojuist gepolijste glazuur enige hersteltijd te gunnen. Want met tandpasta kun je middeldiepe krassen wegpoetsen uit een compact disc (dit was na de langspeelplaat en nog voor Spotify-streaming).
Maar een ongewenste volgorde is voor mij om het behandelplan te laten maken door een onervaren arts,

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

met de kans op allerlei nieuwe, exotische aanpakken en in Nederland nog niet goedgekeurde ‚maar in "Amerika" al wel op knaagdieren geprobeerde, medicijnen. En dat behandelplan daarna te laten challengen (jeukwoord) door een ervaren arts. Daarbij bestaat helaas de kans op twee soorten fouten. De tweede arts kan een nieuwe, maar ineffectieve aanpak ten onrechte in het behandelplan laten staan, bijvoorbeeld omdat hij niet over wil komen als een aanhanger van OLM (Oude L** Methode). En de tweede (ervaren) arts kan ook een nieuwe nog niet uitgebreid toegepaste maar uiteindelijk voor die patiënt toch effectieve aanpak ten onrechte afkeuren. Zodat de patiënt geen (tijdige) genezing vindt, en dat is natuurlijk nog veel erger.

Security lessons learned

Het bovenstaande geldt eigenlijk precies hetzelfde bij security. Stel, u werkt op een afdeling met een stuk of tien middelgrote en kleine security-problemen, die de komende twee tot drie jaar nu toch echt eens een keer opgelost moeten gaan worden. Het opstellen van een totaal actieplan met volgorde, prioriteiten, budgetten, bemensing en geplande oplossingen ligt dan voor de hand. Op basis van bovenstaande is mijn advies: laat de meest ervaren medewerkers van uw afdeling per uitdaging (issue, threat, dreiging et cetera) vanuit hun ervaring een proven oplossing bedenken. Bijvoorbeeld: elk nieuw te bouwen systeem moet als logische toegangsbeveiliging minstens één password van voldoende lengte en ingewikkeldheid hebben. En laat daarna die voorgestelde oplossingen kritisch bekijken door de minder ervaren medewerkers met al hun actuele kennis van wat wel en niet (meer) werkt. Bijvoorbeeld: op een mobiel apparaat kan door misbruik van de overlay-functionaliteit in Android relatief eenvoudig, na een besmetting via phishing waarbij een .APK van buiten Googleplay wordt geïnstalleerd, een man-in-the-middle aanval opgezet worden, die het door de gebruiker ingevoerde wachtwoord onderschept en daarna misbruikt in de onderste app. De second opinion toevoeging kan dan zijn: "… maar bij apps zijn naast het wachtwoord nog deze aanvullende maatregelen nodig…". Een op ervaring gebaseerde proven technology kan natuurlijk ook compleet geschrapt worden uit het actieplan, maar dan wel graag goed gemotiveerd. Dit ook gelet op de toekomstige werksfeer tussen beide groepen medewerkers op de afdeling.

Het actieplan laten opstellen door de 'jonkies', gevolgd door een review door de 'oude rotten' heeft, om de hiervoor genoemde medische redenen en mogelijke fouten, zeker niet mijn voorkeur.

ROBERT WARMOESKERKEN

Toen ik vanuit de redactie werd gevraagd mijzelf als bestuurslid voor te stellen, zag ik dat als een mooie kans. Ik vind dat het bestuur van het PvIB zichtbaar moet zijn voor haar leden en ben blij dat ik hierbij de gelegenheid krijg om het bestuur meer 'gezicht' te geven.

Na de afronding van mijn studie Technische Informatica aan de TU/e startte ik mijn carrière als software engineer in de embedded softwareontwikkeling. In die tijd was geheugen nog duur en werd alles op alles gezet om de omvang (in Kilobytes) van software zo klein mogelijk te houden. Beveiliging was in die tijd nauwelijks aan de orde. Dat is veranderd!
Ondertussen ben ik alweer meer dan 20 jaar actief in IT, informatiemanagement, informatiebeveiliging, business continuity, risicomanagement, audit en advies binnen diverse (internationale) organisaties, vooral in de financiële sector. Binnen deze context heb ik vele jaren geacteerd als manager van (staf)afdelingen, zoals hoofd IT-audit, CISO en waarnemend directeur CIO-office, en als programma- en projectmanager. In het verleden was ik ook parttime docent aan een postdoctorale opleiding IT-auditing en lid van het curatorium dat toezicht houdt op betreffende opleiding. Sinds eind 2016 ben ik als zelfstandig adviseur actief en verzorg ik diverse opdrachten binnen de financiële sector en voor de overheid.

Sinds september 2015 ben ik bestuurslid van het PvIB en verantwoordelijk voor c.q. de linking pin naar de adviesraad en de commissies CISO en K&I. Ik ben indertijd lid geworden van het PvIB om meer te kunnen leren van andere "lotgenoten". Ondanks jarenlange ervaring in informatiebeveiliging kan je bij het gericht en passend toepassen van kennis en ervaring altijd wel wat hulp en visie van anderen gebruiken. Als informatiebeveiliger kom ik uit de tijd dat je er vaak 'alleen' voor stond. Waren we in het verleden nog vaak in de veronderstelling dat we geïsoleerd vanuit de informatiebeveiligingskolom toegevoegde waarde konden leveren, anno 2018 is het overduidelijk dat de samenwerking met de bedrijfsonderdelen, derden, overheid (NCSC), toezichthouders, CERTs en dergelijke essentieel is voor succes. Ik vind dat het PvIB deze 'drive' ondersteunt en een informeel en laagdrempelig platform biedt om kennis en ervaring te delen. Dat is de meerwaarde en dat blijft de komende jaren zo, mits we de betrokkenheid en actieve deelname van onze leden kunnen vergroten. Daar zijn we momenteel als bestuur en commissies mee bezig. Later dit jaar hoor je er meer over.

Ondanks dat relevante wet- en regelgeving wordt aangescherpt en de aandacht voor informatiebeveiliging verbetert, worden we toch nog bijna dagelijks geconfronteerd met beveiligingsincidenten. Door de toenemende groei en afhankelijkheid van IT worden de belangen en de impact van afdoende, passende beveiliging c.q. digitale weerbaarheid steeds groter voor het bedrijfsleven en de maatschappij. Echter, de 'dark side' zit ook niet stil en is ons nog vaak een stap voor. Ik verwacht niet dat dergelijke incidenten de komende jaren verdwijnen. De toegevoegde waarde van ons vakgebied zit nog steeds in het begrijpelijk en navolgbaar faciliteren van de stakeholders bij het in kaart brengen van relevante risico's, het maken van juiste afwegingen en besluiten, het adviseren bij de implementatie en uitvoering van passende beveiligingsmaatregelen, maar zeker zo belangrijk: bij het in kaart brengen van het rendement van de beveiligingsmaatregelen en bijsturing hierop. Dit blijft een continu proces en een traject van 'de lange adem'. Ik sluit af met de woorden: "Zonder business geen security, maar zonder security geen business!" We zullen samen moeten optrekken, sterker nog: ik wel zelfs het onderscheid tussen business en security niet meer maken. We zijn één en dat is nou precies waar het PvIB als vereniging voor staat!

SAMEN WERKEN AAN CYBERSECURITY: DE 'GLOBAL AGENDA FOR CYBER CAPACITY BUILDING'

Eind november presenteerde het Global Forum on Cyber Expertise (GFCE) de 'New Delhi Communiqué' op de Global Conference on Cyber Security (GCCS 2017). Met de ondertekening van dit communiqué onderschrijven de meer dan 60 organisaties en staten die deel uitmaken van de GFCE de 'Global Agenda for Cyber Capacity Building'. Deze agenda beoogt een gezamenlijke en wereldwijde aanpak te bereiken op het gebied van cybersecurity. De penvoerder van deze agenda was TNO. Dit artikel beschrijft hoe de agenda tot stand is gekomen, de hoofdthema's, de lessen die zijn geleerd, en wat de volgende stappen zijn. Tot slot; wat betekent de agenda voor bedrijven en organisaties in Nederland?

