INFORMATIEBEVEILIGING
MAGAZINE

DOSSIER: Internet of Things

- The Attributer geeft zijn identiteit prijs
- IoT: onlosmakelijk verbonden met privacy en security
- Hoe effectief zijn e-mail phishing simulaties?

JAARGANG 21 - 2021 - EDITIE 3

Geheimen

Nicole van Deursen

De derde uitgave van iB-Magazine dit jaar staat in het teken van IoT. Maria Genova schrijft hoeveel slimme apparaten eigenlijk slimme spionnen zijn. Hackers gluren mee in stofzuigers, niets blijft geheim. Maar wat te doen? Er is natuurlijk eerst ons eigen gedrag. Daarnaast is er de multidisciplinaire aanpak, waarbij IoT-projecten samenwerken met privacy- en security-afdelingen. In dit nummer kun je ook lezen over richtlijnen rondom veilige IoT in het artikel van Rik van Dijk. Bovendien kunnen we met Jurgen van de Vlugt filosoferen over de hele manier van denken over het ontwikkelen van nieuwe technologie zoals zelfrijdende auto's en de mens-machine verhouding.

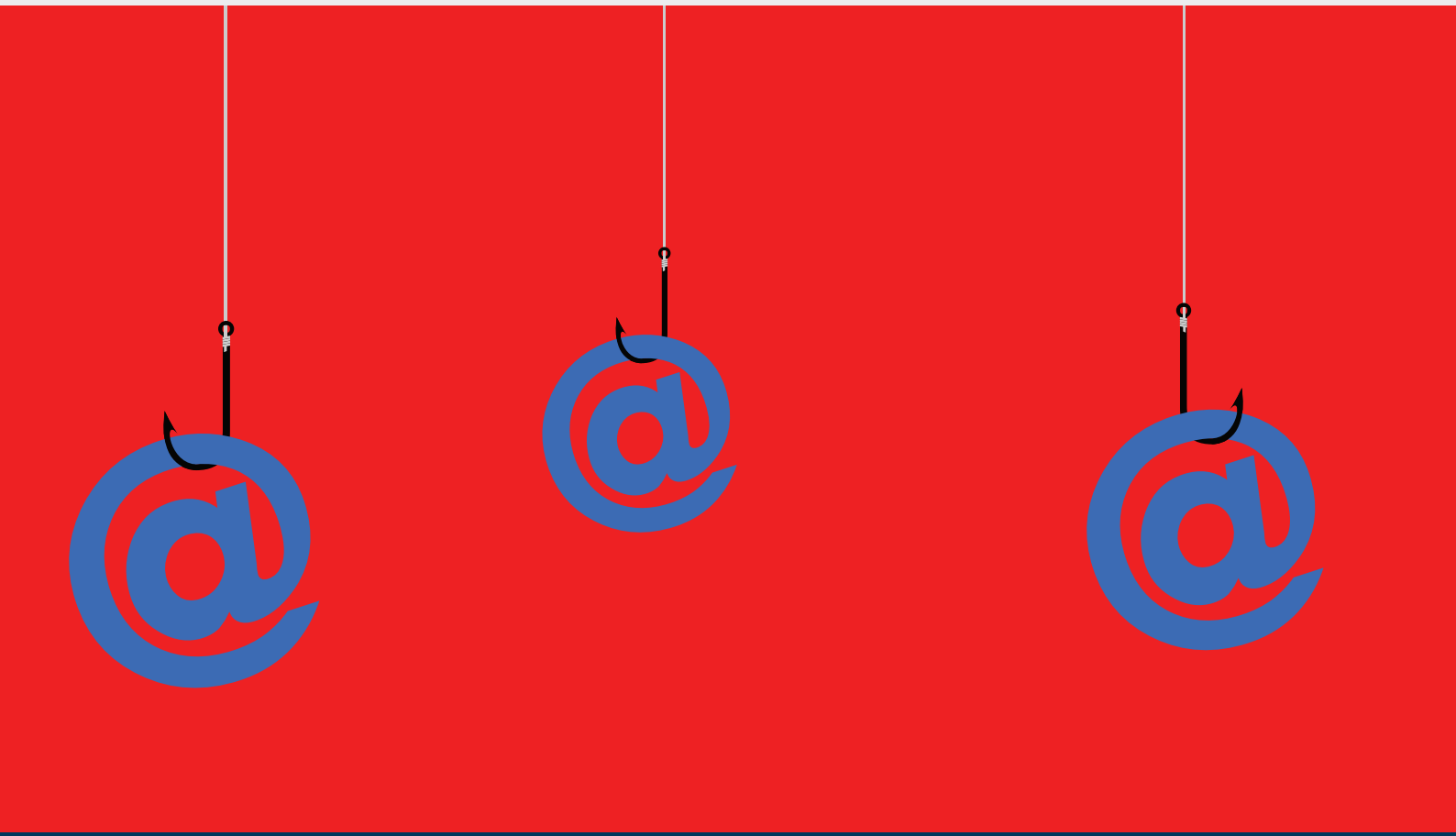
Heb je niet veel met IoT, dan hebben we ook veel andere artikelen. Gert Kogenhop geeft handvatten voor het uitvoeren van een BIA. En wist je al dat de Universiteit Twente een nieuw cybersecurity onderzoekscentrum heeft opgericht? Een boekbespreking over organisatieverandering beschrijft wat we allemaal wel kennen: gedoe! En ikzelf beantwoord de vraag of er aantoonbaar nut is van gesimuleerde phishing campagnes.

Er is deze keer ook een grote onthulling. Trouwe lezers was het al opgevallen: de column The Attributer die tien jaar lang in ons magazine verscheen, is gestopt. Wie was toch The Attributer waarvan de identiteit nog beter geheim werd gehouden dan een wachtwoord? Chris de Vries onthult het in een sympathiek interview. Veel leesplezier gewenst!

Nicole

IN DIT NUMMER

Auteur: Nicole van Deursen is wetenschappelijk onderzoeker en hoofdredacteur van iB-Magazine. Ze schrijft dit artikel op persoonlijke titel en is bereikbaar via nicolevandeursen@pvib.nl.



Hoe effectief zijn phishing e-mail simulaties?

Het aantal phishing e-mails blijft stijgen (1), (2) wat desastreuze gevolgen kan hebben. Het is de mens die op een linkje in een e-mail klikt, dus organisaties willen mensen alert houden. Een phishing simulatie moet de medewerkers wakker schudden, helpen om phishing te herkennen en uitleggen wat te doen als er per ongeluk toch geklikt is. Maar is er eigenlijk wel wetenschappelijk bewijs dat het simuleren van phishing e-mails een effectieve aanpak is tegen ongewenst klikgedrag?

Toen ik nog als ISO werkte voelde ik me altijd ongemakkelijk bij het idee van phishing simulaties. Ik vond het niet prettig om als IT-afdeling onze collega's in een richting te duwen die wij veilig – en dus goed – vonden. Bovendien werd er niet lang nagedacht over de mogelijke impact op het vertrouwen en de al lastige relatie tussen informatiebeveiligers en 'de business'. Het behandelen van collega's als de vijand zint me gewoon niet en ik kon niet worden overtuigd van het nut en de noodzaak van phishing simulaties als training.

Ongewenst effect

Mijn persoonlijke twijfel aan de effectiviteit van phishing simulaties werd versterkt door professor Sasse van University College London. Zij sprak zeer stellig uit dat we moeten stoppen met het op deze manier pesten van onze collega's om informatiebeveiliging te verbeteren (3) en dat het weleens averechts kon werken. Twee jaar later leek ze hierin gelijk te krijgen toen er commotie ontstond rondom een phishing simulatie bij een Nederlandse financiële instelling. De inhoud van de betreffende e-mail raakte bij enkele medewerkers een gevoelige snaar. Zij voelden zich al niet genoeg gewaardeerd, en door de inhoud van de betreffende campagne voelden ze zich extra bekritiseerd. Recent gebeurde zoiets weer. Een Brits treinbedrijf stuurde medewerkers een nep-phishing mail met de belofte van een bonus voor het doorwerken tijdens de pandemie. Dit schoot bij de medewerkers in het verkeerde keelgat omdat zij echt hard gewerkt hadden om te zorgen dat zorgpersoneel naar het werk kon reizen en zij en hun families een hoog risico liepen. Phishing simulaties worden met de beste bedoelingen gehouden, maar vaak binnen een gebrekkig empathisch en ethisch kader. Dit roept de vraag op of er eigenlijk wel aangetoonde effecten zijn (en hoe lang die standhouden) die deze simulaties billijken.

Uit onderzoek blijkt dat ...

Ik ben op zoek gegaan naar wetenschappelijke publicaties over dit onderwerp. Tijdens het zoeken bleek dat ik niet de enige ben met deze interesse. Zwitserse onderzoekers publiceerden in 2020 een paper waarvoor ze 104 publicaties over anti-phishing training hebben bestudeerd (4). Zij zochten naar wetenschappelijk studies die iets zeggen over hoe goede anti-phishing training eruit moet zien, wat de impact is, en hoelang kennis blijft hangen. Uit een aantal publicaties blijkt dat na een algemene training (waar simulaties onderdeel van kunnen zijn) de kans kleiner is dat mensen in een phishing e-mail trappen. Maar er zijn ook publicaties met wisselende resultaten. Twee groepen mensen blijken helemaal niet te beïnvloeden door training: de groep die altijd klikt en de groep die nooit klikt. Over hoelang kennis blijft hangen bestaat geen academische consensus. De veronderstelde retentie na anti-phishing training varieert van zeven dagen tot vijf maanden. Er zijn echter weinig studies die retentie meten.

Veel onderzoek combineert phishing simulatie met andere interventies, zoals training, voorlichting, self assessments, of serious games. Specifiek onderzoek naar het effect van phishing simulaties alleen, zijn zeldzaam. Hieronder bespreek ik een paar onderzoeken die iets zeggen over het effect van simulaties met of zonder andere interventies gecombineerd.

Studies naar effecten phishing simulaties

Eén van de eerste grootschalige studies vond plaats in de Verenigde Arabische Emiraten (5). Bijna 11.000 studenten, alumni en medewerkers ontvingen twee keer een phishing simulatie waarin werd gevraagd een survey op een website in te vullen. Ook tijdens de tweede ronde, waarbij ook een extra waarschuwing voor phishing uitging, bleek het aantal doorklikkers hoog en werden persoonsgegevens en wachtwoorden ingevuld.

De University of Maryland (6) stuurde in 2018 phishing e-mails naar 450 random studenten op drie verschillende dagen (in totaal 1350 studenten). Deze studenten waren vooraf niet op de hoogte van de campagne. Ongeveer 60% van de studenten klikte op de link van een e-mail in tenminste één van de drie experimenten. De link-klikkers ontvingen een survey waarin werd gevraagd hoe goed ze zelf vonden dat ze phishing konden herkennen. Er bleek een omgekeerd verband tussen phishing awareness en weerbaarheid. 80% van de studenten die van zichzelf vonden dat ze goed op de hoogte waren van phishing klikte op de link. Van de studenten die hun kennis laag inschatten klikte 28%. De onderzoekers konden dit resultaat niet verklaren. Misschien werd de vraagstelling in de survey niet goed geïnterpreteerd of overschatten

de deelnemers hun eigen kennis. Een soortgelijk resultaat bleek in Zuid-Afrika, waar studenten vertrouwen hadden in hun securityvaardigheden en zich bewust waren van risico's, maar hun gedrag iets anders aantoonde (7). Zij vertrouwden direct phishing e-mails uit naam van hun vrienden, zelfs als zij van tevoren zelf aangaven goed te zijn in het herkennen van phishing en wisten dat ze er niet in moesten trappen.

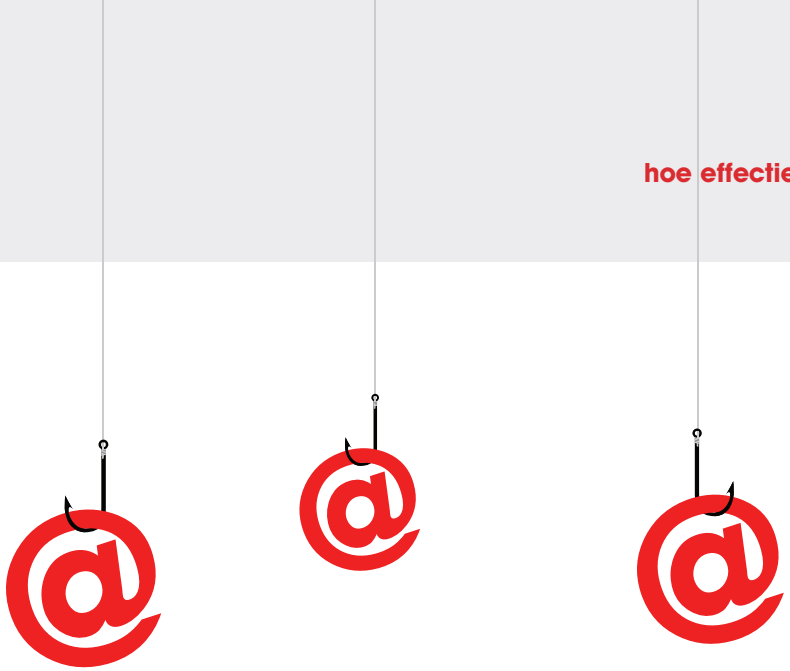
Bij het Ministerie EZK werden ruim 10.000 medewerkers betrokken bij een test naar de vatbaarheid voor phishing (8). De simulatie werd gecombineerd met andere interventies. Een groep ontving vooraf informatie over de procedures rondom phishing en hoe je het kunt herkennen. Een tweede groep ontving een simulatie e-mail, gevolgd door debriefing. Een derde groep ontving beide. Een vierde groep ontving vooraf niets. Daarna kregen alle vier de groepen een gesimuleerde phishing e-mail. Van groep 1 en 4 klikten veel mensen op de link en gaven daarbij hun wachtwoord af. Bij groepen 2 en 3 lag dat met zeven tot negen procentpunten lager met onderling weinig verschil. Dit deed de onderzoekers twijfelen aan de effectiviteit van extra voorlichting. In organisaties waar medewerkers al veel e-mails ontvangen en veel informatie moeten verwerken, kan het effectiever zijn om alleen simulaties uit te voeren. Een studie in een Amerikaans academisch medisch centrum komt tot een vergelijkbare conclusie (9). Daar werd het effect gemeten van twintig simulaties over een periode van drie jaar bij 5.416 medewerkers. Een deel van de medewerkers volgde na de vijftiende ronde verplichte anti-phishing trainingen. Over de tijd gemeten ging het aantal doorklikkers wel omlaag, maar was er geen extra effect meetbaar bij de groep die de trainingen had gevolgd.
In contrast zijn er ook onderzoekers die vonden dat extra training wél het effect van simulaties versterkt. In Portugal werden medewerkers in drie groepen van 100 personen verdeeld (10). Eén groep ontving geen training, een andere groep kreeg een algemene training en groep drie werd gericht getraind in het herkennen van spear phishing. De onderzoekers vonden dat de getrainde groepen beter waren in het herkennen van phishing dan de ongetrainde groep. Er bleek geen verschil tussen de groep met algemene training en de groep met spear phishing training. Het soort training beïnvloedde het effect niet.

Effect meten

Een interessante discussie is ook hoe je effectiviteit het beste kunt meten. In een onderzoek werden bijna twintigduizend medewerkers van een organisatie gedurende acht maanden met meerdere rondes van test phishing mails en trainingen bestookt (11). De pure klik-cijfers schommelden tussen de 0% en 40% per ronde en namen niet zichtbaar af na de herhalingen. De overtuiging van medewerkers om te klikken hangt af van de inhoud en kwaliteit van de phishing e-mail. Hierdoor schommelen de resultaten per simulatieronde, en is er geen dalende lijn van het aantal doorklikkers te zien. Dit komt doordat in verschillende rondes in de simulatie, verschillende soorten phishing e-mails werden ingezet. Sommige waren meer overtuigend en lastiger te herkennen dan andere. Voor het evalueren van een campagne moet je dus niet alleen naar aantallen doorklikkers kijken. Een phishing e-mail moet ook een soort moeilijksheidsscore krijgen om de doorklikaantallen te normaliseren. Puur kijken naar aantallen of percentages doorklikkers geeft dus een totaal verkeerde indruk. Stel dat je in jouw simulatiecampagne begint met een moeilijk herkenbare phishing e-mail en ze over tijd steeds makkelijker te herkennen maakt. Dan is de kans groot dat de aantallen doorklikkers steeds lager wordt. Dan zou je zomaar kunnen denken dat je campagne een succes is geweest.

Discussie

De kwaliteit en de resultaten van onderzoeken naar anti-phishing trainingen zijn wisselend. Ten eerste worden veelal studenten onderzocht. Dit is begrijpelijk omdat het lastig kan zijn om bedrijven te vinden die willen deelnemen aan onderzoek. Toch vormen studenten geen complete afspiegeling van de totale beroepsbevolking. Ten tweede wordt alleen tijdens een korte periode gemeten hoe vaak men doorklikt en niet hoe het effect op de langere termijn is of wat het effect van herhalingen is. Bovendien blijkt dat alleen het tellen van het aantal doorklikkers geen betrouwbare indicatie is van hoe goed of slecht het ervoor staat met de awareness. Sommige mensen klikken expres door om onzin in te vullen. Bij anderen is doorklikken een symptoom van te hoge werkdruk. Het device waarop iemand een e-mail bekijkt heeft ook invloed op hoe e-mail gepresenteerd wordt. Phishing is soms moeilijker te herkennen op een klein scherm. Een derde punt



is dat enkele onderzoekers opmerken dat medewerkers het onderzoek beïnvloeden door elkaar te waarschuwen voor het rondgaan van nep-phishing e-mails. Het effect van dit informele circuit in organisaties kan juist als positief gedrag worden benoemd. Ik denk dat we nog veel kunnen leren over de bijdrage van informele communicatie en 'influencers' op veilig gedrag in organisaties. Tenslotte is er nog de ethische discussie. Wetenschappelijke onderzoekers hebben in hun instelling vaak een ethische commissie die de onderzoeksvoorstellen beoordeelt en de belangen van de respondenten behartigt. In bedrijven is zo'n commissie niet gebruikelijk. Dat ethische overwegingen niet voldoende worden meegenomen leidt ertoe dat in de praktijk een IT-afdeling zelfstandig aan de slag gaat met phishing simulaties. In het gunstigste geval worden deze simulaties achteraf geëvalueerd, maar in hoeverre vooraf het welzijn van de medewerkers wordt overwogen, is nog een vraag.

