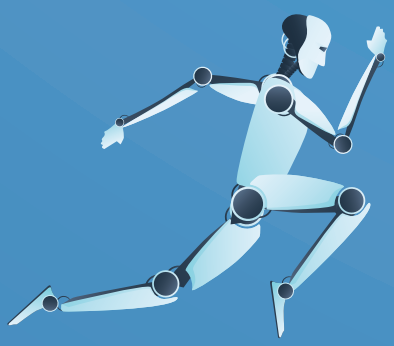
INFORMATIEBEVEILIGING MAGAZINE

future



- Hulpgids beveiliging voor het kleinbedrijf (deel 1)
- Dark patterns in cookie consent notices
- Column: A.I., A.I., Caramba!

JAARGANG 23 - 2023 - EDITIE 2

WAT IS ISO 27701?

De 15 meest gestelde vragen over de privacy management norm ISO 27701.

De garantie dat persoonlijke informatie door organisaties op de juiste manier beschermd wordt, groeit. Privacyrichtlijnen zoals de AVG verplichten organisaties om de bescherming van persoonsgegevens te garanderen. De internationale ISO 27701 standaard is een uitbreiding op de bestaande informatiebeveiligingsnorm ISO 27001 en biedt richtlijnen voor de bescherming van privacy. De norm helpt organisaties om informatie op een correcte manier te beheren en privacywetgevingen na te leven.

Vraagt u zich af wat de meerwaarde van ISO 27701 certificering is of wilt u weten of ISO 27701 certificering voor uw organisatie verplicht is? Rob Jansen, IT-security auditor en trainer, geeft u antwoord op de meest gestelde vragen als het gaat om privacy management en de ISO 27701 norm.

Lees de antwoorden op de vragen op www.dnv.nl/watisISO27701 of scan de QR-code.

DNV

‘Een nieuwe lente en een nieuw geluid’

Chris de Vries

De titel verwijst naar Herman Gorter en naar de openingsregel van het gedicht *Mei*. Hoewel het nog geen lente is, zou dit ook kunnen opgaan voor ons magazine. Ik ervoer de eer uitgenodigd te worden het hoofdredacteurschap op mij te nemen. Dat - na rijp beraad – accepterende, bracht mij ertoe alle redacteuren (en ons bladmanagement MOS) te (gaan) benaderen om te spreken over onze gezamenlijke toekomst. Dat proces loopt nog.
Toch kan ik nu al zeggen dat de inbreng van mijn collega-redacteuren, hun ideeën, suggesties en actieplannen, mij veel vertrouwen geeft in de toekomst. Zij tonen creativiteit, wens tot professionaliteit, het zoeken naar nieuwe wegen en vooral het in contact komen met jullie als lezer/lid.
In de komende maanden formuleren wij onze plannen diepgaander, stemmen we deze met het verenigingsbestuur en haar commissies af en zullen wij ook ‘buitenstaanders’ in onze brainstorm betrekken. Doel: gedachten omzetten in daden.
In deze uitgave tekent zich dat al een klein beetje af. Onze voorzitter, Jessica Conquet, heeft het in haar column over de community, waarin de wereld verbeterende informatiebeveiliger actief bijdragen levert en ook onze vereniging doet groeien.
Dimitri van Zandvliet gaat in zijn column in op de meest recente ontwikkelingen, waaronder AI en haar betekenis voor ons leven in de nabije toekomst. Voor de fervente lezers onder ons gaat Valentijn Ishaqsada in op het boek *Waardering van de informatiebeveiliging* van Clemens Willemsen en als ‘cookie’ bij de koffie brengt Jelle Slotman ons op de hoogte van ‘Dark patterns in cookie consent notices’ met zijn ethische studie om te komen tot een ‘cookie consent design’.
Ook starten we met een artikelenserie: *Hulpgids voor het kleinbedrijf.* Waarin met lezers en niet-lezers/niet-leden de discussie wordt gezocht via het magazine en LinkedIn. Interactie staat centraal, dus voel je niet geremd om de Security Scientist, Vincent van Dijk, met vragen te bestoken.
We vertrouwen erop dat deze eerste stappen/experimenten de weg zal zijn naar een vernieuwend magazine, met actieve participatie van jullie en een professioneel/lezenswaardig niveau dat het leven als informatiebeveiliger verrijkt.

Chris

IN DIT NUMMER

Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl

Hulpgids beveiliging voor het kleinbedrijf (deel 1)

Beveiliging van informatie (data), programmatuur (software), apparatuur (hardware) en ruimte (kantoren) tegen onbevoegden (‘hackers’) en tegen onbedoeld, abusievelijk, naïef handelen (personen/personeelsleden) is de kern van veilig digitaliseren. Elke ondernemer weet dat en ook dat er een oerwoud aan programma’s, apparatuur, handleidingen en adviseurs zijn om je daarmee te helpen.

Er zijn echter beperkingen, te weten: de (relatief) hoge prijzen voor programma’s en apparatuur. De hoge consultancy kosten en de tijd die je als ondernemer er zelf in moet stoppen, terwijl het je vak niet is en *zeker niet je liefde!* Voor instanties, overheden, groot- & middenbedrijven vaak geen probleem, maar voor de kleinbedrijven zeker wel. Vandaar het woordgebruik ‘relatief’.
De overheid, instanties en grootbedrijven spreken daarbij vaak over de ketenafhankelijkheden en de risico’s die daarvan uitgaan. En dus stellen ze eisen aan hun keten, voldoe je er niet aan (!?) … vergeet dan je kansen maar! Eisen zijn simpel, maar er aan bijdragen dat ook de kleinere partner mee kan doen, dat is andere koek. Die koek gaat uit van het kosten-denken, het denken aan sleutel-partners en aan kortstondige winstverlagingen. En wie zijn die kleinbedrijven eigenlijk, een ‘quantités negligeables’!?

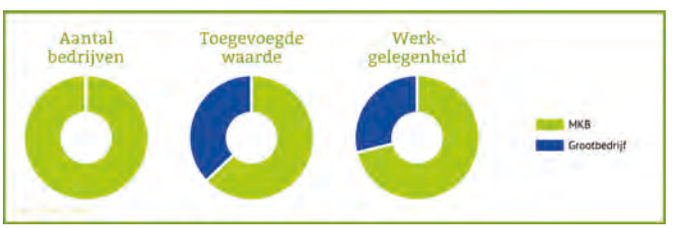
Het kleinbedrijf

De auteurs van dit artikel zien het kleinbedrijf zeker niet als een verwaarloosbare grootheid. Het is ons uitgangspunt dat juist de overheid, instanties en grootbedrijven medeverantwoordelijkheid moeten dragen om kleinbedrijven beter beschermd te laten zijn tegen de groot-hacker-machten. Dus eerst maar even ingaan op wat kleinbedrijf-getallen (uitgezonderd bedrijven met meer dan vijftig werkzame personen):

OK, wij weten dat er een groot aantal kleinbedrijven zijn, maar wat betekent dat nu in omzet? Wel in 2011 stond het MKB-bedrijf voor 888 miljard euro aan omzet en in 2020 voor 1.023 miljard euro aan omzet, dat betekent een groei van 135 miljard euro (15,2%) (2). De MKB-bedrijven zijn goed voor 71% van de Nederlandse werkgelegenheid in 2020 (3) en bijna 60% aan de Toegevoegde Waarde voor onze economie (4).

Werkzame personen	2007.Kw.1	2017.Kw.2	Toe-/afname
1	619.565	1.213.055	+593.490
2	158.445	176.905	+18.460
3 tot 5	81.295	89.490	+8.195
5 tot 10	60.100	62.940	+2.840
10 tot 20	32.635	31.280	-1.355
20 tot 50	20.280	18.865	-1.415
Totaal bedrijven	972.320	1.592.535	+620.215

Bron: Deels bewerkte cijfers, ontleend aan CBS, StatLine MBK, gewijzigd 13.01.2023 (1)



Figuur 1: Economisch belang aandeel mkb (5).

Er zijn in 2023 2,16 miljoen mkb-bedrijven in Nederland. In 2007 waren dat er 1,05 miljoen (6). De positieve/negatieve gang van zaken binnen het kleinbedrijf vertaalt zich in het aantal vacatures. In 2020, kwartaal 1, waren dat er in het kleinbedrijf 57.100. In 2022, kwartaal 3, circa 129.100: een groei dus van 126,1 procent (7). De vacatures bij het MKB, grootte 0-50 werkzame personen, in die jaren (2020 Kw.1 - 2022.Kw.3) waren respectievelijk 70.000 en 107.000 (een stijging van 52,9 procent) (7).

Ons uitgangspunt

Wij menen dat het niet zo kan zijn dat een zo belangrijk deel van het Nederlands macro-economisch belang vanuit data- en ketenveiligheid alsook privacy zo veronachtzaamd wordt. Dit omdat diezelfde groep ondernemingen ICT-organisatie technisch nu eenmaal achterloopt in kennis, (praktijk)vaardigheden en inzichten.

Drie stappen

De auteurs willen in een artikelenreeks de navolgende weg vervolgen:

1. zij begeleiden de ondernemers op hun weg tot Informatie- & Ketenveiligheid;
2. zij doen dat door middel van een vraag- en antwoordaanpak en
3. zij vertrouwen erop dat het midden-, grootbedrijf, de instanties en de overheid meedoen.

1. Ondernemingsbegeleiding
   Wij zullen ondernemers, met name via de artikelen, vertrouwd maken met vrij beschikbare gereedschappen, vanaf de logboeken in hun computersystemen, over de `firewalls/routers/ switches' e.a. apparatuur tot en met Open Source dan wel betaalbare beveiligingssoftware.

2. Vraag & antwoord (in slecht Nederlands: `Q&A')
   Wij zullen vragen in onze artikelenreeks behandelen, welke wij of zelf ter illustratie stellen, dan wel vragen die via het LinkedIn-account van het Platform voor InformatieBeveiliging (PvIB) (8) binnenkomen. Op dat platform zullen wij thema's aankondigen, vragen stellen of vragen ontvangen van de lezer(s) van ons magazine dan wel van lezers van de LinkedIn pagina.

   Ook kun jij suggesties doen met betrekking tot thema's dan wel in rechtstreekse discussie met ons gaan of onze hulp inroepen. Ook zal op de artikelenreeks teruggegrepen worden om de inhoud daarvan te verduidelijken, tips van anderen te delen en verdere uitdieping van de onderwerpen te realiseren.

ACTIEVE INTERACTIE met jullie is gewenst en wordt nagestreefd

3. Wij streven ernaar dat op basis van deze artikelenreeks de grote, professionele organisaties (GO en NGO) hun kans waarnemen om op basis van bewustwording van de problematiek van het kleinbedrijf:
   - gratis kennis te delen,
   - programma's (software) te sponsoren of te schenken,
   - seminars en/of webinars te organiseren met ons (enkel gericht op het kleinbedrijf),
   - hun eigen ketens door te lichten en te zien hoe zij die in de praktijk kunnen steunen.
   En zo zullen er nog wel meer ideeën opduiken, zoals wij ook met universiteiten, hoge scholen en andere onderwijsinstellingen een samenwerking stimuleren.

Tot zover onze vooroverwegingen, nu dan het begin van de artikelenreeks.

De Start

Beste Vincent, als 'security scientist', kijkende naar het kleinbedrijf en uitgaande van zelfstandige computers, laptops, printers, smart-pad en -telefoon; wat zou de eerste stap zijn voor de ondernemer die zijn kennis over beveiliging van data, privacy en apparatuur wil verbeteren?

"Om te beginnen is het belangrijk te begrijpen wat cyberbeveiliging inhoudt. In de bedrijfsvoering heb je altijd een basisbegrip nodig van meerdere onderwerpen zoals onder andere: verkoop, marketing, netwerken. Hetzelfde geldt voor cybersecurity, eerst moet je een goed gevoel krijgen voor wat dát nu echt is.

In mijn eigen bedrijf hielp het mij om korte afspraken te maken met experts, die uit konden leggen over welke onderwerpen ik meer moest weten, dat kan ook voor cybersecurity. Je kan het ook zelf (willen) doen en het internet opgaan om een basisidee te krijgen over cybersecurity. Tegenwoordig kun je ook zelfs met online AI tools - zoals ChatGPT - het gesprek aan gaan. Maar wees je er dan wel van bewust dat deze gereedschappen nog aan het begin van hun ontwikkeling staan en naast zeer zinnige adviezen, opmerkingen en suggesties ook nog fouten kunnen maken. Vaar er dus niet blind op!

Wanneer je een begrip heb gekregen van cybersecurity, kun je overgaan naar de tweede vraag: waarom heb ik cybersecurity nodig? Door die vraag te beantwoorden kun je richting geven aan wat je precies wil beschermen. Ben je bang voor de veiligheid van jouw data, van jouw systemen, voor systemen en processen welke echt nooit zouden mogen omvallen? Van

daaruit rol je natuurlijk in de vraag en jouw antwoord: welke cyberrisico's zijn voor mij belangrijk?"
Vincent, het is duidelijk dat de eerste stappen je tot het besef (kunnen) leiden dat er cyberrisico's zijn, maar hoe kom je erachter welke risico's dat zijn en welke de belangrijkste zijn? Waar moet ik beginnen?
"Risico's kun je met behulp van allerlei handige gereedschappen inventariseren. Ik adviseer om het simpel te houden en eerst zelf te beginnen met het opschrijven van de risico's die je zelf denkt te lopen op het gebied van cybersecurity. Dit doe je vooral om zélf met het onderwerp te worstelen. Dit worstelen helpt je focus aan te brengen, om later de juiste taken uit te besteden dan wel zelf te doen.
Door alle vragen te beantwoorden maak je een begin met de cybersecuritystrategie. In de Cybersecurity Canvas (9), een tool waarmee je een cybersecuritystrategie in 1 slide kunt ontwerpen, zou je met voorgaande stap de linkerkant ingevuld hebben.

Figuur 2: Cybersecurity Canvas opgesteld door de auteur, V. van Dijk.

Dan kun je beginnen met de rechterkant: hoe ga ik deze risico's verminderen? Online kun je tal van maatregelen vinden. Echter, het wordt vrij snel technisch en de mogelijkheden zijn eindeloos. Dit is het juiste moment een expert te betrekken.
Na beantwoording van voorgaande vragen heb je een goed beeld verkregen van wat je precies wilt. Je kunt de expert de juiste vragen stellen. Daarnaast verneemt die van jou de benodigde kaders voor het goed (kunnen) meedenken.

Kies je er toch voor om het zelf te doen dan raad ik je aan om te kijken naar de **C**enter for **I**nternet **S**ecurity Critical Security Controls (**CIS** Controls), een geprioriteerde lijst van 18 maatregelen verdeeld over basis, fundamentele en organisatorische groepen (10).

Op het moment dat je de benodigde maatregelen in kaart hebt, kun je een stappenplan opzetten. Je kunt het stappenplan zo uitgebreid maken, zoals je wilt, maar ik raad aan om het advies van schrijver Patrick Bet-David ter harte te nemen en een 5-stappenplan (ten aanzien van 'Clarity, Strategy, Growth Tactics, Skills & Insight') te definiëren (11)."
Je hebt de eerste fase beschreven van het realiseren van cyberveiligheid binnen het eigen mkb-bedrijf. Zou je een uitdaging aan de lezer willen/kunnen doen welke wij op de PvIB-LinkedIn pagina dan wel in het volgende artikel kunnen opvolgen?

"Ik zou de lezer willen uitdagen om terug te gaan naar de basis en te bedenken waarom je met cybersecurity bezig bent vanuit het perspectief van de organisatie. Is het omdat je je zorgen maakt over mogelijke risico's, vereisten van belangrijke stakeholders of omdat je een goede indruk wilt achterlaten bij de klant.

Ook als grote organisatie, die al druk met cybersecurity bezig is, is het goed te reflecteren waarom je met cybersecurity bezig bent – wat is belangrijk? Dit geeft het benodigde inzicht om een cybersecurity-programma te starten, prioriteiten aan te passen en om mensen mee te krijgen in jouw activiteiten.
Ik ben heel benieuwd waarom mensen nu echt met cybersecurity aan de slag gaan. Ik nodig je uit om me een bericht te sturen met daarin je redenen (voor zover je die mag delen)."