Achtergrond

In 2015 vond in Den Haag de Global Conference on CyberSpace (GCCS 2015) plaats. Nederland was gastheer en startte daar het Global Forum on Cyber Expertise (GFCE). Het GFCE (1) is een organisatie die inmiddels is uitgegroeid tot ruim 65 leden van landen, internationale organisaties en grote ICT-leveranciers die samen een veilige en welvaart brengende cyberspace voor iedereen op de wereld propageren.

In de aanloop naar de GCSS 2017 die eind november 2017 in New Delhi, India, plaatsvond, ontstond binnen het GFCE het plan om te komen tot een gezamenlijke, wereldwijde agenda voor cybercapacity building (CCB). CCB omvat de ontwikkeling en versterking van processen, competenties, gereedschappen en middelen van samenwerkingsverbanden, organisaties en landen om de snelle veranderingen en uitdagingen van de digitale samenleving het hoofd te bieden. Een sterke nadruk ligt daarbij op de veiligheid, beveiliging en openheid van cyberspace.

In de afgelopen jaren zijn er in verschillende regio's van de wereld CCB-initiatieven ontwikkeld. Donorlanden, multinationale organisaties als de EU en organisaties als de Wereldbank sponsoren dergelijke ontwikkelingen. Soms was dat succesvol, soms minder succesvol. In een aantal gevallen werd achteraf geconstateerd dat er onnodige duplicering van inspanningen plaatsvond. Soms bloedde een initiatief dood, omdat een samenhangend beleid ontbrak. Zonde van de investering en inspanning; met minder inspanning was meer te bereiken geweest.

Het plan van een wereldwijde agenda beoogt de internationale coördinatie van activiteiten en het leren van lessen die door anderen gebruikt kunnen worden als 'vaartversneller' en vermindering van kosten en inspanning. Doordat de leden van het GFCE achter de agenda staan en deze propageren in de bredere internationale gemeenschap van landen en organisaties, kan de agenda richting geven voor iedereen die verantwoordelijk gehouden kan worden voor de veiligheid, beveiliging en openheid van cyberspace. Dat geldt niet alleen voor de landen en organisaties die nog aan het begin staan bij het ontwikkelen van nationale capaciteiten, maar ook voor degenen die al een eind op weg zijn, zoals Nederland. Ook zij kennen zwakheden die aanpak behoeven.

Ontwikkeling van de agenda

TNO kreeg de eervolle opdracht om het GFCE te helpen bij het bouwen van de agenda. Hoe hebben we dat aangepakt? Als eerste stap is er achtergrondonderzoek gedaan naar bestaande internationale initiatieven; wat gaat goed, waar liggen drempels en wat zou versterking behoeven? Ook zijn 72 nationale cybersecurity-strategieën geanalyseerd om daarmee capaciteiten te kunnen identificeren. Omdat deze strategieën niet altijd in bekende talen verschenen, zijn vertaalmachines gebruikt om de capaciteiten in de ruw vertaalde tekst te ontdekken. Daarnaast is door de oogharen heen gekeken naar wereldwijde trends en ontwikkelingen. Steeds duidelijker wordt dat op veel plaatsen in de

wereld de tijd van vrijblijvendheid voorbij is; cybersecurity vereist een gestructureerde en breder dan nationale aanpak. Een sense-of-urgency is te ontdekken, ook bij landen in bijvoorbeeld West-Afrika, Midden-Amerika en het Verre Oosten.

Vervolgens is een eerste geclusterde lijst van capaciteiten opgesteld, die eind mei in een GFCE-workshop in Brussel is geprioriteerd en becommentarieerd. Voorbeelden van capaciteiten zijn bijvoorbeeld: crisismanagementoefeningen, opleidingen en trainingen, standaarden, R&D, juridische kaders en nationale CERTs. Ambities werden uitgesproken. In dit proces kwamen de verschillen in culturen en technologiegebruik naar voren. In delen van Afrika vormen mobieltjes bijvoorbeeld het belangrijkste deel van cyberspace, omdat ze ook een middel voor banktransacties vormen.
Na een aantal interacties met de GFCE leden door middel van telefoonconferenties, vragenlijsten en een tweede workshop is het laatste concept van de agenda ontwikkeld. Daarna volgde een politiek proces om de agenda te 'slijpen', zodat deze met name aansluit bij de beleidskaders van met name de donorlanden en -organisaties. In een dergelijk proces komen hoge ambities onder druk te staan, maar uiteindelijk is internationale consensus nodig om een stap voorwaarts te kunnen maken.

Global Agenda

De agenda omvat vier principes, die afgeleid zijn van internationale principes voor ontwikkelingssamenwerking, en zes thema's met veertien CCB-onderwerpen.

De principes zijn:

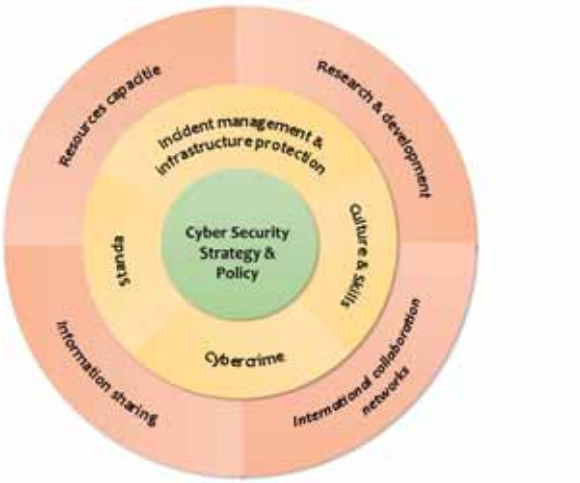
1. Inclusieve samenwerking en gedeelde verantwoordelijkheid: effectieve CCB vereist samenwerking tussen landen en andere belanghebbenden op vele verschillende niveaus.
2. Eigenaarschap: deelnemende landen onderschrijven prioriteit voor capaciteits-ontwikkeling en geven er uitwerking aan
3. Duurzaamheid: doel van CCB is het bereiken van impact ook op langere termijn.
4. Vertrouwen, transparantie en toerekenbaarheid: transparantie en toerekenbaarheid spelen een belangrijke rol in het ontwikkelen van vertrouwen tussen partners, essentieel voor een effectieve samenwerking.

De vijf kernthema's zijn:

- Cybersecuritystrategie en -beleid
- Incidentmanagement en infrastructuurbescherming
- Cybercriminaliteit
- Cybersecuritycultuur en vaardigheden
- Cybersecurity standaarden (en good practices)

De doorsnijdende thema's zijn:

- Resource capaciteiten (effectief beschikbaar stellen & effectief verkrijgen)
- Informatiedeling
- Netwerken voor internationale samenwerking
- Onderzoek & Innovatie



Figuur 1 - Overzicht kern- en doorsnijdende thema's cyber capaciteitsopbouw.

De thema's en de onderliggende CCB-onderwerpen kunnen niet los van elkaar gezien worden en moeten in balans ontwikkeld worden. Alleen wetgeving optuigen zonder opleidingen en handhavingscapaciteit is onvoldoende om bijvoorbeeld cybercriminaliteit aan te pakken. Ondersteunend aan de doelstellingen van de agenda zijn, in samenwerking met andere Nederlandse en buitenlandse specialisten, een aantal good practice documenten ontwikkeld voor Meridian (een internationale conferentie van beleidsambtenaren in het cyberdomein) en het GFCE. Die documenten (2) kunnen u wellicht ook helpen bij uw

Eric Luiijf, Tom van Schie, Theo van Ruijven, Martijn Neef, TNO Defensie en Veiligheid, expertisegroep Networked Organisations. Martijn Neef is bereikbaar via martijn.neef@tno.nl.

beleidsontwikkeling:

1. Good Practice on Coordinated Vulnerability Disclosure (CVD)
2. Good Practice on Critical Information Infrastructure Protection (CIIP)
3. Good Practice on national Computer Security Incident Response Teams (national CSIRTs)
4. Good Practice on the Internet Infrastructure Initiative (III) – standaarden voor veilig internet gebruik.