Conclusie

Onderzoek lijkt wel enig kortetermijneffect aan te tonen wanneer phishing simulaties worden gecombineerd met training of voorlichting, maar we hebben veel meer bewijs nodig voordat we kunnen concluderen dat effectiviteit van phishing simulaties überhaupt meetbaar is en dat het in verhouding staat tot de inspanning en de ethische overwegingen. Ook de toegevoegde waarde van simulaties in het grotere geheel van awareness- en trainingsprogramma's kan nog verder worden onderzocht. De relatie tussen informatiebeveiliging en ethiek staat nog in de kinderschoenen en als meer organisaties zich openstellen voor longitudinale onderzoeken door wetenschappers, kan dat niet alleen helpen om de kwaliteit van awarenesscampagnes te verbeteren, maar ook om meer te leren over de ethische en empathische overwegingen.

Referenties

(1) Autoriteit Persoonsgegevens. Meldplicht datalekken: facts & figures Overzicht feiten en cijfers 2020 (Internet). 2021 maart. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-luidt-noodklok-explosieve-toename-hacks-en-datadiefstal

(2) Warburton D. 2020 Phishing and fraud report. Phishing during a pandemic. Seattle: F5 Labs; 2020. https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf

(3) Sasse A. Scaring and bullying people into security won't work. Lesk M, MacKie-Mason J, editors. IEEE Security & Privacy. 2015;13(3):80–3.

(4) Jampen D, Gür G, Sutter T, Tellenbach B. Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences. 2020 Aug 9;10(1):33.

(5) J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, A. Darwish. Phishing in a university community: Two large scale phishing experiments. In: 2012 International Conference on Innovations in Information Technology (IIT). 2012. p. 249–54.

(6) Diaz A, Sherman AT, Joshi A. Cryptologica. 2020;44(1):53–67.

(7) Chandarman R, Van Niekerk B. Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication. 2017 Dec;20(20):133–55.

(8) Baillon A, de Bruin J, Emirmahmutoglu A, van de Veer E, van Dijk B. Informing, simulating experience, or both: A field experiment on phishing risks. PloS ONE. 2019 Dec 18;14(12):e0224216.

(9) Gordon WJ, Wright A, Glynn RJ, Kadakia J, Mazzone C, Leinbach E, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. Journal of the American Medical Informatics Association. 2019 Mar 12;26(6):547–52.

(10) P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, J. Hong. Lessons from a real world evaluation of anti-phishing training. In: 2008 eCrime Researchers Summit. 2008. p. 1–12.

(11) Siadati H, Palka S, Siegel A, McCoy D. Measuring the Effectiveness of Embedded Phishing Exercises. In: Proceedings of the 10th USENIX Conference on Cyber Security Experimentation and Test. USA: USENIX Association; 2017. p. 1. (CSET'17).

Auteur: Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van business continuity managementsystemen conform de norm ISO 22301. Daarnaast is hij voorzitter van Business Continuity Management en Crisismanagement normcommissie bij NEN. Gert is bereikbaar via gk@bcmplus.nl.

Bedrijfsimpactanalyse

Business Continuity Management (BCM) of bedrijfscontinuïteitsbeheer gaat over het zo optimaal mogelijk voorbereid zijn op het (on)verwachte. In dit artikel wil ik graag aandacht besteden aan één van de belangrijkste onderdelen hiervan: de bedrijfsimpactanalyse, Business Impact Analysis (BIA).

Kort door de bocht gesteld willen we middels een bedrijfscontinuïteitsplan (BCP) of Plan B de organisatie beschermen tegen eventuele onoverkomelijke gevolgen van een ernstige verstoring van het bedrijfsproces, een crisis zoals brand, ICT- of stroomuitval of een pandemie. In de praktijk blijkt dat je in dit soort situaties niet alles tegen alles kunt beschermen, om het zo maar te stellen. Maar wat moeten we dan tegen wat beschermen? Middels de bedreigingenanalyse beoordelen we welke risico's voor onze organisatie actueel zijn en waartegen we ons moeten beschermen. Met de bedrijfsimpactanalyse bepalen we wat onze kritische activiteiten zijn, dus wat we moeten beschermen. De activiteiten die we prioriteren, die we als eerste willen herstellen, om bepaalde redenen.

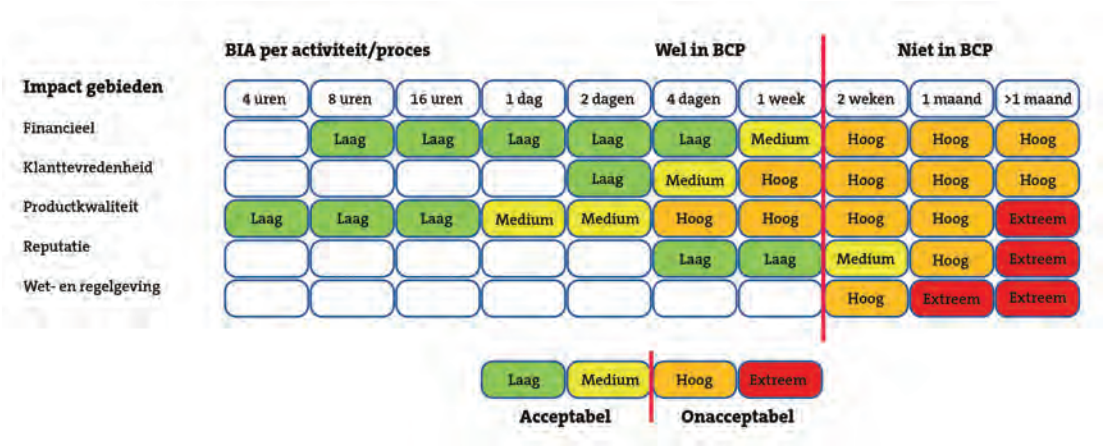
Twee stappen

In twee stappen analyseren we de organisatie. Uitgaande van een bedrijf, bepalen we de belangrijkste producten en/of diensten. Nadat deze zijn vastgesteld worden alle activiteiten tegen het licht gehouden en die activiteiten geselecteerd, die een directe bijdrage leveren aan het tot stand komen van deze producten en/of diensten (scope). Deze binnen de scope vallende activiteiten worden geanalyseerd en beoordeeld in geval van stilstand op gevoeligheid voor een aantal van tevoren vastgestelde impactgebieden zoals bijvoorbeeld financiële impact, wat dit betekent voor onze klanttevredenheid, productkwaliteit, reputatie of het wel of niet voldoet aan wet- en regelgeving.

We bepalen een impactschaal, bijvoorbeeld 'Laag', 'Medium', 'Hoog' en 'Extreem' en definiëren voor elk een waarde. Impact 'Hoog financieel' kan dan bijvoorbeeld zijn: schade bijvoorbeeld als gevolg van margeverlies of extra kosten tussen de €200.000 en €500.000 en Impact 'Extreem op het gebied van reputatie' kan zijn: negatieve landelijke media-aandacht en social media berichten. Vervolgens bepalen we wat wij niet meer acceptabel vinden, bijvoorbeeld in alle impactgebieden willen we nooit op het niveau 'Hoog' komen, dus om te voorkomen dat dit ooit wordt bereikt, willen we een Plan B hebben (BCP). Na deze vaststelling, bepalen we tevens dat wanneer dit niveau 'Hoog' wordt bereikt ná een week, we geen plan nodig hebben. Dat geeft ons voldoende tijd om zonder plan adequaat te reageren. Maar wanneer binnen een week dit niveau wordt bereikt, willen we zo optimaal mogelijk voorbereid zijn om niet verrast te worden en mogelijk de controle te verliezen.

Kritische activiteiten

Deze 'Een week' kan overigens ook vier dagen of twee weken zijn, dat bepaalt de organisatie. De twee drempels, 'Hoog' en 'Een week' zijn onze grenswaardes als het gaat om acceptabele impact. De allesbepalende factoren binnen de BIA. We beoordelen alle activiteiten, die activiteiten waarvan we bepalen dat de impact 'Hoog' is binnen 'Een week', markeren we vervolgens als kritisch. Er wordt niet vooraf een keuze gemaakt in de zin van: 'Dit zijn onze belangrijkste activiteiten, dus daarvoor doen we een BIA'. Alle activiteiten binnen de vastgestelde scope worden beoordeeld. Op deze wijze komen de kritische, geprioriteerde activiteiten bovendrijven en niet middels voorselectie. Deze specifieke activiteiten willen we voorrang geven



Bedrijfsimpactanalyse

als er iets écht misgaat, we willen ze eerder herstellen dan die activiteiten die langer dan een week stil kunnen blijven liggen. Duidelijk mag zijn dat ook binnen die kritische activiteiten een volgorde van aanpak is. Wat binnen vier uren weer moet functioneren gaat voor wat na 48 uren weer moet draaien. Samen sneller herstellen is uiteraard prima, maar om te voorkomen dat we de 'Hoog-waarde' voor ons onacceptabel - bereiken, moeten we de inspanningen en onze aandacht correct verdelen.

Nogmaals, de bedreigingenanalyse geeft inzicht in welke risico's voor de onderneming reëel zijn: algemene risico's, risico's behorend bij de aard van de activiteiten (advocatenkantoor of chemieconcern) en behorend bij de vestigingsplaats (nabij water, het spoor, luchthaven Schiphol of tankstation aan de overkant). Het gaat hier om de kans en de mogelijke impact van het feit dat een bedreiging een ernstige verstoring kan veroorzaken wanneer deze werkelijkheid wordt.

Blauwdruk

Om in het BCP, dat we later inrichten, de juiste scenario's in te kunnen vullen en de juiste acties uit te kunnen voeren hebben we van elke kritische, geprioriteerde activiteit (of proces) een 'blauwdruk' nodig. Dit betekent dat we duidelijk moeten hebben wat er benodigd is om die activiteit uit te kunnen voeren c.q. te herstellen en op welk minimaal niveau. Het hoeft wellicht niet allemaal 100% te functioneren. Dit kan gaan om:

- mensen (aantal, rollen, autorisatieniveau en vaardigheden);
- informatie en gegevens (formulieren, handleidingen, mediatype en hoeveelheid);
- gebouwen, werkplek en bijbehorende voorzieningen (speciale vereisten zoals hoogte, temperatuur, locatie of hoogspanning);
- faciliteiten, uitrusting en verbruiksartikelen (machines en gereedschappen);
- informatie- en communicatietechnologie (ICT)-systemen (type systeem, applicaties, toegang tot specifieke harde schijven of smartphones);
- transport en logistiek (aantal vrachtwagens, vereisten zoals de grootte van de vrachtwagen, voor gekoelde producten);
- financiën (inkomsten, hoeveel geld moet beschikbaar zijn);
- partners en leveranciers (kan niet zonder ...) en
- interne afhankelijkheden (van wie is deze activiteit afhankelijk en omgekeerd, wie is afhankelijk van deze activiteit).

Na bepaling van de 'gevaarlijke' combinatie van bedreigingen en de eerder vastgestelde kritische geprioriteerde activiteiten die onze belangrijke producten en/of diensten ondersteunen, kunnen we nu een BCP inrichten, nu we alle gegevens van de kritische activiteit kennen en tevens weten waartegen we ons moeten wapenen middels de juiste scenario's!

Dit artikel is eerder verschenen in Kwaliteit in Bedrijf nov/dec 2020.

Auteur: Chris de Vries is een zelfstandig professional en werkt onder de naam De Vries Impuls Management. Hij is tevens redacteur van dit magazine. Chris is bereikbaar via impuls@euronet.nl of https://www.linkedin.com/in/chris-de-vries-a7a4b36/.

INTERVIEW

A secret revealed

In the mist of time one lonely figure came forward to help mankind. His name was unknown to many although everyone will recognise him by his pen-name: 'The attributer'. This man born in 1947 became aware of the development of new technology and noticed the risks it beheld for the security of information. He recognised that risk wasn't to be prevented, but that management of risk was the key. Hence, the creation of SABSA i.e. Sherwood Applied Business Security Architecture. His name: John Sherwood!

About a decennium ago John was asked to write for our 'Information Security magazine' a blog addressing the needed architecture of enterprise security. He agreed and added to our magazine not only a broader (international) scope but also his insights on how profiling the attributes (also known as the business requirements engineering framework) in order to create an holistic, integrated enterprise solution being a series of integrated frameworks, models, methods and processes. After about 50 years working from scratch – starting with mathematics, communication and construction via calculation, access timesharing service, microprocessors and the computer – it was time for him to end his active career as manager of the SABSA Institute and as writer i.e. his contributions to our magazine.
We owe John a lot and for that reason we contacted him for an interview in which we want to express our thanks for his knowledge sharing and contributions. We were enriched by his work and thoughtful articles. Happily he accepted our invitation. In the following an overview of the live of this remarkable and friendly man.

John, you told me about your birthdate July 1947, could you elaborate on the place where you came on the world and which formed the hinterland of your youth?

"Of course, I was born in West Yorkshire, near Leeds in a small town. It was situated in the centre of the wool industry, specialised on recycling sheep fibres which was rough work. I was the only child of my parents, father being a butcher and mother working in a shop. So I came out of a shopkeeping family and received from them the encouragement / stimulation to study and to flee their environment."

So what curriculum did you follow?

"You should keep in mind that there was a cultural abide between my place of birth and the outside world. My world in West Yorkshire comprised of sheep, heavy industry (coal mining, steel, ship building) and at the other end for example London (trade oriented), in fact for us the end of the world although only 272 Km per airplane and about 314 Km when driving."
"So my studies started at Leeds grammar school when I was eleven. This study was financed over a government scheme and involved substantial repayment obligations for my parents, which at that time I wasn't aware of and which responsibility eluded me. Luckily I was an achievement driven person (and I'm still that driven). So that character quality translated into: 'achievement was everything'."
"In that time I spent a lot of time walking & camping in the rural surroundings of Yorkshire. I visited the industrial sites and studied the architectural of the mills. Most of those sites, when preserved are now transformed to other uses (e.g. apartments, restaurants, touristic). Also I had an eye for the canals in Leeds and Manchester, formerly a means of transport for the industry nowadays for pleasure cruising (leisure). You can derive from my above description that architecture has always been an underlying current in my life."
"After grammar school I went to the university of Birmingham. I studied their two years chemistry, but it showed to be a wrong choice. Therefore I switched college and went to the university of Aston where I enrolled in the chemical engineering course. That university had its roots in the industrial society and had a much more practical character. I followed that up with teaching 16 to 18 year olds and courses on mathematics, communication and construction. At that time (1970) I was twenty-three."

How did you came from that position to computing?

"In 1970 I worked at the college of further education and got access to a timesharing service on a Honeywell mainframe as well as a teletype in the far off corner which had the unthinkable velocity (at that time) of 10 characters per second. These apparatus I used as a device for processing numbers, much more was impossible. I used it for my mathematics teachings."
"Calculation was in those days a lot different from now. Then it was a calculation tool in an engineering environment. So basic programming was the core of it, small applications its tools and images part of it. So I arrived in 1980 to one of the important decisions of my life i.e. to specialise, to see computing as a career. I went to City University and after two years I got my master degree in computer science."

Could you elaborate on the facts of that time? What was computing then?

"In the seventies a change was happening from the main frames tot the micro-computers. In the eighties micro-computers became affordable and therefore they were everything. It started with a multigraph with one button to open a root and another button to close it. It meant that

programming could let do the computers almost anything, their ability was risen. The computer could move anything mechanical. See the physical-world versus the virtual-world."

"In that time (i.e. starting from 1969 on) it came to the development of the concept step motor. (To be clear: 'motion control is the process of accurately controlling the movement of an object, based on speed, distance, load, inertia or a combination of all these factors' (1).
"In first instance it considers the moves in steps especially regarding direction & velocity. So the question is: 'How to do useful things?' and that requires a system engineer, who in a creative process programmes the steps and foremost keeps aware of security."

"I would define 'Usefulness' as follows: 'Don't presume to tell users what is useful, it are the users who tell us the determinants of usefulness!' The underlying logic is that the engineer doesn't see all the uses and applications intended and/or existing. If they do, they act out of a feeling of system superiority and when doing so they enter the realm of risks. Like a good ancestor, the system engineer should become ethical resilient (part of the risk profile). And that is the emphasis of SABSA: 'Live = risk; risk is unpreventable, but it is manageable; so any system engineering should look into the ratio of functionality and usefulness!'"
"During the sixties and seventies of the last century risks were defined as the things going wrong. However, you should approach it dually since risks can be found in threats as well as in opportunities. This recognition implies that system engineers should look for ways to optimise just that system. As mentioned in the early days risk thinking looked for ways to prevent bad things from happening. In present day, IT is looking for the potential opportunities, not seen so far.

How would you place SABSA within this view, what are its characteristics?

"SABSA emphasises the discussion about the requirements, which should be well defined. My strengths lies in the conceptual way of thinking which forms an essential part together with the art of philosophical thinking. Since I'm not an expert of everything, I concentrate on conceptual aspects and let others develop it in a more detail. From my conceptual train of thought I'm driven towards system engineering."
"SABSA delivers business requirement tools and that leads to business attributes profiling and I would like to stress the element of attributes which should define the performance requirements. So it was logically for me that when starting my series of articles for iB-Magazine, I choose the name: 'The Attributer'!"