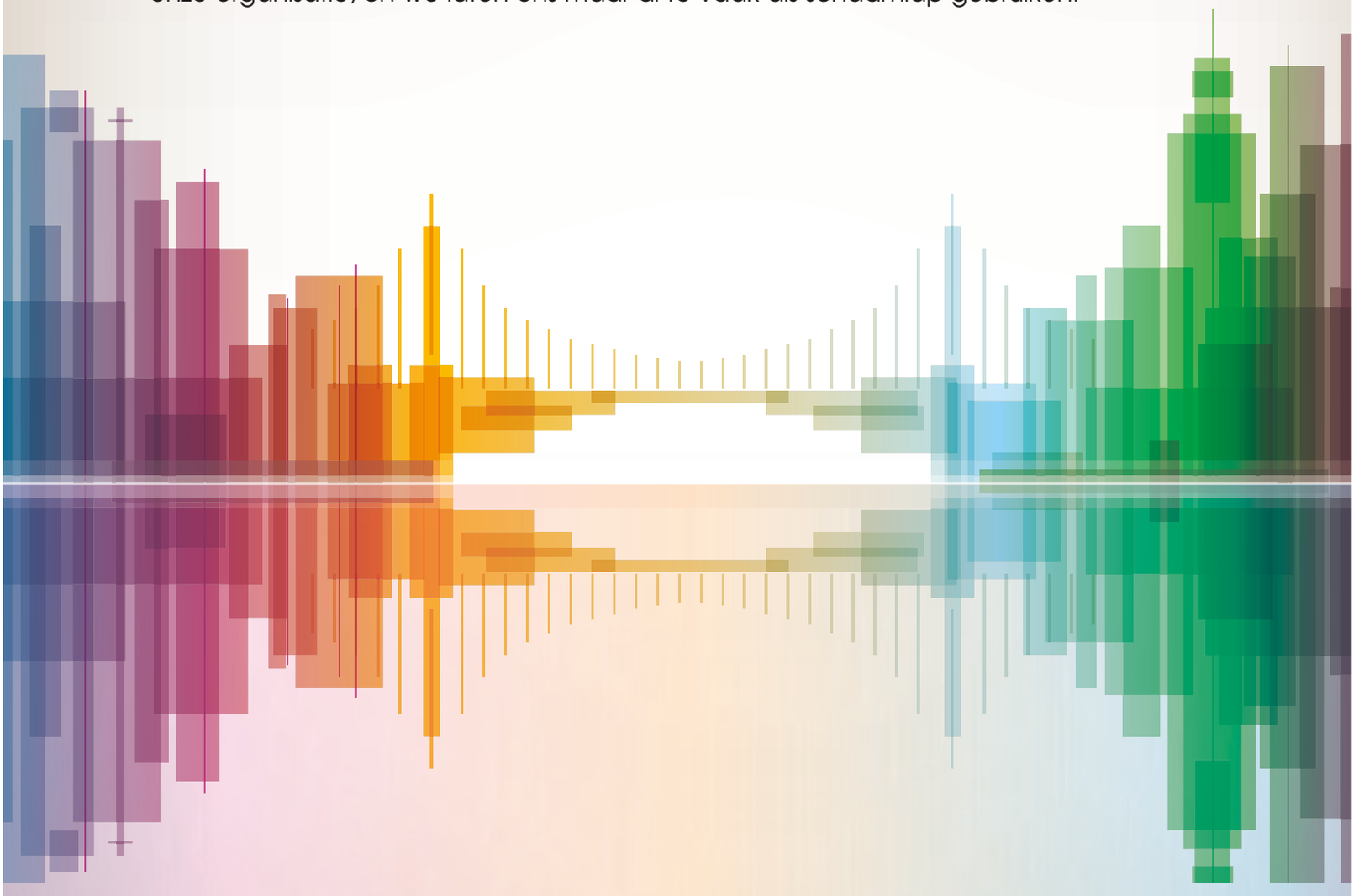
Referenties

(1) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48015NED/line?dl=30B3
(2) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-omzet-mkb
(3) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-werknemers-mkb
(4) https://studiozakelijk.nl/hoe-belangrijk-is-het-mkb-voor-de-nederlandse-economie/ , hun website 13.06.2018
(5) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-aantal-mkb-bedrijven
(6) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/line?graphtype=-Line&ts=1498474760139
(7) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/line?graphtype=Line&ts=-1498474760139 en https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/table?ts=-1677668553426
(8) https://www.linkedin.com/search/results/all/?fetchDeterministicClustersOnly=-false&heroEntityKey=urn%3Ali%3Agroup%3A133202&keywords=pvib%20-%20platform%20voor%20informatiebeveiliging&origin=RICH_QUERY_SUGGESTION&position=1&searchId=bb89db86-3e58-484c-86b7-cd71a0dc056a&sid=t~)
(9) https://www.securityscientist.net/content/files/2022/11/Cybersecurity-Canvas.pdf
(10) https://www.cisecurity.org/controls
(11) Your next five moves, master the art of Business Strategy;22.07.2021; auteurs Patrick Bet-David en Greg Dinkin – 320 pagina's, EAN code: 9781982154813 / ISBN: 1982154810; (Paperback € 11,09 bol.com d.d. 23.01.2023)

Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken via: andre@octopus-ib.nl of via LinkedIn (1).

Maesbruggen 4

Afgelopen februari, in mijn eerste bijdrage aan dit blad, heb ik de vloer aangeveegd met óns, de ISO's. We bakken er niets van, zo was mijn stelling in het artikel *De falende CISO*. Vóór publicatie van dat artikel heb ik het artikel vaak met vakgenoten besproken en in alle gevallen instemming op mijn diagnose mogen constateren: we zijn niet effectief in het realiseren van control, van passende beheersing van risico's bij onze organisatie, én we laten ons maar al te vaak als schaamlap gebruiken.



Het neersabelen van de hele beroepsgroep is natuurlijk makkelijk, ongenuanceerd. Velen zullen zich minder aangesproken voelen, hopelijk terecht. Maar ik moet ook uitleggen hoe het (volgens mij) wél moet. Daarover gaat de komende reeks bijdragen van mijn hand over het ISMS, eigenaarschap, risico's vinden en het 'Register'. Maar we beginnen met de belangrijkste: **Maesbruggen bouwen**.

De implementatiekloof

Een Maesbrug overspant een van de belangrijkste obstakels die de informatiebeveiliger moet zien te overwinnen: 'de kloof' tussen ivoren toren en werkvloer, tussen beveiligingsopdracht en -realisatie, tussen vragers naar en aanbieders van veiligheid; de **implementatiekloof**. Risicoanalyses en normen leiden tot opdrachten voor beveiliging die ergens in de organisatie moeten worden omgezet -geïmplementeerd - naar effectieve maatregelen.

• *Over de muur*

Zó gaat het vaak: je maakt als adviseur een mooi lijstje met actiehouders bij IT, huisvesting, PZ et cetera. Waaraan je de norm-controls toewijst. Je nodigt jezelf uit op de koffie en je legt uit dat het belangrijk/verstandig is (en dat het moet van de baas) en je keert vervolgens hoopvol terug naar je ivoren toren. De actiehouders zijn nu aan zet, want implementeren is tenslotte niet jóuw, maar hun werk.

• *Vraagtekens*

Na een paar weken/maanden kom je dan terug en vraag je hoe het ermee staat. 10 tegen 1 is het er nog niet van gekomen, waren er andere prioriteiten, zijn ze het vergeten … óf hebben ze nog iets meer uitleg nodig. Want zeg nou zelf: wat is eigenlijk de bedoeling van die vage normteksten?

• *Ondertussen*

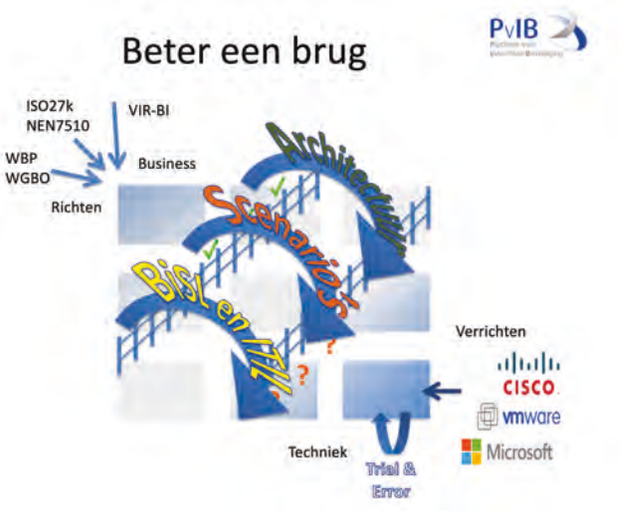
Voor veel bestuurders en toezichthouders begint ook de belangstelling voor informatiebeveiliging toe te nemen, maar dan in de trant van 'waar staan we'? Hoever zijn we al met de implementatie van BIO/NEN/ISO? Wat zeg je dan als (C)ISO wanneer je dit wordt gevraagd? De waarheid is vaak dat we van alles vermoeden, geen zekerheid hebben en het alleen anekdotisch kunnen illustreren. Incidenten verraden intussen dat verbetering mogelijk is.

Merk op dat niet alleen wij het niet kunnen beoordelen, maar ook de actiehouders niet, terwijl het wel hún 'pakkie-an' is: *implementeren en rapporteren*.

Maesbruggen

Wie mij een beetje heeft gevolgd binnen het PvIB weet dat ik sinds 2014 al publiekelijk worstel met dit kloof-probleem. Ik hanteer daarbij al sinds die tijd het 9-vlaksmodel van Professor Rik Maes.

De bruggen die ik probeer te slaan, over de kloof, heten bijgevolg Maesbruggen. Dat heeft onder meer geleid tot drie PvIB-bijeenkomsten met de titels Maesbruggen 1 t/m 3 (2014, '18 en '19).



Figuur 1: Beeld bij Maesbruggen 1.

In die bijeenkomsten hebben we allerlei opties verkend: architectuur kwam voorbij, BiSL + ITIL en bedrijfsbrede scenario's als cultuurkader, Mintzbergs organisatiemodellen, Agile werken, BCM-governance, zelfs een werkmodel voor duidelijker teksten en ook een praktijkcasus. Helaas, geen van al die mogelijkheden leverde een stabiele brug op. Het is gebleven bij genoeglijke avonden met collega's.

> De hamvraag is: Wat ís *implementeren*? Hoe doe je dat en wanneer is het goed genoeg? Als de opdracht aan de actiehouder niet duidelijk is, kan diegene er ook weinig mee.

• *Meetbare MaatregelAanpak - MMA*

In de loop der jaren heb ik mijn hoofd vaak gestoten bij mijn pogingen om het *implementeren* te bevorderen, maar uitein-

delijk heb ik toch een opening gevonden in de vorm van een gemeenschappelijke 'taal'. Die taal is in de kern heel eenvoudig: ik ga in gesprek met de actiehouders aan de hand van tien vragen over de *proceskwaliteit van de implementatie*. Deze taal biedt de actiehouder zowel een werkinstructie alsook een instrument om het resultaat van zijn werk te beoordelen.

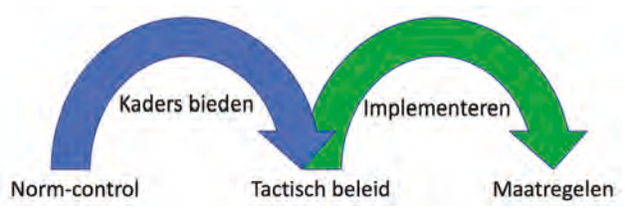
Ik, de ISO, ben alleen gespreksleider en kritisch meedenker. Ik ga niet over de antwoorden en niet over het oordeel of het goed genoeg is. Dat is de verantwoordelijkheid van de eerste lijn, van de actiehouder.

• *Doorvragen naar control*
Het gesprek gaat bij alle vragen over de 'control', de beheersing van het kwaliteitsaspect: hoe beheers je scope, je verantwoordelijkheid, de omgang met risico's, wet en regels et cetera. Krijg ik antwoorden in de trant van 'zo doen we dat' dan reageer ik met 'waarom'? Als men zegt 'dat doet Jantje', dan vraag ik 'is hem daarvoor een opdracht, instructie, tijd toegewezen'? Bij alles volgt de vraag naar documentatie en bij KPI's volgt de vraag: 'weet je het zeker?' en 'hoe ben je tot die keuze gekomen?'.

Steeds ben ik op zoek naar de 'rationale', een goed onderbouwde keuze en ook goed gedocumenteerd. Hoe beter de uitwerking van de control is onderbouwd en hoe beter de maatregelen zijn verankerd, des te volwassener is de implementatie.

Eerst tactisch beleid

De afstand (de kloof) tussen norm en werkvloer is zo groot dat die in twee stappen overbrugd moet worden. Te beginnen met de vertaling van de norm, en in details dus de controls, naar bedrijfseigen keuzes oftewel organisatiekaders. De norm vraagt er in meerdere controls ook om: het komt een keer of vijftien terug als eis, náást het algemene IB-beleid.



Figuur 2: Kaders als eerste stap bij het implementeren.

Hiermee sla je het eerste deel van de Maesbrug, het geeft duidelijkheid over waaraan de implementatie moet voldoen om te passen bij de bedrijfseigen middelen en manier van werken. Tactisch beleid moet liefst verre blijven van het 'hoe', maar zich beperken tot het 'wat'. Kaders dus, waarbinnen je moet blijven en minimumeisen aan de implementatie et cetera.

En dan implementatie

Implementatie is niet zozeer het 'doen' van dingen, maar met name ook het herhaalbare proces dat leidt tot een passende en effectieve maatregel. Dit proces kent meerdere stappen die allemaal uitgevoerd en ook gedocumenteerd moeten worden. Op die manier kom je navolgbaar in control en is je implementatie ook verifieerbaar voor intern- of extern toezicht. De volgende stappen zijn noodzakelijke aspecten van de implementatie.

1. *Bereik:*
   Waarover gáát de control, wat hoort erbij, wat valt erbuiten? Hoe is het vastgelegd waar deze control over gaat? En wie gaat er over de rest van al wat relevant is voor de control, dus meerdere deeleigenaren voor één control? Denk aan meerdere bedrijfslocaties of screening van medewerkers op afdelingen.
2. *Control-eigenaarschap [2]:*
   Naast *Verwerkingseigenaren* (ook wel 'proces-eigenaar' of 'systeem-eigenaar' genoemd) die de **vraagkant** van informatiebeveiliging vertegenwoordigen hebben we eigenaren aan de **aanbodkant** van informatiebeveiliging nodig: *Control-eigenaren*. Ze zijn te herkennen aan het feit dat ze macht en middelen hebben en zich ook verantwoordelijk achten, *liefst organisatiebreed*. Op die manier is 'control' te organiseren: een beperkte groep eigenaren bepaalt en weet hoe het zit. *Deze eigenaren rapporteren ook periodiek over de staat van de implementatie!*
3. *Kennis vereist:*
   Een goed geïmplementeerde control omvat kennis en vaardigheden van mensen en de toepassing van hulpmiddelen, allemaal op de juiste manier ingezet. Dus de mensen met kennis van zaken moeten in actie komen. Niet de CISO in zijn ivoren toren, maar de inhoudelijk deskundige.
4. *Competentie:*
   Hebben de mensen die de control moeten laten werken en gebruiken, de juiste competenties? Hebben ze voldoende scholing en ervaring? Hoe borgen we dat over de tijd?
5. *Samenwerking:*
   Controls worden maatregelen die in samenhang moeten werken, dus is overleg nodig om het functioneren te bewaken, gebreken op te sporen en verbetering door te voeren. Wie overleggen, hoe vaak, wordt er verslag van opgemaakt en worden actiepunten bijgehouden?

6. *Beleids- en risico-input:*
   Om een control zo te ontwerpen dat het 'passend' (3) kan worden genoemd moet de relatie worden gelegd met tactisch beleid, wetten, regels en organisatie-, verwerkings- en maatregelspecifieke risico's. Bij een verschuivend risicobeeld, in algemene zin of voor een specifieke informatieverwerking is dat dubbel van belang. Merk op dat ik drie niveaus van risico-informatie aanwijs, eigenlijk zijn er nog meer. Het tactisch beleid levert heel duidelijke aangrijpingspunten op voor implementatie en KPI's.
7. *Ontwerp:*
   Een maatregel kan alleen goed werken als hij goed ontworpen is. Dat betekent nadenken over preventie, detectie en repressie.
   • Preventie = de kernmaatregel in de control, deze bestrijdt het risico;
   • Detectie = deze maatregel merkt het falen van de preventie op;
   • Repressie = het handelingsperspectief van de eigenaar om de impact van falende preventie te beperken (bijvoorbeeld het 'stekkermandaat' bij het vermoeden van inbraak).

Voorbeeld van het wijzigingsproces:
De gecommuniceerde plicht om het wijzigingsproces geheel te doorlopen, is je preventieve maatregel. Als je vervolgens geen middel hebt om een ongeautoriseerde wijziging (het falen van de preventie) te detecteren, zal dat onopgemerkt gebeuren. Zonder mandaat om de ongeautoriseerde wijziging te stoppen (of terug te draaien) zul je de gevolgen daarvan niet kunnen beperken (geen repressie).

8. *Realisatie:*
   Het is aan de control-eigenaar om de bedachte werking te realiseren in processen, taken en middelen op alle relevante plekken in de scope, conform het ontwerp van de control. Hiervan maakt hij documentatie beschikbaar voor uitvoerders en toezichthouders.
9. *KPI's:*
   Monitoren en meten is alleen zinvol als er betekenisvolle meetpunten (KPI's) zijn gedefinieerd, zowel SMART als relevant voor de werking en effectiviteit. Deze vloeien voort uit het ontwerp en zijn te vinden in de gerealiseerde maatregelen. Relevante en meetbare KPI's zijn verplichte output in de MMA.
10. *Evalueren en verbeteren:*
    Niemand beter dan de maatregelverantwoordelijke en -uitvoerder kan beoordelen of alle bekende (en vermoede) risico's effectief worden bestreden. Samen met de CISO doet hij/zij een analyse van de control-implementatie alsook de effectiviteit van de maatregel. Daar komen onvermijdelijk verbeterpunten naar voren, die in een verbeterplanning thuishoren.

From the horse's mouth

Op basis van de 10 vragen krijgen we informatie 'from the horse's mouth', dus van de bron, van degene die het inzicht heeft en die verantwoordelijkheid draagt voor implementatie. Beter wordt het niet als het gaat om het inzicht in de maatregelen en of deze 'passend' zijn voor de organisatie en haar risico's.

Restrisico's en verbeteracties:
Met de MMA kan restrisico worden ingeschat: immers een control dekt een risico af, een onvolkomen implementatie laat dreigingen bestaan: dat noem ik het restrisico van de control-implementatie.

Rapporteren & bijsturen:
Elk restrisico moet leiden tot een actie: vermijden / verdragen / behandelen of accepteren: daarin kan de control-eigenaar een keuze maken, maar niet zonder afstemming met de 'hogere' risico-eigenaren. De risico-eigenaren: ten eerste de verwerkings-/procesverantwoordelijken en natuurlijk ook de directie kunnen op basis hiervan keuzes maken (de ACT-fase).

Nog meer voordelen

Toezicht:
Ik - de informatiebeveiliger en beheerder van het ISMS - notuleer, reflecteer en adviseer. En als ik zie dat een vraag niet serieus wordt opgepakt, heb ik natuurlijk de plicht om dat te melden. Implementatie die niet serieus wordt opgepakt, waar niet goed wordt geanalyseerd, waar risico's worden genegeerd vormen een risico voor de organisatie en die *moet* ik melden.

3 lines model:
Merk op dat de adviseur in de tweede lijn, de ISO/ CISO/ adviseur informatiebeveiliging, in dit alles de rol heeft van gespreksleider en adviseur, maar dat de ondersteuners in en van de eerste lijn, zoals IT, HR, Facilities, inkoop en anderen, hun rol pakken: zij zorgen voor de implementatie en rapportage. Zij zijn degenen die de opdracht hebben gekregen van de directie, althans dat is de juiste manier.