Deze verzameling good practice documenten vormt een uitbreiding op de reeds eerder uitgebrachte good practices voor critical information infrastructure protection (3), informatiedelen (4) en de veiligheid van industriële procesbesturing (5). De ontwikkeling van de Global Agenda heeft veel inzichten opgeleverd over de staat van cybersecurity wereldwijd, en hoe er in verschillende landen tegenaan wordt gekeken. Bij het ontwikkelen van een wereldwijde agenda en good practices spelen veel verschillende achtergronden, culturen, talen, juridische systemen en dergelijke een grote rol. Per ongeluk de term publiek-privaat gebruiken kan al leiden tot negatief commentaar en terzijde leggen in bepaalde landen. Sommige landen hebben een 'presidential decree' in plaats van een afgewogen democratisch proces. Zorgvuldig, simpel, precies en waardevrij formuleren op een wijze die voor alle beoogde doelgroepen acceptabel is, vergt continu oplettendheid. Cyberdiplomacy is een nieuwe vaardigheid voor overheden die ze nog aan het leren zijn. Vaak is men het niet oneens met het einddoel, maar één term of verkeerde toonzetting kan leiden tot onbegrip en enorme discussies. Het hoofd koel houden, het doel (nogmaals) uitleggen en vragen om suggesties voor 'juistere' bewoordingen, is dan de oplossing.

Gaandeweg realiseerden we dat cybercapaciteiten ruwweg in drie categorieën in te delen zijn:

1. Capaciteiten die een land (vrijwel) geheel zelf zal moeten ontwikkelen, bijvoorbeeld een nationale cyber security strategie. Externe consultants kunnen een rol spelen bij de ontwikkeling van een nationale strategie, maar het grootste deel van de strategie kan alleen een overheid zelf ontwikkelen.
2. Capaciteiten die landen deels zelf zullen moeten ontwikkelen, maar waarbij goed samengewerkt kan worden met andere landen in de regio. Dit soort capaciteiten zijn nauw verbonden met de nationale cultuur, wet- en regelgeving en organisatorische structuren, maar kennen algemene patronen en best practices die goed gedeeld kunnen worden over grenzen heen. Denk aan het opzetten van een CERT/CSIRT, of de bescherming van vitale infrastructuren tegen cyberdreigingen.
3. Capaciteiten die elders ontwikkeld zijn en die met minimale inspanning lokaal bruikbaar gemaakt kunnen worden. Denk bijvoorbeeld aan opleidingscurricula en -materialen.

De volgende stappen van de Global Agenda

In het komend jaar gaan de GFCE leden en andere landen en organisaties die de Global Agenda onderschrijven werken aan een gecoördineerde uitwerking. Coördinatie van activiteiten is hierbij cruciaal om te voorkomen dat onnodige duplicatie van initiatieven plaatsvindt. Tevens zijn de doorsnijdende thema's, zoals aangegeven in figuur 1, van cruciaal belang. Het uitvoeren (of agenderen) van kernthema's vereist simultaan aandacht voor de doorsnijdende (ondersteunende) thema's. Nederland onderschrijft de Global Agenda ook en zal, via de ministeries die betrokken zijn bij nationale en internationale cybersecurity, de agenda mede gebruiken om nieuwe activiteiten vorm te geven en samenwerkingen aan te gaan op de verschillende thema-gebieden. Als u internationaal werkt, is het goed om te weten dat er initiatieven komen die gebaseerd zijn op deze Global Agenda. Het zoeken van aansluiting bij dergelijke initiatieven kan de impact van uw werk versterken en onnodige kosten voorkomen. TNO kan voor u een rol spelen bij het identificeren van relevante activiteiten en bruikbare best practices.

Conclusie

De ontwikkelde Global Agenda on Cyber Capacity Building zet een stip op de horizon en toont een gezamenlijke ambitie. Deze ambities worden gedragen door een groot aantal landen en organisaties, en laten zien dat de wereld steeds meer beseft dat cybersecurity een globale uitdaging is, en dat informatie-uitwisseling en samenwerking de sleutels tot een veiligere digitale wereld zijn. Gedurende het ontwikkelingsproces van de Global Agenda kwam temeer naar voren dat er een grote behoefte is aan beleidsmatige cyberinzichten (lessen, ervaringen, basisbeginselen en handelingsperspectieven). Technische informatie-uitwisseling blijft belangrijk, maar ook aan het proactief uitwisselen van ervaringen over het opbouwen van cyber capaciteiten is wereldwijd een grote behoefte.

Referenties

(1) GFCE: thegfce.com

(2) Good Practice on Coordinated Vulnerability Disclosure (CVD), Critical Information Infrastructure Protection (CIIP), national Computer Security Incident Response Teams (national CSIRTs) en Good Practice on the Internet Infrastructure Initiative (III). Deze zijn onder andere te vinden op de site van het GFCE.

(3) Companion document uit 2017 en het Meridian/GFCE Good Practice on Critical Information Infrastructure Protection document for policy-makers uit 2016: https://www.tno.nl/media/10425/companiondocument_gpg_ciip.pdf en https://www.meridianprocess.org/siteassets/tno-jrv161031-02_hr.pdf

(4) Sharing cyber security information: https://www.tno.nl/en/focus-areas/defence-safety-security/cyber-security-resilience/sharing-cyber-security-information/

(5) Cyber security of industrial control systems: https://www.tno.nl/en/focus-areas/defence-safety-security/cyber-security-resilience/cyber-security-of-industrial-control-systems/

Titel: Digitale Stormvloed
Ondertitel: The Internet of Humans
Auteur: Brenno de Winter
Taal: Nederlands
Pagina's: 170
Uitgever: Einstein Books, Den Haag
Datum: 2017
ISBN: 978-94-92460-11-0
Prijs: € 15,- (incl. BTW), € 9,95 (eBook)

BOEKREVIEW

DIGITALE STORMVLOED

Hoewel het volgens de auteur niet een boek is dat specifiek over informatiebeveiliging gaat, loopt er in grote lijnen wel een rode draad door het boek over risico's. Het boek neemt een aantal huidige en toekomstige ontwikkelingen onder de loep: de 'digitale stormvloed' die op ons afkomt. Alles komt voorbij: de toenemende rekenkracht, Big Data, KI, robotisering, 3D-printers, blockchain et cetera. De auteur bespreekt de positieve technologische ontwikkelingen, maar daarnaast ook de negatieve gevolgen. Juist daar komen ook de security- en privacyaspecten naar voren. Er is ook een hoofdstuk dat specifiek over de beveiligingsrisco's gaat.

De omslag van het boek toont de ondergang van het 'onzinkbare' cruiseschip Titanic. Diverse rampen in het verleden hebben geleid tot maatregelen (regelgeving) om de veiligheid te verbeteren. Zo bestond er voor de ondergang van de Titanic geen regelgeving. Het bedrijfsleven van toen zag regelgeving als een belemmering van de commerciële vrijheid in de zeevaart en 'hield de boot af'. Tot aan de ramp met de Titanic. In no-time was regelgeving omtrent veiligheid in de scheepvaart een feit. Niet alleen met betrekking tot de verkeersregels op zee maar ook voor zeeschepen zelf (met de Titanic was qua veiligheid van alles mis). De vraag is of dat ook zo zal gaan (of gaat) met informatiebeveiligingsincidenten. De vergelijking is snel gemaakt. 'Het lijkt er op dat de wereld wacht op de digitale ondergang van de Titanic', aldus de auteur.

De kern van het boek de is de veranderende maatschappij. Zo schetst de auteur dat we van een Verticale (lees hiërarchische, industriële) naar een Horizontale (netwerk of platte) maatschappij gaan. Dit heeft grote gevolgen voor de samenleving op allerlei gebieden. Worden mensen overtroefd door alle technische ontwikkelingen? Is er straks nog werk? Zetten bedrijven en overheid de mens nog steeds centraal, zien ze technologie en de mens in het juiste perspectief? Juist door deze vragen en de vlotte manier van schrijven van de auteur is het boek zeer lezenswaardig, voor een veel breder publiek dan alleen informatiebeveiligers. Iedereen: bedrijven, overheid en burgers, moeten goed voorbereid zijn, zodat men niet overvallen wordt door de Digitale Stormvloed.