Coming to that, how do you see yourself and what is your legacy to us?

"As told, I'm a conceptual thinker, communicate easily and am achievement driven. Besides that I trust that I'm a responsible entrepreneur for which reason I looked for a way to secure the SABSA Institute for which reason I incorporated a Community Interest Company (CIC). The beauty of this construct is that this company is owned by the collective membership of the international SABSA Community for the benefit of the Community. The SABSA Institute itself exists to own and govern the body of knowledge as well as to catalogue the intellectual property rights known as 'SABSA®'."
"Since it is a CIC the articles dictate that the company is 'not for profit', clarifying that eventual trading profits must be reinvested in developing the assets of the company in this case the SABSA IP-rights. Secondly the 'asset lock' clause assures that no assets of the company may be exported other than at true market value (the SABSA Institute assets are mainly the IPR, the SABSA brand and marque)."
"Many people are working for the future of SABSA, I can't name all of them, but I would like to mention the editor in chief: John J. Czaplewski, acting as source of a lot of new ideas out of Washington State, USA. Presently he and I are discussing how the philosophical ideas of the Stoic: Marcus Aurelius (121-180 AD) (2) would attribute to our profession and what his significance would be in our world and time."'
"Besides securing the company and its assets I believe that my greatest legacy will be that I have assisted in developing a new way of thinking and in a lot of enthusiastic contacts between SABSA members, which in itself is gratifying. Moreover, personally my greatest legacy is that moment in

"So there is a coin with two sides:

Description	Old	New
Approach	-	New: NEN-ISO 31000
Risk	Mitigate threats	Manage threats
Business	Mission to fulfil	Discussion about requirements

Table 1 - The two sides of the coin.

"Besides securing the company and its assets I believe that my greatest legacy will be that I have assisted in developing a new way of thinking and in a lot of enthusiastic contacts."

time when someone is understanding the concepts and his face shows that light. That is really marvellous, rewarding, seeing that someone develops his/her capability exceeding those of my and/or their own expectations. This satisfaction, combined with my curiosity: 'What will they do with it?'"

How did you came into contact with our magazine and what was your objective?

"Lex Dunn was the person who contacted me one day, I believe in 2012, and asked if I would be willing to write for you all. And yes I was willing and I could. Of course I saw also the opportunity of working and training in The Netherlands."

Your articles are well read and appreciated, was it easy for you to write them?

"Yes and no. When starting it is really an empty page and a blank mind to start with. I'm looking around for the happenings around me, in the world of IT and security, sensing for ideas and impulses. Very often the BBC News website gave me clues about what to address in my articles. I consider them to be a trustworthy source with a broad scan of the sector."

What are your plans for now?

"I ended my work as Attributer as a consequence of a sort of 'end-life' or should I, might I call it a 'mid-life' crisis?! The question arises if anyone is ready for that occurrence? My answer was to focus. So I decided to reinvent myself. Taking into consideration my uncertain health condition we (my wife and I) decided to focus on garden landscaping, our home and travelling."

"Besides that we live in an interesting time as in the Chinese saying. Have we (the society) learned our lessons or have we forgotten the lessons from our industrial age? Here lies for me a relation towards risk management and the growing-up of IT. Like in the industrial age there is an evolution in the IT. So we should keep aware of our origin as well as our destination as society. My fear is that young people miss that experience, they were not there in the past to learn the lessons, so we have a responsibility to recycle that know how in order to enable them to learn anew."

"And of course I will spend time with my family, consisting of my wife, two sons and 5 grandchildren. My sons have meanwhile gone their own routes. Jason is a finance teacher and has his own training company, while Michael is also an entrepreneur. I'm proud that my children follow their father in their own way, making their own choices and based on their own vigour."

John, on behalf of your readers in The Netherlands, our editorial staff and myself, I thank you for your contributions to our magazine and we appreciate very much the quality of it. We wish you good health and good times with your dearests.

References

(1) AMS Stepper Motor System Basics, http://stepcontrol.com/stepping101/

(2) For the interested, Marcus Aurelius was a roman emperor, governing from 161 to 180 AD, and considered to be one of the best emperors of all time since he lived according the Stoic's virtues. https://nl.wikipedia.org/wiki/Marcus_Aurelius.

Auteur: Ir.drs J. van der Vlugt CISA CRISC. Jurgen is zelfstandig professional voor Information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl

Goto HumanDriver Considered Dangerous

Tsja, auto's en security. Het is het bekende verhaal, nog steeds … Zijn er technologische of andere ontwikkeingen de afgelopen halve eeuw waarbij security nou eens echt vanaf het begin is meegenomen, of blijven we met alle OT om ons heen doorgaan met de put dempen, security er een beetje (sic) opschroeven als het al te laat is?

Deel 1 van 3: Auto's, besturing en reflexen

Bij auto's is dat ook het geval. Met als complicatie dat we niet alleen snel de auto omvormen tot software-platform op wielen (1), maar gelijk ook het geheel liefst zo volledig mogelijk zelfrijdend willen maken. Zelfrijdend, in de chaotische context die het wegverkeer is. De mogelijkheden en oplossingen kennen drie grote issues, die in een drieluik van artikelen aan bod zullen komen. 1. Wat kan de machine, wat kan de mens (dan nog); 2. Individuele besturing of uniforme softwarebesturing: het risico op class breaks; en 3. Dan maar de Totalitaire Verkeerscentrale voor de aansturing?
In dit eerste artikel is er vooral aandacht voor een element uit het 'system' (2) dat we, of het nu homo 'sapiens' is of HAL, in de auto de functie heeft van Central Scrutiniser (3): de bestuurder. Wat kán die, hoe beslist die ...?

Trolley problem

De meesten van u zullen het wel hebben meegekregen: het resultaat van een groot onderzoek van MIT (4) over beslissingen die een Moral Machine zou moeten nemen om aan te sluiten bij wat wij mensen moreel handelen vinden. Nou ja, het ging eigenlijk alleen over een klein, bekend onderdeeltje van moreel redeneren, het trolley problem. Waarin de keuze moet worden gemaakt om één of meerdere mensen om te brengen, of om één of (nog) meer anderen te redden. Een besluit is verplicht, nietsdoen is een keuze voor een van beide alternatieven.
Uit het onderzoek kwam van alles naar voren – dat er over de wereld gezien culturele verschillen zijn in de statistisch 'ideale' keuzes. Dat het nogal uitmaakt wat er precies aan binaire alternatieven voorhanden is. Dat het uitmaakt wie je het vraagt: man of vrouw, jong of oud. Dat dat allerlei verschillende maar moeilijk voorspelbare antwoorden geeft. Dat was nog enigszins voorspelbaar. En dat de resultaten desondanks een zware bias hebben doordat de deelnemerspopulatie stevig leunde naar man, hoger opgeleid, welvarend en dus waarschijnlijk meer kosmopolitisch (en dus mogelijk minder religieus), en sowieso deelnemend. Dat soort beperkingen aan de representativiteit worden wel vermeld maar de impact op de resultaten niet (voldoende). Waarmee we dus niet weten of de resultaten bij voldoende biascorrectie wellicht grijs, middelmatig, vlees noch vis zouden zijn. Zoals bij de debatten onder ethici over dit soort zaken: er wordt fraai gedebatteerd en wat was het een interessante uitwisseling van argumenten en filosofische uitgangspunten – maar een eenduidige, snel beslisbare oplossing komt daar nooit uit. Als het probleem in de praktijk zo onbeslisbaar (5) lijkt, dan kunnen we misschien beter ophouden.
Dat het onderzoek beperkt was (is) tot het trolley problem, maakt de resultaten nou ook niet bepaald geschikt voor praktijkgebruik bij bijvoorbeeld zelfrijdende auto's (6). Die Auto's zullen heus in veel situaties terechtkomen waar wel meer dan twee alternatieve wegen voorwaarts zijn. Dat er wordt geleerd van de praktijk, is niet noodzakelijkerwijs een oplossing, of beter. Neem het geval van de overstekende voetganger met fiets aan de hand – de Auto herkende dit te laat (als obstakel) om nog rustig te kunnen remmen. De Auto had geleerd om vooral niet te gemakkelijk tot remmen te beslissen omdat bumperklevers al zo vaak schade gaven aan de achterbumper. Dan maar liever doorrijden tot het echt niet anders kan, oftewel: het is te laat voor een noodstop. Exit voetganger. Tsja, economische argumenten gaan nu eenmaal voor.
Dat was eigenlijk al duidelijk toen bleek dat Auto's veel defensiever reden dan mensen. Er was kennelijk nogal wat te processen aan informatie en better be safe than sorry – voor de Auto's ... Hetgeen overigens de ruimte schiep (schept?) voor fervente automobilisten om dan nog veel meer plezier te beleven aan hun hobby, maar dat terzijde (7).
En er was nog een aspect, dat verder niet aan bod kwam: het onderzoek vroeg naar de reacties van het (Kahnemanse (8)) System II. U weet wel, het cognitieve, denkende maar vooral ook langzame deel van uw hersenactiviteit waar morele en ethische overwegingen worden geprocest. Dit blijkt alleen al uit de koppeling met taalverwerking in de beschrijving aan de inputzijde en in de (weergave en selectie) van de keuze aan de outputzijde. En alle tijd werd gegeven voor bewuste, oftewel System II overwegingen. Vooral het laatste is hinderlijk als het aankomt op praktische toepasbaarheid.
Want net als in de menselijke praktijk zullen in Auto's alleen System I systemen voldoende snel zijn om tijdig 'morele' beslissingen te kunnen nemen én dan hopelijk juist te kunnen ingrijpen. Willen de resultaten van Machine Learning (of wellicht in een veel verdere toekomst (sic) zelfs van AI-systemen ...) enig nut hebben, dan zullen ze daartoe moeten worden gereduceerd.

Morele beslissingen

En wat moet er dan aan rules voor morele beslissingen worden ingebouwd? Nou ja, wat in het MIT-onderzoek aan mensen werd gevraagd. Of ... zou het niet beter zijn als het onderzoek had getest hoe mensen reageren? Maar hoe dan!? Want ook als er een prachtige VR-omgeving zou worden gebruikt, zou een ongeloof, hoe licht ook, de werkelijkheidswaarde van de proefopstelling reduceren. Of we krijgen juist ongemak en slechte resultaten door een uncanny valley.
En uiteindelijk is 'ik raakte in paniek' een prima excuus. Voor een mens, omdat het O/S in de bovenkamer op tilt ging, al of

niet door ongerijmdheden – geldt dat dan niet ook voor een Auto met bugs en software failures …? Hoe zit dat juridisch? SystemIPanic()➔EffectSomeReflex() dus. Mensen paniekeren, en reageren intuïtief. Maar werden Auto's nou net niet getraind om System II beslissingen te nemen voor System II- én System I-situaties? Zo niet, dan moet het hele idee dat Auto's veiliger zijn dan mensen achter het stuur, worden verlaten. En ziedaar, nog een hele tijd zal praktisch en juridisch verplicht gelden:

```
IF SystemIPanic() Then
  HandBackControlToCluelessHuman();
Else
  NothingInsurmountable();
```

Mijn cursief. Want vergeet niet: als Auto's in steeds meer standaardsituaties zelfstandig kunnen opereren – en niemand wil niet uiteindelijk naar Level 5 onafhankelijkheid (9), dan zullen betreffende chauffeurs-voor-noodgevallen steeds meer alleen nog worden ingeroepen voor steeds extremere System I panieksituaties.

Die dus ook tot volledig Level 5, het stuur en andere controls bij de hand moeten hebben, contra de wens van iedere ontwerper waarschijnlijk (10). Maar ook: steeds meer zal pas op het écht allerlaatste moment naar de mens worden overgeschakeld.

Wat er dan gebeurt, is dat juist de mens des te minder in staat is dan nog wat uit te richten. Niet alleen zal het menselijk System I toch trager zijn dan het Auto System I en dus als het alsnog nodig is, te traag of in ieder geval te laat blijken. 0,3 seconden voor een reflex, was het niet? Helaas, dat is te lang als de Auto ook al wat van die tijd verbruikt om te beslissen de boel aan de mens over te laten.

Belangrijker nog, de mens zal het eigen System I niet hebben getraind op werkelijke System I respons. Want die komt uit ervaring en als de Auto in de toekomst tot dan toe alle rij-werk deed en zo vele niet zo extreme noodsituaties oploste, voordat de tot mobiel Netflixen teruggetreden mens (11) een reflex zou hebben kunnen ontwikkelen op basis van what-if. Als dat al zou

kunnen. What-if is typisch een System II idee, echte System I reflexen zijn zoveel moeilijker aan te leren.
Waar dat laatste overigens een beetje goed gaat, is in de luchtvaart: piloten, en ook vliegers (12), moeten liefst in een simulator nog heel veel uren oefenen juist op noodsituaties, opdat eventueel ingrijpen in noodsituaties dan hopelijk op routine kan worden afgehandeld. Train like you fight, then you'll fight like you trained. Dat werkt, enigszins. Er valt niet op te vertrouwen helaas, maar we lezen ook regelmatig dat het goed gaat met zulke getrainde reflexen. Waar overigens nog heel, heel veel System II denken bij komt kijken; er blijkt dat daar in bijvoorbeeld uit de lucht vallende (even niet meer vlieg)tuigen nog wel een paar seconden of zelfs minuten beschikbaar voor System II-reacties gelukkig. Zo niet, dan is het prompt te laat.

Veiligheid

Maar als het gaat om wegverkeer … Gaan alle bestuurders, die in zo'n Auto willen rijden, omdat ze dan zelf niet meer hoeven rijden, ergo geen rijlessen meer willen hoeven nemen en zeker geen échte ervaring willen opdoen, in de nabije toekomst dan massaal juist wél slipcursussen etc. nemen vaak herhaald, om current te blijven waar ze geen praktijk meer in doen?
Als dat al alles was … Hoe gaan we zo meteen om met verzekeringskwesties? Kan men de mens in extremis nog de schuld geven de control niet tijdig en juist te hebben aangenomen als bij voorbaat bekend is dat die mens onvoldoende getraind en ervaren is om die taak uit te voeren en 'we' die mens alsnog de weg op lieten gaan? Kan de mens de schuld krijgen als de Auto bij voorbaat te laat de control overgaf? Waar ligt de scheidslijn tussen `de mens handelde dus is aansprakelijk, op basis van een kennelijke ethische beslissing waardoor morele aansprakelijkheid volgt' versus `ik raakte in paniek'..?
Wat nu …? Kinderen inzetten (13) ...? Of liever even serieuze literatuur (14) bestuderen? Eén voordeel: `clueless humans' kunnen dan ook tegen zichzelf worden beschermd. Rijbewijs inleveren gaat dan heel simpel (15). Of kiezen we voor een puntenrijbewijs waarop we naar mate onze ervaring met zélf rijden in crisissituaties stijgt (of uit decennia verleden van zelf rijden is opgebouwd), méér punten krijgen en juist daarmee de Auto méér mogen laten doen? Dat valt vrij gemakkelijk met NFC te regelen, toch? Dan regelen we ook gelijk dat een Auto kan weigeren met déze chauffeur achter het stuur (?) de weg op te gaan, omdat er meer chaos op de weg (route uiteraard vastgelegd) wordt verwacht dan volgens de punten door deze chauffeur kan worden gehandled.
Alleen: hoe tonen wij, om aan bekwaamheidspunten te komen, aan al échte panieksituaties te hebben doorstaan (met beperkte blikschade…)? Hoeveel punten kost anderzijds rijden onder invloed, of leveren veel ervaringspunten `vrijstelling' op voor een promilletje meer? Is er een verschil of de `back-up'chauffeur dan wel het doel van het transport is, van A naar B wil, danwel dat het puur om de vracht (echtgeno(o)t(e), kinderen, lading) gaat? Waarom zouden we anders non-human berijders willen, als die als hierboven weergegeven, niet echt helpen qua veiligheid.
Waarop `jongeren' van zeg ná de doorbraak van de draadloze telefoon ongetwijfeld zullen claimen dat ze door al het gamen (GTA springt in gedachte) de facto in een simulator hebben geoefend. Jammer maar helaas, ook vliegers geven aan dat ze door simulatoroefening weliswaar tot 80% minder vlieguren zouden hoeven maken in hun F35 (over een geïntegreerd system gesproken), maar ze zijn nogal zeker dat voor die 20%+ die over blijft, simulators nooit goed genoeg zullen zijn. De praktijk is toch een stuk je ne sais quoi anders. Dus piloten in de simulator: ja, alle, graag, en veel en vaak. Net als senior accountancypartners ongeacht alle AI-koppeling van process mining en 100% datagerichte ML-controle toch nog heel veel handmatig zullen (moeten) laten vinken: ja dat moet (16). Kunnen we voor alle rijbewijshouders ook zo'n soort `handmatig steekproeftoezicht' regelen, zonder al te veel bureaucratische missers?
Misschien moeten we al die jongeren zonder ervaring dan maar wel de weg op laten gaan en ze op random momenten als er nog geen sprake is van echte paniek, plots zelf in control brengen en zien hoe ze het er vanaf brengen (17). Hoewel: Wat als het dan misgaat …?
Dan is de conclusie:
We moeten bij voorbaat bovenstaande

```
If SystemIPanic() Then
  HandBackControlToCluelessHuman();
Else
  NothingInsurmountable();
```

vervangen door

```
If SystemIPanic() Then
  GiveUpAlreadyAsTheHumanWillAlsoBeClueless();
Else
  NothingInsurmountable();
```

En dat willen we nou net niet… We willen toch een Auto die ons vrijlaat om met 130km/u onze (?) Insta te checken? Het moge duidelijk zijn: het system als geheel moet even resilient zijn als nu. Dus waar nu de mens als centrale component heel veel

Als een auto wordt gehackt, hoe kun je deze dan handmatig weer overnemen als een overname door de hacker kan worden tegengegaan?

opvangt, zal zo meteen 'iets anders' dat moeten zijn. Helaas, wie daarbij beweert dat mensen daar goed in zijn maar machines niet, of dat machines (Auto's) het uiteindelijk wel zullen kunnen, verwijzen we naar James Gleick's Chaos (18): juist zeer eenvoudige en uiterst rationele systemen met feedbackloops kunnen (alleen al in een gesloten omgeving, waar bij wegverkeer geen enkele sprake van is) zeer chaotisch, onvoorspelbaar gedrag vertonen. Dat kennen we wel van de echelons boven ons in de organisatie, maar willen we liever niet in tegemoetkomend verkeer. Dit alles dus nog afgezien van de hackability van de Auto. We hebben voor het gemak het onderwerp van adversarial attacks nog maar even niet genoemd. Die zijn asymmetrisch: één hacker (en dat hoeft in dit geval niet eens zo'n slimme te zijn) hoeft maar één serieus adversarial example te bedenken en het verkeer is danig geraakt. De exploit scalet direct naar alle zelfde-softwaretype (19) Auto's. En als een auto wordt gehackt, hoe die dan manual over te nemen als een overname door de hacker kan worden geblockt? À la ransomware wordt u vanzelf naar een duister afgelegen industrieterrein gereden. Over het scalen zal het in het volgende artikel gaan. Als oplossing, en als probleem. Waarom wilden we ook alweer zelfrijdende Auto's...?