Audits:
De derde lijn, de formele toezichthouder (intern/extern auditor, rekenkamer et cetera) krijgt met de MMA-documentatie op een presenteerblaadje gestructureerde informatie over (de kwaliteit van) het implementatieproces, de gemaakte keuzes. Hij/zij kan op basis van deze informatie een uitspraak doen die niet voortkomt uit zijn/haar mening, maar uit voorliggende - gecontroleerde - feiten. Het auditproces wordt op die manier zuiverder voor auditor en auditee.

Maesbrug – Meetbare MaatregelAanpak

Alle elementen van een goede control-implementatie heb ik aldus verwerkt in mijn aanpak. Mijn eigen MMA die ik sinds 2017 bij een brede waaier van organisaties in de zorg, lokale, regionale en nationale overheden heb gebruikt.

De gebruikers van de methode zien de voordelen:

- Inzicht door een gesprek: geen meningen meer uit interviews, maar controleerbare feiten aan de hand van een eenvoudige structuur van 10 aspecten van kwaliteit;
- Maatwerk: implementatie die past bij de organisatie die ook uitgaat van wat er al is, wat goed werkt, ook al is het met `papiertjes en postduiven';
- Betrokkenheid: de 'werkvloer' geeft aan eindelijk te snappen wat de norm van hen vraagt. De opdracht is niet meer vaag, de veiligheidsbrengers komen aan het woord;
- Controleerbaarheid: de Control-documentatie (een word-document waarin elk van de 10 aspecten aan bod komt) biedt het perfecte vertrekpunt voor periodieke evaluatie van de Control, zowel voor de Control-eigenaar, voor de informatiebeveiliger als ook voor de derde lijn: de auditor;
- 3 lines: de verhoudingen tussen de rollen worden duidelijker en de informatiebeveiliger komt toe aan zijn kerntaken van advies en ondersteuning.

Natuurlijk zijn er ook nadelen:

- Arbeidsintensief: met name de eerste kennismaking neemt enkele uren per control in beslag, maar daarna wordt het per doorloop makkelijker want de IST is vastgelegd en de SOLL volgt uit de verbeterpunten;
- Gesprekstechniek: niet meer luisteren naar 'zo doen we dat', maar praten over beheersing, over control op de kwaliteitsaspecten. Dat valt, zeker in het begin, niet mee.

De voordelen wegen ruimschoots op tegen de nadelen, zo blijkt in de praktijk, maar het is wel belangrijk de betrokkenen ook op de nadelen voor te bereiden.

De kloof gedicht

Ben je erin geslaagd met tactisch beleid en methodische implementatie (zoals met de MMA) een brug te slaan naar de leveranciers van veiligheid, dan kun je met recht stellen dat je in control bent. Je hebt het gesprek tussen de ivoren toren en de werkvloer op gang gebracht. Zo kun je samenwerken aan continue verbetering, zoals de normen van je vragen.

PvIB-bijeenkomst

Het plan is om op 7 juni de MMA te presenteren in een PvIB AC-bijeenkomst, waarbij ik ook op het gebruik in de praktijk zal ingaan en mogelijk nog wat meer nieuws over de adoptie met jullie kan delen. De belangrijkste toevoeging die ik ga tonen, is hoe je op basis van de methode volwassenheid kunt claimen, en communiceren, die niet meer steunt op checklijsten of vage organisatiebrede concepten.

Wie hier niet op wil wachten en nu al meer wil weten kan me bereiken op andre@octopus-ib.nl of 06-12 72 72 38. Ik deel alle kennis en middelen voor mijn MMA zonder kosten met als enige voorwaarden dat je er niet aan sleutelt zonder mijn instemming en altijd verwijst naar de bron.

Referenties

(1) https://www.linkedin.com/in/andrebeerten/
(2) Ik gebruik liever het woord 'eigenaar' dan verantwoordelijke, het is persoonlijker
(3) Art 32 AVG: '..passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen'

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Risicoprofileren als nieuw risico

In een baanbrekend vonnis gooide het Hof in Den Haag het roer om voor etnisch profileren. In de zaak tegen de Marechaussee oordeelde zij dat het gebruik van huidskleur bij risicoprofilering discriminerend is. De kern van de zaak zit hem in de opmerking van de rechter dat het enkele feit dat iemand een bepaalde huidskleur heeft, nog helemaal niets zegt over de plaats van herkomst en/of diens nationaliteit. En dat laatste werd door de Marechaussee nu juist als redengevend voor het gebruik ervan aangevoerd. Hoewel dit een voor de hand liggende opmerking lijkt, heeft dit vergaande consequenties voor het gebruik van data voor risicoprofielen.

De rechter legt hier namelijk een belangrijk pijnpunt bloot. Een algoritme doet uiteindelijk precies dat wat het 'moet' doen aan de hand van wat je erin stopt aan data en rekenmethodes. In dit specifieke geval was een cruciaal stuk data (de huidskleur) gebaseerd op een verkeerd onderliggende waarde (namelijk dat je nationaliteit en herkomst zou kunnen afleiden uit huidskleur) en heeft dit geleid tot discriminatie (disproportioneel vaak 'aan de kant' gezet worden ter controle). Je krijgt eruit wat erin gestopt wordt.

Overigens is dit ook vergelijkbaar met hoe mensen in elkaar zitten, in een rapport over etnisch profileren van de politie geeft zij zelf aan dat agenten op straat (logischerwijs) disproportioneel vaak te maken krijgen met negatieve situaties waarin personen met een niet-witte huidskleur betrokken zijn. En dat dit hun visie en daardoor hun handelen kan kleuren. Ook nu uitdrukkelijk in de eigen richtlijnen is opgenomen dat onderscheid op huid geen criterium voor selectie is. Je krijgt eruit wat erin gestopt wordt.

Precies dit punt speelt natuurlijk niet alleen bij huidskleur. Je ziet exact hetzelfde gebeuren bij geslacht en seksualisering. In februari publiceerde het Engelse The Guardian een artikel over de discriminatie en seksualisering van vrouwen door het algoritme wat ingezet wordt bij social media als Instagram en LinkedIn. Uit eigen onderzoek van de krant blijkt dat de artificiële intelligentie die ingezet wordt door de platforms, foto's van vrouwen in alledaagse situaties als zeer seksueel aanmerkt. Bij mannen in vergelijkbare situaties is dat niet het geval. Content van vrouwen wordt daardoor systematisch onderdrukt (een zogenaamde *shadow ban*). Als waarschijnlijke verklaring voor dit effect geven de auteurs aan dat vermoed wordt dat dit specifieke algoritme gevoed wordt door voornamelijk heteroseksuele mannen. En dat deze logischerwijs bij vrouwen een seksueel beeld hebben en bij mannen juist totaal niet. Je krijgt eruit wat erin gestopt wordt.

Juridisch gezien is het allemaal niet zo moeilijk: je mag niet discrimineren en je bent verplicht ervoor te zorgen dat data correct is en je moet fouten in data corrigeren. Maar in de praktijk lijkt het nog steeds moeilijk te voorkomen dat het misgaat. En hoewel geen enkele gediscrimineerde groepering (hoe klein of groot zij ook is) de verplichting heeft om de 'normgroep' uit te leggen waar het fout gaat, denk ik wel dat het enorm veel zou helpen als personen die afwijken van de 'normgroep' meer actief betrokken worden in het ontwikkelen en doortesten van dergelijke technologie.

Rachel

Auteur: Drs. Robert Metsemakers RA RE CISSP is als ervaren auditor en informatiebeveiligingsexpert beschikbaar voor securityadviesopdrachten en bereikbaar op robert.metsemakers@gmail.com.

BLOG

Hoe je ruzie en discussie over (security)rapportages kunt vermijden

Wanneer professionals securityrapportages of -adviezen schrijven voor lezers, inclusief (betalende) opdrachtgevers, kunnen ruzies of discussies ontstaan over de tekst. Hieronder toon ik mogelijke probleemgebieden en geef ik ook schrijfadviezen.

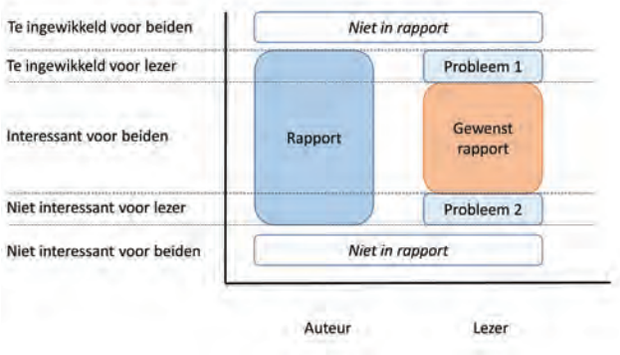
Ieder mens heeft zijn eigen waarneming van de werkelijkheid en vindt dat 'de ware'. In die werkelijkheid zijn security-onderwerpen te zien. Maar niet alle mensen vinden exact dezelfde dingen 'eigenlijk een security-onderwerp'. In het leven bestaan risico's: dingen die fout kunnen gaan. Een voor jou relevant risico vormt een dreiging. Schat je de kans dat het je ooit overkomt zeer laag in, dan noem je het een 'threat', die een manager dan kan 'parkeren' (lees: geen geld aan besteden).

Een security officer moet volgens mij zijn collega's waarschuwen voor die risico's, dreigingen of threats. Als er meer dan drie mensen in je bedrijf werken, is het handig dit niet mondeling, maar schriftelijk te doen. Regelmatig schrijft een security officer voor gelijkgestemden, die ongeveer hetzelfde van security weten. Soms voor opdrachtgevers die er méér van weten – dit vrijwel alleen in opleidingen wanneer een docent je als test iets laat opschrijven wat hij allang heel goed weet. En als security professional schrijf je vaak voor 'managers', die (veel) minder van security weten dan jij.

Schrijver en lezer verschillen dus qua kennisniveau op het vlak van security. Er is een deelgebied dat beiden begrijpen. Onderwerpen boven dat gebied zijn te moeilijk. Onderwerpen eronder zijn te gemakkelijk en daardoor niet 'interessant' genoeg om op te nemen in het rapport. In het algemeen signaleert een schrijver meer securityrisico's dan een lezer wanneer er sprake is van:

- hogere of meer security opleiding
- langere en/of bredere ervaring (binnen de huidige organisatie of de branche)

Figuur 1: (Gewenste) rapportinhoud



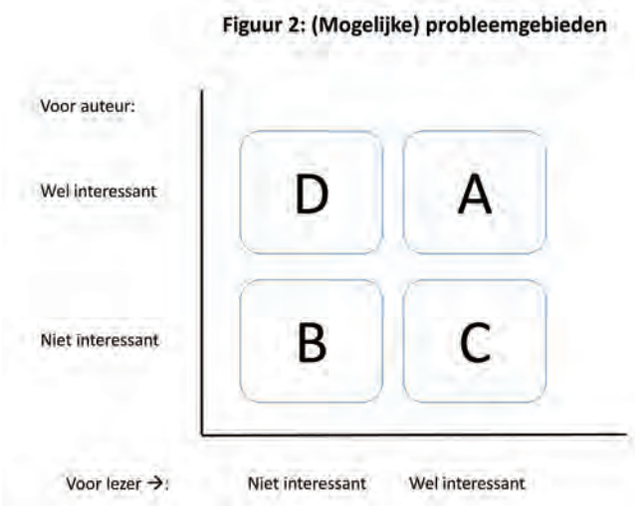
Figuur 1: (Gewenste) Rapportinhoud.

- een advies of rapportage meer op de lange termijn (strategisch) dan op de korte termijn (operationeel/brandjes blussen) gericht
- een advies of rapportage meer op detail dan op de grote lijn gericht
- meer technische (inhoudelijke) belangstelling, inzicht en ervaring dan uitsluitend 'loopt het proces?'

Een lastige combinatie om securityrapporten in te bespreken is een inhoudelijk zeer ervaren professional als auteur versus een onervaren manager in haar/zijn eerste algemeen (proces) leidinggevende rol als lezer/opdrachtgever.

Zoals bij veel ingewikkelde situaties kan een 2x2 matrix hier verduidelijking brengen. De probleem 1 en probleem 2 gebieden uit figuur 1 vormen samen groep 'D' in figuur 2. Let op: de schei-

dingslijn is onduidelijk. De meeste opdrachtgevers die ik heb ontmoet, geven namelijk niet graag toe dat een security-onderwerp voor hen 'te moeilijk' is. Ze zullen het onderwerp daarom 'onbelangrijk' noemen.



Figuur 2: (Mogelijke) Probleemgebieden.

Er zijn onderwerpen (of risico's) die voor zowel schrijver als lezer belangrijk en begrijpelijk zijn. Deze komen daarom in het rapport en gaan over het te analyseren onderwerp. Daar wil de lezer immers wat over weten, daar betaalt de opdrachtgever voor en dat is het kennisgebied van de schrijver. Deze punten geven in het algemeen geen aanleiding tot discussie (zie A).

Er zijn ook onderwerpen (of risico's) die zowel schrijver als lezer onbelangrijk of oninteressant vinden (zie B). Deze staan dus niet in het rapport en kunnen daarom per definitie niet tot discussie leiden - althans, niet reeds bij bespreking van het concept-rapport.

Er zijn onderwerpen die voor de schrijver niet belangrijk zijn, maar voor de lezer wel. Vooral als deze ook de opdrachtgever is. Wie gaf de onderzoeksopdracht? Is daarbij naar de letter het correcte (EU) aanvraagprotocol gevolgd? Is het onderzoek een week later opgeleverd dan tijdens de opdrachtverstrekking was beloofd? Is er ontzettend goed meegewerkt door de lezer aan de totstandkoming van het rapport en heeft de auteur zoiets positiefs nog nooit meegemaakt en mag dat ook wel eens gezegd worden?

Deze dingen zijn gemakkelijk toe te voegen, omdat ze meestal voor de schrijver de strekking van het rapport (of: 'de conclusie') niet wezenlijk veranderen. En ze verbeteren wel de sfeer en samenwerking met de lezer/opdrachtgever. Zeker wanneer er nog vervolgopdrachten moeten worden uitgevoerd. Ook onderwerpen in groep C hoeven dus geen reden tot discussie te zijn. Of zijn het alleen bij conceptbespreking van het eerste rapport in een serie – want je kunt je eigen schrijfstijl natuurlijk voortaan *aanpassen* op een vaste lezer. Zo, een extra gratis schrijftip!

Lastig wordt het pas in groep D. De schrijver schrijft ze op, want vindt ze belangrijk, maar de lezer vindt dat niet en wil die onderwerpen eruit hebben of sterk afgezwakt in hun formulering.

Ik noem hier enkele zaken die je beter niet in een securityrapport kunt opnemen.

1. Het probleem is **onoplosbaar**. Dit kan op zich natuurlijk wel het geval zijn. Maar als je het zo opschrijft, loop je grote kans dat lezers jou als auteur 'een pessimistische, negatieve zwartkijker' gaan noemen - en je niet meer inhuren als externe adviseur. Of juist 'verzuurd, te lang op dezelfde plek, niet meer passend in het team' - en je als interne adviseur een nieuwe kans elders gaan gunnen.
2. De oplossing is **onbetaalbaar**. Ook dit komt in de praktijk wel regelmatig voor. Als de kosten de baten overstijgen bijvoorbeeld. Het is echter van groot belang louter het *bedrag* van de door jou ingeschatte kosten te noemen. De conclusie dat dit belachelijk veel is voor wat het oplevert, moet je aan de lezer zelf overlaten. Het mooiste is als je rapport uiteindelijk bij de baas van de opdrachtgever terechtkomt en dat die hoogste baas meteen inziet dat het onbetaalbaar is. Karma!
3. Het probleem is **veroorzaakt door persoon X.** Vooral niet als persoon X de opdrachtgever is. Dit feit kan natuurlijk heel goed des poedels kern zijn qua 'Root Cause Analysis', maar je moet het niet opschrijven als je daar wilt blijven werken (intern of extern). Uiteindelijk komt de waarheid wel boven. Op dat waarheidsmoment moet je overigens ook niet in gezelschap zeggen: 'told you so'.
4. Een oplossing is in principe mogelijk, **ware het niet dat persoon X** dit niet heeft gedaan, of dat wel heeft nagelaten, of niet in staat is tijdig te besluiten over zus en zo, of te incompetent is om een genomen besluit uitgevoerd te krijgen. Dit is eigenlijk hetzelfde als (3). Omdat je als auteur nog allerlei oplossingen, verbetermogelijkheden en mogelijke correcties ziet, probeer je die – positief denkend als je bent – toch aan de lezer aan te reiken. Niet doen.

Als je deze vier weglaat, blijven er nog enkele potentiële discussiepunten over, maar die moet je dan als professional zelf maar even oplossen. En als je er echt goed naar kijkt, zie je ze mogelijk toch in het rijtje staan en kun je zo ruzie en discussie over je rapport of advies vermijden.

Auteur: Jelle Slotman is Senior Security Consultant bij Sogeti Nederland en onlangs als Master afgestudeerd aan de Hogeschool Utrecht. Hij is te bereiken onder jelle.slotman@tutanota.com. Dit artikel is een excerpt van de master scriptie van de Master of Informatics aan de Hogeschool Utrecht dd. november 2022.

Dark patterns in cookie consent notices

Wie regelmatig surft op het internet wordt doodgegooid met allerlei cookie verzoeken. Waar 'cookie consent notices' ooit zijn bedacht om de eindgebruiker te voorzien van zelfbeschikking en transparantie, lijkt het alsof websites alle mogelijkheden aanwenden om het tegenovergestelde te bereiken door het gebruik van 'dark patterns'. In dit artikel wil ik de lezer meenemen in de door mij uitgevoerde studie en de mogelijke oplossing voor een ethisch 'cookie consent design'.

Wat zijn cookies en wat is het probleem?