(Door Tom Bakker, redactielid iBmagazine. Tom is te bereiken via tom.bakker@hccnet.nl.)

ZICHT EN GRIP OP INFORMATIE

We lezen steeds vaker in het nieuws over vertrouwelijke informatie die op straat komt te liggen, het (D)DoS-en van webdiensten, het op afstand overnemen van systemen en andere gelijksoortige incidenten. Informatiebeveiliging wordt steeds belangrijker. Het staat zelfs op de politieke agenda. We schenken steeds meer aandacht aan het beveiligen van vertrouwelijke en belangrijke informatie, maar het lijkt net zo vaak weer mis te gaan. Grip krijgen op informatiebeveiliging blijkt voor veel organisaties een uitdagende opgave.

De onderliggende uitdaging

Als onvoldoende duidelijk is om welke informatie het gaat, is het beveiligen van deze informatie een lastige of zelfs onmogelijke opgave. Zicht en grip op informatiebeveiliging vereist namelijk zicht en grip op de informatie zelf. Het hebben van zicht en grip op informatie, namelijk weten om wat voor een soort informatie het gaat, wat de waarde is van de informatie, waar die informatie zich bevindt, welke verwerkingen en uitwisselingen plaatsvinden, wie daarvoor verantwoordelijk is et cetera, valt onder de noemer informatiemanagement.
Informatiemanagement vormt daarmee een noodzakelijke basis voor informatiebeveiliging.

Bij een organisatie waar informatiemanagement niet goed is ingericht, is de kans aanwezig dat de ICT-manager half op de stoel van de informatiemanager gaat zitten. Het risico daarvan is, dat de ICT-beheerorganisatie levert wat niet echt door de organisatie gevraagd wordt of zelfs niet levert wat juist wel gevraagd wordt. Dat kan zijn uit gemakzucht, uit een kostenoverweging, vanwege kennis en/of capaciteitsgebrek, om bij te blijven qua techniek of omdat een bepaalde techniek leuk en uitdagend is voor techneuten. De ICT-beheerorganisatie heeft in die situatie teveel macht over ICT binnen de organisatie, waarbij de organisatie zich in bochten moet wringen om met de geleverde ICT haar werk te kunnen doen. Het gevaar daarvan is weer, dat medewerkers - buiten de ICT-beheerorganisatie om - zelfstandig ICT-zaken gaan inrichten of externe middelen gaan gebruiken, zoals Gmail of Dropbox. Het zicht op waar bedrijfsinformatie zich bevindt, is dan nog meer zoek.

Dit document beschrijft het belang van informatiemanagement, welk voordeel een organisatie kan hebben van het goed inrichten daarvan en hoe dit kan helpen bij het aanpakken van informatiebeveiliging. Het is geschreven vanuit de belevingswereld van een informatiebeveiliger en bevat dus geen volledige beschrijving van wat informatiemanagement allemaal inhoudt.

De ondersteuning bij informatiebeveiliging

Goed ingericht informatiemanagement is noodzakelijk om informatiebeveiliging tot een succes te kunnen maken. Is informatiemanagement niet goed ingericht, dan ondervindt de persoon die verantwoordelijk is voor het inrichten van informatiebeveiliging, daar hinder van. Hieronder volgt een overzicht van een aantal onderdelen van informatiemanagement die een Information Security Officer kunnen helpen bij het inrichten van informatiebeveiliging.

Systeemeigenaarschap

Voor ieder informatiesysteem dient iemand aangewezen te worden als formeel systeemeigenaar. Dit is bij voorkeur een lijnmanager met voldoende bevoegdheid (tijd, inzet van

personeel en budget) om zaken rondom beheer in te (laten) richten. Door het toewijzen van een systeemeigenaar voor ieder informatiesysteem heeft de Information Security Officer een aanspreekpunt om de beveiliging van een informatiesysteem te bespreken.

In de praktijk gebeurt het vaak dat meerdere managers zeggen eigenaar te zijn bij vragen over wie wat mag met de in het systeem opgeslagen informatie, maar een andere kant op kijken in het geval van problemen of bij vervelende vragen, zoals vragen over informatiebeveiliging. De manager die de meeste pijn voelt van het uitschakelen van het betreffende informatiesysteem, is vaak de best aangewezen persoon om eigenaar te zijn.

Veel organisaties maken gebruik van cloud services voor hun ICT. De veronderstelling dat eigenaarschap daarbij niet meer nodig is, is onjuist. Het gaat namelijk niet om de systemen, maar om de informatie in die systemen. De informatie dient ook bij cloud services nog steeds een eigenaar te hebben. Het gebruikelijke woord 'systeemeigenaar' is dan ook misleidend. 'Informatie-eigenaar' zou eigenlijk een betere term zijn.
Een systeemeigenaar is verantwoordelijk voor het organiseren van de volgende zaken rondom het goed en veilig omgaan met informatie:

- Goed afgestemd SLA: Een systeemeigenaar is verantwoordelijk voor een informatiesysteem in het geheel, maar legt de taak van het up-and-running houden van het systeem meestal neer bij de ICT-beheerorganisatie of de SAAS-leverancier. Echter, het is en blijft de verantwoordelijkheid van de systeemeigenaar om daarover juiste afspraken te maken. Afspraken over beschikbaarheid, frequentie van het maken van back-ups, hoelang het maximaal mag duren om een gecrashte applicatie weer werkend te krijgen en hoeveel dat dan mag kosten, zijn daar belangrijke onderdelen van. Zeker met een interne ICT-afdeling kan het voorkomen dat voor informatiesystemen geen expliciete afspraken worden gemaakt en dus de standaard SLA gehanteerd wordt, waarbij systeemeigenaren eigenlijk geen beeld hebben van wat die standaard SLA inhoudt. Een incident met een kritische applicatie zorgt dan voor grotere problemen dan nodig is.
- Noodplannen: Zoals hierboven beschreven, behoort een systeemeigenaar afspraken te maken met een ICT-beheerorganisatie over de beschikbaarheid van een applicatie. Daarin staat hoe vaak en voor hoe lang een systeem voor onderhoud of voor welke reden dan ook, offline mag zijn. Ook worden afspraken gemaakt over hoe snel en met hoeveel moeite een ICT-beheerorganisatie aan de slag moet op het moment dat een applicatie crasht of ongepland offline gaat. Echter, het kan gebeuren dat een applicatie een probleem heeft waar de ICT-beheerorganisatie niks aan kan doen, waardoor de SLA niet waargemaakt kan worden. Daarnaast houdt een ICT-beheerorganisatie zich alleen maar bezig met de beschikbaarheid van een applicatie, niet met de integriteit of vertrouwelijkheid van de in het systeem opgeslagen informatie. In geval van problemen met de beschikbaarheid, waarbij de SLA niet waargemaakt kan worden, of problemen met de integriteit en/of vertrouwelijkheid van de informatie is sprake van een incident. Om goed met een incident om te kunnen gaan, om - in andere woorden - goed weerbaar te zijn, is het verstandig om een noodplan te hebben. Dit dwingt je om na te denken over wie en wat geraakt worden door het uitvallen van de applicatie, wie wat gaat doen om het probleem aan te pakken, welke interne en externe communicatie je doet, wat nodig is om tijdelijk zonder de applicatie verder te kunnen werken, wat nodig is om, na het weer beschikbaar komen van de applicatie, de resultaten van het offline werken weer op te nemen in de applicatie et cetera. Zonder zo'n noodplan bestaat de kans dat door de uitval van een systeem onnodige problemen ontstaan en deze problemen groter worden en langer duren dan noodzakelijk is. Een Information Security Officer kan met behulp van noodplannen beter inschatten of een organisatie goed is voorbereid op incidenten.
- Voldoen aan de privacywetgeving: Sinds 2001 heeft Nederland een wet ter bescherming van persoonsgegevens, de Wbp. Sinds 2016 is deze wet uitgebreid met onder andere regelgeving over het melden van datalekken en wordt per 25 mei een Europese wet, de Algemene Verordening Gegevensbescherming (AVG), van kracht die de Wbp vervangt. Om zaken goed op orde te hebben wat betreft deze wetgeving, zoals een rechtmatige verwerking van