Referenties

(1) Waarbij de softwarekwaliteit en de niet-zo-standaard IAM rond software-updates inderdaad enorme problemen geven, maar ook de primaire kwaliteit van al die steeds meer zelfrijdende code. Er is meer aan de hand dan alleen het wat minder hackbaar maken van Musk'se model T maar daarover zal elders in dit IB Magazine wel voldoende te vinden zijn.

(2) Waaronder hier te begrijpen: De auto met al haar elementen waaronder de besturingssoft- of -wetware én de chaotische omgeving waarin de Auto zich bevindt.

(3) https://en.wikipedia.org/wiki/Joe%27s_Garage#central

(4) https://www.nature.com/articles/s41586-018-0637-6

(5) https://en.wikipedia.org/wiki/Undecidable_problem

(6) Dat is overigens een tautologie; auto als afgeleide van auto-mobiel vertaalt toch naar zelf (voort)bewegend of hoe was het ook alweer. Vandaar de notatie vanaf hier: Auto

(7) https://maverisk.nl/bring-on-the-future-it-belongs-to-me/

(8) https://www.bol.com/nl/s/?searchtext=kahneman+thinking+fast+and+slow

(9) https://en.wikipedia.org/wiki/Self-driving_car#Levels_of_driving_automation

(10) Waarom rijden we nog niet met side stick (https://en.wikipedia.org/wiki/Side-stick) ..?

(11) https://www.engadget.com/2018/05/17/tesla-crash-autopilot-driver-checking-phone/

(12) https://www.eugeneleeslover.com/aviator_slang.html#D

(13) https://twitter.com/page_eco/status/1351526891354685441?s=20

(14) https://www.wired.com/2013/07/the-surprising-ethics-of-robot-cars/

(15)https://twitter.com/getchepi/status/1372606580450074627/photo/1

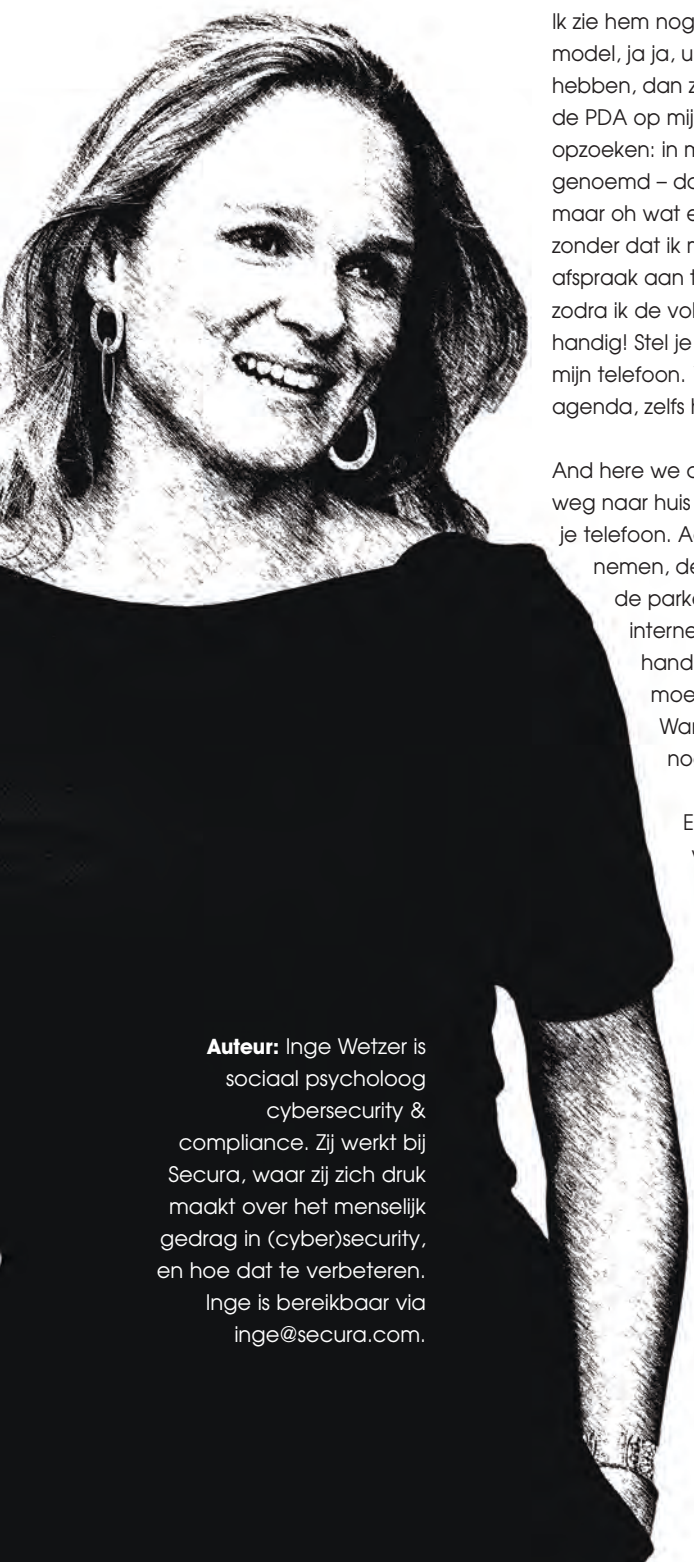
(16) Omdat zij hun handtekening zetten; hoe meer ze afhankelijk zijn van de machine alleen, hoe minder assistenten er zijn voor de details én hoe minder zij zelf zullen zijn getraind in herkenning van hiding in plain sight fraudeurs et al. – Hetzelfde probleem: Grotere afhankelijkheid, minder ervaring, inzicht en kunde met name voor de uitzonderingen...

(17) Een idee van college Maarten Souw. Die heeft wel vaker dat soort verhelderende insights en oplossingen.

(18) https://libris.nl/boek/?authortitle=gleick-james/chaos--9780749386061

(19) Nóg zo'n probleem: Mogen Auto's zonder alle laatste patches de weg niet meer op? Wat te doen bij een fabrikant die een patch te laat levert? Wat als de patch buggy is?

IoT: voor alles een ander wachtwoord



Ik zie hem nog zo voor me: mijn collega zwaaiend met zijn Nokia (een uitschuifbaar model, ja ja, uitklappen was niet meer hip): "Straks is dit het enige apparaat dat we nog hebben, dan zit alles hierin en heb je dit soort dingen niet meer nodig", – wijzend naar de PDA op mijn bureau. Ja, zo oud ben ik. Voor de mensen die nu snel 'PDA' willen gaan opzoeken: in mijn eerste baan had ik dus een apparaat – Personal Digital Assistant genoemd – dat diende als mijn digitale agenda. Groter dan de smartphones van nu, maar oh wat een ding! Als ik dan onderweg was, kon ik gewoon mijn agenda inzien zonder dat ik met zo'n papieren ding hoefde te slepen! En als ik er op locatie een afspraak aan toevoegde, dan synchroniseerde hij die vanzelf met mijn Outlook-agenda zodra ik de volgende keer op kantoor was en hem aansloot op de computer, su-per handig! Stel je eens voor dat dat handige apparaat óók nog eens geïntegreerd werd in mijn telefoon. "Straks hebben we één apparaat waar we alles mee doen: bellen, je agenda, zelfs het licht aandoen …". "Straks …"

And here we are. Sterker nog, in een paar jaar tijd zijn wij eraan gewend geraakt om op weg naar huis alvast de verwarming aan te zetten of de lampen even te dimmen vanaf je telefoon. Aan de auto die waarschuwt dat je beter een alternatieve route kunt nemen, de televisie die je op pauze zet als je wat te drinken wilt halen, de lampjes in de parkeergarage die aangeven waar nog plek is en ga zo maar door. Het internet is overal. Dat is handig, superhandig. Maar het is niet alleen maar handig. Op een ander vlak vraagt het ook wat van ons: al die accounts moeten namelijk ook beveiligd worden. En dat is nou juist weer minder handig. Want voor elke app een ander wachtwoord is ingewikkeld, zeker als het ook nog sterk moet zijn, en tweefactorauthenticatie kost extra tijd en moeite.

Een grote stap in de goede richting is het gebruiken van een wachtwoordmanager: een soort digitale kluis die al jouw wachtwoorden voor je genereert én onthoudt, die je beveiligt met één sterk 'masterwachtwoord'. Veel veiliger, niet moeilijk, wel even werk. En voor mensen die niet zoveel affiniteit met veiligheid hebben, natuurlijk niet zo aantrekkelijk om eens goed voor te gaan zitten. Het is nou eenmaal leuker om uit te zoeken hoe je nieuwe draadloze luidsprekersysteem werkt. Dat begrijp ik ook wel.

Maar mensen, willen we met de ontwikkelingen mee, dan hoort daar ook een extra inspanning bij. Als je kunt overstappen naar een slimme energiemeter en naar online bankieren, dan kun je ook overstappen naar een wachtwoordmanager. Voor je lampen ineens door de overbuurjongen worden uitgezet, in het beste geval … Dus, maak deze week nog even dat halfuurtje vrij, installeer die app en voeg je belangrijkste wachtwoorden toe (of laat de wachtwoordmanager even nieuwe maken als ze te zwak zijn). Maar als je dit nou écht te veel moeite vindt, dan kun je altijd nog terugvallen op een Nokia 3310, een PDA en een analoge camera.

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Auteur: Maria Genova is schrijfster van Komt een vrouw bij de h@cker en van het kinderboek What the h@ck!. Ze geeft (online) presentaties aan bedrijven en overheidsorganisaties over privacy, cybersecurity en digitale trends. Haar missie is om zoveel mogelijk mensen weerbaar te maken tegen hackers en online oplichters. Maria maakt geregeld cyberquizzen en stelt ze gratis beschikbaar. Wil je de quiz over de gevaren van het IoT ontvangen? Dat kan door een mail te sturen naar genova@casema.nl of een bericht via de website www.mariagenova.nl.

Hoe gevaarlijk is de ‘smart’ trend?

Alles wordt digitaal en ook ‘smart’. Steeds meer apparaten ‘praten’ met elkaar. Deurbellen, thermostaten en zelfs wasmachines wisselen gegevens uit met smartphones en andere apparaten. ‘Wat hebben mijn wasmachine en mijn koelkast elkaar te vertellen?’, was vroeger een gekke vraag, maar over een paar jaar hoor je daar niemand meer over. Tegenwoordig kun je zelfs een mobiele verbinding met een schaap maken. Niet om het te horen blaten, maar om de locatie te lokaliseren, zodat je haar lammetjes kunt bekijken. Dat heeft de VVV op Texel bedacht voor de toeristen, dus de schapen kregen een tracker.

Eén van mijn vriendinnen koopt zowat alles wat met een app te bedienen is, van een slimme koelkast tot een robotstofzuiger en van een wifi koffiezetter tot een smart wasmachine. "Straks kunnen ze met je wasmachine een bank aanvallen," zei ik een keer. Ze keek me glazig aan. "Hoe dan?" "Nou, dat soort apparaten zijn vaak zo slecht beveiligd dat hackers ze met honderdduizenden tegelijkertijd overnemen. Jouw wasmachine samen met honderdduizenden andere wasmachines, robotstofzuigers, babyfoons, beveiligingscamera's etc. kan grote bedrijven platleggen. En als bijvoorbeeld je bank door dat soort apparaten aangevallen wordt en je bent op dat moment in de supermarkt, dan doet je bankpas het niet meer. Dus dankzij je wifi wasmachine kun je niet meer pinnen en als je geen contant geld bij je hebt, kun je de boodschappen ook niet meenemen." Mijn vriendin keek me nu met nog grotere ogen aan. "Meen je dat nou?"

Voor veel mensen is het vrij nieuw, maar het is al jaren gaande. Een groot gedeelte van het internet kan platgelegd worden via op het eerste gezicht onschuldig ogende babyfoons, smart tv's, slimme verlichting of smart koelkasten. Met het Mirai-botnet vielen hackers met heel veel gehackte huishoudelijke apparaten bekende websites aan. Ook Thuisbezorgd.nl werd getroffen. Een samenzwering tussen slimme koelkasten en keukenmachines tegen een maaltijdbezorgsite? Bij de eerste massale aanval door middel van een bonte verzameling van miljoenen slecht beveiligde slimme apparaten legden hackers ook grote websites zoals Netflix, Spotify, Amazon en Twitter plat. Dat was vrij simpel, omdat de eigenaren de standaard wachtwoorden van hun nieuwe gadgets niet aangepast hadden. Zo konden hackers ze met duizenden tegelijk overnemen en aansturen.

Meegluren

Soms kun je niet eens iets aanpassen. Ondanks herhaaldelijke waarschuwingen voor onveilige beveiligingscamera's, blijven de winkels ze verkopen. Mijn vriendin heeft een hippe stofzuiger uitgerust met een camera en een microfoon. Hackers bewezen al dat ze via dat soort stofzuigers in alle kamers konden meegluren. Ze konden ook de wifi gegevens kapen om te zien wat de huiseigenaren allemaal op hun computers bewaren. Geen idee of ze al in de computer van mijn vriendin zitten om haar e-mails te lezen, maar ik sluit het niet uit. Ze vertelde me dat ze ook een slim deurslot wil kopen. "Kost een paar centen, maar wel zo handig," zei ze. Ze keek me verwachtingsvol aan. "Tja, voor de inbrekers kan het ook handig zijn." Ik verzon het niet, want er zijn al best veel slimme deursloten ontmaskerd als onveilig. Het bluetooth-deurslot Ultraloq van 250 dollar kon bijvoorbeeld door onbekenden uitgelezen worden, inclusief de locatie van het huis. Kwaadwillenden konden de pincode op afstand veranderen en de deur openen.
Een slimme deurbel lijkt minder gevaarlijk, maar is dat zo? De Ring is een van de meest bekende en daarmee wisten hackers het wifi wachtwoord in een huis te ontfutselen en alle internetverkeer te onderscheppen. En dan kom je vrij simpel iemands geheimen te weten: de brave vader die vreemdgaat, de directeur van een groot bedrijf die naar kinky porno kijkt of … verzin het maar. Zelfs als je niets ergs doet, is het geen prettig idee dat iemand je e-mails zit te lezen via een deurbel.

Mijn vriendin maakt zich totaal niet druk om haar privacy, maar veel slimme apparaten in onze huizen zijn vooral slimme spionnen. Ze snapt er helemaal niets van en wijst naar haar robotstofzuiger die in de gang bezig is, terwijl we koffiedrinken. "Wat voor spion is mijn stofzuiger dan?" "Die zuigt niet alleen stof, maar ook gegevens uit je huis op," zeg ik. "Ik neem aan dat je eerst een schoonmaakster had? Vroeg ze je wel eens of ze een plattegrond van je huis mag tekenen en ook van alle spullen een foto maken?"
"Natuurlijk niet," zegt mijn vriendin, "waarom zou mijn schoonmaakster dat willen doen? Dat zal ik sowieso nooit toestaan."
"Grappig, want als je stofzuiger het doet, dan vind je het wel goed. Je stofzuiger bewaart echt deze gegevens en het staat in je contract dat ze die mogen doorverkopen aan derde partijen."
Ze kijkt me verbijsterd aan. "En nu?"
"Geen idee. Een schoonmaakster die een aanslag op je privacy pleegt, ontsla je meestal binnen de kortste keren, maar wat doe je met een slimme stofzuiger?"

Slimme zonnepanelen

Onderzoekers van Princeton maakten een tool om te kijken wat slimme apparaten op de achtergrond doen en schrokken zich rot. Een Chromecast zocht continu verbinding met Google, zelfs als de eigenaar die niet gebruikte. Een slimme lamp verstuurde elke paar seconden data naar China. Ook smart tv's en camera's wisselen voortdurend informatie uit.
Het Britse consumentenprogramma Which testte negentien apparaten die met internet waren verbonden. Een slimme stofzuiger vroeg om toestemming om het geluid van de smartphone op te nemen, een printer stuurde de namen van alle geprinte documenten door naar de fabrikant en een slimme tv

maakte binnen vijftien minuten verbinding met zevenhonderd verschillende internetadressen. In de Verenigde Staten moest tv-fabrikant Vizio ruim twee miljoen dollar boete betalen omdat die zonder toestemming volgde waar klanten allemaal naar keken en verkocht die informatie samen met data verzameld uit de laptops en de mobieltjes van de kijkers aan adverteerders, inclusief leeftijd, geslacht en inkomen.
De fabrikant van de robotstofzuiger Roomba liet weten dat de stofzuiger in de toekomst niet alleen stof maar ook data over je woning zal opzuigen en doorverkopen aan bedrijven zoals Google en Amazon. Hoe meer zij over je weten, hoe beter ze advertenties op maat kunnen maken, bijvoorbeeld over huisdecoratie. Na negatieve reacties liet het bedrijf weten de gebruiker van de stofzuiger toch om toestemming te vragen. Hoe dat gebeurt, is een kwestie van ontwerp. Veel mensen weten trouwens sowieso niet waar ze allemaal toestemming voor geven, ze klikken gewoon op 'akkoord' zodra er iets van voorwaarden op hun scherm verschijnt.