Web services gebruiken cookies voor het volgen van gebruikers met verschillende doeleinden. Cookies zijn kleine bestanden die het volgen van gebruikers mogelijk maakt. Zo kunnen webshops door middel van cookies een digitale winkelwagen of (anonieme) analytics bijhouden over het gebruik van de website. Deze cookies worden functionele of analytische cookies genoemd. De kern van eerder genoemde verwerkingen is dat deze anoniem zijn. Echter, als de gebruiker geïdentificeerd kan worden dan dient deze goedkeuring te geven in lijn met de Privacy richtlijn 2002 (ook wel bekend als de cookiewet) en de Algemene Verordening Gegevensbescherming (AVG).

Dit kan bijvoorbeeld gaan om verwerking voor bepaalde marketing activiteiten of het bijhouden van data om de gebruiker een gepersonaliseerd beeld te geven. Het belangrijkste punt hierbij is dat de website de gebruiker voldoende middelen geeft om op een geïnformeerde wijze een besluit te kunnen maken over de verwerking van persoonsgegevens.

Dit is precies het punt waar het in de praktijk verkeerd gaat. Verschillende studies binnen het praktische en wetenschappelijke domein hebben aangetoond dat veel websites gebruikmaken van verschillende visuele of tekstuele implementaties van het geven van een 'consent' om te bereiken dat de eindgebruiker zo snel mogelijk op de 'accept all cookies' klikt. Deze implementaties worden ook wel 'dark patterns' genoemd. Dark patterns zorgen ervoor dat het gebruikers (nagenoeg) onmogelijk gemaakt wordt om geïnformeerde beslissingen te nemen over het verwerken van persoonsgegevens. Een voorbeeld is te vinden in figuur 1, weergave van de website van gereedschapcentrum.nl (24-01-2023).

Figuur 1, bron: gereedschapscentrum.nl.

Er zijn een paar dingen die de gebruiker bijna dwingen tot accepteren. Als eerste valt op dat het lijkt alsof je de cookies alleen maar kunt accepteren door op de groene

Dark pattern	Description
Presentation	The desired choice is highlighted (e.g., color, text) in such a way that users may oversee other options.
Forced action and timing	The user is forced into a certain action on the spot.
Understanding mapping	Mapping information makes it difficult to evaluate into familiar evaluation schemes
Providing feedback	Feedback is used to steer users into the desired choice.
Providing Incentives	Incentives are used to reward the desired choice.
Expecting Error/Reversibility	Expecting users to make errors and being as forgiving as possible
Overly complex or easy information or structures	Information or information structures are either too simple or complex and hidden so that users are unable to provide their informed consent.
Bad defaults	Specific defaults are used by the company in the hope users do not decline them.

Tabel 1

button te klikken. Echter, bij het lezen van de tekst blijkt er wel de mogelijkheid om te weigeren, al wordt de gebruiker overduidelijk gestuurd om op de button te klikken en impliciet alle cookies te accepteren. Hoewel dit slechts een klein voorbeeld is, zijn er legio verschillende manieren om gebruikers te beïnvloeden. De irritatie die dit bij mij opwekte heeft er uiteindelijk voor gezorgd dat ik deze patronen (of patterns) ben gaan bestuderen en daarmee verandering hoop te brengen in het huidige klimaat. Dit heb ik gedaan door een lijst criteria op te stellen die zorgen voor een ethisch verantwoorde en GDPR compliant cookie consent notice.

Uitvoering van de studie

De uitgevoerde studie is gebaseerd op de Design Science methodologie van Peffers. Dit is een wetenschappelijke benadering voor het uitwerken van een design artefact en leent zich uitstekend voor het ontwikkelen van de checklist. De in het onderzoek gebruikte methodologie is opgebouwd uit vijf stappen, te weten: het definiëren van het probleem, het definiëren van de oplossing, het ontwikkelen van de oplossing, demonstratie van het artefact en het communiceren van de resultaten.

- *Definiëren van het probleem en definiëren van de oplossing*
  Door middel van literatuurstudie in professionele en wetenschappelijke context is de probleemstelling opgesteld. Uit het onderzoek is gekomen dat er op het moment een disconnect heerst tussen **compliance** en **ethiek**. Ethische richtlijnen voor gebruik van dark patterns zijn onvoldoende meegenomen en geven onvoldoende richtlijnen om 'informed consent' mogelijk te maken.
  Om bovenstaand probleem op te lossen zou er een checklist moeten komen die ervoor zorgt dat een cookie consent notice compliant is en dark patterns voorkomt. Door gebruik van het anti-pattern zou een weg naar ethisch cookie consent mogelijk gemaakt moeten worden.

- *Design en development van de checklist*
  De basis voor de checklist is een lijst van items uit de AVG guidelines (consent en transparantie) die samen het geheel aan richtlijnen toont. Deze lijst vormde een opsomming van alle vereisten die gesteld worden door de Europese commissie. Vervolgens is er op basis van wetenschappelijk onderzoek een specifieke lijst met dark patterns (tabel 1) gevonden, die van toepassing zijn op consent.

De eerste versie van het model is bereikt door een mapping uit te voeren van de dark patterns op de lijst met compliance criteria. Deze gezamenlijke lijst heeft tot de eerste versie van de checklist geleid.

Tabel 2 toont de checklist items met daarbij het/de relevante dark pattern(s).

Basic requirements		
Requirement (compliance criteria)	**Notes**	**Related Dark pattern(s)**
(1) The consent notice doesn't block users from accessing the website.	Consent is not blocking, ensuring that consent is freely given.	Forced action and timing
(2) Consent is required, besides cookies (strictly) necessary for communication, for servicing the user, and/or to obtain information about the quality and/or efficiency of the service. (3) No information is processed before consent is obtained.		
(4) A layered and standardized approach is used for different types of consent (e.g. basic advertisement, market research).		Overly complex or easy information or structures
(5) Consent is only obtained through a clear and affirmative action (no pre-checked boxes).		Bad defaults
(6) The following information is presented in the notice (link to the privacy policy is allowed): 1. The controller's identity. 2. The purpose for each of the processing operations where consent is sought. 3. What data will be collected and used. 4. How users may withdraw their consent at any time. 5. Information about the use of data for automated decision-making. 6. (Where relevant) inform the user of the risk of data transfers out of the territorial scope.		
(7) All consent is logged in order to demonstrate user consent.		
(8) Withdrawing consent is as easy as providing it.		
(9) Processing stops immediately, and stored information is deleted after user has withdrawn consent.		

Requirements for communication toward the data subject		
Requirement	**Notes**	**Related Dark pattern(s)**
(10) Privacy-related communications are clearly distinguishable from non-privacy-related information.	Communications must be concise, transparent intelligible, and easily accessible (art. 12(1) GDPR)	Overly complex or easy information or structures
(11) The entity uses communications understandable by an average member of the target audience.	Intelligible communications	

Requirements for communication toward the data subject		
Requirement	**Notes**	**Related Dark pattern(s)**
(12) The user should be able to determine in advance the scope and consequences of the processing (no surprises afterward).		Overly complex or easy information or structures
(13) The presented information makes it immediately clear how users can access their personal data.	Information is easily accessible.	
(14) Users are not steered towards desired choices through the use of feedback, incentives, and/or reversible actions (e.g., error messages).		Providing feedback, Providing Incentives, Expecting Error/Reversibility

Language/readability requirements for clear and plain language toward the data subject		
Requirement (grey text is used as a recommended requirement)	**Notes**	**Related Dark pattern(s)**
(15) Use sentences with a maximum of 20 words and use as many simple words as possible.		Overly complex or easy information or structures
(16) Active language is used to improve the directness of the message		Overly complex or easy information or structures
(17) No false friends*, jargon, and abbreviations are used, especially for websites over multiple languages *Words in different languages that look or sound the same but have different meanings.		Overly complex or easy information or structures
(18) Icons and visualizations may be used to strengthen the message. However, the icons/visualizations may not replace the written message. Highlighting visualizations or text is highly forbidden.		Presentation

Requirements when addressing offering services where children and/or vulnerable people may be the audience		
Ethical compliant requirement	**Notes**	**Related Dark pattern(s)**
(19) When addressing vulnerable people or children, use vocabulary, tone, and style so that the children know that the information is directed to them.		
(20) Seek an appropriate manner to provide transparency to vulnerable persons (physical/mental disability).		

Tabel 2

Deze eerste checklist is voorgelegd aan een panel van security/privacy specialisten (n=10), waarbij de bruikbaarheid van de items is getoetst en een rangschikking is gemaakt op basis van de belangrijkheid voor cookie consent design. Dit leverde een gevalideerde en gerangschikte lijst op, die aan de hand van een case is voorgelegd aan twee design specialisten.

- *Demonstratie*
  Het doel voor de onderzoeksfase was het demonstreren van het artefact in een praktische situatie (n=2). De demonstratie leverde feedback op ter verbetering van het artefact. Hierbij is voornamelijk gefocust op het opstellen van guidelines ter verduidelijking van de checklist. Verder is aan de hand van feedback discussie op de resultaten gevoerd.
- *Eindresultaat*
  Het uitvoeren van de studie heeft geleid tot onderstaande checklist (tabel 3). De guidelines zijn beschreven op basis van de input van de design professionals en de uitkomsten van de Delphi study.

Criterion	Guidelines
The consent notice doesn't block users from accessing the website (e.g. cookie wall).	1. There is a difference between public (open) and private (paid) services. For private services, a wall may be implemented prohibiting users to access the (private) website. 2. For the processing of personal information where consent is used as the basis of processing, the consent notice is still obligated. Cookie walls are prohibited.
Consent is only obtained through clear and affirmative action (no pre-checked boxes).	1. Pre-checked consent boxes are prohibited in most cases. Website users should have the autonomy to choose what personal information is processed from them. 2. Pre-checked boxes can only be used when certain processing activities rely on legitimate interest. 3. Specific color schemes can be used but these should be there to assist in making informed choices.
Withdrawing consent is as easy as providing it.	1. Withdrawing consent does not have to be done through the use of cookie banners. 2. Simple withdrawal is key.
Users are not steered towards desired choices through the use of feedback, incentives, and/or reversible actions (e.g. error messages).	1. These tricks may be used to make consent more informed. 2. An example could be to show feedback on processing consequences when users provide their consent. Note that this is a grey area as this also could steer website users.
When addressing vulnerable people or children, use vocabulary, tone, and style so that the children know that the information is directed to them.	1. Parents/caretakers should provide their consent. 2. Greater responsibility is necessary for situations where vulnerable persons and/or children are within your target audience.
Where consent is the basis of processing, no personal data is processed before the cookie consent is obtained.	1. Functional (e.g. tracker on shopping basket) and analytical (e.g. visitor statistics) cookies can be processed without consent. 2. Legitimate interest (when processing is necessary) is still optional for certain processing activities. Processing based on legitimate interest does not require consent.
All consent is logged to demonstrate user consent.	1. Not necessary for situations where consent is not required (legitimate interest, functional/analytical cookies)
The user should be able to determine in advance what the scope and consequences of the processing entail (no surprises afterward).	1. The consent notice should make the scope and consequences very clear. Make the message as comprehensive and compact as possible. 2. Example of this criterion would be that website users could click through the scope/ consequences per processing activity.
Seek an appropriate manner to provide transparency to vulnerable persons (physical/mental disability).	1. Also, in this context, mind that caretakers/parents need to consent on behalf of this target group. Be very strict about using language as plain and simple as possible. 2. Target group analysis helps find out how relevant this criterion is.

Criterion	Guidelines
The following information is presented in the notice (a link to the privacy policy is allowed): 1. The controller's identity. 2. The purpose for each of the processing operations where consent is sought. 3. What data will be collected and used 4. How users may withdraw their consent at any time. 5. Information about the use of data for automated decision-making. (Where relevant) inform the user of the risk of data transfers out of the territorial scope.	1. The information may also be provided through references (links etc.). 2. Use a concise version within the cookie consent notice. 3. For #2 describe who are the third parties with whom the data is shared and what is the legal basis for the activities. 4. For #3 also include how long the information will be retained. 5. Also include the contact details for the Data Protection Officer (DPO)
Presented privacy information is the same across multiple devices and device types (phone, laptop, tablet).	1. Ensure the provided information is the same across different platforms. 2. For convenience the information may be provided in a (slightly) different format if that improves comprehensibility.
Consent is required, except for cookies (strictly) necessary for communication, cookies necessary for servicing the user, and cookies to obtain information about the service's quality and/or efficiency.	1. Consent may not be provided through a default 'yes' as consent is provided through a clear and affirmative action. 2. Only request consent for processing activities that need consent (everything besides functional and analytics cookies). 3. Where consent is required make it clear what the scope and consequences entail. 4. Only request the strictly necessary processing activities.
The entity uses communications understandable by an average member of the target audience.	1. An analysis of the target audience helps to find the tone and voice required for the message (e.g. education and background analysis). 2. Creativity is key when implementing these messages. E.g., videos could be used to display the message. However, a written message is obligated.
No false friends*, jargon, or abbreviations are used, especially for websites over multiple languages. *Words in different languages that look or sound the same but have different meanings	1. Only use these words if necessary. It also helps to have the target group in mind. 2. Align language use over multiple languages.
Processing stops immediately and stored information is deleted after consent is withdrawn	1. Exceptions may exist in certain salutations where legal obligations apply (e.g tax, fraud investigations, product reliability, tax laws, and medical records). Generally, these are based on another basis of processing but keep this in mind. 2. It is not forbidden to anonymize after consent is withdrawn. For more details art. 29 WP216 provides the guidelines for proper anonymization techniques.
The presented information makes it immediately clear how users can access their personal data.	1. This could be done through a link or other means where users can see what data is processed by the organization. 2. The information could also be presented in the privacy statement.
Use sentences with a maximum of 20 words and use as many simple words as possible.	1. 6-8-year-old children should be able to understand this message. 2. E.g. uses B1 language, which is also used for Dutch government communications. 3. Align the message to the target audience.

Criterion	Guidelines
Active language is used to improve the directness of the message.	1. Active language uses verbal forms (to do) instead of passive voice using combinations (have done). 2. In combination with a limited word count the directness and ease of the message improve greatly. 3. Look at the message from a communication perspective instead of a legal perspective.
A layered and standardized approach is used for separating multiple consent requests (e.g. basic advertisement, market research).	1. Make it transparent for each processing activity when, and where, consent is provided. This enables users to make their own choices based on the information. 2. Make the requests as simple and concise as possible. 3. With layered is meant that website users should be presented with different categories that require consent. Each separate category should receive separate consent.
Icons and/or visualizations may be used to strengthen the message. Icons and/or visualizations may not replace the written message. Highlighting visualizations or text is highly forbidden.	1. Icons/visualizations should never replace text. The use of text is obligatory. 2. Highlighting is forbidden if this steers users towards the desired behavior. Highlighting may be used to improve the understandability of the message.
The cookie consent notice only includes communications necessary to explain the data subject for what purposes consent is requested. Other information may be provided through references and/or links.	1. Other information is all non-privacy-related information. 2. For cookie banners the purposes of processing are important to explain. Other information could also be described in the privacy statement.

Tabel 3

De studie heeft een goede eerste versie geleverd voor de checklist. Met bovenstaande checklist kunnen design professionals een cookie consent notice beschrijven op basis van de criteria. Hoewel er een aantal praktische uitdagingen zijn met betrekking tot het gebruikte jargon en de structuur van de checklist, kan dit artefact als succesvol en bruikbaar bestempeld worden.

Opmerkingen en aanbevelingen

Naast aanpassingen qua structuur en jargon, is een aanbeveling voor vervolgonderzoek om de demonstratiefase uit te voeren met een bredere 'sample group'. Dit zou ertoe kunnen leiden dat de checklist bruikbaarder wordt voor verschillende doelgroepen. Verder is het vervalmoment van consent een terugkerend thema geweest binnen de studie, waarbij zowel binnen de Delphi studie als bij de demonstratie genoemd werd dat een gegeven consent niet voor altijd zou moeten zijn. Vervolgonderzoek zou kunnen uitwijzen of dit een relevant thema is en op welke wijze het vervalmoment van consent geïmplementeerd kan worden.

Afsluitend is er in de praktijk een ontwikkeling te bemerken als het gaat om cookie consent. Waarbij in de 'oude' situatie voornamelijk gebruik werd gemaakt van een doorzichtige implementatie van de 'bad defaults' (zie ook de tabel 1 met dark Patterns) is er in het veld te zien dat steeds meer websites gebruikmaken van de 'legitimate interest', welke default op aan staat.

Hoewel er voor marketing speciale wetten gelden binnen de AVG, valt hier vooral de niet-transparante wijze op met als doel zo veel mogelijk data te vergaren.

Vervolgonderzoek zou kunnen focussen op hoe groot het huidige probleem van onjuist gebruik van legitiem belang is en voorstellen kunnen doen om de huidige regels duidelijker te kunnen stellen. Dit zorgt voor verbetering van de checklist en zorgt ervoor dat eindgebruikers zonder beïnvloeding keuzes kunnen maken over de verwerking van persoonsgegevens.

COLUMN LEX

Password mismanagement

LastPass is gehackt vorig jaar. Moet je je zorgen maken over jouw wachtwoordkluis in LastPass?
Ik ben een grote fan van password managers. Handige programma's die wachtwoorden voor je genereren, onthouden en invullen. Onontbeerlijk voor je eigen wachtwoorden, maar ook voor die onvermijdelijke momenten dat je wachtwoorden moet delen met collega's.

Na de LinkedIn hack van 2012 moest ik bijna al mijn wachtwoorden veranderen - daarvoor onthield ik mijn wachtwoorden en had ik veel hergebruik. Dat is niet goed en na zo'n hack voel je ineens waarom dat zo is. Je beseft dan dat niet alleen je LinkedIn wachtwoord op straat ligt, maar ook het(zelfde) wachtwoord voor zo'n twintig andere sites. Inmiddels is mijn collectie wachtwoorden gegroeid tot boven de tweehonderd en ik kan melden dat ze allemaal verschillen en random gekozen zijn.

Een password manager is tegenwoordig ook geschikt voor het beheer van je andere digitale geheimen. Naast wachtwoordbeheer helpt het je om OTP-waarden te genereren, gevoelige informatie en geheime sleutels te bewaren. Denk hierbij aan uiteenlopende soorten registratiegegevens, geheime vragen voor wachtwoordherstel en privésleutels van cryptowallets. Wanneer je een password manager in volle glorie gebruikt, zit je ziel en zaligheid erin, jouw kroonjuwelen.