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.

persoonsgegevens, het respecteren van de rechten van de betrokkenen, goede beveiliging et cetera, is het belangrijk dat iedere systeemeigenaar dit voor zijn of haar applicaties zelf organiseert. Zij zijn namelijk als eigenaar verantwoordelijk voor de in die applicaties opgeslagen informatie.
Verwachten dat een Privacy Officer of Information Security Officer dit oppakt, is niet terecht, want zij beschikken niet over het juiste mandaat. Eén van hen dat mandaat geven, is de verkeerde aanpak, want dan krijg je twee kapiteins op één schip met verschillende belangen. Bij een incident met privacygevoelige informatie loopt de organisatie het risico op een flinke boete vanuit de Autoriteit Persoonsgegevens (AP), indien je je zaken niet aantoonbaar op orde hebt. Zicht op de verwerking van persoonsgegevens (een vereiste volgens artikel 30 van de AVG) is een belangrijke eerste stap in het voorkomen van een datalek.

- Toegang tot een applicatie: Bepalen wie toegang krijgt tot (delen van) een applicatie, is bij uitstek een taak van iemand die verantwoordelijk is voor de in die applicatie opgeslagen informatie en die tevens kennis heeft van de waarde van deze informatie. Deze persoon is niemand minder dan de systeemeigenaar. Het is dan ook zijn of haar taak om de toegangscriteria op te stellen en te regelen dat deze bij het toekennen en voor het intrekken van toegangsrechten worden gehanteerd. Het goed inrichten van de toegang tot applicaties helpt de organisatie bij het voorkomen dat meer medewerkers toegang hebben tot bedrijfsvertrouwelijke of privacygevoelige informatie dan wenselijk of wettelijk toegestaan is.

- Documentatie: Voor een informatiesysteem is vaak tal van documentatie beschikbaar. Denk aan een functioneel en technisch ontwerp bij zelfbouw, een installatiehandleiding, beheerhandleiding en gebruikershandleiding. Bij voorkeur wordt dit soort documentatie centraal beheerd, maar het is de verantwoordelijkheid van een systeemeigenaar om deze documentatie bij ontwikkeling of aanschaf te (laten) verzamelen en aan de juiste persoon aan te (laten) leveren. Daarnaast verzamelen medewerkers (zowel beheerders als gebruikers) een hoop kennis. Het is verstandig om ook deze kennis te laten documenteren. Maar weinig mensen realiseren zich hoeveel kennis een organisatie kan verlaten bij de uitdiensttreding van een medewerker.

Overzicht applicatielandschap

Een ICT-beheerorganisatie heeft vaak een overzicht van haar digitale infrastructuur. Daarop staan servers, routers, firewalls et cetera aangegeven. Dit is echter onvoldoende voor een Information Security Officer om zicht te krijgen op de informatievoorziening. Een Information Security Officer houdt zich namelijk op de eerste plaats bezig met het beveiligen van informatie, niet van hardware. Een applicatielandschapsoverzicht is dan ook een heel ander soort overzicht. In een applicatielandschap staat de informatie en het gebruik en de uitwisseling van deze informatie centraal. Het niet hebben van een applicatielandschapsoverzicht maakt het voor een Information Security Officer lastig om te achterhalen welke informatie een organisatie in huis heeft en waar zijn aandacht qua beveiliging naar toe moet gaan.
Vanwege het belang van het hebben van een goed overzicht van het applicatielandschap, wordt dit onderwerp in een later hoofdstuk verder toegelicht.

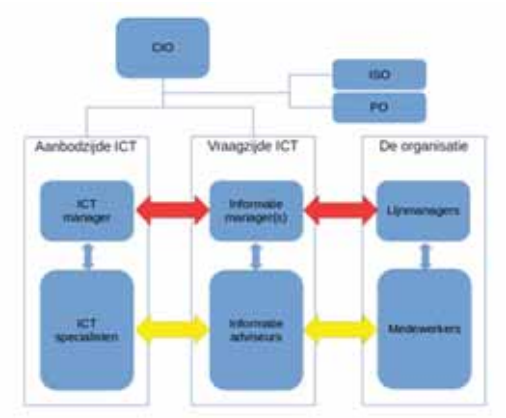
Informatie en processen

Veel van de informatie waar we vandaag de dag mee werken, bestaat in digitale vorm. Waar bijvoorbeeld vroeger een gemeenteambtenaar een papieren dossier tevoorschijn haalde als iemand een nieuw paspoort kwam aanvragen, treffen we nu een gemeenteambtenaar achter een PC aan. Met behulp van de ICT-beheerorganisatie is de beschikbaarheid van informatie veranderd van een analoge vorm naar een digitale vorm. De transitie van analoge informatie naar digitale informatie is bij de meeste organisaties voor het belangrijkste deel wel voltooid. Al vele jaren is er ook een andere transitie gaande. In plaats van langs gaan bij het gemeentehuis, bestaat voor veel zaken ook de mogelijkheid om dit te regelen via de website van de gemeente. Het proces van het aanvragen van een paspoort is daarbij verwerkt in de werking van de website. Niet alleen informatie is gedigitaliseerd, ook processen worden dus steeds meer gedigitaliseerd. Maar waar een ICT-beheerorganisatie de juiste partij is voor het digitaliseren van informatie, is dat niet het geval voor het digitaliseren van processen. Een ICT-beheerorganisatie gaat immers alleen over de beschikbaarheid van informatie. Voor het digitaliseren van processen is meer kennis nodig, namelijk kennis over de organisatie en de processen zelf. Dit is het werkterrein van informatiemanagement. Bij onvoldoende kennis over het verschil tussen het digitaliseren van informatie en het digitaliseren van processen kijken organisaties onterecht naar de ICT-beheerorganisatie voor ondersteuning bij het digitaliseren van processen. Zo'n organisatie blijft daardoor teveel leunen op de ICT-beheerorganisatie, terwijl ze feitelijk met informatiemanagement aan de slag moet gaan.

Organiseren van de informatievoorziening

Het helder definiëren van de verschillende taken en verantwoordelijkheden en het beleggen daarvan bij de juiste personen, is belangrijk bij het op orde krijgen van informatiemanagement binnen de organisatie. Zorg daarbij voor een goede verdeling tussen de vraagzijde en de aanbodzijde van ICT. De ICT-manager is verantwoordelijk voor de inrichting en organisatie van de aanbodzijde en de informatiemanager is verantwoordelijk voor de inrichting en organisatie van de vraagzijde. De informatiemanager brengt de behoefte aan informatievoorzieningen vanuit de organisatie in kaart. Deze behoefte is het uitgangspunt voor een gesprek tussen de

informatiemanager en de ICT-manager. De ICT-manager beperkt de levering van ICT tot wat nodig is om aan de vraag te kunnen voldoen.



Figuur 1 - Inrichting van informatievoorziening.