Uit onderzoek van IT-beveiliger Zscaler blijkt dat medewerkers steeds vaker hun eigen apparaten aan het netwerk van bedrijven koppelen. Ze beseffen niet dat dit gevaarlijk kan zijn. Zscaler blokkeert 14.000 pogingen per maand om via IoT-apparaten kwaadaardige software te installeren.
Uit onderzoek door Trend Micro blijkt dat 39% van alle werknemers toegang verkrijgt tot bedrijfsgegevens via persoonlijke apparaten. Deze persoonlijke smartphones, tablets en laptops zijn blootgesteld zijn aan kwetsbare IoT-apps en -gadgets in het thuisnetwerk. Vooral apparaten van minder bekende merken hebben allerlei zwakheden die hackers gebruiken om toegang te krijgen tot het thuisnetwerk om vanaf daar bedrijven aan te vallen.

Ook de zonnepanelen zijn inmiddels slim. Honderden inwoners in Emmen werden slachtoffer van een datalek door onvoldoende beveiligde datakastjes van hun zonnepanelen. Via de kastjes voor energieopbrengst kon je inloggen op hun thuisnetwerk en bijvoorbeeld hun e-mails lezen. De woningcoöperatie waarschuwde meteen na de ontdekking de huurders dat ze hun wachtwoorden moesten wijzigen.

Hackers

Zijn slimme apparaten het nieuwe normaal? Waarschijnlijk wel. Gemiddeld hebben we er al vijf per persoon. Accountant Kees Tegel heeft ze ook: van een smart tv tot een moderne printer. Maar toen kwam de installateur van zijn sauna langs.
"Wat is uw wifi wachtwoord?", vroeg hij.
"Mijn wifi wachtwoord? Waarvoor?"
"Om de sauna op het internet aan te sluiten."
Kees keek hem verbaasd aan. "Moet dat dan?"
"Nee, maar het heeft wel die functie, dus je kunt het net zo goed aansluiten. Dan kun je het ook op afstand bedienen."
Zo dacht Kees er niet over. Eerder had hij heel bewust zijn crosstrainer niet op het internet aangesloten, terwijl het ook die functie had. "Veel mensen zien slimme apparaten niet als gevaar, maar de hack-aanvallen nemen toe. Des te minder apparaten je aan je netwerk hangt, des te veiliger je bent. Ik denk overigens niet dat we zonder smart apparaten kunnen, want veel van die functies zijn heel handig, ook voor bedrijven. Ik voorspel een gouden toekomst voor alle apparaten die met voorraad te maken hebben: van wc-rollen tot koffiemachines. Maar ik ga niet blind met de hype mee en dat is ook mijn advies aan anderen: denk na hoe groot het voordeel is als je een apparaat met het internet verbindt. Als je tevreden bent over hoe een wasmachine zonder internet wast, gewoon niet verbinden.

Meer dan de helft van de mensen die slimme apparaten in huis heeft, vindt updates een overbodige luxe of stelt ze te lang uit. Dat blijkt uit een onderzoek van het ministerie van Economische Zaken. Eén op de zes verwacht niet dat internetcriminelen belangstelling hebben voor hun apparaatjes.
Onveilige slimme apparaten kun je uiteraard weer veiliger te maken via een update, maar zitten we te wachten op een stroom updates? Ik ken veel mensen die nu al klagen over te veel updates voor hun computer en mobiel. Ze klikken ze weg of drukken op 'later, later, later'.
Dat wordt dan heel leuk in de toekomst: elke maandag moet je je smart tv updaten, elke dinsdag je koelkast, elke woensdag de stopcontacten, elke donderdag je smart wc die je gewicht meet met sensoren, elke vrijdag je wasmachine en elke zaterdag je wifi koffiezetter. En wanneer je denkt dat zondag je vrije dag is: nee, dan moeten alle andere slimme apparaten een veiligheidsupdate krijgen om niet gehackt te worden, van je tandenborstel tot je robotstofzuiger en van je broodrooster tot je slimme elektrische deken. Mocht je denken dat dit een slecht scenario is: als de fabrikanten niet geregeld met updates komen, dan wordt het nog erger. Dan is het niet de vraag óf maar wanneer hackers je computer of mobiel binnendringen.

Auteur: Rik van Dijk is student Cyber Security Engineering aan de Haagse Hogeschool en is bereikbaar via r.c.m.vandijk@student.hhs.nl.

Wat te doen aan kwetsbaarheden in TCP/IP-Stacks?

Eens in de zoveel tijd worden we opgeschrikt met berichten over miljoenen kwetsbare IoT-apparaten door fouten in TCP/IP stacks. Deze componenten bevinden zich in de keten van onderdelen waarmee veel IoT-apparaten worden gebouwd. Hoe gaan we om met zulke kwetsbaarheden? En wat zeggen nieuwe richtlijnen voor veilige IoT in de Europese Unie en Singapore over het voorkomen en oplossen van problemen in de keten van IoT-apparaten?

Op 12 april 2021 bracht beveiligingsbedrijf Forescout het nieuws naar buiten dat zij in vier bekende TCP/IP-stacks, de protocol suite om apparaten over het internet te laten communiceren, een aantal kwetsbaarheden gerelateerd aan de implementatie van DNS hadden ontdekt. Techwebsite ZDNET meldde een dag later dat miljoenen IoT-apparaten mogelijk kwetsbaar zijn (1). Het interessante? Precies hetzelfde verhaal speelde zich het afgelopen jaar twee keer eerder af.

In juni 2020 ontdekte beveiligingsbedrijf JSOF een serie fouten in de protocol suite van Treck, een bedrijf dat zich specialiseert in het ontwerpen van stacks voor embedded apparaten. Onderzoekers van JSOF doken in de code van de veelgebruikte suite. Zij ontdekten een serie kwetsbaarheden van bugs die Denial of Service mogelijk maakten tot fouten die Remote Code Execution (RCE) toelieten op het apparaat (2).

De fouten zitten bijna allemaal in het afhandelen van geheugen. De library, geschreven in C, mistte checks op het verwerken van input en typecasting waardoor een aanvaller memory corruption aanvallen kon uitvoeren. In totaal ontdekte JSOF 19 kwetsbaarheden, die zij passend Ripple20 noemden. ZDNET en andere securitywebsites meldden prompt dat miljoenen apparaten kwetsbaar waren door de ontdekking. In november 2020 voerde beveiligingsbedrijf Forescout een soortgelijk onderzoek uit naar negen andere populaire open source TCP/IP Stack libraries. Ook hier kwamen soortgelijke fouten naar voren. Bugs door verschillende overflows en underflows leidden tot kwetsbaarheden. In het minst erge geval maakten de fouten een DoS mogelijk en in het ergste geval stonden ze RCE toe (3). Deze serie kwetsbaarheden, genaamd Amnesia33, toonde nogmaals de gevoeligheid aan van fouten in deze suites. De componenten worden namelijk door een grote hoeveelheid verschillende producenten gebruikt, waardoor de impact groot is. De kwetsbaarheid van Internet-of-Things apparaten staat al langer in de schijnwerpers. Kwetsbaarheden zoals gevonden in Name:Wreck, Ripple20 en Amnesia33 zijn ook lang niet het zwaarste beveiligings-

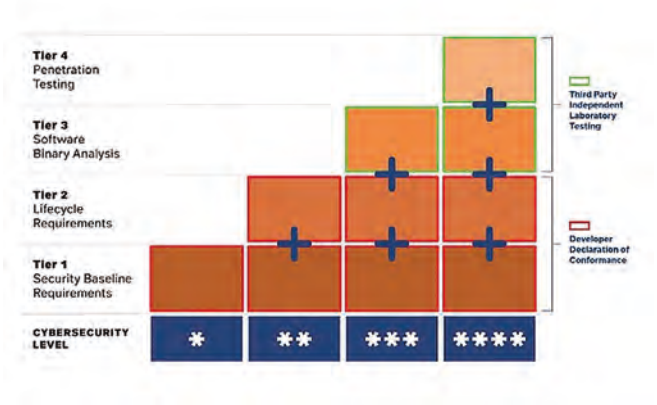
probleem waar apparaten mee te kampen hebben. Veel meer basale problemen zoals standaardwachtwoorden (admin/admin iemand?) en openstaande telnet-poorten zijn dringender.
Echter het interessante aan de problemen die JSOF en Forescout naar voren brachten, is dat het kwetsbaarheden zijn die niet direct het eigendom zijn van de producent van het apparaat. Het zijn fouten die verstopt zitten in de keten aan componenten die het apparaat gebruikt en door organisaties en sectoren wordt gedeeld. In een tijd waarin overheden meer en meer richtlijnen ontwikkelen om kwetsbaarheden in Internet-of-Things-producten aan te pakken, rijst de vraag: wat wordt er geëist van producenten voor het verhelpen van dit type kwetsbaarheden? We kijken naar twee initiatieven, de eerste van de Europese Unie, de tweede uit Singapore.

De vendoren

Laten we beginnen bij de vendoren van de apparaten die gebruik maakten van de kwetsbare TCP/IP-stacks. Volgens Forescout troffen de Ripple20 kwetsbaarheden in de Treck TCP/IP-stack 90.000 verschillende apparaten van 50 verschillende vendoren. Forescout herleidde ongeveer 50.000 apparaten naar de medische sector, bijna zeven keer meer dan de nummer twee, de retailsector. Op de derde plaats staan apparaten gelinkt aan de manufacturingsector (4).
De maker van de stack, Treck, ging na de melding door JSOF van de kwetsbaarheden aan de slag met het updaten van hun suite. Bleepingcomputer heeft de reacties op Ripple20 van getroffen vendoren verzameld. Zij categoriseerde reacties van 24 verkopers van mogelijk kwetsbare producten (5). De communicatie en geboden oplossingen verschillen sterk per producent, als er überhaupt al aandacht aan wordt besteedt. Van HP die firmware updates uitbracht voor hun getroffen printers, tot B. Braun, een bekende producent van medische apparaten, lieten weten dat 20 van de 24 aangeboden oplossingen van Treck niet werkte en dat de overige vier nog geanalyseerd werden. Of B. Braun uiteindelijk een oplossing heeft geboden, is niet terug te halen uit hun publieke communicatie (7). Als de analyse van Forescout klopt, betekent dit dat meer dan de helft van de vendoren helemaal niet is ingegaan op de kwetsbaarheden. Mogelijk wisten ze niet eens dat hun producten gebruikmaakten van de Treck suite of vonden ze het niet de moeite om een oplossing te bieden.

Regelgeving voor veilige apparaten

Beleidsmakers hebben de problemen met kwetsbare apparaten ook gezien en werkten de afgelopen jaren aan richtlijnen om de IoT-markt veiliger te maken. Ik wil hier twee initiatieven uitlichten: de richtlijnen rondom veilige IoT van de Europese Unie en Cybersecurity Labelling Schema uit Singapore.
De European Union Agency for Cybersecurity (ENISA) brengt al enkele jaren richtlijnen uit om IoT-apparaten veiliger te maken. Onder andere de Baseline Security Recommendations for IoT uit 2017 en Good Practices for Security of IoT uit 2019 bieden ontwikkelaars op verschillende niveaus handvatten om veiligere producten te ontwikkelen (7), (8). Bijvoorbeeld door standaardwachtwoorden af te raden of het opzetten van een Software Development Life Cycle. In de beschrijving van de Life Cycle, noemt ENISA dat ontwikkelaars bewust moeten zijn dat het gebruik van componenten van derde partijen risico's met zich meebrengt en dat deze gecontroleerd moeten worden op onder andere bestaande CVE's. Dat zou inhouden dat de oude versies van Treck's TCP/IP-stack niet meer zijn te gebruiken.
Maar wat wordt van een vendor verwacht als een nieuwe kwetsbaarheid in een component van het product wordt ontdekt? In november 2020 heeft ENISA een rapport gepubliceerd gericht op het veilig maken van de IoT-supply chains. Hier wordt expliciet als good practice genoemd software van derde partijen te categoriseren en te testen (9). Ook moet de vendor in ieder geval tot het verstrijken van de garantie beveiligingspatches aanbieden.
Een probleem met good practices is, zoals altijd, dat er nauwelijks consequenties zijn wanneer ze niet worden opgevolgd. Het blijft bij een uitgestoken hand die gemakkelijk kan worden afgewezen. De EU is bezig om te kijken of labels voor veilige producten een oplossing zijn, maar is op dit moment nog niet zo ver. Het is daarom interessant te kijken naar een land dat wel een labelschema heeft ingevoerd, Singapore.
Het Singaporese Cyber Security Labeling Scheme is in oktober 2020 ingesteld om consumenten te beschermen tegen slecht beveiligde IoT-producten. De start van het programma richtte zich op consumenten routers en smart home apparaten en is uitgebreid naar alle consumenten IoT-producten. Het schema kent vier niveaus waarbij aan elk opvolgend niveau zwaardere eisen worden gesteld (8).



Figuur 1 - Cyber Security Labelling Scheme uit Singapore.

Op niveau 1-2 volstaat een verklaring van de producent zich te houden aan de gestelde eisen. Op niveaus 3 en 4 komt er een onafhankelijke partij aan te pas die het apparaat test middels onder andere binaire software analyse (niveau 3) en pentesting (niveau 4). Het gehaalde label blijft geldig zolang de ontwikkelaar security patches blijft uitbrengen, tot een maximum van drie jaar. Bij grote verandering, zoals aanpassingen in de firmware moet het apparaat, wil het een label van niveau 3 of hoger krijgen, opnieuw getest worden.

Bekende kwetsbaarheden in suites van derde partijen zoals Ripple en Name:Wreck worden op niveau 3 naar alle waarschijnlijkheid door de onafhankelijke partij gevonden. In de meegeleverde checklist wordt voor niveaus 2 t/m 4 geëist dat zij kunnen aantonen dat componenten geen kwetsbaarheden bevatten. Bij niveau 2 wordt dit alleen niet door de onafhankelijke partij gecontroleerd. Ook wordt voor deze drie niveaus geëist dat patchinformatie tijdig en duidelijk wordt gecommuniceerd en kwetsbaarheden en oplossingen bekend worden gemaakt.

Conclusie

De serie kwetsbaarheden die in TCP/IP-stacks zijn gevonden zullen verre van de laatste zijn. Nu beveiligingsonderzoekers deze componenten onderzoeken, zullen steeds meer kwetsbaarheden in deze onderdelen naar boven komen. Het is aan ontwikkelaars van de componenten en de vendoren die ze gebruiken de taak om de kwetsbaarheden tijdig te verhelpen en afnemers van hun producten te informeren. Vanwege de brede verspreiding van componenten zoals TCP/IP-stacks zullen veel sectoren worden getroffen en zijn one size fits all oplossingen vaak lastig, waardoor patches moeilijker zijn dan een simpele druk op de knop.

Dat betekent niet dat producenten daarmee de verantwoordelijkheid kunnen afschuiven. Regelgeving is een goede stap om verantwoordelijkheid vast te leggen en het nemen van de juiste maatregelen ook te belonen. De Europese Unie biedt producten een hoop handvatten om hun productie en beheer veiliger in te richten, maar er is voor verantwoordelijke producenten niet een directe mogelijkheid dit duidelijk over te brengen naar kopers. Singapore biedt met het aanbieden van hogere labels aan producenten die investeren in beveiliging een mogelijkheid om die verantwoordelijkheid te tonen.

Hoewel de tijd moet leren of de onafhankelijke testinstantie genoeg capaciteit heeft en grondig onderzoek doet, is het opzetten van labels een goede eerste stap om kwetsbare componenten uit IoT-apparaten te halen.

Referenties

(1) https://www.zdnet.com/article/these-new-vulnerabilities-millions-of-iot-devives-at-risk-so-patch-now/

(2) https://www.jsof-tech.com/disclosures/ripple20/

(3) https://www.forescout.com/research-labs/amnesia33/

(4) https://www.bleepingcomputer.com/news/security/list-of-ripple20-vulnerability-advisories-patches-and-updates/

(5) https://www.forescout.com/company/blog/identifying-and-protecting-devices-vulnerable-to-ripple20/

(6) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

(7) https://www.bbraunusa.com/content/dam/b-braun/us/website/customer_communications/Update_Cybersecurity_Vulnerability_Ripple20_Letter_FINAL_090120.pdf

(8) https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

(9) https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain

(10) https://www.csa.gov.sg/programmes/cybersecurity-labelling/for-manufacturers

Auteurs: Beaubine Adriaansen is consultant privacy en informatiebeveiliging bij Strict B.V. en bereikbaar via b.adriaansen@strict.nl.
Charles Maas is Smart Technology Expert en projectleider bij diverse IoT-projecten bij Strict B.V. en bereikbaar via c.maas@strict.nl.

Internet of things, onlosmakelijk verbonden met privacy en security

Auto's die zelfstandig kunnen rijden, artsen die van een afstand patiënten kunnen monitoren, afwasmachines die aangeven dat ze defect zijn en het volgen van goederen/assets in de transportsector. Ondernemers, grote bedrijven, universiteiten en zelfs regeringen spreken erover. Het internet der dingen, of Internet of Things (IoT) houdt iedereen bezig.