In de basis is een password manager niet meer dan een digitale kluis met wat gebruikslogica er omheen. Er zitten wachtwoorden in, maar ook metadata bij die wachtwoorden zoals de gebruikersnaam en de URL van het domein waarvoor het wachtwoord gebruikt wordt. Deze metadata is op zich niet geheim, maar collectief vormen ze wel de inhoudsopgave van de kluis, iets waar cyberaanvallers op zich al veel aan hebben.

De metadata kan worden gebruikt om een profiel van jou op te stellen. Dat zou al genoeg kunnen zijn om een lijst van jouw aliassen op te stellen. In grotere collecties van gegevens kun je alle gebruikers vinden die een account hebben bij een gevoelige website, vraag dat maar aan de gebruikers van Ashley Madison (gehackt 2015).

Hoe privé is de digitale kluis? Denk aan de softwareontwikkeling, in het speciaal de encryptie (algoritmen, implementatie, sleutelbeheer). Het gebruik: hebben admins ook toegang? Kunnen ze dat forceren door hun hoge rechten? En dan bieden de leveranciers van password managers nog allerlei extra diensten (wachtwoorden op sterkte/ voorkomen in dumps controleren, je waarschuwen voor gehackte sites). Dit maakt jouw beleving in het geheel veiliger, maar doet niets voor de digitale kluis.

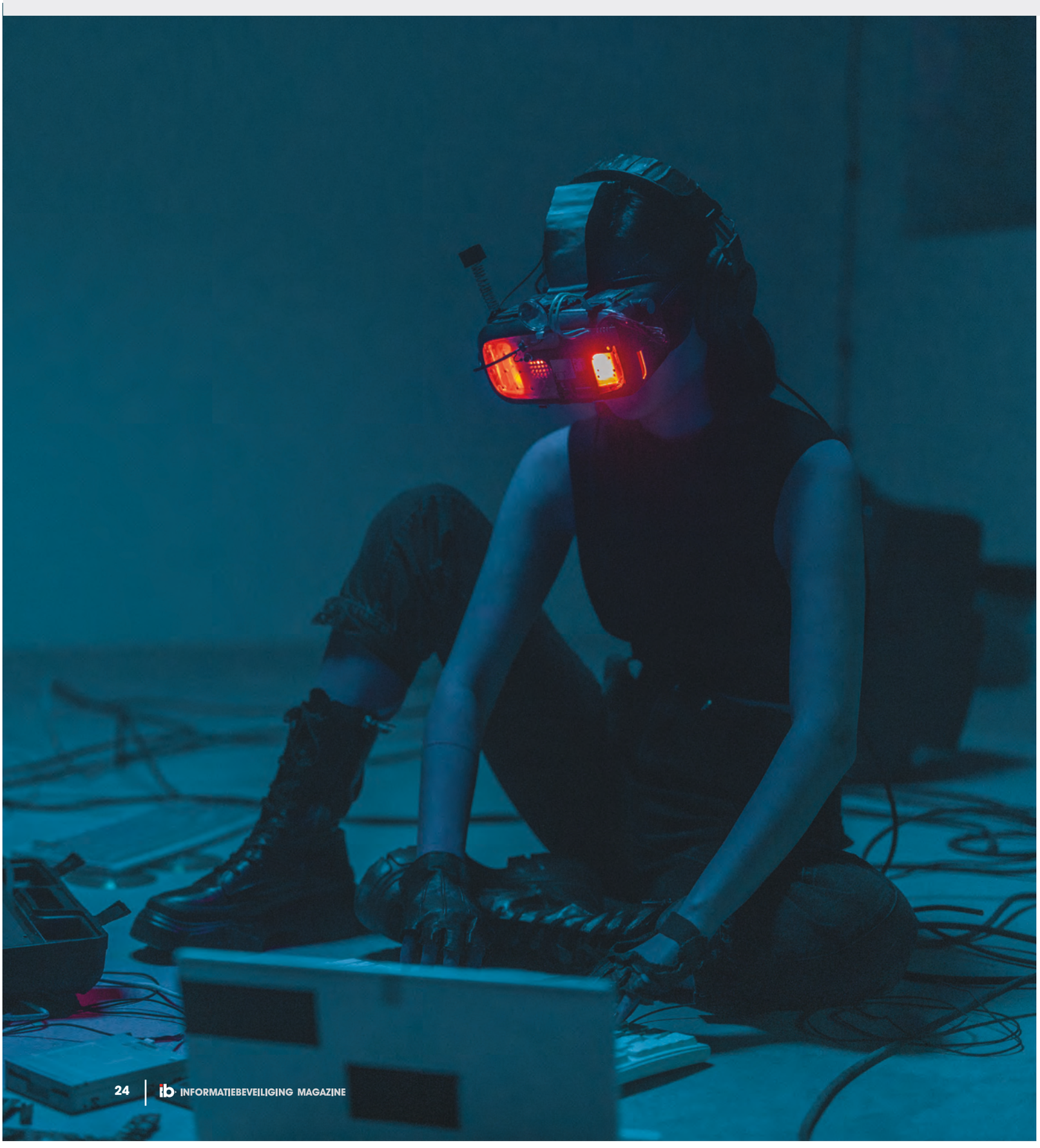
Wat wel effect heeft op de kluis is opslaglocatie - lokaal of in de cloud. De beschikbaarheid van de cloud geldt ook voor een aanvaller. Versleuteling is dan je enige beveiligingsschil, dus cruciaal dat die goed werkt, zelfs als je zelf een te eenvoudig wachtwoord hebt. De grootste dreigingen zijn verlies van toegang tot of diefstal van de inhoud van je kluis.

En die dreiging van diefstal is nu net waar door de LastPass hack van augustus vorig jaar bij veel gebruikers een verhoogde kans op is. En dat komt omdat LastPass zijn zaakjes niet goed voor elkaar had. De lengte van het kluiswachtwoord en de sterkte van de kluisversleuteling zijn mogelijk onder de maat omdat LastPass de versterkingen van beide aspecten over tijd niet goed heeft doorgevoerd. Vele gebruikers zitten nu met de gebakken peren. Hun geheimen liggen potentieel op straat, ontsleuteld, voordat zij de gelegenheid hebben gehad om alternatieve maatregelen te nemen.

Wat kun je doen? Met LastPass niets meer. Maar wellicht een goed moment om eens stil te staan bij alle geheimen in je kluis en je af te vragen of je die wel echt nodig hebt in je kluis, of dat je ze wellicht op een andere manier gaat veiligstellen.

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van iB-Magazine. Lex is bereikbaar via lex.borger@tesorion.nl

Auteur: Stefan Tezgel is sinds 2015 cybersecurity-adviseur bij CGI. Sinds 2011 is Stefan actief in de informatiebeveiliging met een achtergrond in de ICT en in digitaal onderzoek. Door de jaren heen heeft hij heel breed ervaring opgedaan aan zowel de functionele als technische kant van de informatiebeveiliging. Hij is te bereiken onder stefan.tezgel@cgi.com.



De ontwikkelingen van een vrijwillig cyberleger

Daar stond ik dan op de 'ONE', met natte handen die een papiertje met mijn laatste krabbels vasthielden. Mocht de techniek falen dan had ik altijd nog mijn verhaal bij de hand. 973 vakgenoten keken mij vanuit het donker aan, een 'make-it-or-break-it' moment. 'Cyberwarfare', een belangrijk en zeer actueel onderwerp. 'Go hard or go home.' Een zachte 'hit-it' en de zelfgemaakte compilatie van beeldmateriaal begon te spelen. Ik ga het nu echt doen! 'Spot on' en ik begon aan het verhaal…

Het is eind februari als de eerste berichten over het begin van de oorlog tussen Rusland en Oekraïne mijn telefoon bereiken. Ik lees de berichten met verbazing en tegelijkertijd voel ik mijn maag omdraaien. Het zal toch niet… maar het nieuws laat me vanaf dat moment niet meer los. Ik bedenk hoe het zal zijn voor al die arme mensen. Wat een hel om in te belanden. Ik kan me niet inbeelden hoe het voor de mensen daar moet zijn, want ik heb altijd in een vrij land en in een veilige situatie gezeten.

Dan, een paar dagen later. Het ministerie van Digitale Transformatie van Oekraïne roept een vrijwillig cyberleger bijeen (1). Oekraïne is al langer bezig met het idee om een cyberleger in te zetten, maar roept nu de wereld op om mee te denken en mee te doen. Ik ben geïntrigeerd, een eerste cyberoorlog en eentje die opvallend open en zichtbaar plaatsvindt! Hoe zou zich dat gaan ontwikkelen? Wie sluit zich daarbij aan? En ook wat zijn ieders motieven? Ik besluit me dan ook aan te melden via het kanaal op Telegram (2) alleen dan wel in de observatiestand.

Ik ben ervan overtuigd dat wij als security professionals op het scherpst van de snede moeten snappen wat er in de wereld van digitale veiligheid gebeurt. Het leert ons de tactieken, technieken en procedures die ingezet worden om systemen te compromitteren. Op die manier krijgen we meer inzicht in de 'modus operandi' en kunnen we daar ook de passende maatregelen op inzetten en onszelf beter beschermen.

De eerste dertig dagen

Tegen mijn verwachtingen in was er in de eerste dagen niet echt veel tractie. Het startte met een oproep van het ministerie van Digitale Transformatie en die was vrij duidelijk: *'voer cyberaanvallen en DDoS-aanvallen uit', 'zorg dat men weet wat er gebeurt in Oekraïne', 'val media aan en rapporteer propaganda en desinformatie'*. Een breed geformuleerde opdracht dus. De eerste gesprekken en kleine discussies vinden plaats in de Telegram groep. Ik besluit een aantal mensen via privé chat te benaderen met vragen over waarom ze meedoen, wat ze hopen te bereiken en hoe ze zelf denken te kunnen bijdragen. Het valt me op dat ik meteen in gesprek raak met mensen die allerlei beroepen uitoefenen: leraren, kantoormedewerkers, cybersecurity-specialisten en zelfs een lasser. Eén ding is duidelijk: de informatieoorlog is begonnen en er zijn op dag één al 160.000 mensen (3) die daaraan willen bijdragen.

In de eerste dagen worden enkele doelwitten genoemd, instructies gaan over en weer en ook persoonlijke informatie van vooraanstaande tv-sterren en -presentatoren wordt gedeeld. De effectiviteit van DDoS-aanvallen varieert van takedowns van 5 tot 45 minuten. De eerste 'defacements' (4)(5) vinden plaats en er wordt een dashboard geïntroduceerd waarop duidelijk wordt welke systemen er onbereikbaar worden gemaakt en ook gehouden. Ook wordt er buitgemaakte informatie gedeeld: persoonlijke informatie en duizenden actieve creditcards van Russische burgers. Deze informatie wordt vervolgens gebruikt om mensen geautomati-

seerd te laten bellen door bots en foto's van het slagveld worden via sociale media verspreid. Daar wordt zelfs een video over gemaakt (6).

In de resterende dagen van de eerste oorlogsweek vinden de eerste optimalisaties plaats. URL's worden IP-adressen met specifieke poortnummers en bepaalde targets worden nader onderzocht op (nog) meer relevante doelen. Korte tijd daarna verschuiven de doelwitten die in het Telegram kanaal gedeeld worden van financiële systemen naar systemen die betrokken zijn bij de oorlogvoering op de grond, waaronder GLONASS (het Russische satelliet navigatie systeem), transport (Belarus Railway Network) en later ook telecom (MTS, Beeline). Zoals via de oproep: *'stop de navigatie en de supply chain van Rusland'* (7)(8).

In de tweede week blijven systemen die betrokken zijn bij de oorlogvoering op de grond het primaire doelwit. Secundair worden de eerder al gemarkeerde doelwitten, waaronder media, overheid en de financiële sector. Vanaf 11 maart wordt ook de civiele infrastructuur betrokken in de targets: bezorgdiensten, nieuwssites, apotheken en bioscopen worden in datzelfde weekend massaal aangevallen (9).

De derde week worden nieuwe verdedigingstechnieken waargenomen aan de kant van Rusland. Bepaald netwerkverkeer lijkt niet meer aan te komen in Rusland. Vanaf dat moment gaan de aanvalstechnieken op de schop, iedereen krijgt het advies een VPN te gaan gebruiken, voorzien van de instructie hoe dat op een succesvolle wijze in te zetten. De dagen erna volgt optimalisatie na optimalisatie, met de constante boodschap om vooral de voornoemde doelwitten te blijven aanvallen.

De laatste week van deze eerste maand wordt er ingezet op de pakketdiensten, dat blijkt tal van leveringen te vertragen en het blijkt een groot effect te hebben (10)(11). Dit wordt ook het doelwit voor de resterende dagen van de eerste maand. Ook wordt deze week voor het eerst opgeroepen om een specifieke tool te gaan gebruiken (12), DB1000N ofwel 'Death by a 1000 Needles'. Een tool die op Oekraïense bodem is ontwikkeld. Deze tool is open source en te vinden op Github (een open-source samenwerkingsplatform) (13) en kan worden gezien als een heus 'cyberwapen' met meer dan 59 unieke 'contributors'.

De dagen die volgden

In de dagen die volgen gaan de aanvallen verder, de impact wordt groter en de eerste grote gevallen van computervredebreuk worden bekend. Er blijken op grote schaal cyberaanvallen uitgevoerd te zijn onder de regen van DDoS-aanvallen. De televisiemedia wordt gehackt, EGAIS (gebruikt voor alcohol tracking) wordt zodanig geraakt dat brouwerijen en fabrieken moeten sluiten en Rutube (de Russische equivalent van YouTube) wordt compleet overgenomen.

In het laatste geval werd de systeembeheerder vanwege abnormaal systeemgedrag naar de serverruimte gelokt. Eenmaal aangekomen in de serverruimte werden zijn inloggegevens onbruikbaar gemaakt en werd het systeem van toegangspassen overgenomen. Hierdoor kon hij niet alleen de serverruimte niet meer verlaten, hij moest ook moedeloos toekijken hoe er petabytes aan data onherstelbaar werden vernietigd (14)(15).

Wat je de afgelopen maanden ziet gebeuren als je de berichten in het Telegram kanaal analyseert, zijn verdere optimalisaties die in stappen worden doorgevoerd. Daar waar het begon met een tool (DB1000N) worden er nu meerdere tools aangeraden (MHDDOS, Distress en uaShield). Er zijn nu uitgebreide instructies over het gebruik van een VPN en er is een officiële chatbot waarbij mensen zich kunnen aanmelden om deel te nemen aan een vrijwillig botnet. Een belangrijke, naar mijn mening zorgwekkende ontwikkeling is dat er geen doelwitten meer 'omgeroepen' worden, maar dat er nu wordt gewerkt met een 'target list' die gesloten is voor de vrijwillige deelnemers.

Nu de tijd verstrijkt komen er meer en meer datalekken aan het licht. Onder de regen van alle DDoS- aanvallen blijken er diepgaandere cyberoperaties te hebben plaatsgevonden. De gekozen doelwitten waren niet zomaar gekozen en de DDoS-aanvallen bleken niet alleen tot doel te hebben systemen onbereikbaar te houden. Roseltorg (een belangrijk Russisch procurement platform), Right Line (belangrijke cloudopslag), Gazprom (belangrijke Russische gasleverancier) en Wagner (een particulier militair bedrijf) zijn allemaal gehackt en hebben kostbare informatie verloren aan het Oekraïense cyberleger. De werkwijze van deze hacks verschillen enorm (van gestolen accounts tot maandenlang wachten op het juiste moment) en elk van deze acties zijn het waard om nader te bestuderen. Datzelfde geldt voor het open source zijn van de ingezette tooling en het gekozen communicatieplatform (Telegram).

Ik ben ervan overtuigd dat er maar weinig mensen notie hadden genomen van het feit dat zij volledig zichtbaar voor de buitenwereld hun activiteiten uitvoerden. Ik heb tientallen mensen gesproken die zich voordeden als zijnde een lid van bekende hacking groepen, die vervolgens ook tools deelden waarvan ze zelf niet begrepen wat die tools exact deden. Zij deelden deze informatie en tools ook open en bloot vanaf hun eigen persoonlijke mailadres zonder zich bewust te zijn wat voor spoor van vernieling zij achterlieten en hoe hun naam en hun informatie terug te leiden was naar hun eigen persoon.

De vier belangrijkste lessen

De belangrijkste lessen wil ik hier ook graag delen. Dat zijn er vier:

1. Het vrijwillige cyberleger werd een snelgroeiende community die gecentraliseerd was opgezet en in de eerste weken een groei naar volwassenheid doormaakte. Mensen werden meer betrokken ook onderling, men wilde elkaar technieken en werkwijzen bijbrengen en men reageerde actief op aankondigingen in het kanaal.
2. Vanaf de eerste dagen was er sprake van een daadkrachtig optreden van het vrijwillige cyberleger. In zeer korte tijd is de effectiviteit toegenomen en ontstond er duidelijkheid in hoe mensen konden bijdragen.
3. Als er een verdeling wordt gemaakt tussen de 'goede' en 'slechte' partij, lijken legaliteit en ethische principes te verdwijnen. Niet-militaire doelwitten werden ook aangevallen, privésystemen werden binnengedrongen en de bijkomende schade door de uitgevoerde acties leken deelnemers aan het vrijwillige cyberleger minder te interesseren.
4. Het ad hoc oproepen om aan te sluiten bij het cyberleger creëerde een enorme valse start. Het doel was duidelijk, maar de manier waarop die doelen bereikt moesten worden niet, met als gevolg een enorme chaos. Er kwam een separaat chatkanaal (17) waarin deelnemers ook weer subkanalen deelden. Men verspreidde diverse uitvoerbare bestanden, potentiële malware, verschillende handleidingen, malafide websites, spyware en andere narigheid.