De strategische keuzes rondom informatievoorziening en ICT worden gemaakt door de directie, in nauwe samenspraak met de informatiemanager en de ICT-manager. De directie is en blijft eindverantwoordelijke voor zowel informatiemanagement als informatiebeveiliging. Eén van de directieleden (in de praktijk vaak de CIO of de CFO) is vanuit de directie aanspreekpunt voor informatiemanagement en informatiebeveiliging.
De tactische keuzes worden gemaakt door de informatiemanager, de ICT-manager en de lijnmanagers (rode pijlen in figuur 1). De Information Security Officer (ISO) en de Privacy Officer (PO) adviseren daarbij op het gebied van informatiebeveiliging en privacy en zijn staffuncties van de directie. Zowel de ICT-manager als de informatiemanager worden op gelijke hoogte in de organisatie geplaatst, namelijk direct onder de directie.
De concrete, operationele keuzes worden gemaakt door de ICT-specialisten en de informatieadviseurs, waarbij zij nauw contact hebben met de medewerkers die uiteindelijk met de oplossing aan de slag zullen gaan (gele pijlen in figuur 1). Het is zeer belangrijk dat de mensen uit alle kolommen goed met elkaar in contact blijven, zodat de juiste keuzes gemaakt worden (blauwe pijlen in figuur 1).
De kans is aanwezig dat de ICT-manager door deze werkwijze minder vrijheid heeft in de levering van ICT of minder verantwoordelijkheid heeft dan in de oude werkwijze. Om problemen in de onderlinge verstandhoudingen te voorkomen, dient zo'n transitie op een zorgvuldige en tactische wijze te worden aangepakt.
Binnen de organisatie dient afgesproken te worden, dat iedere vraag op het gebied van ICT of informatievoorziening via een informatieadviseur loopt. Een informatieadviseur zorgt ervoor dat de vraag op een goede en helder omschreven manier vast komt te liggen, dat voldaan wordt aan het ICT-beleid, informatie-beveiligingsbeleid en het privacybeleid en dat de ICT-oplossing voldoende toekomstbestendig is. Hierdoor draagt een informatieadviseur bij aan de kwaliteit van de informatievoorziening, waardoor kosten en tijd bespaard worden.

Vastleggen van het applicatielandschap

Zoals eerder gesteld, is het hebben van zicht op de informatie zelf noodzakelijk om deze goed te kunnen beveiligen. Het maken van een overzicht van het applicatielandschap is slechts één van de taken die hoort bij informatiemanagement. Maar omdat zo'n overzicht een goed startpunt is voor informatiemanagement en een goed hulpmiddel bij de verdere aanpak daarvan, is dit een belangrijk onderdeel. Om die reden wordt dit onderdeel hier apart besproken.
Hoewel gesproken wordt over een applicatielandschap, gaat het daarbij niet zozeer om de applicaties, maar om de informatie die in deze applicaties opgeslagen ligt. Het zou dus beter zijn om te spreken van een informatielandschap. Echter, de meeste informatie zit vandaag de dag opgeslagen in applicaties. Om die reden spreekt men van een applicatielandschap. Het is uiteraard toegestaan om plekken waar informatie in opgeslagen ligt, maar die geen applicatie zijn, zoals een papieren archief, in het overzicht op te nemen.
Zicht op de eigen informatieverwerking kan het beste verkregen worden door een organisatiebreed applicatielandschapsoverzicht te maken. In zo'n overzicht kan de volgende informatie opgenomen worden:

- Applicaties: Het overzicht bevat een lijst van alle applicaties binnen de organisatie. Een applicatie die, vanwege bijvoorbeeld capaciteitsredenen of geografische redenen, meervoudig is geïmplementeerd, wordt slechts eenmaal genoemd. Per applicatie wordt aangegeven welke informatie daarin opgeslagen ligt en de classificatie voor beschikbaarheid, integriteit en vertrouwelijkheid die daarbij geldt. Voor iedere applicatie wordt opgegeven welke koppeling deze heeft met een andere applicatie, welke informatie daarbij wordt uitgewisseld, in welk formaat en via welk protocol, hoe vaak en om welke reden dit gebeurt.
  n dit overzicht kan ook de verwerking van persoonsgegevens opgenomen worden, zoals vereist in artikel 30 van de Algemene Verordening Gegevensbescherming.
- Dataverzamelingen: Sommige systemen, meestal fileservers, bevatten meerdere verzamelingen van informatie die niet aan één eigenaar kunnen worden toegewezen. Deze verzamelingen dienen apart te worden geïdentificeerd, geclassificeerd en aan een eigenaar te worden toegewezen.
- Business: Hierbij wordt aangegeven welke afdelingen gebruik maken van welke applicatie of wie de systeemeigenaren zijn van de verschillende applicaties. Deze informatie is

noodzakelijk om bij een (beveiligings-)incident tijdig de betrokken afdelingen en verantwoordelijken te kunnen waarschuwen.

- Hardware: Het opnemen van een lijst van de (virtuele) hardware waar de applicaties op draaien, is puur om te zien welke applicaties op dezelfde hardware draaien. Deze informatie is belangrijk bij het maken van een impactanalyse in het geval van een (beveiligings-)incident met een applicatie of server.

In figuur 2 is een voorbeeld applicatielandschap volgens bovenstaande beschrijving schematisch weergegeven.

Figuur 2 - Voorbeeld van een schematisch applicatielandschapsoverzicht.

Managers hebben vaak weinig tot geen technische ICT-kennis. Door een applicatielandschap op deze manier vast te leggen, is de werking van de informatievoorziening binnen een organisatie ook aan hen uit te leggen. Het applicatielandschap kan gebruikt worden om aandacht te vragen voor zaken die inzet en/of geld nodig hebben. Hierdoor is het voor managers mogelijk om te sturen op informatiebeveiliging en privacyzaken.
Is bijvoorbeeld applicatie Y uit figuur 4 gehackt, dan is het voor een manager zonder zo'n overzicht lastig om daarop te sturen. Maar mèt zo'n overzicht kan hij, zonder verstand te hebben van alle techniek, vragen naar de impact voor afdeling B en C, of de hack via server 1 ook invloed heeft op applicatie X en dus op afdeling A, of de hack eventueel via de database ook vloed heeft op applicatie Z en dus op afdeling D en met de verantwoordelijke systeemeigenaren praten over de impact en het afhandelen van het incident. Doordat hij zicht heeft op de informatievoorziening, is hij in staat om te sturen op informatiebeveiliging.
Een voorbeeld van een tool waarmee het applicatielandschap op bovenstaande wijze is vast te leggen, is te vinden op https://github.com/hsleisink/landscape.

Samenvattend

Goed informatiemanagement is noodzakelijk om informatiebeveiliging tot een succes te kunnen maken. Maak het beheren van informatie een belangrijk thema binnen de organisatie. Stel daartoe een informatiemanager aan die een volwaardige partner is voor de ICT-manager in het spel van vraag en aanbod van ICT. Voer een periodiek overleg in tussen de informatiemanager, de ICT-manager, de Information Security Officer, de Privacy Officer en de CIO. Gebruik het applicatielandschapsoverzicht als beginpunt van deze gesprekken.

FAKE PROTECTED

Selling fake goods is nothing new. It dates back to the beginning of commerce. Making fraudulent claims about patent medicines was very common in the 18th and 19th centuries. In the 20th and 21st centuries regulations and laws started to limit the possibilities. The emergence of a consumer society during the late 20th century led to a vigorous trade in fake goods, especially fashion clothing and accessories – from designer dresses to handbags to gold watches. Now in the 21st century with the ubiquity of digital products and services we are experiencing the same thing with information. Fake news is a recent development. Selling of fraudulent financial investments is another area where criminals have been very successful at exploiting peoples' greed. Fake services sold by fraudulent marketing claims are a new problem.

The SABSA Institute knows this only too well from its own experiences. More than once we have faced unofficial training offered by apparently reputable training providers purporting to offer authentic SABSA training and certification. In one case, a large bank decided to train some people in SABSA to boost their security architecture team expertise. They identified a firm advertising local training – a firm with a global reputation as a consulting house and corporate auditor. They bought the course and sent their people to training, with the certification exam to be scheduled later. It never was. The provider was not accredited to provide certification training.

All this was before The SABSA Institute was incorporated as an official body. Before that, the Institute was a concept rather than an incorporated body. There was no public reference point for the bank to check on the authenticity of the training. Now the Institute regulates training through Accredited Education Partners, although that does not prevent unauthorized training companies from continuing to offer fake certification training. Only recently another case has come to light.

This begs the question "Who are the victims?" In the case of fake certification SABSA training, several groups. Firstly, there are those members of the SABSA Community that are sold fake certification training, believing it to be authentic. In the case of the bank, they eventually understood that it was a fraud by the continual postponement of the certification exam. In the end, the bank received compensation. However, there was a risk that the whole reputation of SABSA in the marketplace might be damaged. The Institute now exists to protect the intellectual property rights on behalf of the Community through the use of trademarks and copyright.