Het internet der dingen gaat in essentie over 'dingen' of objecten die via het internet met elkaar verbonden zijn. In feite wordt door deze koppeling een model van onze realistische wereld in het internet afgebeeld. Een model waarvan we de elementen kunnen 'voelen' en 'beïnvloeden', onafhankelijk waar wij ons bevinden. In het algemeen zie je dat IoT wordt gebruikt om slimmer om te gaan met alles wat al bestaat, door de eigenschappen te meten en deze waarden naar een platform op het internet te sturen. Dit platform kan vervolgens besluiten hier iets slims mee te doen, bijvoorbeeld de omgeving aan te passen. Vandaar dat de term 'smart' vaak valt in combinatie met IoT. Er gaat geen dag voorbij of je hoort over Smart City, Smart Industry, Smart Home, Smart Energy en ga zo maar door. IoT maakt het mogelijk om steeds meer privacygevoelige data te generen en te combineren. Door de toename van dit soort toepassingen, vormen privacy en security een steeds grotere uitdaging binnen dergelijke ontwikkelingen.

In gesprek met…

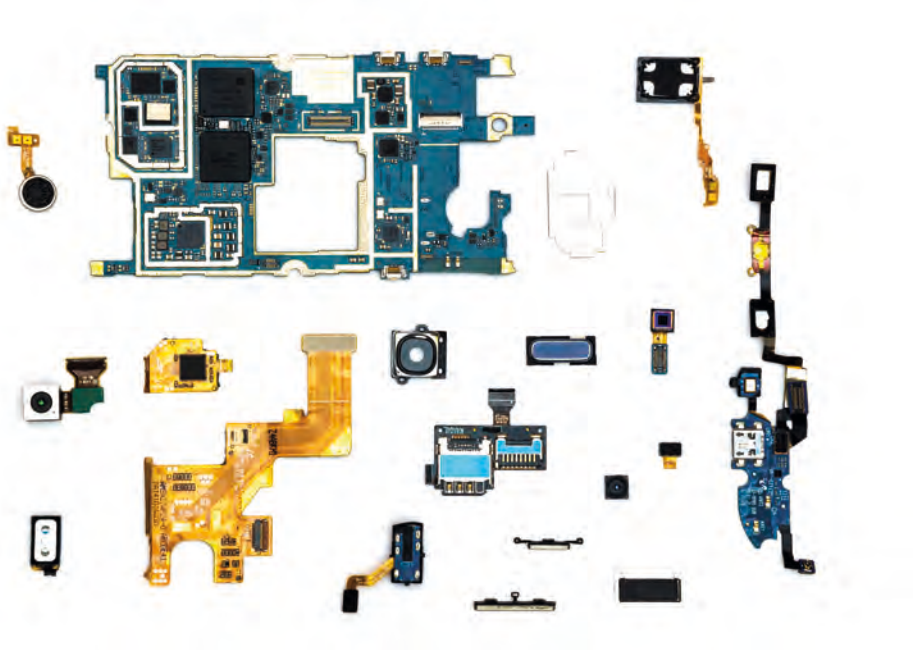
Met een achtergrond in ICT-recht ben ik werkzaam als consultant privacy en informatiebeveiliging. Vanuit die expertise adviseer ik klanten bij technologische ontwikkelingen zoals IoT. Privacy en security spelen bij dit soort projecten immers vaak een grote rol. Of zouden dit moeten spelen. Mijn ervaring leert namelijk dat deze onderwerpen niet altijd worden meegenomen in de uitrol van een project, of in ieder geval niet altijd even welkom zijn. Maar hoe ziet een projectleider dit zelf? Ervaart hij dit ook zo? Ik ben benieuwd waar men, op het vlak van privacy en security, in de praktijk tegenaan loopt bij het realiseren van nieuwe IoT-toepassingen. Daarom ga ik in gesprek met Charles Maas, Smart Technology Expert en projectleider van diverse IoT-projecten namens Strict.

Privacy en security vanaf de start

Zelf merk ik in mijn dagelijks werk dat de afdelingen privacy en security vaak (te) laat worden betrokken bij een project. Het komt regelmatig voor dat op de valreep wordt gevraagd of je 'even' een blik kan werpen op een innovatieve toepassing. Dit leidt vaak tot negatieve gevolgen voor het project zoals vertraging (tijd) en toenemende kosten (budget). Vaak blijkt dat er alsnog een Data Protection Impact Assessment (DPIA) of pentest moet worden uitgevoerd. In grote lijnen bepaalt de mate van volwassenheid van een organisatie op welke wijze privacy en security is ingebed in de beginfase van een project. We spreken hier in vaktaal over 'privacy en security by design'. Dit betekent dat er in een vroeg stadium, zowel technisch als organisatorisch, een zorgvuldige omgang met, en beveiliging van, (persoons)gegevens wordt afgedwongen. Zeker bij de start van IoT-projecten is dit belangrijk, omdat met IoT grote hoeveelheden data gegenereerd kan worden.
Organisaties zijn op dit vlak wel in ontwikkeling, aldus Charles. Toen hij begon als projectleider stond de brede inzet van IoT nog in de kinderschoenen. Aandacht voor privacy was er vier, vijf jaar geleden in zijn ogen nog weinig. Om dit tot de verbeelding te brengen vertelde hij me over een van zijn projecten waarin slimme sensoren werden ingezet om het volgen van devices mogelijk te maken. Waar vandaag de dag de alarmbellen voor een DPIA meteen zouden gaan rinkelen, werd destijds volstaan met een korte notitie waarin werd gesteld dat er geen personen gevolgd zouden worden. De afgelopen jaren zijn privacy en security binnen de wereld van IoT steeds belangrijker geworden. De komst van de AVG heeft de verplichtingen voor organisaties aangescherpt en daardoor is er automatisch ook meer aandacht voor beveiliging van informatie. Organisaties worden op dat vlak steeds professioneler, maar is nog voldoende ruimte voor verbetering.

Korte lijntjes

Het 'lastige' aan innovatie is dat je voorafgaand aan een project niet precies weet hoe een IoT-toepassing eruit gaat zien. Er is vaak sprake van een continue doorontwikkeling gedurende het project. Dit heeft als gevolg dat de scope van het project gaandeweg kan veranderen en dus ook de eisen die er gesteld moeten worden. Volgens Charles is het daarom verstandig om gedurende het project korte lijntjes met de privacy en security officers te houden. Ter illustratie, Charles is betrokken geweest bij een project voor de inzet van slimme



camera's. In een later stadium bleek dat er extra sensoren moesten worden toegevoegd omdat de slimme camera's niet aan alle eisen van de Business konden voldoen ...
Zo'n verandering brengt teweeg dat een nieuwe blik vanuit privacy en security vereist is. Dit kan wijzigingen tot gevolg hebben waar je niet omheen kunt. Naast vertraging en de nodige frustratie, heeft dit logischerwijs ook effect op de budgettering. Charles benadrukt dat het voor een innovatief project dus belangrijk is om naast je risicobudget ook een potje apart te houden voor extra kosten in het kader van privacy en security. Een pentest, de aanpassing van de security baseline of heronderhandeling van contractuele afspraken met leveranciers kosten immers tijd en geld.

De rekening voor de pentest

Bij IoT-toepassingen ben je in grote mate afhankelijkheid van de leverancier. Nadat de keuze voor een leverancier is gemaakt, is het volgens Charles belangrijk om goed in gesprek te gaan én te blijven. Met het oog op privacy en security is het vastleggen van bepaalde zaken van groot belang. Wie is waar verantwoordelijk voor? Is er al een verwerkersovereenkomst afgesloten? En hoe is het Identity and Access management (IAM) ingericht? Charles merkt dat organisaties daarin steeds hogere eisen durven te stellen, simpelweg omdat het markt-aanbod steeds groter wordt. Voor leveranciers is het dus belangrijk dat zij hun zaken goed op orde hebben. Wie de rekening mag betalen voor de ontwikkelkosten van de devices blijft soms lastig, geeft Charles aan. Enerzijds wil je als organisatie zelf een device testen, anderzijds wil je niet dat jij voor de kosten opdraait zodat de leverancier een veilig product kan leveren. De keuze om een pentest bij de leverancier te beleggen brengt weer risico's met zich mee. Charles heeft geleerd dat je de leverancier niet zomaar op zijn blauwe ogen kan geloven. Zo was er in een van zijn projecten een leverancier die aangaf dat een device aan alle beveiligings-eisen voldeed. Ter controle liet Charles een ethical hacker een pentest doen. En wat bleek? De beveiliging was verre van op orde.

Innovatie op de rem of wet- en regelgeving in de versnelling?

Terugkijkend op ons gesprek kan ik concluderen dat de werkvelden van Charles en van mij elkaar sterk raken. Dit zal alleen maar toenemen nu IoT een belangrijke drijfveer is voor innovatie. Er zullen steeds meer geavanceerde mogelijkheden zijn om veel data te genereren en te combineren en daarbij moet altijd rekening gehouden worden met (strenge) wet- en regelgeving op het gebied van privacy en security. Charles ervaart dat de AVG nu vaak belemmerend werkt en ook ik merk dat innovatie op dat gebied voor steeds meer nieuwe vraagstukken zorgt. Organisaties zullen door IoT steeds meer data verkrijgen en we moeten gaan nadenken hoe hiermee om te gaan. Moet innovatie op de rem? Of moet wet- en regelgeving in de versnelling? De toekomst zal het leren. Het is hoe dan ook duidelijk dat Charles en ik in de wereld van IoT met elkaar in verbinding blijven staan.

COLUMN Berry

Ik heb niets te verbergen

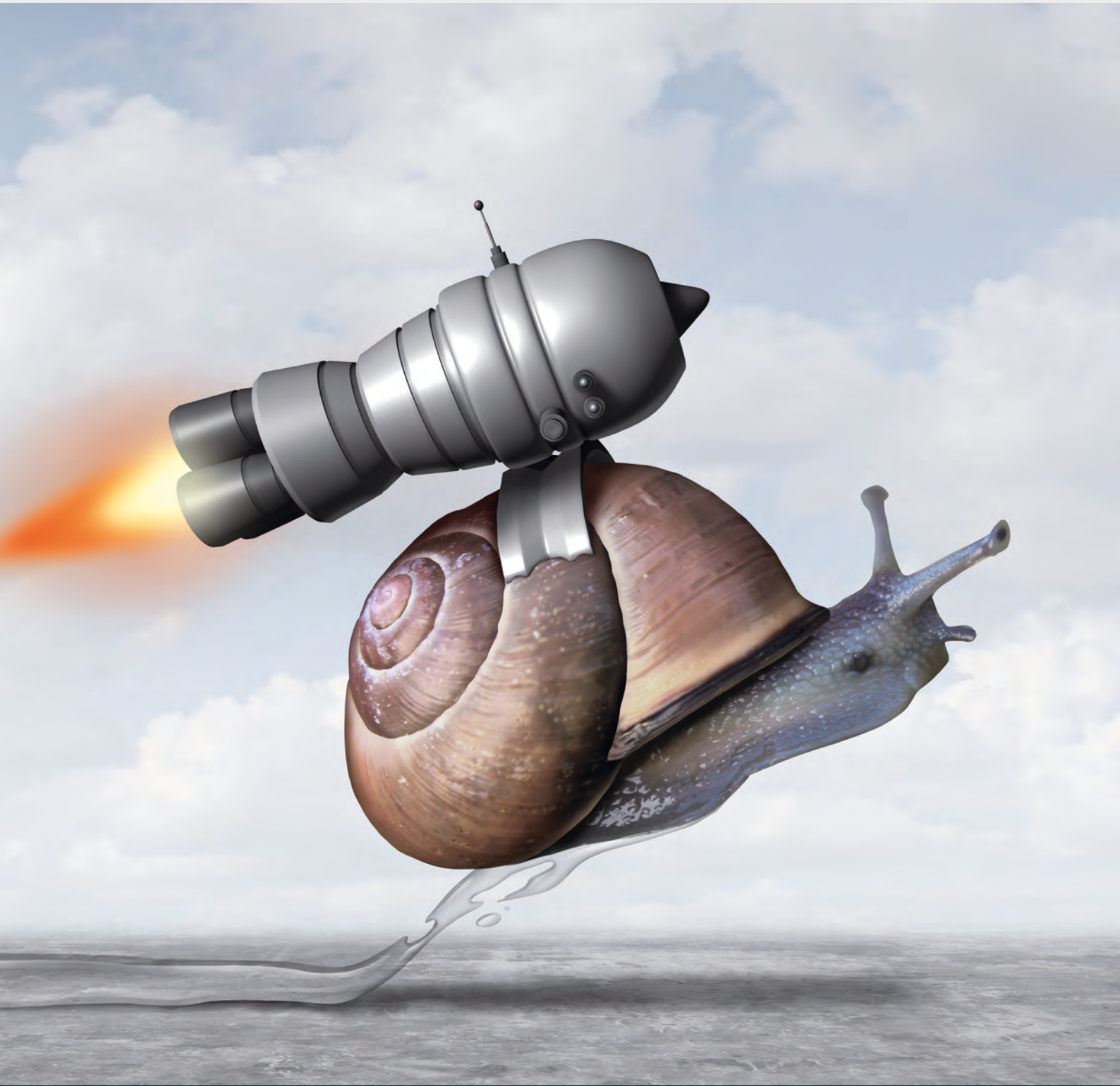
Ongemerkt zijn we de hele dag bezig bestanden te vullen van anderen. Als ik tank weet iemand dat ik om 15.34 uur 40 liter diesel tankte (sorry, ik ben nog van de oude stempel) en dat ik dat deed met een auto met het volgende kenteken. Om 17.00 uur rekende ik bij de kassa van de AH een kratje bier en 3 flessen wijn af. Ook die gegevens worden weer geregistreerd en de bonuskaarthouder weet dat ik wel een drankje lust. U kunt vast invullen waar u of uw acties geregistreerd worden buiten de deur.

Inmiddels werken we al een hele tijd vanuit huis en zal de controle iets minder zijn. Nee hoor, mijn baas weet precies met wie ik bel, hoe lang mijn gesprekken duren en hoe vaak ik met dezelfde persoon telefoneer. Hij wist al waar ik woon, hoe groot mijn gezin is, wat ik verdien, wat mijn BSN-nummer is, maar ook hoeveel toetsaanslagen ik maak (door de ARBO-software die mij bijtijds moet wijzen op het nemen van een pauze). Hij kent mijn surfgedrag en zou mijn mail kunnen bekijken, met nadruk op zou, want een klein beetje volwassen bedrijf heeft de verschillende functies goed gescheiden en zorgt ervoor dat expliciete toestemming moet zijn verleend om mijn gegevens in te zien.

Op verjaardagen vertel ik vaak over de grootste doomscenario's die kunnen gebeuren als mensen misbruik maken van de mogelijkheid data te verrijken met data uit andere databases. Een van mijn kinderen liep stage bij de IT-afdeling van de gemeente waar ik in woon. Net als zijn vader is hij van het nieuwsgierige soort en kwam erachter wat hij allemaal over mij kon vinden. Correspondentie, de WOZ-waarde van mijn woning, hypotheekinschrijvingen en ga zo maar even door. Is dat dan anders dan in het verleden, toen je ook alles kon vinden als je maar lang genoeg zocht? Ja dat klopt, maar een nieuwsgierige stagiair die zo snel veel gegevens vindt? Als je opgenomen wordt in een ziekenhuis en je heet Barbie en er duiken 85 niet behandelende ziekenhuismedewerkers in je gegevens, is dat dan goed te praten? Nee natuurlijk niet. Is het helemaal te voorkomen? Nee ook niet. Dat soort dingen is nauwelijks te voorkomen. Vooral niet als die vertrouwelijke gegevens ook nog veel geld waard zijn. Ik heb weleens geprobeerd bij te houden hoe vaak mijn gegevens in illegaal verkregen bestanden stonden. Ik wil en kan niet eens bijhouden wie allemaal min of meer terecht of onterecht bij mijn gegevens mogen komen. Als ik voor een te hoge bloeddruk bij de praktijkverpleegkundige terechtkom, zou die dan weten dat ik die week daarvoor bij de huisarts was wegens psychische klachten? Nee toch? Nee joh.

Berry

Auteurs: Jeroen Willemsen is security architect at Xebia Security and focuses on security automation, coaching & assisting development teams, and modern platform security. Jeroen can be reached at jwillemsen@xebia.com. Anne-Sophie Teunissen is Security Consultant at Xebia Security. She guides companies to treat security as a business responsibility. Anne-Sophie can be reached at ateunissen@xebia.com. This article is a follow-up to Dave Stein's article, 'Krijg je organisatie mee door de business te begrijpen en te sturen op waarde', iB-Magazine 2-2021.



Dear CISO: grow your organization. Don't be just the gatekeeper, be an accelerator

To get security right, we see at least three focus areas that need your attention as a security professional: risk appetite, security knowledge, and security culture. The recommendations for each of these focus areas will differ depending on where the organization is in its journey. In this article we look at the focus areas for a start-up, a scale-up and an enterprise...

DevSecOps! Shift left! These are terms you hear on stage, read in articles, and see in the media. Embedding security in your DevOps strategy starts with a strong collaboration between the security team and the engineering teams. After all: security is the responsibility of everybody. So far so good. But what does this mean? What should you do in your organization? Let us start with risk appetite: there are various definitions for risk appetite, but it basically boils down to: how much risk do you want to accept as an organization in order to create value. The higher the risk appetite, the more risk you are willing to take to create the value you persuade as an organization. Risk appetite can vary per area: you can have a very low risk appetite when it comes to public image (e.g. being marketed as a secure partner to collaborate with), but a high-risk appetite when it comes to how you craft your products (e.g. work on functions only, and no security checks).

Next up is security knowledge, the body of knowledge required to secure the IT of the organization. It comprises the various fields required to safely develop, deploy and run the IT stack used by the organization. This includes various activities, such as creating architecture definitions, threat modelling, defensive programming, (continuous) security validation, vulnerability verification, monitoring, and executing compliancy processes.