En hoewel deze inzichten waardevol zijn, hoop ik vooral dat er liever gisteren nog dan vandaag een einde komt aan de oorlog in Oekraïne. Ondanks intensieve grip op de media in Rusland zijn er inmiddels serieuze tegengeluiden van publieke figuren (18)(19) te lezen op sociale media (20) en ook te horen van politieke leiders uit het oosten (21) en verzetsgroepen (22). Dit biedt hoop voor de toekomst en de betrokken families. Будь мужнім.

Referenties

(1) https://t.me/mintsyfra/2609
(2) https://t.me/s/itarmyofukraine2022
(3) https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers
(4) https://t.me/itarmyofukraine2022/175
(5) https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/
(6) https://www.youtube.com/watch?v=1sfpTldvpPE
(7) https://www.reuters.com/world/europe/ukraines-it-army-targets-belarus-railway-network-russian-gps-2022-03-03/
(8) https://t.me/itarmyofukraine2022/120
(9) https://t.me/itarmyofukraine2022/197
(10) https://t.me/itarmyofukraine2022/235
(11) https://t.me/itarmyofukraine2022/236
(12) https://t.me/itarmyofukraine2022/229
(13) https://github.com/arriven/db1000n
(14) Rutube https://www.nbcnews.com/tech/tech-news/rutube-down-russia-hack-attack-ukraine-rcna28299
(15) Rutube https://www.youtube.com/watch?v=pggg8sEDhjA
(16) https://itarmy.com.ua/instruction/
(17) https://t.me/+H6PnjkydZX0xNDky
(18) https://nos.nl/artikel/2445109-russische-popster-veroordeelt-oorlog-in-oekraine-maakt-van-ons-een-paria
(19) https://www.pzc.nl/buitenlands-voetbal/ex-captain-russisch-voetbalelftal-keert-zich-tegen-poetin-misschien-beland-ik-in-de-cel-of-word-ik-vermoord~abe076b1
(20) https://www.volkskrant.nl/nieuws-achtergrond/kritiek-op-oorlog-zwelt-aan-op-ruslands-grootste-sociale-medium-poetin-is-een-pathologische-leugenaar~bc2a848d/
(21) https://www.bnnvara.nl/joop/artikelen/china-en-india-laten-rusland-vallen-poetin-verder-in-het-nauw
(22) https://nos.nl/artikel/2423515-partizanen-in-belarus-leggen-spoor-plat-om-russisch-leger-te-dwarsbomen

Geef-nooit-op-mentaliteit

Onlangs ben ik gaan werken voor een grote internationale organisatie. In mijn rol als CISO heb ik de mogelijkheid om met informatiebeveiligers van diverse pluimage te werken. Bij het denken over waar ik het in deze column over wilde hebben, dacht ik meteen aan wat mijn werk zo fantastisch maakt.

De informatiebeveiliger, cybersecurity-expert, securtity analist, security architect, security champion binnen de DevOps teams, IT auditor… Ik kan nog even doorgaan met titels, maar we hebben eigenlijk allemaal een aantal gemeenschappelijke eigenschappen:

• **Wereldverbeteraar**
We hebben een drive om impact te maken, dienen graag het maatschappelijk belang. We willen het bedrijf waarvoor we werken behoeden voor ernstige incidenten en daarom kunnen we niet op dinsdag wel waakzaam zijn en op woensdag even niet.

• **Leergierig**
De wereld om ons heen verandert continu. Niet alleen qua technologie, maar ook onze klanten veranderen. Denk aan de manier waarop ze naar risico's kijken en hoe ze risico's ervaren. Daarbij verandert ook de identiteit en het motief van de aanvaller en daarmee ons dreigingsveld. En het bedrijf waarvoor we werken, tot slot, verandert: het expandeert, verandert van technologie, leverancier en/of samenwerkende partners. In al deze veranderingen moeten wij, als informatiebeveiligers, mee. Leergierigheid helpt ons, leidt ons en maakt het werk superinteressant.

• **Community-denken**
We weten dat we allemaal in hetzelfde schuitje zitten in de zogeheten 'Security Ratrace'. Je kunt het je niet permitteren om de zwakste schakel te zijn of om zwakke schakels over het hoofd te zien. Dus werken we dagelijks zoveel mogelijk samen met onze collega's: architecten, developers, scrum masters, agile coaches, digital officers, CIO's, CTO's, maar ook met juristen, auditors, data privacy officers en hard core systeembeheerders. En sinds enkele jaren ook met onze afdeling inkoop, ofwel procurement, waar afspraken met onze derde partijen bewaakt worden. Zonder in systemen, ketens en patronen te denken en zonder samen te werken, trekken we het niet.

Binnen het PvIB staat dit community-denken centraal. Wat weet jij, waar ik wat van kan leren? Waar denk jij waartoe dit leidt en hoe bereid jij je voor op de wereld van morgen?

Ben je ook zo leergierig? Vertel ons waar je meer over wilt weten! Heb je impact gemaakt, schroom niet om het te delen. Wees een inspirator voor de mensen om je heen. En heb je ideeën hoe we onze inzichten met elkaar nog beter kunnen delen, als vakbroeders, maar ook met collega's die niet direct in het vak zitten: deel het!

Zo wil ik het PvIB als vereniging nog verder zien groeien. Gedreven door ons DNA van leergierigheid, gedrevenheid en community-denken.

Jessica Conquet,
Voorzitter PvIB

Dimitri van Zantvliet is CISO bij de Nederlandse Spoorwegen en columnist van IB Magazine.

COLUMN DIMITRI

A.I., A.I., Caramba!

Tussen kerst en de tweede week van het nieuwe jaar was ik vrij. Mijn echtgenote houdt echter altijd rekening met mijn soms overdreven verantwoordelijkheidsgevoel om lekker mee te draaien tijdens cyberincidenten. Goede WiFi is dus prio1, naast Bollo de Beer of Koos Konijn animatie voor de kinderen natuurlijk. Maar het bleef rustig dit jaar (er wordt druk gewerkt aan 'backdoors' voor het tweede hybride offensief in de Oekraïne vreest men) en ik hoefde me niet te bemoeien met CITRIX of Log4J zero-days, criticals of leaks. We wisten met z'n allen even niet wat we met mij aan moesten deze vakantie dus. Ik heb het gezin gemeld dat het zeker leuk was, maar dat ze er maar niet aan moeten gaan wennen. Inmiddels is het eind januari en is het nog steeds relatief rustig.

Ik heb mijn vrije tijd echter toch wel weer weten te vullen met allerlei experimenten met nieuwe technologie anders dan crypto. Eind 2022 kwam OpenAI namelijk uit met 'het gratis' ChatGPT3 en na een paar weken heeft de media dit ook massaal opgepikt. Inmiddels ben ik ook vele uren verder met het uitproberen van tientallen nieuwe AI tools en kan ik gegenereerde tekst (ChatGPT, ChatSonic, KafkAI) samenvoegen met een mooi gerenderd plaatje (Dall.E2, Midjourney, BlueWillow, Stable Diffusion) in een video generator (D-ID, Pictory, Lumen5). Bij NS wordt A.I. en Machine Learning al langer gebruikt voor complexe knooppunt logistiek en chatbots. Nu worden de mogelijkheden breder en zie ik ook meer collega's om mij heen zaken uitproberen. Die kansen komen weer met de nodige risico's, maar daar ga ik een andere keer wel weer eens over uitweiden.

De ChatGPT medewerkers in Kenia hadden overigens geen vakantie het afgelopen jaar. De OpenAI organisatie huurt daar namelijk, volgens website TIME, goedkope krachten in voor 2 dollar per uur om de misogyne, banale en discriminerende output van het Large Language Model (LLM) te filteren naar de ethische normen en waarden van vandaag de dag. Het deed me denken aan de robot Sophia die ooit zei dat ze de mensheid wilde vernietigen en kon schelden als de Amsterdamse Glenda Batta, totdat ze een filter voor haar Python mond programmeerden. Terwijl ik dit schrijf speelt Pink Floyd *Welcome to the machine* op de achtergrond. Volgens Spotify wil ik hier nu naar luisteren. Iemand nog een 'cookie' bij de koffie?

ChatGPT4 is inmiddels in aantocht, brace for impact! Nadat Elon Musk het bedrijf startte en Amerikaanse Venture Capitalists in een lange rij stonden om er honderden miljoenen dollars in te pompen, stapte Microsoft er begin dit jaar met niet minder dan 10 miljard dollar in. Gaan ze daar nu de Kenianen 5 miljard uur voor uitbuiten? Waar het GPT1 model begon met 117 miljoen parameters zal GPT4 er naar verluidt 100 triljoen kennen. Gratis zal het ook zeker niet blijven nadat we het model zelf via crowdsourcing hebben getraind. We hebben overigens nog geen flauw idee wat dit gaat betekenen, maar dat het een quantum leap wordt dat is inmiddels wel duidelijk.

Met de kinderen heb ik trouwens de grootste lol om dit samen uit te proberen. Ze pikken het een stuk sneller op dan ikzelf. De digitale wereld gaat de komende jaren radicaal veranderen en A.I. dendert Op Volle Toeren ons leven binnen. Ik sluit daarom maar af met de vermaarde tekst van de wijlen Brabantse volkszanger Tony Bass en zeg: **'A.I., A.I., Caramba!'**

Auteur: Valentijn Ishaqsada is bestuurslid PvIB, portefeuille Public Relations & Communicatie, en als consultant actief voor zijn bedrijf YourAlly. Met zijn bedrijf adviseert hij publieke en private organisaties bij de beheersing van hedendaagse uitdagingen rondom informatiebeveiliging en privacy. Valentijn is te bereiken via: valentijnishaqsada@pvib.nl.

Titel boek:	*Waardering van de informatiebeveiliging*
Auteur:	dr. Clemens H.J. Willemsen
Taal:	Nederlands
Bindwijze:	Paperback
Aantal pagina's:	61
EAN:	9789403676159
Prijs:	€ 17,95

BOEKREVIEW

Waardering van de informatiebeveiliging

Hoe waardeer je informatiebeveiliging? Wat is de weg naar een objectievere waardering van betrouwbaarheid? Wat schuilt er achter beschikbaarheid, integriteit en vertrouwelijkheid? In het boek *Waardering van de informatiebeveiliging* neemt auteur dr. Clemens H.J. Willemsen de lezer mee in het onderwerp kwantificering en informatiebeveiliging.

Aspect	Kengetal	Laag	Midden	Hoog
Beschikbaarheid in enge zin	% beschikbaarheid	90% (36 dagen niet)	99% (3,6 dagen niet)	99,9 % (1 dag niet)
	oftewel in dagen*uren	5*8	5*11	7*24
Stabiliteit/robuustheid	maximaal dataverlies RPO	28 uur	24 uur	18 uur
Continuïteit/ herstelbaarheid	maximale hersteltijd RPO/MTTR	40 uur	16 uur	8 uur
	geprogrammeerde controles	Beperkt	Voldoende	Uitgebreid
Tijdigheid	kritieke momenten	Geen	periode-afsluiting, kortstondige piekperiode	Langdurige piekperiode
Toegankelijkheid bij beperkingen	Belemmeringen	Enkele belemmeringen	Gedeeltelijke belemmeringen	Grote belemmeringen

Figuur 1: Kengetallen voor BIV-factor beschikbaarheid (bron: Waardering van de informatiebeveiliging)

Dr. Willemsen studeerde in 1985 af in de Bestuurlijke Informatica en promoveerde in 2019 aan de Faculteit der Rechtsgeleerdheid van de Tilburg Universiteit. Hij is werkzaam als CISO (Chief Information Security Officer) en beleidsadviseur informatievoorziening bij het ministerie van Justitie en Veiligheid en is in deze functie al jaren betrokken bij informatiebeveiliging en informatievoorziening.

Willemsen opent het boek met de observatie dat informatiebeveiliging tot op heden vaak vanuit een kwalitatief oogpunt wordt benaderd. Hij betoogt dat een juiste waardering van betrouwbaarheid nodig is om werkzaamheden op het gebied van informatiebeveiliging te kunnen prioriteren en in tijd te kunnen uitzetten, met daarbij de benodigde financiering. Een meer kwantitatieve benadering kan tenslotte leiden tot een meer objectieve waardering.

Voor alle informatiebeveiligingsprofessionals zijn de BIV-factoren (beschikbaarheid, integriteit, vertrouwelijkheid) onlosmakelijk verbonden met de betrouwbaarheid van informatiesystemen binnen organisatorische processen. Willemsen stelt echter eerst de vraag of een bredere benadering van andere elementen, naast de welbekende BIV-factoren, niet passend en gerechtvaardigd zou zijn. Diverse bronnen worden voor de beantwoording van deze vraag onderzocht: ISO-standaarden (ISO 25012, 25010, 27000), CoBiT, CIA-triad, 5 Pillars en Nora. In deze uitvoerige bespreking worden de elementen achter deze bronnen beoordeeld op de vraag of deze een rol naast of achter de BIV-factoren zouden kunnen vervullen.
Dan volgt de kwantificering van de BIV-factoren. Voor elk van de drie factoren bestaat dit uit een definiëring, een uiteenzetting en de aanpak waarmee een meting en waardering kan plaatsvinden. Dit geheel voegt dr. Willemsen samen in een model waarin niveaus (laag, midden, hoog), aspecten en kengetallen samenkomen (zie figuur 1). Door het gebruik van concrete voorbeelden ontstaat zo een uitgebreid en integraal beeld waarmee voor de verschillende BIV-factoren, de achterliggende kwantificering kan worden bepaald.

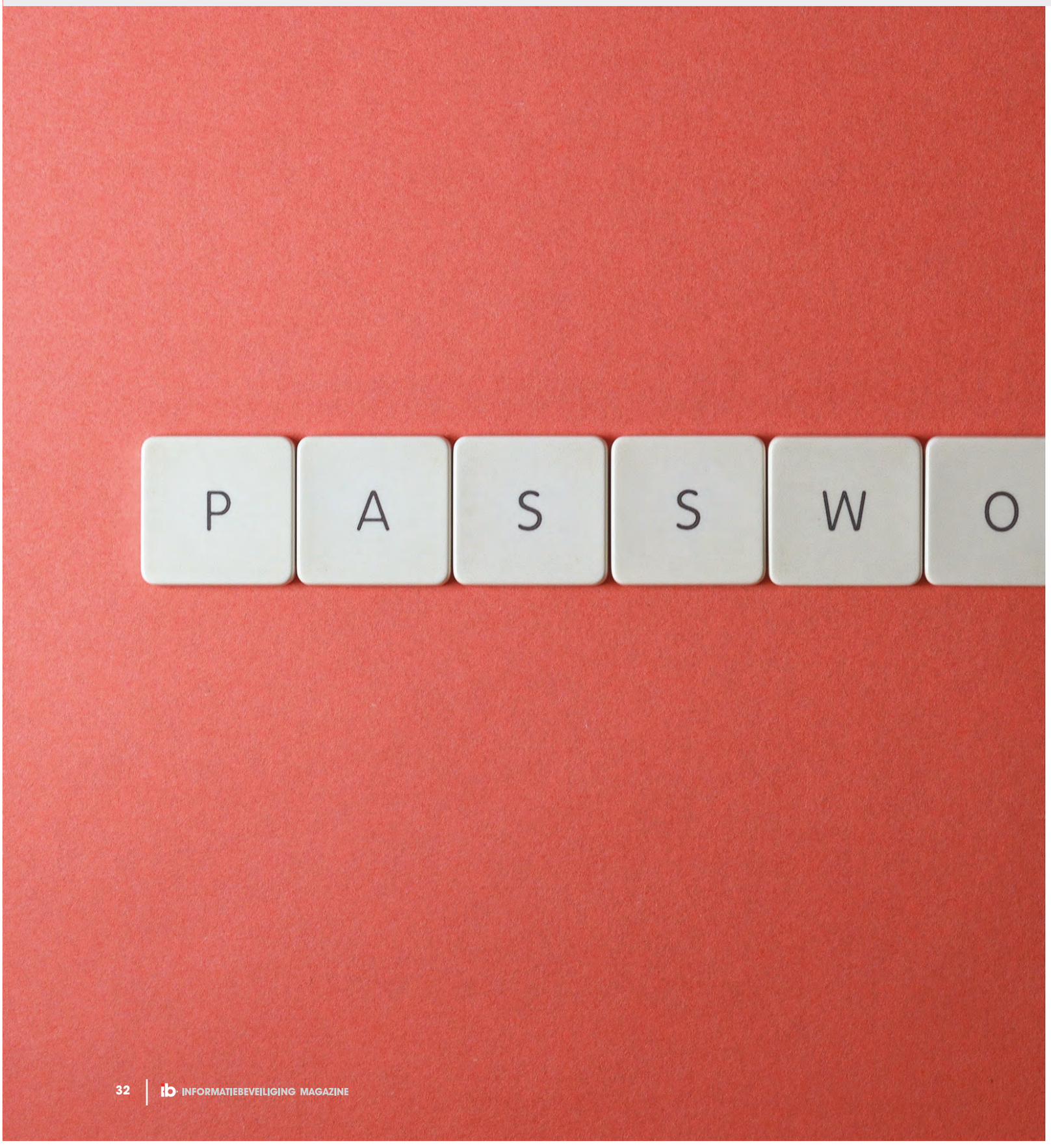
Dan volgt een laatste hoofdstuk waarin de BIV-factoren als geheel samenkomen. Willemsen beschrijft op welke manier er sprake is van een mogelijke samenhang tussen de BIV-factoren en de verschillende methoden voor de bepaling van welk niveau voor individuele BIV-factoren passend is. Onder andere de BIO-(toets), het ISACA IT Asset Valuation, Risk Assessment and Control Implementation Model, Quickscan Information Security (QIS) en de In Control Verklaring komen ter sprake.

Aan de hand van verschillende figuren leidt het traject van de waardering van niveaus naar de waardering van de daadwerkelijke betrouwbaarheid. De methoden worden naast elkaar geplaatst en vergeleken, hetgeen leidt tot een sluitend geheel waarin alle inzichten samenkomen. Als praktisch hulpmiddel levert de auteur online ook nog een spreadsheet aan zodat de lezer zelf met kwantificering aan de slag kan gaan.