Secondly, there is an entire SABSA eco-system. Accredited Education Partners, examiners, exam markers, trainers, courseware authors, and other bona fide third parties offering authorized SABSA-related products and services. All of these parties make money from fees and royalties. The fraudulent offering of fake certification training courses deprives these parties of revenue – revenue that is effectively stolen by the fraudulent training company.

So what have we learned on our way through this legal maze? What advice can we give to those who are victims of fake news or fake information services? Most important is awareness of the problem. If you have people making decisions by what they read on the web or social media, make sure they approach their work with a skeptical mind. The human mind has a default setting of 'trust,' and it is this that can be socially engineered and exploited to sell us any fake product or service. If it seems too good to be true, then it probably isn't true, but then many fakes can look real too. Develop a policy framework and make sure you are compliant with any and all license arrangements that you enter. If you are an information provider, make sure you protect your product with suitable copyright and trademarks. Most of it is common sense – but then that's SABSA for you – common sense packaged into a framework.

The Attributer

Artikelen

(A) Artikel
(V) Verslag
(I) Interview
(O) Opinie

Thema's

Boekbesprekingen

Achter het Nieuws

Column Attributer

Column Berry

Column Privay

Voorwoord

Jaaroverzicht 2017

Achter Het Nieuws

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

WIE BEWAAKT DE BEWAKERS?

Recent verhuisde Apple de data van Chinese gebruikers van Amerikaanse servers naar Chinese servers. Tijdens deze verandering kwamen ook de encryptiesleutels van iCloud data weer ter sprake. Met de Chinese verhuizing zullen ook de sleutels van versleutelde data naar China verhuizen. Tot op heden zijn de sleutels van alle wereldwijde gebruikers in de Verenigde Staten opgeslagen. Een onderwerp dat minder ter sprake kwam, is de vraag waarom Apple eigenlijk de beschikking over deze sleutels heeft. Zou het niet veel beter zijn als alleen de eigenaar van de data deze kan ontsleutelen?

Maarten Hartsuijker

Naar aanleiding van een uitgevoerde pentest zat ik onlangs voor een klant bij een leverancier de beveiliging van een daar afgenomen webapplicatie door te nemen. Aangekomen bij de autorisatie-implementatie kwam ook de opslag van wachtwoorden ter sprake. Men was erg trots op de opslag van wachtwoorden. Die waren namelijk sinds enige tijd versleuteld, zodat ze niet meer leesbaar in de database stonden. Ze waren met de hoogst mogelijke beveiliging beschermd. Absoluut niemand kon er bij. Hoewel, na enig doorvragen (en een poging om het verschil tussen hashing en encryptie uit te leggen) bleek


Maarten Hartsuijker


Lex Dunn


Tom Bakker

dat uiteráárd de systeembeheerder en de helpdesk de wachtwoorden van de gebruikers konden inzien. Want hoe moest je anders een gebruiker helpen die belt dat hij zijn wachtwoord is vergeten...

Met de datalekken bij organisaties als LinkedIn nog vers in het geheugen behoeft aan niemand die dit blad leest nog uitgelegd te worden hoe je wachtwoorden veilig opslaat. De discussie zal hooguit gaan over de vorm van hashing en passende aantallen (PBKDF2) iteraties. Maar als het veilig opslaan van wachtwoorden inmiddels zo vanzelfsprekend is, waarom accepteren we van de grote tech-bedrijven dan nog steeds dat ze onze encryptiesleutels centraal opslaan? Een datalek bij zo'n bedrijf is vrijwel een gegeven. Zodra er wordt ingebroken, zou het helpen als zoveel mogelijk van de vergaarde data waardeloos is. Bijvoorbeeld omdat het krachtig versleuteld is. Dat kan prima, maar niet als je de sleutel in dezelfde IT-omgeving als de data bewaart. En aangezien niemand toegang tot mijn data hoeft te hebben, kan het sleutelmateriaal prima decentraal (bij mijzelf) worden opgeslagen of deels worden afgeleid van een door mij in te voeren code. De provider verzorgt dan de verwerking zonder te kunnen zien wat er wordt verwerkt. Zero access noemen we dat ook wel.

Het zou mooi zijn als meer IT bedrijven zich op volwaardige zero-access oplossingen zouden gaan richten. Of (wanneer men van mening is dat het op onderdelen de gebruikersbeleving schaadt) dit tenminste als optie aanbieden, zodat gebruikers het kunnen inschakelen wanneer ze dit willen.

Tom Bakker

Volgens de Chinese wet moeten data en blijkbaar ook encryptiesleutels van Chinese burgers en bedrijven in China opgeslagen zijn. Om zaken te kunnen blijven doen in China zullen ook niet-Chinese bedrijven aan de wet moeten voldoen. In Europa hebben we ook zoiets. Persoonsgegevens moeten in de EU opgeslagen worden. Maar hoe zit het met de Chinese bedrijven in Europa? Staan onze gegevens dan (ook) in China? Dat kan nog interessant worden gezien de GDPR straks.
Ik denk dat de Chinezen zich zeker zorgen moeten maken omdat de Chinese overheid, nu Apple iCloud naar China verhuist, (veel makkelijker) toegang krijgt tot alle versleutelde iCloud data. Waarschijnlijk konden de Amerikanen dat ook al. Maar (officieel) alleen via een court order.
Verder is het heel vreemd dat niet alleen de data eigenaren in het bezit zijn van hun encryptiesleutels, maar ook de cloud providers. Zo kunnen (private) keys best wel in de cloud opgeslagen worden, zolang alleen de eigenaar maar toegang heeft (zogenaamde sole control). Wie zegt ons dan dat straks de andere, niet-Chinese sleutels en dus ook data, niet in gevaar zijn? Welke garantie is er?

Lex Dunn

Vandaag de dag is ook de consument er wel van doordrongen dat alleen wachtwoorden niet voldoende zijn om zijn/haar eigen informatie goed te beschermen. Steeds meer wordt gebruik gemaakt van enerzijds de standaard versleuteling die in de grote suites (Google, Apple, Microsoft) beschikbaar is, anderzijds van gespecialiseerde applicaties zoals VPN software of wachtwoord tools. Dat is een goede zaak, omdat hiermee de kans dat credentials uitlekken vermindert. Uiteraard moeten dan de websites ook hun verantwoordelijkheid nemen en zorgen dat wachtwoordbestanden niet in platte tekst worden opgeslagen, maar als hashed, en dat er uiteraard een snufje zout aan die hashes wordt toegevoegd. Maar dan de vraag of die grote leveranciers wel verantwoord omgaan met de aan hun toevertrouwde encryptie sleutels, want dat kan de gemiddelde consument moeilijk zelf beoordelen. Is het in dat kader nou goed huisvaderschap om de sleutels van Chinese Apple gebruikers juist in China op te slaan? Op zich is dat in lijn met wat de GDPR/AVG ons zegt: opslag in de regio, tenzij ....
Maar is het wel zo'n goed idee om de sleutels van Chinese staatsburgers, waaronder vermoedelijk ook de nodige dissidenten, min of meer op een presenteerblaadje aan het regime aan te bieden? Ook al zal Apple vermoedelijk niet direct alles open zetten voor de Chinese overheid, je kunt erop wachten dat die overheid snel met een wet komt waardoor grootschalig gebruik van die sleutels mogelijk wordt. En waar dat toe kan leiden, beschreef George Orwell al treffend in '1984'. Als de goede man niet al in 1950 was overleden, zou 'ie mogelijk een tweede deel gewoon '2018' hebben kunnen noemen ;-)

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
Kas Clark
Lex Dunn
Maarten Hartsuijker
Hugo Leisink
Rachel Marbus
Bart van Staveren

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

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

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

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

ISSN 1569-1063

HET BEGON MET EEN E-MAILTJE...