Last is security culture. This goes beyond the security awareness program. It is about taking ownership of the product that the organization builds, deploys and operates. Ownership comes with a sense of responsibility. This responsibility includes a need for employees to be aware, vigilant, and take security as serious as the risk appetite requires. Another facet of this focus area is trust. For every member of the organization, the same questions are relevant: do you trust that others take ownership and responsibility for security as well? Do you trust others to have operational excellence? And can you trust others when you share security issues? Trust and a sense of belonging are intricately connected. A well-functioning team, which engineers want to be part of, builds on trust, which then contributes to a culture of feedback and transparency. This greatly benefits the security practice. After all, an open culture helps to identify threats early on and to recognize security incidents faster.

Start-up!

When you are a start-up, there is often one goal: survive and grow. Whether you have a focus on getting a product out and capital in, or on getting your first chunk of market share: you will have a risk appetite which is relatively high. The primary worry is not about detecting and fixing every security vulnerability, it is about showing the value of the product that you are developing. In this stage we recommend focusing on the low-hanging fruit. For starters, get threat modelling off the ground and make sure you can fix your high-risk issues first. Next, create your core security building blocks, such as an authentication & authorization setup, and data encryption controls. Do not spend time on defence-in-depth controls that hardly reduce risks. Once you got the right investors on board to grow, you can start hardening the product more. Having the necessary security knowledge is key. We often see that the lead-developers and tech-savvy platform engineers have some basic security knowledge. This initially might be enough, but a security knowledgeable colleague can add a lot of value to the team, if they help developing the product further. This makes them the ideal start-up's security champion, who is eager to help the engineers to get somewhere fast. We recommend to `first have business to secure, then secure that business'. Start with big blocks, and do not mitigate every small risk before the idea behind the start-up comes to fruition. Unless the security of your product is one of the main selling points, of course.

Scale-up!

When you are a scale-up, the main goal is: get more sustainable. Grow features, show your value, get more customers, challenge and take-over the market. Given that you are now present and visible in the market and have more to lose, your risk-appetite might decrease. What are you willing to risk? How will this impact your growth? Risk appetite will vary given the sector you operate in and the investors you operate with. But in the end, you will have to keep taking risks to continue growth. Those risks should not get too big though, so it is time to further invest in your risk management processes to keep an overview of all the information risks. Unlike for start-ups, it becomes key to focus on lower risk issues as well. Given the increase of the amount of IT components in the organization, simplifying life-cycle management activities is key. This means that teams will have to follow sane rules of creating and maintaining IT components without too many manual interventions or inherent high risks. While your organization grows, so does the challenge of getting the right spread of security knowledge across your organization. At this point you might want to consider investing in automation and standardisation of best practices. Often a cure-all is hoped for by creating a security team. The security team should focus on helping the engineers forward: spread the knowledge, train people, raise security champions, and support engineering teams to become more self-sustainable. This enables them to do secure development, do threat modelling, and maintain a security pipeline. Is something high risk? Support in every step of the way when it comes to designing and implementing security controls. Do not be "just" the gatekeeper, be an accelerator. Obviously, at some point you will need to invest in some form of an oversight function. But in the early phases of your scale-up it is more important to grow a security community and start an educational program. One underestimated challenge when it comes to the security culture, is getting the scale-up through the growth spurt. Throughout this process you need to make sure that teams don't lose their sense of ownership, so that they will take the end-to-end responsibility for the security of the product seriously. Given this growth spurt, mutual trust can be under pressure as well. For instance, senior teams

might wonder whether the newly introduced engineering teams take care of the quality of the products equally well. Another example can be found in "us" versus "them" situations, between the engineering teams and the security team. We recommend investing in creating a secure base for the product the organization makes. Automate your security testing, foster champions, share knowledge, and make sure that teams experience ownership.

Enterprise & Government

When you are an enterprise or government organization, more is at stake, because you are a well-established name in the market. Similarly, the stakes rise when you have a big responsibility for society as an organization. You may have more to lose if something goes wrong, so the risk appetite of your organization lowers in comparison to the scale-up. This also has an impact on how you handle security but does not mean a culture of better safe than sorry is the ideal approach. Making a set of heavy-duty security controls mandatory for every part of the organization does not always make sense. For example, requiring a pentest on every change of a static website hosting the lunch menu of the canteen. The trick is to strike a balance. Your organization especially benefits from identifying information risks in the IT-stack and methods such as threat modelling are still of great value. It helps engineering teams to apply enough security. Enough security evolves around questions such as "Do I need to solve this vulnerability?" and "What is the risk if not doing so?". And it eventually gives the second line (and third line) of defence insight on whether decisions are in line with the existing risk appetite. When organizations get bigger, it is tempting to let security knowledge become a thing of the security team. It is quite difficult to bring the right level of security knowledge to an ever growing and changing workforce. Wouldn't it be convenient if a centralized team of security specialists has all the knowledge to help out the rest of the organization? The answer is no. The danger which rises here, is that a centralized security team cannot keep up with the engineering teams, and therefore slows down the development process. Instead, invest in role-based security awareness and knowledge, from developers to product owners to helpdesk employees. As for the security culture: when evolving to a reality where the security team is primarily responsible, the ivory tower is lurking. This creates the friction between security and engineering teams that so many organizations currently experience. Our advice would be: learn from the scale-up. Create an environment where the engineering teams have enough security capabilities – with or without the support of local information security specialists – and the centralized security team can advise on risk mitigation and at the same time perform their reporting role as a second line of defence.

We recommend investing in the trust between the security team(s) and engineering teams. And, at the same time keep building on creating a secure base.

While your organization grows, you will go through various transformations and adopt new processes as well as new technologies. Each of these will change your way of working. Each of these changes offers an opportunity for you as a CISO / security professional to grow and strengthen your bond with the organization. This can help you to tackle security the best way possible: together.

This article was published in Europe Cyber Security Perspectives 2020.

Auteur: Nouschka Auwema MSc, adviseur en onderzoeker cybersecurity bij de Rijksoverheid. Nouschka is bereikbaar via https://www.linkedin.com/in/nouschkaauwema/.

Titel	: Gedoe komt er toch. Zin en onzin over organisatieverandering
Schrijvers	: Joop Swieringa en Jacqueline Jansen
Taal	: Nederlands, Engels, Frans, Spaans
Aantal pagina's	: 101
ISBN	: 9789055943982
Uitgever	: Scriptum
Prijs	: € 17,50

BOEKREVIEW

Gedoe komt er toch. Zin en onzin over organisatieverandering

Mijn eerste gedachten bij het woord 'gedoe' zijn: vervelend, irritant, vermijden indien mogelijk, het is ongezellig en er komt conflict van. Toen ik er wat langer over nadacht, kwamen eigenlijk juist ook de voordelen ervan naar boven. Immers, door wrijving ontstaat glans. De auteurs van het boek *Gedoe komt er toch, zin en onzin over organisatieverandering* hebben daarom ook als boodschap: probeer gedoe niet te vermijden, maar zorg juist dat het op tafel komt. Een organisatieverandering is pas echt geslaagd als het werken daarna ook plezieriger is geworden.

Aan de hand van tien klassieke wijsheden over organisatieverandering laten de auteurs zien hoe een organisatieverandering succesvol tot stand kan komen. Waarbij gedoe onvermijdelijk is door het juist bewust ruimte te geven. Immers, de uitkomst van een organisatieverandering wordt bepaald door de manier waarop die verandering wordt aangepakt. De wijsheden die wat mij betreft het meest in het oog springen zijn: 'het goede van gedoe', 'een goed besluit behoeft geen draagvlak' en 'goed veranderen is jezelf worden'.

Bij het goede van gedoe beargumenteren de auteurs dat gedoe onvermijdelijk is en dat het er juist op wijst dat mensen in de organisaties iets met elkaar hebben. Daarmee begint iedere samenwerking. Op het moment dat er juist onverschilligheid ontstaat, is er een nog veel groter probleem dat gedoe dat aan het licht komt. De echte kunst van succesvol samenwerken is juist goed met gedoe omgaan. Daarbij horen zeker ongemakkelijke gesprekken en moeilijke blikken en uiteindelijk is het zaak om de opgeslokte energie om te zetten in een positieve samenwerking.

Onzekerheden op tafel

Wie heeft geen organisatieverandering meegemaakt zonder klankbordgroepen, stuurgroepen, projectgroepen en welke varianten nog meer? Wie er ooit in heeft gezeten, kan zich vast wel het gevoel voor de geest halen dat er soms meer niet dan wel naar je geluisterd wordt. Dat is onbevredigend. De auteurs laten zien waar dat door komt. De functie van dergelijke praatgroepen is meestal niet zozeer om mee te denken over veranderingen, ze te bevorderen en aan te jagen, maar juist om ze tegen te houden. Het probleem ontstaat als het formeren van deze groepen als doel heeft om draagvlak te creëren en acceptatie te verkrijgen. Hier zit echter vaak de managementgedachte achter dat er per definitief weerstand zal zijn tegen veranderingen. In de meest penibele situatie kan het zelfs leiden tot wantrouwen in het proces en uiteindelijk de mensen. Vanuit het management richting werknemers en vice versa. De oplossing hiervoor is niet om nog meer praatgroepen in te stellen om nog meer draagvlak pogen te krijgen, maar juist om onzekerheden en angsten op tafel te leggen. Daarmee wordt juist vertrouwen in en respect voor elkaar gecreëerd. Draagvlak ontstaat juist als het management de beslissingen neemt over organisatieverandering en die op een heldere manier naar diens werknemers communiceert. Belangrijk daarbij is ook om werknemers niet enkel bij de verandering te betrekken en ze er ook (mede)verantwoordelijk voor te maken.

Goed veranderen is jezelf worden. Of gaat het juist om jezelf blijven? De kunst van het permanent of lerend veranderen vereist dat een organisatie heel helder heeft wat moet blijven. Veranderen geeft immers gedoe. Wellicht de beste manier om houvast te bieden bij dat gedoe, is te weten wat je niet wilt veranderen. Te vaak draait een organisatieverandering om 'of-of' beslissingen. We gaan of veranderen of we blijven doen wat we altijd al deden. De kunst van een succesvolle verandering is de vraag stellen: wat willen we blijven doen en houden uit het verleden? En wat willen/moeten we anders doen? Daarbij is het cruciaal dat een organisatie scherp heeft wat de missie is: waartoe zijn wij op aarde en waar staan wij voor? Oftewel zoek uit wat de kernopdracht is en welke kernwaarden daarbij horen. De bijbehorende identiteit van een organisatie blijft vaak hetzelfde, terwijl gedrag juist veranderd. Stel hiervoor een missie op die aangeeft wat in alle komende veranderingen onveranderd blijft. 'Een missie geeft niet aan waar we naar toe moeten, maar wel of we afdwalen'.

Juich voor gedoe

Dit vrij intense digitale tijdperk waarin we al enkele decennia verkeren, heeft, al dan niet ongemerkt of bewust, vele organisatieveranderingen met zich meegebracht. Binnen enkele seconden (of minuten afhankelijk van je internetsnelheid) kun je contact maken met een wildvreemde aan de andere kant van de wereld. Digitalisering heeft veel voordelen, maar denken we ook eens aan hoe al die verregaande digitalisering effect heeft op onze samenwerking met de mensen direct om je heen? Overschatten we daarmee niet juist de connectiviteit en onderschatten we niet het sociale aspect van samenwerken met je collega's? We lijken soms geen moeite te hebben om in bijvoorbeeld videogames met diverse mensen uit diverse culturen en landen samen te spelen, maar verandering teweegbrengen of gedoe aan het licht brengen in je eigen organisatie lijkt daarentegen best lastig in de praktijk.

Laten we daarom de adviezen van Swieringa en Jansen ter harte nemen en 'juich voor gedoe'! Maak het expliciet, ga met elkaar in gesprek en lucht je hart, zeg wat je denkt en voelt, veronderstel geen weerstand en een gebrek aan draagvlak, communiceer helder en vertrouwen en verantwoordelijkheid zijn de basis voor elke succesvolle organisatie(verandering). Een beetje humor kan meestal ook geen kwaad.

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

BLOG

Security sneltest

In zeven vragen zelf bepalen hoe je security erbij staat: hier kan het. Natuurlijk alleen voor algemeen bekende pijnpunten en best practices, maar het geeft toch snel een beeld.

1. Heb je inzicht in je security-incidenten?
2. Heb je een piepsysteem voor autorisaties?
3. Heb je inzicht in de mate van patching van software?
4. Werkt je back-upsysteem?
5. Heb je een gedragscode computergebruik voor alle medewerkers?
6. Heb je inzicht in de mate van naleving van die gedragscode?
7. Werk je op het gebied van information security samen (met externe partijen)?

Een 'ja' op deze vragen is helaas vaak ongefundeerd en daarom het slechtst denkbare antwoord.

Het is een gebluft 'ja', omdat een woord in de vraag ergens wel vaag bekend klinkt. Of omdat het lopende security-project met een beetje goede wil eigenlijk 'logische toegangsbeveiliging' is. Of omdat je gezien de gedane inspanningen de project-deelnemers gemotiveerd moet houden. Of een bang 'ja', omdat je de veeleisende nieuwe manager niet wilt teleurstellen met de melding dat na maar liefst twee volle werkweken de informatiebeveiligingsvolwassenheid ('security maturity') nog niet één niveau hoger is gebracht.
Een 'ja' is gegokt als over bestaan en werking van een systeem (zoals bij 2, 4 of 5) geen regelmatige rapportage bestaat, door een van de uitvoerder onafhankelijke, inhoudelijk deskundige persoon. Of die rapportage is er, maar de sneltest-beantwoorder leest hem niet iedere keer. Of leest hem wel, maar begrijpt hem nooit helemaal door jargon, afkortingen en onduidelijke lijnkleuren in grafieken. Ook is 'elk jaar met Olympische Zomerspelen' wel zeer regelmatig, maar niet frequent genoeg om security gericht te kunnen bijsturen.
Een 'buiten je boekje ja' kan ook: de sneltest-beantwoorder weet dan meteen het antwoord doordat hij/zij op security gebied alles zelf doet. Dus zonder activiteiten te delegeren aan medewerkers met meer beschikbare tijd en deskundigheid, of zonder verantwoordelijkheden zoals toepassen van softwarepatches op de juiste (technische) plaats in de organisatie te leggen. Daarom zijn in deze sneltest soms, af en toe, regelmatig, vaak of best wel iets betere antwoorden. Die zijn weliswaar niet objectief te meten, maar deze antwoorden kun je wel onderling rangschikken. Je twijfel of je

inderdaad van alle gevallen binnen de organisatie op de hoogte bent (‘voor Windows 10 werkplekken hebben we het lek dicht, maar hoe staat het met die oudere servers?’) is nuttig. Net als het realistische inzicht dat er in de praktijk uitzonderingen zijn in de toepassing van algemeen geldende beleidsregels. Met ‘een beetje’ of ‘niet zoveel als we zouden willen’ antwoorden ben je op de goede weg. Het allermooiste antwoord is een hartgrondig ‘nee’. Daaruit blijkt namelijk dat de beantwoorder de waarde van het onderwerp erkent. Hij weet dat het gevraagde niet altijd aanwezig is, dat het niet altijd perfect werkt, dat er personeelsverloop is in de uitvoerende functionarissen, of dat we al meer dan een jaar corona hebben. Soms bestaat het bedoelde systeem wel, maar pas sinds een week. Het is daarom hier beter een negatieve instelling te hebben en ‘soms’ te veranderen in ‘nee’. En niet een ‘soms’ werkelijkheid innerlijk te presenteren als ‘regelmatig’ en daarna te antwoorden met ‘ja’.

Een negatieve uitkomst levert in deze sneltest dus het meeste op. Dan heb je immers meteen je actiepunten te pakken. Want iedereen begrijpt dat je vraagt om securityproblemen wanneer je zelfs deze bescheiden zeven stuks nog niet hebt geïmplementeerd.
Om je te helpen ‘negatief te denken vind je hieronder een toelichting per vraag.

Ad 1. Incidenten

Inzicht betekent dat je uit geregistreerde melddatum+tijd weet hoeveel security-incidenten er zijn per tijdsperiode. Hoe ze zijn verdeeld over kleine, gemiddelde en grote impact. Over gemakkelijk, gemiddeld en gecompliceerd om op te lossen. Naam van indiener en oplosser zijn bekend, zodat je ziet wie de moeilijkste gevallen ontdekt en wie ze herstelt. De oplosduur tussen melden en definitief afgemeld (sommige incidenten worden op de melddag zelf al opgelost). En een extra kolom ‘kan nooit meer optreden J/N’ naast de ‘quickfixed’ kolom.

Ad 2. Piepsysteem

Bij een piepsysteem krijgt iedereen net iets te weinig toegangsrechten om hun werk te kunnen doen – en je wacht tot ze gaan piepen om het ontbrekende stukje. Iedereen beseft dat dit een speciaal verzoek is, dat gemotiveerd moet worden en daarna beoordeeld namens de systeemeigenaar. Die verzoeken moeten betaald worden en de motiveringen kun je bewaren. Zo kun je bij een incident objectief bepalen welke medewerkers die bijzondere rechten hebben waarmee het incident (zoals: ‘hele database gewist’) is veroorzaakt.

Ad 3. Patching

Als de leverancier uit zichzelf en gratis een herstelpleister (patch) aanbiedt voor zijn software kun je die maar beter meteen toepassen. Zeker bij een wereldwijd bekend gemaakte kwetsbaarheid. Het inzicht is nodig voor alle software (soorten) die je gebruikt (zie: ‘keten en wakste schakel’).

Ad 4. Back-up

Het back-upsysteem moet de gemaakte veiligheidskopieën op het gewenste moment terugplaatsen. En gericht, alleen voor die ene gebruiker of zelfs uitsluitend dat ene bestand. In plaats van dat alleen de complete data-kubus voor de afdeling kan worden teruggezet naar de stand van gisteren (of eind vorige maand …). Dat moet je regelmatig testen want ‘echt’ restoren komt hopelijk niet zo vaak voor. Zorg ervoor dat bij een ransomwarebesmetting de malware niet ook je back-up versleutelt.

Ad 5. Gedragscode

Een gedragscode maakt medewerkers duidelijk wat op informatiebeveiligingsgebied wel en niet van hen verwacht wordt. Wel security incidenten melden, ook de zelf veroorzaakte. Geen ergens gevonden USB-sticks in het productiesysteem steken. Geen export maken van de database met persoonsgegevens van alle door jouw organisatie op corona geteste personen en die op Marktplaats (of het Darkweb) verkopen. Wel kritisch zijn op ‘te mooi om waar te zijn’ e-mails, die meestal phishing aanvallen zijn.

Ad 6. Naleving gedragscode

Nalevers, uit zichzelf of niet, hoeven niet meer (opnieuw) getraind te worden. Voor getrainde niet-nalevers is iets anders dan training nodig om het gewenste gedrag te verkrijgen. Bij 90% naleving en 90% (eerder) getraind heeft een generieke security training voor slechts 1 procent (= 0,10 x 0,10) van je populatie nut.

Ad 7. Samenwerking

Zoals De Dijk al zong: ‘Ik kan het niet alleen’, is het ook op security gebied noodzakelijk om net als cybercriminelen samen te werken met lotgenoten in dezelfde branche en onderling vertrouwelijk maar openhartig jullie lessons learned, best practices en take aways uit te wisselen. Want ‘Together Everyone Achieves More’ (= TEAM).

Auteurs: Prof. Aiko Pras is werkzaam bij de Universiteit Twente en is hoogleraar cyberveiligheid en initiatiefnemer van Twente University Centre for Cybersecurity Research. Hij is bereikbaar via LinkedIn: https://www.linkedin.com/in/aiko-pras-6999a86/?ppe=1, en: https://people.utwente.nl/a.pras. Chris de Vries is een zelfstandig professional en werkt onder de naam De Vries Impuls Management. Hij is tevens redacteur van dit magazine. Chris is bereikbaar via impuls@euronet.nl of LinkedIn: https://www.linkedin.com/in/chris-de-vries-a7a4b36/

INTERVIEW

Nieuw onderzoeks-centrum TUCCR

Op 5 maart jl. is Nederland een nieuw onderzoekscentrum rijker geworden: TUCCR en zoals de fonetische uitspraak van dit acroniem al aangeeft, heeft het zijn oorsprong in Twente. De oprichters zijn: de Betaalvereniging Nederland, BetterBe (Automotive Technology Solution Providers), Cisco, NCSC, NDIX (een open en onafhankelijk breed-bandnetwerk in Duitsland en Nederland), SIDN, SURF, Thales, TNO en de Universiteit Twente. TUCCR is een initiatief van hoogleraren Willem Jonker en Aiko Pras.

Redacteur Chris de Vries interviewde prof. Aiko Pras over dit initiatief. Zijn insteek: hoe maken zij een verschil uit met wat er nu al op de Nederlandse markt bestaat? TUCCR is een publiek-private-samenwerking (pps) waarbij het doel is, tot de top van Nederland in zijn soort te gaan behoren. Medio april was het moment voor een aangenaam, diepgaand gesprek.

Om met de naam te beginnen, is die toevallig gekozen of …?

"Zeker geen toeval, het is enerzijds een kwinkslag naar onze regio, maar anderzijds praktisch, want deze naam was vrij."

Eerst even een vraag over uzelf, wie bent u en hoe bent u in ons metier terechtgekomen?

"Zoals zo vaak speelt toeval een rol. Ik had interesse voor techniek en op de universiteit kwam ik bij de groepsonderzoek netwerkbeheer. Belangrijkste uitgangspunt destijds was de veiligheid. Een goede motivator was dat ik een soort van 'kleine jongen verbazing' ervoer, hoe van alles gebouwd kon worden als ware het speelgoed. Het raakte ook alle facetten van de samenleving en als onderzoeker was je bevoorrecht om – aan het begin staande – een pril idee zien te ontwikkelen tot het bewustzijn dat er een innovatie mogelijk was. De samenleving verandert, maar het is soms/vaak nauwelijks te begrijpen."

Is er te weinig IT-kennis in Nederland, waardoor TUCCR haar bestaansrecht heeft?

"Op het individuele terrein zeker niet, dan behoren Nederlanders tot de wereldtop, maar bij het algemene publiek ontbreekt die kennis en is er sprake van te veel naïviteit. Dit is ook bij de politiek het geval. Denk maar eens aan het zwart-wit beeld dat zo makkelijk geventileerd wordt, een zich afzetten tegen IT; met als meest recent voorbeeld de discussie rondom de vaccins tegen corona. Dus het TUCCR heeft zijn bestaansrecht omdat het de kennis op het gebied van cybersecurity wil verbreden."

Het TUCCR richt zich op drie thema's: 1. de netwerkveiligheid; 2. de dataveiligheid en 3. de daarbij behorende sociaaleconomische aspecten. Wat beoogt u met het derde thema?

"De eerste twee thema's zijn de focusgebieden van cybersecurity die we in Twente met `High Tech' aanduiden, en de laatste als 'Human Touch'. Informatici bedenken diensten vanaf scratch en achten hun oplossing als veilig. Maar de wereld is zoals zij is en bestudering van de werkelijkheid is noodzakelijk om zodoende ook de oplossing daarop af te stemmen. Hier ligt de kans om de techniek te koppelen aan ethische-, juridische-, bedrijfskundige-, psychologische-, wiskundige-, rechts- en andere (sociale) vakgebieden. Je kunt namelijk niet alles vanuit slechts één discipline oplossen!"

U benoemt als ethische vraagstuk 'het onderzoek naar zwakheden'. Waarom? Een huisarts onderzoekt toch ook de zwakheden van een patiënt en dan spreken wij niet over een ethisch vraagstuk?

"Het verschil is dat een huisarts gericht op zoek is op basis van de antwoorden van zijn patiënt. Zijn vragen krijgen ter zake doende antwoorden, wellicht vaag, maar toch. Een cybersecurity specialist stelt ook vragen, maar vaak open en dus generiek. Hij kan dan zaken vinden waarnaar hij niet op zoek was, bij een partij die hem niet kent. Dus hoe moet je als onderzoeker omgaan – indien je een backdoor ontdekt, al of niet van een veiligheidsdienst – met mogelijke consequenties van het technisch falen van een systeem. Het verschil zit hem dus in het open of gesloten karakter van de vragen en de bestaande of niet-bestaande relatie tussen de onderzoeker en de of het onderzochte."

Hoe selecteert u uit deze vakgebieden de juiste vraagstukken, waar richt u zich dan op?

"Onze focus is netwerk en data gedreven veiligheid. Je kunt niet alles doen en hoe interessant ook, onze focus ligt niet op crypto-algoritmen noch op privacyvraagstukken. En

Lager bedrag en/of `in kind' bijdrage aan onderzoek	Betalen voor tweejarige ontwerpers (PDEng)	Betalen voor promovendi (PhD)

Tabel 1 - Overzicht lidmaatschappen TUCCR.

vanuit o.a. dat netwerk veiligheidsdenken beschouwen wij dus bijvoorbeeld malafide webshops en phishing sites niet als onbelangrijk. Wij zullen dus gigantische hoeveelheden Domain Name System (DNS)-data verzamelen en doorzoeken op patronen op basis van de inherente afhankelijkheden. Ultieme vraag: wat als één partij (bijvoorbeeld DigiD) wordt aangevallen, omvalt en onbereikbaar wordt? Wat zijn de economische en sociale gevolgen? En hoe beperken wij dat risico? Om maar een paar voor de hand liggende vragen te noemen."

Uw definitie van een data gedreven benadering lijkt daarop aan te sluiten, maar is dat niet enkel het thema 'big data' en is er dan wel een onderscheid?

"Voor mij zijn big data en artificiële intelligentie (ai) slechts gereedschappen en niets meer. De data gedreven benadering omvat meer dan security by design. Het reikt verder en wel naar de ontsluiting van grote hoeveelheden data uit de harde werkelijkheid en het verkrijgen van inzichten uit de analyse van de veiligheidsproblemen. Om pas dan bestaande systemen te verbeteren en nieuwe te ontwerpen."

De multidisciplinaire benadering staat dus centraal?

"Ja, wij volgen een sociaalpsychologische aanpak en benadrukken niet enkel de techniek. Wij proberen potentiële hackers ertoe te brengen dat zij bewust worden van dat hun handelen dat tot een eerste stap naar een strafbaar feit kan leiden. Wij maken inzichtelijk dat naast de mogelijk grote economische effecten van een DDoS-aanval er nog veel grotere, belangrijkere, andere effecten kunnen ontstaan. Deze aanpak leidt tot inzicht en remt jongeren af het gevaarlijke pad op te gaan. TUCCR ziet bewustwording als één van haar doelen."

Als voorbeeld van het fenomeen DDoS werd op de website van TUCCR de casus bij SURFnet aangehaald waar nu een onderzoeksteam van vijf tot tien mensen is op gezet. Is dat niet veel te weinig?

"Het probleem deed zich voor in 2012-2013 toen bij SURFnet het probleem van DDoS-aanvallen aan de orde werd gesteld. Na onderzoek bleek het te gaan om gamers die `onder water' actief waren. Tot dat moment was het probleem bij ons nog niet onderkend en zette de markt dus de universiteit op het spoor. Deze ervaring leidde tot een community opbouw (DDoS clearing house) en uiteindelijk tot een anti-DDoS coalitie. Dit kleine begin werd door opschaling een belangrijk onderdeel in het Europese Concordia project, en daardoor recent door de Europese Commissie als High Potential Innovation aangemerkt. Via het Concordia project zijn er weer goede contacten met het recent in Boekarest gevestigde Cybersecurity Competence Centre (2020). Voluit heet het European Cybersecurity Industrial, Technology and Research

"You can enter anytime you like, but you can never leave!"

Competence Centre en het wordt aangevuld met een netwerk van nationale coördinatiecentra."
"Terugkomend op jouw vraag, ja het lijkt erop dat het een (te) klein team is, maar de community opbouw (o.a. als Horizon 2020 project), de opschaling met deelnemers uit de multinationale bedrijfsomgeving (circa 33%) en het Midden- & Klein Bedrijf (ook circa 33%) compenseren dat op hun beurt weer. Het onderzoek wordt goed gecoördineerd."
"Wat mij wel zorgelijk lijkt is dat DDoS-aanvallen effectiever kunnen plaatsvinden indien die rechtstreeks de applicatie laag kunnen benaderen. Neem als voorbeeld digitale betalingen die via versleutelde verbindingen lopen. Als er een DDoS-aanval op de applicatielaag wordt uitgevoerd, moet vaak de applicatiedata worden geanalyseerd om de aanvalsdata te filteren. De versleuteling loopt dus tot het systeem dat deze analyse uitvoert. Maar als dat een systeem is van een Amerikaans bedrijf, kan de Amerikaanse veiligheidsdienst meekijken. Dit maakt de verdediging tegen statelijke actoren en slimme hackers opeens een heel stuk moeilijker. Wie kijkt dan allemaal digitaal mee?"

Hoe past een lidmaatschapsstructuur in een publiek-private samenwerking?

"In cybersecurity komt de hockeystickbenadering binnen het bedrijfsmodel zelden voor, bij bedrijven veelvuldig. Daar zit een deel van de toegevoegde waarde en het motief voor een lidmaatschap, waarbij wij gradaties kennen van brons tot goud. Wij vragen van onze partners serieuze betrokkenheid, waarbij het wel mogelijk is te onderscheiden in commerciële en niet-commerciële partijen. Een voorbeeld van dat laatste is het Nationaal Cyber Security Centrum (NCSC) dat bijdraagt door de inzet van mensen."

Wat houdt de financiële garantiestelling in bij de partnerschappen?

"Dat varieert naar partnerschap, waarbij een goud-lid betaalt voor de promovendi (€ 90.000,00 per jaar) en dat over een periode van vijf jaar. Bij een brons-lid spreken wij over een minimale 'in kind' bijdrage en dat zal dus afhangen van het aantal personen en de duur dat een brons-lid hen vanuit de eigen organisatie inzet."

Eén van de benoemde vraagstukken voor TUCCR is de privacy van burgers. Nu mis ik in de publiek-private samenwerking juist die burger als deelnemer of partner. Hoe ziet u dat?

"In principe hoort de burger erbij, maar de realiteit is dat een publiek-private samenwerking gedragen moet worden door financiële dan wel 'in kind' bijdragen. En een burger stopt daar niet veel geld in. Anderzijds zouden wij in gemeenten, als vertegenwoordiger van, wellicht wel de burger terugvinden."
"Mogelijk dat de burger wel een rol zou kunnen spelen bij interessante ontwikkelingen zoals: 'Social Licenses to …' en crowd funding, hetgeen slechts een model is. Noodzakelijk is wel dat de overheid structureel meer geld ter beschikking stelt, zoals vastgelegd in het rapport van de Cyber Security Raad (1), (2). En dan schiet mij ook een prachtig voorbeeld te binnen van 's werelds eerste non-profit computer security consultancy bedrijf: 'Radically Open Security' van Melanie Rieback (3). Zij streeft er naar de samenleving te helpen een omgeving te creëren waarbinnen digitale veiligheid voor iedereen vanzelfsprekend is. Dus transparantie is essentieel (4)."

Hoe moeten wij de verhouding zien tussen TUCCR en EIT Digital?

"Ook hier speelt toeval weer een grote rol. Professor Willem Jonker (mede-initiator van TUCCR) en ik kennen elkaar al heel lang. Alhoewel we complementair werken, hebben we eenzelfde gedachte over wat nodig was binnen ons vakgebied. Willem is een man met politieke visie en connecties, hij is daarnaast de CEO van EIT Digital (5), een door Europa medegefinancierd digitaal innovatie en

"Cybersecurity is niet het probleem over de schutting gooien, maar pak het zelf op. Het gaat ons allen aan!"

opleiding ecosysteem. Ik zie mijzelf meer als de man voor de technische inhoud. Samen waren wij de mening toegedaan dat er te weinig IT-kennis in de regio en Nederland geborgd was en daarom namen wij het initiatief. Vooralsnog is TUCCR voor 50% lokaal en 50% nationaal. Op termijn zullen wij ook internationaal actiever worden, maar een substantiële lokale component zal altijd blijven bestaan."

Stelt TUCCR zich misschien te bescheiden op door te stellen dat Nederland te veel IT-kennis mist? Dit als je bijvoorbeeld kijkt naar Nederlandse game-ontwikkelaars en hun positie en naam in de wereld en eveneens de bereidheid van de Nederlander tot acceptatie van IT-innovatie?

"Zoals ik eerder al zei, op individueel niveau komen wij goed mee, maar als het gaat om bedrijven en samenwerkingen hebben wij nog te leren. Neem bijvoorbeeld de veelvuldige hacks (onlangs waren de kaasschappen bij Albert Heijn leeg, door een hack op een exchange server). Veel bedreigingen van deze aard worden uitbesteed in de cloud of in Office365, maar wat zijn de consequenties van die uitbesteding? De wetgeving van de Europese Unie met betrekking tot de Amerikaanse cloud noodzaken vroeg of laat dat bedrijven terugkeren naar Europese servers."

"De Europese rechter heeft om privacyredenen de uitbesteding aan Amerikaanse IT-bedrijven al een aantal keren teruggefloten. Een strategische terugkeer 'out of the US-cloud' is te verwachten, maar de strategie van deze spelers is vooral vendor-lock-in! Daar komt bij mij het gezegde op: 'You can enter anytime you like, but you can never leave!'."

"De Nederlandse positie op de wereldmarkt is eveneens een kwestie van digitale soevereiniteit. Nederland bezit een open samenleving, wij zijn een sociaaldemocratie. Toch beleefden we in 1989 een omslag. Het kapitalisme declareerde haar zege over het communisme en veel teugels werden gevierd onder leiding van Thatcher, Reagan en Clinton. Dat leidde tot een zorgelijke ontwikkeling met betrekking tot juist die digitale soevereiniteit, want burgers geven – in goed vertrouwen – niet hun data, maar hun gedrag. Voorbeelden hiervan: Google en Facebook die het openbare debat vanuit de VS beïnvloeden, niet alleen als het gaat om Nederlandse tradities zoals Zwarte Piet of de schilderijen van Rubens, maar ook de Brexit-uitslag en Trumps presidentiële verkiezingswinst 2017 tonen de macht van deze bedrijven en de gevaren van het verlies aan digitale soevereiniteit."

Tot slot, u bent toegankelijk gebleken om over het TUCCR initiatief te spreken, wat motiveerde u daarin?

"Het thema cybersecurity, omvattende netwerk- en dataveiligheid ingebed in een multidisciplinaire omgeving moet aandacht krijgen. Wij hebben daar allemaal een rol in te spelen. Willen wij de (informatie)maatschappij verbeteren dan moeten wij alle doelgroepen weten te benaderen. Het iB-Magazine is een onderdeel van deze maatschappij en kent onder haar leden velen uit onze doelgroep. Het is dan logisch om met en via jullie te communiceren met partners in het vak. Cybersecurity is niet het probleem over de schutting gooien, maar pak het zelf op. Het gaat ons allen aan!"

Referenties

(1) https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

(2) https://www.cybersecurityraad.nl/documenten/mediateksten/2021/04/06/infographic-csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

(3) https://www.radicallyopensecurity.com/team/MelanieRieback/

(4) https://www.ictu.nl/publicaties/interview-met-melanie-rieback-van-radically-open-security

(4) https://www.eitdigital.eu/

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

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
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 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Provide a root of trust and end-to-end data protection for your IoT with Entrust nShield HSMs.

LEARN MORE AT ENTRUST.COM/HSM

ENTRUST

SECURING A WORLD IN MOTION