Al met al slaagt Willemsen zeker in zijn doel om bruikbare inzichten te geven die helpen bij de objectivering van informatiebeveiliging. Het boek blinkt uit door de abstracte materie concreet te maken, de diverse bronnen die worden besproken en door praktische hulpmiddelen te bieden. Wanneer je aan de slag wil met kwantificering of wanneer je simpelweg nieuwsgierig bent en verdieping zoekt, zul je je bij dit boek goed thuis voelen.

Het boek is onder meer verkrijgbaar via managementboek.nl en de reguliere boekhandel.

Auteur: Menno Vermeulen is security consultant bij CGI Nederland B.V. Hij is bereikbaar via: menno.vermeulen@cgi.com.



De werking en vele functies van wachtwoordmanagers

Stel je voor dat je in een webshop eindelijk het artikel hebt gevonden dat je wil kopen. Je stopt het in het winkelmandje, maar er komt een ander scherm dat aangeeft dat je eerst een account moet maken. Dit komt vaak voor, omdat er steeds meer online diensten zijn die een account vereisen. Je vult je e-mailadres in en bedenkt een nieuw wachtwoord, waarna je een melding krijgt dat het te kort is én dat je nog een speciaal teken mist. Zonder erbij na te denken voeg je de gevraagde tekens toe en nu heb je een wachtwoord dat je niet meer kunt onthouden

Iedereen weet dat een wachtwoord niet gemakkelijk te raden moet zijn en niet te kort. Veel online diensten helpen je hierbij door bepaalde voorwaarden aan een wachtwoord te stellen, zoals een minimum of een maximum wachtwoordlengte, ten minste één speciaal teken, ten minste één getal, et cetera. Dit verhoogt de *entropie* van het wachtwoord, wat een maatstaf is die beschrijft hoe sterk een wachtwoord is. Een langer wachtwoord met verschillende categorieën van tekens heeft een hogere entropie dan een kort wachtwoord zonder hoofdletters.

Een sterk wachtwoord moet ook uniek zijn en het moet niet worden gebruikt voor verschillende accounts. Als een hacker toegang weet te krijgen tot één account, dan heeft hij ook toegang tot alle andere accounts die hetzelfde wachtwoord gebruiken. Gezien het grote aantal online diensten dat je moet gebruiken, is het echter onmogelijk om al deze wachtwoorden te onthouden. Sommige diensten vereisen zelfs om je wachtwoord periodiek te wijzigen, wat het probleem alleen maar erger maakt.

Een *wachtwoordmanager* lost dit probleem op door al je wachtwoorden in combinatie met je accounts veilig op te slaan. In dit artikel laten we zien hoe wachtwoordmanagers dit doen op het technische vlak. Aan het einde bespreken we veelal aangeboden functionaliteiten van verschillende commerciële wachtwoordmanagers. Zo kun je zelf een goede beslissing maken.

Hoe slaat een wachtwoordmanager alle wachtwoorden op?

Het idee van wachtwoordmanagers is om wachtwoorden op te slaan voor al je accounts, waardoor het heel belangrijk is dat dit veilig gebeurt. Over het algemeen worden de data niet zomaar opgeslagen, maar worden deze eerst versleuteld met behulp van encryptie. *Encryptie* is een proces waarbij data worden gecodeerd naar iets wat geen betekenis meer bezit. Dit met behulp van een *codeersleutel*. Diezelfde codeersleutel kan worden gebruikt om de encryptie om te draaien, waardoor je dus weer de originele data kunt krijgen. Dit heet *decryptie* of *ontsleutelen*.

Het meest gebruikte (symmetrische) encryptie algoritme dat wordt gebruikt in wachtwoordmanagers, is de Advanced Encryption Standard (AES). Dit algoritme voert complexe,

omkeerbare wiskundige bewerkingen uit op blokken data van 128 bits, op basis van de gebruikte codeersleutel. Het resultaat van die bewerkingen is een blok van 128 bits dat versleuteld is, waarvan het origineel alleen maar terug te krijgen is met behulp van de gebruikte codeersleutel. De data, die versleuteld worden, zijn vaak niet precies 128 bits. Als de gegevens meer dan 128 bits zijn, worden ze verdeeld in deze blokken en als er niet genoeg gegevens zijn om een blok te vullen, wordt opvulling gebruikt tot dat wel het geval is.

De codeersleutel die wordt gebruikt in AES kan verschillen in lengte. Volgens de officiële specificatie moet de sleutel 128, 192 of 256 bits zijn (16, 24 of 32 bytes). Hoe langer de codeersleutel, hoe meer moeite het kost om de juiste codeersleutel te raden. Als je de sleutel niet weet, kun je proberen om de versleutelde data te ontsleutelen door iedere mogelijke codeersleutel te proberen. Het zou de beste supercomputer ter wereld al triljoenen jaren kosten om alle mogelijkheden van een codeersleutel van 128 bits te proberen. Door de lengte van de codeersleutel te verhogen, groeit dit aantal exponentieel. Echter, als kwantumcomputers toegankelijker worden, is het mogelijk veel sneller om alle mogelijkheden te proberen. Daarom gebruiken bijna alle wachtwoordmanagers AES-256, met een codeersleutel van 256 bits. De rest van dit artikel gaat uit van een codeersleutel van 256 bits.

Codeersleutel als geheim

Zolang je codeersleutel geheim is, zijn je versleutelde data dat ook. Dit maakt een codeersleutel vergelijkbaar met een wachtwoord en je moet deze dan ook nooit met iemand delen. Er zijn echter cruciale verschillen. Een codeersleutel bestaat uit 256 bits, dat betekent dat iedere bit gebruikt kan worden. Een wachtwoord wordt vaak ingevoerd in een computer. Een computer werkt slechts met bits en bytes, dus ieder teken dat je invoert wordt gecodeerd naar bits.

Een computer kent vaak verschillende coderingen en die moeten ieder teken, inclusief de enter-, backspace- en deletetoets, dat je mogelijk kan invoeren in een computer naar een waarde in bits vertalen. Niet ieder teken kun je gebruiken in een wachtwoord, waardoor er een aantal combinaties van bits zijn die je niet kunt invoeren in een computer. Daardoor is het onmogelijk om met een wachtwoord van 32 tekens iedere mogelijke codeersleutel weer te geven.

In plaats van rechtstreeks een wachtwoord te gebruiken van 32 tekens, wordt een codeersleutel van een wachtwoord afgeleid. Veel wachtwoordmanagers gebruiken hiervoor de 'Password-Based Key Derivation Function 2' (PBKDF2) algoritme. Dit is een 'hash algoritme', dat een algoritme is om met behulp van onomkeerbare wiskundige bewerkingen een unieke code te berekenen voor data. Deze unieke code heet 'hash' of 'hashwaarde', en kan dus niet gebruikt worden om de originele invoer te herleiden. In ons geval is de invoer het wachtwoord dat we hebben en de resulterende hash is de codeersleutel voor onze versleutelde gegevens.

Het PBKDF-algoritme is ontworpen om vele malen herhaald te worden, wat ook wel *iteraties* worden genoemd. Hoe meer iteraties er worden gebruikt, hoe meer moeite een computer moet doen om een hash te berekenen. Als je het wachtwoord weet, hoef je de vele iteraties maar één keer te berekenen, waardoor het alsnog redelijk snel is. Het grote aantal iteraties wordt gedaan om hackers die het wachtwoord willen raden te ontmoedigen, omdat die dan de vele iteraties voor ieder mogelijk wachtwoord moeten berekenen. Het OWASP *Password Storage Cheat Sheet* geeft als advies om PBKDF2 te gebruiken met ten minste 310.000 iteraties.

Om een wachtwoordmanager te gebruiken, heb je een hoofdwachtwoord nodig. Uit dit *hoofdwachtwoord* wordt een codeersleutel afgeleid, die wordt gebruikt om de wachtwoordgegevens te versleutelen voor al je accounts. Omdat dit hoofdwachtwoord **de** sleutel is tot al je accounts, moet het een heel sterk wachtwoord zijn; de entropie moet dus hoog zijn. De meeste wachtwoordmanagers geven ook advies over hoe je een hoofdwachtwoord kunt kiezen.

Bestaande wachtwoordmanagers

Een wachtwoordmanager slaat al je wachtwoorden veilig op. Laten we aannemen dat het bestand met alle inloggegevens voor al je accounts op je computer staat. Om toegang te krijgen tot al je wachtwoorden, moet je het bestand op je computer eerst ontsleutelen. Maar wat als je geen toegang hebt tot die specifieke computer, de computer wordt gestolen of het bestand raakt beschadigd? Dat zou betekenen dat je helemaal geen toegang meer kan krijgen tot al je accounts.

Er zijn veel verschillende wachtwoordmanagers die je kunt gebruiken. Alle wachtwoordmanagers slaan je wachtwoorden veilig op en daarvoor vereisen ze, zoals besproken, een hoofdwachtwoord. De exacte algoritmes die gebruikt worden, kunnen echter verschillen. Daarnaast bieden sommige wachtwoordmanagers extra functies, die worden aangeboden in verschillende soorten abonnementen. Hier bespreken wij een aantal van deze extra functies die bekende wachtwoordmanagers aanbieden, zodat je zelf een weloverwogen beslissing kunt nemen. Er zijn een groot aantal wachtwoordmanagers,

waardoor wij onze beschrijving moeten beperken tot de functies van: LastPass (1), KeePassXC, LessPass, BitWarden, Dashlane en 1Password. Het grote voordeel van het gebruik van een wachtwoordmanager service in vergelijking tot het zelf opslaan, is dat de wachtwoordgegevens worden geback-upt. Met uitzondering van LessPass vereisen alle wachtwoord-managers dat je een account maakt. Voor dit account heb je een hoofdwachtwoord nodig en door daarmee in te loggen heb je toegang tot al je andere wachtwoorden, ongeacht vanaf welk apparaat je inlogt. Als het apparaat waarmee je normaal gesproken je wachtwoorden opzoekt kapot gaat, kun je met een ander apparaat alsnog toegang krijgen tot je wachtwoorden.

Toegangsbeperkingen

De apparaten waarmee je mag inloggen bij je wachtwoord-manager kan afhangen van het abonnement dat je kiest. Met de gratis versie van LastPass kun je bijvoorbeeld ofwel inloggen met je browser vanaf een computer, ofwel inloggen via de app op je mobiel. De betaalde versie heeft deze beperking niet en daarmee kun je dus vanaf ieder apparaat inloggen.
Sommige wachtwoordmanagers bieden ook de optie om een account aan te maken voor meerdere gebruikers. Dit kan aantrekkelijk zijn voor bedrijven, organisaties of grote vrienden-groepen. Eén van de gebruikers moet dan betalen en kan dan anderen uitnodigen. Iedere gebruiker die je toevoegt, kan vervolgens zelf een account aanmaken en gebruikmaken van de functies van de wachtwoordmanager. Als je echter op zoek bent naar een persoonlijke wachtwoordmanager is dit misschien niet de beste optie. Dashlane biedt op dit moment een 'Starter' abonnement aan voor twee dollar per gebruiker per maand, maar je bent verplicht om minimaal tien 'seats', of gebruikers, af te nemen. Hierdoor kost dit abonnement bij Dashlane minimaal twintig doller per maand, omdat je dan ook betaalt voor negen extra gebruikers. Wees op de hoogte van het feit dat dit soort abonnementen bestaan, anders kun je negatief worden verrast.

Wachtwoordgenerators

Bijna alle wachtwoordmanagers hebben een ingebouwde wachtwoordgenerator, die snel willekeurige wachtwoorden genereert op basis van de eisen die je zelf stelt. Zo kun je bepalen uit welke soorten tekens het wachtwoord wordt gegenereerd, of er hoofdletters in kunnen zitten en hoe lang het wachtwoord moet zijn. De gegenereerde wachtwoorden zijn vaak lastig te onthouden, maar ook heel lastig om te raden. Dit is gelukkig geen probleem, omdat de wachtwoordma-nager er juist voor zorgt dat je wachtwoorden niet hoeft te onthouden. De lastig te raden wachtwoorden maken je accounts juist veiliger!

Wachtwoorden delen

Het delen van wachtwoorden is ook een functionaliteit die door veel wachtwoordmanagers wordt aangeboden. Dit lijkt misschien vreemd, omdat een wachtwoord juist geheim moet blijven. Echter, voor sommige onlinediensten kun je een familie-account hebben, of een ander soort account waar misschien verschillende mensen op moeten inloggen. In sommige wacht-woordmanagers kun je je wachtwoord delen door het e-mailadres van iemand in te voeren. Zij krijgen dan een e-mail en als zij inloggen of een account maken bij dezelfde wacht-woordmanager, krijgen zij meteen toegang tot het gedeelde wachtwoord. Als de deler van het wachtwoord het originele wachtwoord verandert, zal deze verandering voor de anderen ook zichtbaar zijn. Er zijn twee verschillende manieren om een wachtwoord te delen. Er is 'one-to-one' delen, waarbij je een wachtwoord kan delen met één ander persoon. Ook is er 'one-to-many' delen, wat het mogelijk maakt om een wachtwoord te delen met een groep personen. LastPass maakt een onder-scheid tussen deze twee manieren en alleen one-to-one delen is beschikbaar voor de gratis versie. Alle andere wachtwoord-managers maken geen onderscheid tussen deze twee typen.

Extra data opslag

Zoals eerder besproken kunnen wachtwoorden opgeslagen worden in een bestand en wachtwoordmanagers kunnen dit op een veilige manier doen. Sommige wachtwoordmanagers gebruiken deze functionaliteit om ook extra bestandopslag aan te bieden. Dit maakt het mogelijk om veilig notities of andere belangrijke documenten op te slaan in je wachtwoord-manager. Doordat de data worden versleuteld, kunnen zelfs hackers zónder jouw hoofdwachtwoord de data niet lezen als het bedrijf achter de wachtwoordmanager wordt gehackt!
Niet alle wachtwoordmanagers bieden deze optie. De wacht-woordmanagers die dat wel doen, bieden verschillende opslagopties, afhankelijk van hoeveel je ervoor wilt betalen. Hoewel dit een leuke toevoeging is aan een wachtwoordma-nager, moet dit niet een reden zijn om een bepaalde wacht-woordmanager te gebruiken. Als de wachtwoordmanager die je wilt gebruiken dit niet heeft, kun je altijd een online dienst vinden die dit wel doet en de accountgegevens in je wacht-woordmanager opslaan.

Waarschuwingen voor inbreuken op de beveiliging

Bijna iedere dag is er een datalek. Het kan zijn dat de website waar jij een account hebt, te maken heeft gehad met zo'n datalek. Sommige wachtwoordmanagers kunnen een notificatie geven als dit het geval is. Soms worden e-mailadressen buitgemaakt, wat ervoor kan zorgen dat je extra spammail krijgt. Cybersecurity-bedrijven houden nauwkeurig in de gaten wat voor datalekken er zijn en wat voor data er op straat liggen. Zodra je wachtwoordmanager ziet dat jouw data daartussen zitten, word je daarop geattendeerd en zul je daar actie op moeten ondernemen. Je zou bijvoorbeeld je wachtwoord moeten veranderen voor dat account.

Multifactor-authenticatie

Het idee van multifactor-authenticatie is dat je meerdere factors gebruikt om je identiteit vast te stellen en om zo in te loggen bij een dienst. Er zijn drie verschillende factoren, die als volgt worden beschreven: 'iets wat de gebruiker weet', 'iets wat de gebruiker heeft' en 'iets wat de gebruiker is'. Een wachtwoord dat je moet invoeren is een typisch voorbeeld van de eerste factor, want dat is iets wat je als gebruiker weet. Een toegangspasje of een authenticator-app op je mobiel is een voorbeeld van de tweede factor. Biometrische gegevens, zoals een vingerafdruk of een gezichtsidentificatie, worden beschreven met 'iets dat de gebruiker is'.

Bij multifactor-authenticatie is het de bedoeling dat je op zijn minst twee factoren gebruikt om je identiteit vast te stellen. Om toegang te krijgen tot je account heb je bijvoorbeeld zowel een wachtwoord nodig als een code die wordt gegenereerd in de authenticator-app op je mobiel. Zelfs als iemand anders dan je wachtwoord weet, heeft diegene alsnog je mobiele telefoon nodig om toegang te krijgen tot je account.

Een wachtwoordmanager is de sleutel tot al je accounts, dus die moet je te allen tijde goed beschermen. Als jouw wachtwoordmanager geen mogelijkheid heeft om multifactor-authenticatie in te stellen, moet je zeker heroverwegen om een andere wachtwoordmanager te nemen.

Automatisch wachtwoorden en gevoelige informatie invullen

Sommige wachtwoordmanagers geven een mogelijkheid om een browser extensie te installeren, waarmee (wachtwoord)velden op websites automatisch kunnen worden ingevuld. Als je je wachtwoord opslaat in een wachtwoordmanager, kun je ook de website waar die op wordt gebruikt toevoegen. Zodra de wachtwoordmanager ziet dat je op die website bent, wordt het wachtwoord automatisch ingevuld, zodat je alleen nog maar op de login-knop hoeft te drukken.

De wachtwoorden die een wachtwoordmanager genereert zijn lastig te onthouden, waardoor dit een uiterst handige functie is. Echter, het makkelijker maken hiervan maakt het minder veilig. Als iemand dan toegang krijgt tot je ontgrendelde computer, worden de wachtwoorden automatisch ingevuld en heeft die persoon dus ook toegang tot al je andere accounts. Multifactor-authenticatie verhelpt dit probleem, omdat er dan nog een extra factor nodig is.

Als je deze functie wel wilt gebruiken, zorg er dan voor dat je je hoofdwachtwoord eigenlijk iedere keer moet invullen voordat de velden worden ingevuld. Dit maakt het misschien iets minder gebruiksvriendelijk, maar het veilig houden van al je accounts gaat niet altijd over gebruiksvriendelijkheid. Een algemeen advies dat altijd geldt: laat je wachtwoord nooit onbeheerd achter!