In de begintijd van het internet moest je lid worden van een provider en kon je met behulp van je modempje met duizelingwekkende snelheden websites benaderen en je mail ophalen. Vaak kreeg je een e-mailadres van de provider en kon je daarmee je mail ontvangen. Natuurlijk was dat een klantenbinder, want een overstap naar een nieuwe provider betekende dat je iedereen moest uitleggen dat je een nieuw e-mailadres zou krijgen. Dat was wel lastig en ik was dan ook bijzonder blij toen Google op een bepaald moment een zogenaamd gmailadres aanbood, waarmee je gratis van Google een aantal GB's in gebruik mocht nemen. Naïef als ik ben, liet ik mij inschrijven op de wachtlijst (!) en gelukkig als een kind nam ik mijn nieuwe e-mailadres in ontvangst. Ik kan nu net zo vaak van provider wisselen als ik wil. Ik heb mijn emailadres al heel veel jaren en het adres is betrouwbaar gebleken, dus ben ik nog steeds blij. Google is niet de enige, ik kan nog wel een tiental e-mail providers noemen die de ruimte gratis ter beschikking stellen. Deze (veelal) Amerikaanse bedrijven schijnen dat te doen om data te verzamelen van hun klanten en deze data door te verkopen aan de hoogst biedende. Als ik aan alles mee zou doen wat Google aanbiedt, dan weten ze wie mijn contacten zijn, met wie ik bel via hun app, waar ik geweest ben, waar ik nu ben enzovoort. Als ik nu de goede contacten heb en alles zou opzoeken wat van mij geregistreerd is op internet, dan weten ze eveneens hoe zwaar ik ben via mijn weegschaal, wat ik eet via mijn koelkast, hoe vaak en hoe sterk ik mijn koffie drink door mijn koffiemachine, waar mijn auto staat en hoe zuinig ik rijd via mijn auto, hoe laat ik naar bed ga via mijn thermostaat … en zo kan ik nog wel een tijdje doorgaan. Maar bij het intypen merk ik een toenemende onrust bij mijzelf. Iedereen verzamelt gegevens en soms komen die verzamelaars heel dicht bij elkaar. Toen Facebook de overname van Whatsapp aankondigde, beloofden ze de data niet te combineren. De eerste rechtszaken lopen nu. Facebook gaat een stapje verder met haar Onava protect, een VPN dienst waar je normaliter veilig data over kunt verzenden. Facebook haalt echter alle data binnen zoals naam, gebruikersgegevens, locatie en dergelijke onder het mom daarmee misbruik te voorkomen. Op pagina 37 van de volledige privacy verklaring geeft Facebook aan dat ze dit na accordering van de verklaring mogen. In de verkorte versie komt het helemaal niet voor en doet Facebook of de gebruiker akkoord heeft gegeven. In een verklaring geeft Facebook aan dat ze deze tool alleen gebruiken om te herkennen of kwaadwillende gebruikers data proberen te misbruiken. Op de een of andere manier heb ik niet veel vertrouwen in hun verklaring. Ik denk dat het verzamelen van data, en niet alleen dat, maar ook het verkopen van data, een meer voor de hand liggende verklaring is.

Berry

Bouwt u goed **beveiligde** software?

Op tijd mooie applicaties leveren aan uw klanten; prachtig werk, maar enorm veeleisend. Welke maatregelen moet je treffen om ook de security-kwaliteit van uw producten te borgen en hoe voorkom je tijdig datalekken?

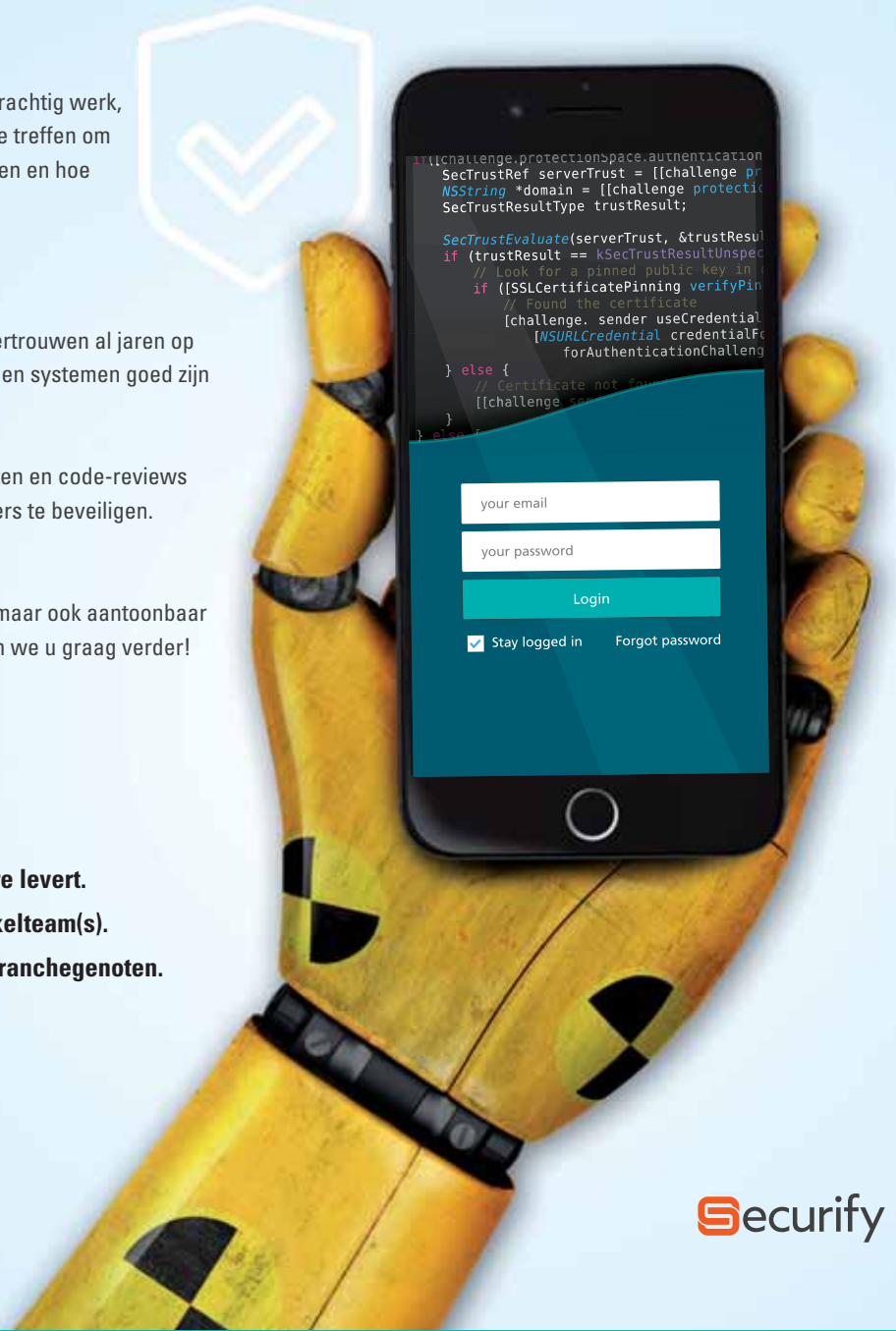
Uw applicaties goed beveiligd

Veel bedrijven – van start-ups tot grote banken – vertrouwen al jaren op Securify om er zeker van te zijn dat hun applicaties en systemen goed zijn beveiligd.

Zo helpen wij bijvoorbeeld met honderden hacktesten en code-reviews per jaar om de gegevens van miljoenen Nederlanders te beveiligen. Daar zijn we trots op!

Wilt u er ook zeker van zijn dat u niet alleen mooie maar ook aantoonbaar écht goed beveiligde applicaties levert? Dan helpen we u graag verder!

https://www.securify.nl/kennismaken



- **Voorkom datalekken.**
- **Maak aantoonbaar dat u veilige software levert.**
- **Boost de awareness binnen uw ontwikkelteam(s).**
- **Leer waar u staat ten opzichte van uw branchegenoten.**

Securify

securify.nl

Securify is specialist in web- en mobiele-applicatiebeveiliging en helpt bedrijven met het identificeren, verhelpen en voorkomen van technische beveiligingsrisico's.
Securify is opgericht door voormalig beveiligingsspecialisten van ABN AMRO, Delta Lloyd en Rabobank.