Ondersteuning

Het is belangrijk om te weten dat je ondersteuning kunt krijgen als je problemen hebt met je wachtwoordmanager. Sommige wachtwoordmanagers zijn 24/7 bereikbaar, andere alleen tijdens kantooruren. Ook kan het afhangen van je abonnement, met een duur abonnement word je vaak eerder geholpen dan wanneer je er gratis gebruik van maakt.

Ondersteuning kan bestaan uit een live-chat, per e-mail, of telefonisch. Niet alle wachtwoordmanagers bieden alle opties en ook dit kan afhankelijk zijn van je abonnement. Als je problemen het liefst wilt oplossen via de telefoon, zorg er dan voor dat je een wachtwoordmanager kiest die die service ook biedt.

Reputatie

Ook de reputatie van een wachtwoordmanager kan bepalend zijn voor je keuze. De reputatie van een wachtwoordmanager wordt ondersteund door de functies die geboden worden, de specifieke algoritmes die worden gebruikt om de wachtwoorden te versleutelen, de technische ondersteuning die geboden wordt, maar ook datalekken die in het verleden zijn gebeurd. Wachtwoordmanagers zijn een belangrijk doelwit voor hackers, omdat ze toegang kunnen krijgen tot iedere account van iedere gebruiker wanneer ze toegang krijgen tot alle gegevens van een wachtwoordmanager.

Een datalek is een serieus probleem, maar soms is het onmogelijk om het te voorkomen. Of een wachtwoordma-

De beste wachtwoordmanager is degene die je gemakkelijk kunt gebruiken en degene die je vertrouwt om jouw accounts veilig te houden.

nager betrouwbaar is of niet hangt ook af van hoe het bedrijf is omgegaan met de datalekken die hebben plaatsgevonden. Wat voor soort gegevens zijn er gestolen? Heeft het bedrijf de inbreuk op een verantwoorde manier afgehandeld? Een bedrijf dat een datalek verantwoord heeft afgehandeld, is misschien betrouwbaarder dan een bedrijf waar nog nooit een datalek heeft plaatsgevonden.
Denk eraan dat de reputatie van een wachtwoordmanager een belangrijke factor is, maar niet de enige factor. Het is ook belangrijk om de functies en beveiliging van een wachtwoordmanager zorgvuldig te evalueren om er zeker van te zijn dat deze voldoet aan je eigen behoeften en dat deze het beschermingsniveau biedt dat je zelf nodig hebt.

'Stateless' wachtwoordmanager

LessPass is een heel ander type wachtwoordmanager, want deze is 'stateless'. Dit betekent dat de wachtwoordmanager helemaal geen informatie opslaat. In plaats daarvan worden wachtwoorden gegenereerd met behulp van een 'pure function'. Dit is een concept in programmeren waarbij een functie of algoritme altijd exact hetzelfde resultaat geeft zonder bijwerkingen, mits je dezelfde invoer geeft. De functie wordt altijd berekend op je eigen systeem, waardoor er nooit iets verstuurd wordt naar een server. Als invoer heb je de naam van een website nodig, de loginnaam en je hoofdwachtwoord. Daarnaast kun je nog extra opties kiezen waar het wachtwoord aan moet voldoen. Dit is eigenlijk hetzelfde als een traditionele wachtwoordmanager, maar het gebruikt de naam van de website, je loginnaam en je hoofdwachtwoord samen om een uniek wachtwoord te genereren.
Het grootste probleem met dit systeem is dat je voor iedere website de specifieke opties moet onthouden, als je niet de standaardopties gebruikt. Dit is juist het probleem dat we proberen op te lossen met een wachtwoordmanager. LessPass lost dit op door ook de optie te bieden om een account aan te maken waar al die opties voor al je accounts worden opgeslagen. Hiervoor kun je de publieke online LessPass server gebruiken, maar je kunt die server ook zelf opzetten, omdat alle code open-source (publiek beschikbaar) is. Doordat deze methode fundamenteel anders is dan de andere wachtwoordmanagers, biedt LessPass ook niet dezelfde extra functies als de andere wachtwoordmanagers.

Conclusie

In dit artikel zijn veel functies belicht die bekende wachtwoordmanagers bieden. Deze functies kunnen het inloggen bij diensten gemakkelijker maken, maar ze kunnen je accounts ook minder veilig maken. Het is belangrijk om zelf deze overwegingen te maken en ik hoop dat je met de kennis uit dit artikel een weloverwogen beslissing kunt nemen. Houd in gedachten dat de kernfunctie van een wachtwoordmanager het veilig opslaan van wachtwoorden is. Uiteindelijk is de beste wachtwoordmanager degene die je gemakkelijk kunt gebruiken en degene die je vertrouwt om jouw accounts veilig te houden.

[1] Noot van de redactie:
In zijn column in deze uitgave van IB Magazine gaat Lex Borger in op het fenomeen passwordmanagers en de hack van LastPass vorig jaar. Dit onder de kop 'Password mismanagement'. Lees zeker deze column op pagina 23 (nog) eens wanneer je op het punt staat een keuze te maken voor een wachtwoordmanager.

Achter Het Nieuws

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

Chris de Vries | Fook Hwa Tan | Leo van Koppen

Toenemende spanningen tussen de Verenigde Staten en China

We horen veel nieuws over toenemende conflicten tussen de Verenigde Staten en China. Het is jaren geleden begonnen met spionageverhalen door Chinese producenten zoals Huawei en TikTok. Onlangs waren Chinese spionageballonnen in het nieuws. Deze zijn uiteindelijk door de VS neergeschoten en onderzocht (1). Vervolgens gaf China als respons aan dat de VS ook ballonnen om te spioneren boven China heeft (2). In al deze gevallen worden bewijzen niet publiekelijk gemaakt. Hoe moeten we vanuit Europa hiermee omgaan? Kiezen we de kant van onze bondgenoot of moeten we een onafhankelijke positie innemen?

Je zou zeggen, met onze vrijheid van informatie, dat we gemakkelijker beschikken over alle 'feiten'. Maar wat zijn dan alternatieve 'feiten'? Is er wel een waarheid of is alles relatief?

Fook Hwa Tan - Bevooroordeelde media; bestaan er nog onafhankelijke media?

Zoals in het nieuws bijna dagelijks is terug te lezen, zien we langzaam een escalatie tussen het Westen en China. De berichtgeving over spionage, maar ook over de oorlog in Oekraïne zorgt ervoor dat iedereen benieuwd is naar hoe de overheid van China gaat acteren.

Als Chinees, geboren en getogen in Nederland, is het soms lastig om feiten van alternatieve feiten te onderscheiden. Ik heb nooit geweten, na velen jaren onderwijs, dat er zoiets bestaat als alternatieve feiten. Ik dacht altijd dat een feit iets vaststaands is. Iets dat wetenschappelijk, oftewel herhaaldelijk door toetsing kan worden bewezen. Nu word ik geconfronteerd met een rijzend sentiment tegen China. Dit was al begonnen vóór de COVID-19 jaren en werd door het virus uit China alleen maar erger. Onder invloed van de huidige geopolitiek lijkt het conflict nog heviger te worden.

In het Westen zijn we tegen China vanwege: het autoritaire regime, communisme, gebrek aan mensenrechten, de nog steeds groeiende Chinese economie en onze toenemende afhankelijkheid van het land. Vanuit de Chinese media hoor ik echter over het irrationele en moralistische vingertje van het Westen. Wat is een feit en wat is het alternatieve feit? Of kan het ook zo zijn, dat beide waar zijn en dat het alleen ligt aan je uitgangspunt? Dan hebben we in het Westen nog de linkse en de rechtse media. Ondanks dat ze het vaak over dezelfde 'feiten' hebben, interpreteren ze deze vaak heel anders. Hoe kan dit dan?

Wat, denk ik, belangrijk blijft, is allerhande informatie tot je te nemen en altijd in gesprek te gaan om elkaar beter te leren begrijpen. Neem niet op voorhand een standpunt in, maar wees objectief en zorg dat je alleen de feiten als feiten behandelt!

Leo van Koppen - Wie is er te vertrouwen in de zoektocht naar de waarheid?

Collega-redacteur Fook Hwa kaart in deze aflevering van Achter Het Nieuws wel een heel lastig probleem aan. Heel simpel geformuleerd: 'Wat is de waarheid?'. Beatrice de Graaf zou zeggen 'de geschiedenis heeft ons geleerd dat…' en komt vervolgens met een mooi lijstje casussen uit de rijke historie van waaruit in veel gevallen een alleszins plausibele redenering volgt over hoe in het huidige tijdsgewricht om te gaan met het probleem van de juiste feiten en alternatieve feiten.

Helaas is Beatrice niet op chat bereikbaar, dan maar even voorleggen aan ChatGPT. Ik word gerustgesteld met de conclusie: *"Het is belangrijk om te erkennen dat er geen eenvoudige oplossing is voor dit*

probleem". Vervolgens volgt een benadering voor het probleem in de trant van: *"Een multifaceted benadering is waarschijnlijk het meest effectief, waarbij zowel individuele mediaconsumenten als organisaties en beleidsmakers samenwerken om het probleem aan te pakken."*
Het antwoord is in lijn met de benadering die Fook Hwa aanbeveelt. Toch ben ik nog niet tevreden met het overigens zeer logische antwoord. De crux zit volgens mij in de (on)mogelijkheden om met elkaar vanuit al die verschillende invalshoeken daadwerkelijk een serieuze dialoog te voeren. Vanuit welke politieke overtuiging, welke religie of welk kennisdomein voer je het gesprek? Wat zijn je onbewuste vooroordelen (bias)? En wat zijn je belangen en motieven? Al die factoren beïnvloeden de dialoog en de uitkomst van de dialoog is dan de waarheid?

Ik twijfel en mijn twijfel wordt sterker als ik net het laatste deel van *Planet Finance* heb gezien. De (financiële) geschiedenis heeft ons geleerd dat manipulatie heel vaak is gebeurd en nog steeds gebeurt. Zojuist de volgende voorbeelden gezien: Lernhout & Hauspie (3), het bedrijf dat aan het eind van de vorige eeuw de wereld zou gaan veroveren met spraaktechnologie, maar in 2001 failliet ging. Of heel recent nog de teloorgang van Wirecard (4), een soortgelijk geval van manipulaties in de financiële markten. Zelfs de leden van de Duitse regering waren ervan overtuigd dat dit bedrijf de wereld van de digitale betalingen ging veroveren. Beide casussen zijn voorbeelden van een massale manipulatie. Dat is het grote gevaar in die dialoog bij het achterhalen van de waarheid.

Aardig betoog Leo, maar wat heeft het te maken met ons vak? Heel veel zou ik denken, het gaat immers over het vertrouwen van mensen in informatie, over integriteit van mensen en data, de regulering via wet- en regelgeving. Boeiend vakgebied waarin we werken!

Chris de Vries - {Cultuur + filosofie + informatie ≥ ware feiten} = informatiebeveiliging!?

Het leuke van het redacteurschap is dat je regelmatig kwesties krijgt voorgelegd, welke je uitdagen om anders tegen feiten en waarheden aan te kijken. Een les in bescheidenheid, compassie, empathie en flexibel denken. Zo ook ons *Achter Het Nieuws*-thema van deze uitgave.

Het begint met cultuur. Is er een grotere tegensstelling denkbaar dan tussen China (Confuciaans denken) en de Verenigde Staten (liberalistisch denken)? Het plannen op de lange termijn (familie/voorouder gebaseerd – eer/respect/ondergeschiktheid) versus het kwartaal denken (stakeholders gebaseerd – winstmaximalisatie en elk individu is zelf verantwoordelijk, vrij).

De cultuur leidt tot filosofie; vanuit Azië (Confucius, Boeddhisme, TAO, Sun Tzu, Feng Shui), vanuit het Westen (`Laissez faire', scientific management, bureaucratie, Keynes, Taylor, Max Weber).

Deze reis door de landschappen brengt ons waarnemingen (locaties, volkeren, gedragingen; data) geïnterpreteerd als ware feiten. Of …? Wij spreken over het Verre - dan wel het Midden-Oosten; de Chinezen spreken over (Centraal) Azië en West Azië. Het is maar waar je staat op deze aarde om feiten te kunnen catalogiseren als ware feiten.

Ware of niet-ware feiten voegen zich samen tot meta-feiten, zoals een rups tot vlinder – feiten tot informatie. Afhankelijk van hoever een volk begrip heeft voor `haar afstand tot de macht' (5) zo zal zij ook omgaan met deze informatie. Voor zich houden of delen.

En daar komen wij om de hoek kijken: wij beschermen. Dat doen wij vanuit onze culturele & filosofische achtergrond, opvoeding, normen & waarden, overtuigingen. Hoe moeilijk voor eenieder, die strijdigheid ervaart tussen de cultuur en filosofie (geboren in Nederland en Chinees van afkomst). En dat maakt dat informatiebeveiliging een vak is, dat het een wedstrijd is tussen `hackers' en verdedigers, maar ook een theater voor (cyber)oorlog.

En waar staan wij, als Europeanen? Vanuit mijn kaders zie ik als *'waar feit'* het Rijnlands denken. Gericht op duurzaamheid, (sociale) zorg voor de mens & voor de medewerker (gericht op participatie en medezeggenschap), innovatief georiënteerd. Met als voorbeelden: Erasmus, Geert Groote, Descartes, Jean Monnet.

Gericht op een leven lang leren en groei. Europa als voortrekker in klimaatzaken, het nemen van eigen verantwoordelijkheid - nu en niet morgen. Europa ook als collectief, maar niet zo `(im)perfect' als de bekende wereldrijken. Wij bewandelen onze eigen weg, groeien met vallen en opstaan. Het lijkt wel informatiebeveiliging.

Om met de Chinezen te spreken: 'Wij leven in interessante tijden' en dat is een vloek.

Referenties

(1) https://nos.nl/artikel/2463723-witte-huis-verdedigt-neerhalen-objecten-chinese-ballon-geborgen
(2) https://www.theguardian.com/world/2023/feb/16/china-claims-us-balloons-flew-over-tibet-and-xinjiang-as-spying-row-rumbles-on
(3) https://nl.wikipedia.org/wiki/Lernout_%26_Hauspie
(4) https://duitslandinstituut.nl/artikel/52453/proces-rond-wirecard-schandaal-van-start
(5) Geert Hofstede: "Cultures and organizations", onderzoek bij IBM-medewerkers.

Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via m.hoogesteger@s-rminform.com.

COLUMN MARTIJN

Een sprintje in de wapenwedloop

De wapenwedloop in cyber is de afgelopen jaren niet heel hard gegaan. Cybercriminelen hadden het duidelijk voor het zeggen en hadden vrij spel. Ransomware was, en is, de modus operandi om geld te verdienen. De afgelopen jaren hebben we hard gewerkt om daar wat aan te doen. We beveiligen onze maatschappij beter, we weten beter blokkades op te werpen voor de 'ransomware businesscase' en we weten de boeven steeds vaker op te sporen en te pakken.

Dit zorgt ervoor dat we eindelijk wat hebben ingehaald in de race en dat er weer gerend moet worden aan de criminele kant. Dit zien we de afgelopen tijd steeds duidelijker terug, met nieuwe technieken en strategieën die oppoppen. Het nadeel van de afgelopen jaren: cybercriminelen hebben een aardige pot geld kunnen opbouwen om nu te investeren.

Ten eerste zien we dat een deel van het geld duidelijk wordt geïnvesteerd om kwetsbaarheden in software te vinden. Dit is een duidelijke reactie op het beter beveiligen van gebruikers met bijvoorbeeld MFA. Door kwetsbaarheden in (externe) software te benutten, kunnen criminelen op een andere manier een eerste stap in een netwerk zetten. Ze kopen deze kwetsbaarheden in op het darknet of ze huren mensen in om doorlopend dit soort onderzoek te doen.

Ten tweede zien we dat ransomware en 'ransomware as a service' steeds toegankelijker worden. De tools om een aanval uit te voeren zijn meermaals gelekt en worden gebruikt door minder geavanceerde splintergroepen. Die zijn vaak wat luidruchtiger en onhandiger, waardoor ze weer makkelijker te ontdekken zijn voor ons! De grote groepen blijven echter bestaan en ontwikkelen ook hun tools en technieken door.

Door de sancties van afgelopen jaren, en de volwassenheid die we hebben als maatschappij, worden er minder ransomware betalingen gedaan. Dit zorgt ervoor dat criminelen naar andere modus operandi moeten zoeken. Zo zien we dat ze weer meer met 'business email compromise' bezig zijn en daar ook weer innovaties in verzinnen.

Een voorbeeld van zo'n innovatie is EvilProxy, een nieuwe dienst voor criminelen om niet alleen een gebruikersnaam en wachtwoord van een gebruiker af te troggelen, maar ook hun MFA-code. Op die manier zien we criminelen nu ook weer binnendringen. De dienst is (relatief gezien) niet duur en wordt aangeboden voor een flinke lijst websites, waaronder: Google, Microsoft, Facebook, Apple, maar ook specifieker gericht zoals GitHub.

Het tempo van de wapenwedloop is weer verhoogd. Waardoor we weer moeten nadenken over de volgende verdedigingsstappen die we moeten zetten. Er is meer aandacht dan ooit en de bereidheid om te bewegen is er. We moeten samen weer puzzelen met betrekking tot de volgende stappen. Weer scherp zijn op 'business email compromise' en mogelijke nieuwe soorten aanvallen. Niet alleen MFA, maar 'trusted access'. Nog scherper op de rechten van gebruikers.
Laten we zorgen dat we in het volgende rondje voorop gaan lopen in de wapenwedloop!

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Leo van Koppen
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
Eric Noordam
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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 2023 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

iSOC24
be in control

Intelligence-driven operations

24/7 real-time inzicht in de status van uw informatiebeveiliging

Wij helpen organisaties met ons ecosysteem om in control te geraken over hun informatiebeveiliging zodat de relevante risico's het hoofd worden geboden en tot een acceptabel niveau kunnen worden teruggebracht.

Meer weten?
Kijk op iSOC24.com

- Cloud Security
- Security Testing
- Threat Intelligence
- Deception & Counter-intelligence
- Security Orchestration Automation & Response

10 YEAR ANNIVERSARY

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2023

WR - Workshop Ransomware
EHE - Ethical Hacking Essentials
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 - Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen