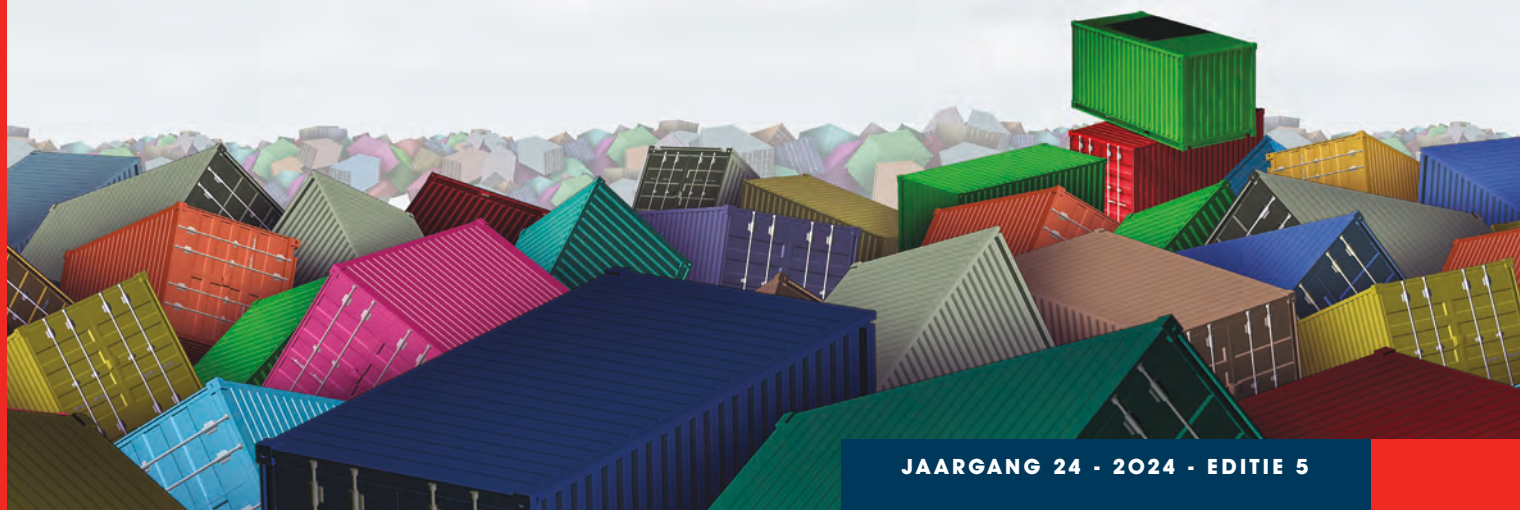
INFORMATIEBEVEILIGING MAGAZINE

Thema: Supply chain management in informatiebeveiliging - deel 2

- De spagaat van de CISO
- Bye bye Chinees, welkom Pool
- AHN: De invloed van de wereld op onze leveranciers



JAARGANG 24 - 2024 - EDITIE 5

ISOPlanner

Eenvoudig Compliance Management in **Microsoft 365**

Hoe Gemeente Waterland structuur en controle heeft bij de invoering van BIO-maatregelen

De gemeente had een duidelijk doel: controle houden op de uitvoering van maatregelen om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO).

Door de samenwerking met ISOPlanner:

- ✓ Heeft de gemeente een ISMS dat overzicht biedt in benodigde acties.
- ✓ Bespaart de gemeente tijd door gebruik te maken van voorbeelddocumenten.
- ✓ Borgt de Microsoft-integratie het doorvoeren van maatregelen.

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365. Uiteraard ook voor ISO 27001, NEN 7510 en NIS2.

Snelle implementatie door meegeleverde templates en naadloze integratie met Teams, SharePoint, Outlook en Power Automate.

We kozen voor een snelle implementatie waarbij veel voorwerk was gedaan. En dat aansloot bij onze beveiligingseisen zoals single sign-on. Ook de Microsoft-integratie was een veriste.

Jimmy Voskuil
Gemeente Waterland

Kijk op **www.isoplanner.app** voor meer informatie en jouw gratis proefperiode.

ISO 27001 2024 COMPLIANT
GDPR 2024 COMPLIANT
PENTEST 2024 SECURE

Voortzetting

Chris de Vries

Onze huidige uitgave is een voortzetting van ons vorig magazine met als thema: *Supply chain management in informatiebeveiliging*. De toestroom van artikelen noodzaakte ons daartoe en dat ervaren wij als vertrouwensvotum van onze leden, lezers en auteurs. Dank aan jullie allen.

In dit nummer vraag ik aandacht voor onder meer de column van Rachel Marbus. Een open en moedige reflectie over privacy, anonimiteit en online haatuitingen. Een zeer lezenswaardig stuk en een aansporing voor ons allen.

Wat daarnaast aandacht vraagt is het interview met Enovation. Oorspronkelijk gepland voor de AI-uitgave iB2-2024, echter, AI bleek géén test-succes voor ons om een goed artikel te redigeren, vandaar het uitblijven daarvan. Door het succes van iB3 en iB4 paste het ook daar niet en daarom pas nu in deze uitgave. Het interview biedt een boeiend en leerrijk inzicht in de (ontwikkel)visie van Enovation op AI en is actueel als je het plaatst in de overname (april 2024) van Enovation door de Franse fabrikant Legrand voor een bedrag van ruim een half miljard euro (aldus Bloomberg). Wij komen in de toekomst op Enovation terug.

Leerzaam en leuk om te lezen is het artikel van Ronald Eygendaal: Bye bye Chinees, welkom Pool. En wat voor vele CISO's onder ons interessant zal zijn is De spagaat van de CISO uit de koker van Edwin Franse. De essentie van het artikel volgens onze redacteur Alex Dingemanse: hoewel IT-beveiliging een volwassen vak is geworden, is de rol van de CISO binnen een organisatie nog steeds in ontwikkeling. Dat wordt voornamelijk bepaald door de plaats van IT-beveiliging in de volwassenheid van de organisatie zelf. Edwin Franse geeft een helder beeld, hoe de CISO zelf door middel van: educatie, samenwerking en communicatie, zijn rol als onderdeel van de bedrijfsstrategie kan borgen.

Laat niemand zeggen dat ons werk als informatiebeveiliger niet kunstig is!

Veel leesplezier,

Chris

IN DIT NUMMER

Auteur: Edwin Franse is CISO bij Van Oord.

De spagaat van de CISO: beheersbaarheid versus verantwoordelijkheid

In de steeds complexere digitale wereld wordt van de Chief Information Security Officer (CISO) meer verwacht dan enkel technische expertise. De CISO moet een strategische rol vervullen en de balans vinden tussen operationele controle en langetermijn-doelstellingen. Daarbij is het essentieel om draagvlak te creëren bij de directie en het senior management, bijvoorbeeld door middel van educatie en strategische communicatie. Van de CISO wordt ook verwacht dat hij of zij actief bijdraagt aan bredere bedrijfsdoelstellingen en risicobeheersing. Dit artikel bespreekt hoe de CISO deze spagaat kan overbruggen, samenwerkingsverbanden binnen de organisatie versterkt, en informatiebeveiliging positioneert als een strategisch voordeel dat niet alleen groei bevordert, maar ook voldoet aan belangrijke regelgeving.

De rol van de Chief Information Security Officer (CISO) is zowel veelzijdig als veeleisend, met als grootste uitdaging het vinden van een evenwicht tussen strategische verantwoordelijkheid en operationele controle. Afhankelijk van de organisatie kan de invulling van de functie sterk verschillen, wat de complexiteit van de rol alleen maar vergroot. De CISO is altijd verantwoordelijk voor het waarborgen van informatiebeveiliging, maar de mate waarin hij of zij betrokken is bij operationele of strategische taken, varieert aanzienlijk per organisatie.

Rol van de CISO

In sommige organisaties is de CISO nauw betrokken bij de technische uitvoering van beveiligingsmaatregelen en is sprake van een hands-on rol in operationele activiteiten. In andere gevallen werkt de CISO voornamelijk op strategisch niveau samen met het topmanagement om beleid te ontwikkelen dat de organisatie beschermt tegen een breed scala aan risico's. Vooral in grotere organisaties, met complexe IT-infrastructuren, opereert de CISO op strategisch niveau. In kleinere bedrijven is de CISO daarentegen vaak meer direct betrokken bij de praktische uitvoering van maatregelen en dagelijkse beveiligingsprocessen.

Een veelvoorkomend probleem is dat organisaties niet altijd goed inzicht hebben in de positionering van de CISO binnen hun bredere risicobeheerstructuur. Het 'Three Lines of Defense'-model kan daarbij nuttig zijn. In dit model is de eerste lijn verantwoordelijk voor de uitvoering van operationele beveiligingsmaatregelen, de tweede lijn voor toezicht en risicobeheersing, en de derde lijn voor onafhankelijke audits. Binnen dit model opereert de CISO strikt genomen vanuit een tweede lijn. Hoewel dit model een theoretisch duidelijke scheiding van verantwoordelijkheden biedt, vervagen in de praktijk deze grenzen vaak. Dit ondermijnt de effectiviteit van de CISO, die verantwoordelijk is voor strategische besluitvorming, maar beperkt wordt door een gebrek aan directe controle over de implementatie.

De rol van de CISO vereist dat zij flexibel blijft, inspelend op dreigingen en beperkte middelen en politieke uitdagingen binnen de organisatie. Budgettaire beperkingen kunnen het werk van de CISO verder bemoei-

lijken, vooral wanneer de directie kiest voor het uitstellen of afzwakken van cruciale beveiligingsmaatregelen. Dit creëert een lastige situatie waarin de CISO verantwoordelijk is voor het rapporteren van risico's die niet volledig beheersbaar zijn, omdat de benodigde middelen of het mandaat ontbreekt om adequate maatregelen te nemen.

Het spanningsveld tussen verantwoordelijkheid en beheersbaarheid creëert aanzienlijke druk op CISO's. De combinatie van hoge verwachtingen, beperkte operationele controle en de voortdurende dreiging van cyberaanvallen draagt bij aan een groeiend aantal gevallen van burn-out. Uit een Gartner-onderzoek uit 2023 bleek dat 62% van de CISO's minstens één keer met burn-out te maken heeft gehad, terwijl 44% dit meerdere keren heeft ervaren. Deze cijfers benadrukken niet alleen de intensiteit van de rol, maar ook de persoonlijke tol die het kan eisen van degenen die verantwoordelijk zijn voor de bescherming van steeds complexere digitale omgevingen.

Om de effectiviteit van de CISO te vergroten, het welzijn van de persoon in deze cruciale functie te waarborgen en de rol beter te verankeren binnen de organisatie, is het essentieel om de CISO strategisch te positioneren binnen het bredere management en risicobeheer. Dit vraagt niet alleen om een duidelijke afbakening van verantwoordelijkheden, maar ook om het toewijzen van voldoende middelen en operationele ondersteuning. De CISO is dan niet alleen verantwoordelijk voor het bepalen van de strategische richting, maar beschikt ook over middelen om deze effectief te realiseren.

Een voorbeeld hiervan is dat mijn team beveiligingsrisico's heeft vertaald naar de taal van de business, zodat de business begrijpt waarom maatregelen essentieel zijn voor het succes en continuïteit van de organisatie.

Strategieën voor succes: hoe de spagaat te overbruggen

Wanneer de rol van CISO nieuw wordt ingevoerd binnen een organisatie, biedt dit zowel kansen om informatiebeveiliging strategisch te verankeren als uitdagingen in het balanceren tussen strategische verantwoordelijkheid en operationele controle. Het opbouwen van een effectieve beveiligingsfunctie begint vaak met het ontwikkelen van meerjarige roadmaps, die de lange termijndoelen en prioriteiten vaststellen. Deze roadmaps bieden duidelijke richting en helpen de strategie af te stemmen op veranderingen in technologie, processen en medewerkers.
Als eerste CISO bij Van Oord kreeg ik de unieke kans om deze cruciale functie vanaf de grond op te bouwen. Ik ontwikkelde een driejarige roadmap, waarin ieder jaar specifieke projecten werden gerealiseerd om de weerbaarheid van de organisatie te versterken. Bij elk initiatief zorgde ik ervoor dat processen, technologie en mensen nauw op elkaar afgestemd waren.
Zo maakten we niet alleen risico's beheersbaar, maar ondersteunden we ook strategische groei en continuïteit. Deze aanpak stelde ons in staat om flexibel in te spelen op zowel groeiende dreigingen als veranderende bedrijfsprioriteiten. Bovendien zorgde de jaarlijkse realisatie van nieuwe capabilities voor vertrouwen in de roadmap en versterkte het de beveiligingspositie van de organisatie.

Een veelvoorkomende valkuil in organisaties die nog in de opstartfase zitten, is dat de CISO te veel betrokken blijft bij de operationele uitvoering van beveiligingsmaatregelen. Binnen de organisatie is de functie vaak onvoldoende strategisch gepositioneerd of beschikt over te weinig operationele ondersteuning, wat leidt tot inefficiënties en de CISO belemmert om zich effectief te richten op strategische prioriteiten.

Ook in meer volwassen organisaties blijft het een uitdaging om de CISO effectief te positioneren binnen het bredere risicomanagement, vooral wanneer de functie nog sterk operationeel is. Hoewel de CISO verantwoordelijk is voor het beheren van beveiligingsrisico's, is dit slechts één onderdeel van het grotere bedrijfsrisicobeheer. Idealiter wordt de CISO geïntegreerd in de bredere corporate risk-strategie, waarin informatiebeveiliging als een cruciale pijler fungeert. Door informatiebeveiliging op deze manier strategisch te positioneren, kan het een integraal onderdeel worden van de bredere bedrijfsdoelstellingen, in plaats van een geïsoleerd proces. In de praktijk blijft de focus van corporate risk management echter vaak beperkt tot financiële risico's, waardoor de informatiebeveiligingsfunctie onvoldoende wordt benut en de CISO niet de mogelijkheid heeft om effectief te opereren op strategisch niveau. Dit creëert een gemiste kans om informatiebeveiliging volledig te integreren als een cruciaal onderdeel van het bredere risicobeheer.

Om deze balans tussen strategische verantwoordelijkheid en operationele controle te realiseren, is het cruciaal dat bestuurders en directie actief samenwerken met de CISO om diens rol duidelijk te definiëren binnen de tweede lijn van risicobeheer. Voor CISO's is het van groot belang om proactief het gesprek aan te gaan met de directie om hun strategische positie te versterken, zodat hun rol niet alleen operationeel blijft, maar actief bijdraagt aan de algemene bedrijfsdoelstellingen.

Het creëren van een helder risico en control framework helpt om rollen en verantwoordelijkheden af te bakenen, waardoor de CISO het overzicht behoudt zonder vast te lopen in operationele details.

Bovendien is het essentieel dat de CISO verandert van een top-down controlerende functie naar een vraaggestuurde rol. Een vraaggestuurde aanpak houdt in dat beveiligingsinitiatieven worden afgestemd op de strategische prioriteiten van de organisatie en niet slechts worden opgelegd vanuit compliance-oogpunt. Dit versterkt de samenwerking tussen de beveiligingsfunctie en de business, waardoor beveiligingsmaatregelen beter aansluiten op de operationele behoeften van de organisatie.

Mijn team heeft van mij de opdracht gekregen om samen met de bedrijfsonderdelen verschillende informatiebeveiligingsdiensten te ontwikkelen die inspelen op hun specifieke behoefte. Deze benadering stimuleert een cultuur van waardecreatie, waarbij het CISO-team zich richt op het leveren van beveiligingsdiensten die bijdragen aan bedrijfscontinuïteit en winstgevende groei. Door duidelijke performance indicatoren te hanteren, zoals KPI's en SLA's, maken we de impact en waarde van onze diensten transparant en meetbaar. Dit klantgerichte model zorgt ervoor dat beveiligingsoplossingen relevant zijn voor de business en breed worden geaccepteerd. Het vermindert weerstand omdat de oplossingen zijn afgestemd op de strategische doelen van de organisatie en bijdragen aan de algehele bedrijfscontinuïteit. Hierdoor wordt beveiliging niet langer gezien als een kostenpost, maar als een strategisch voordeel. Dit stelt een CISO in staat om zich te positioneren als een onmisbare, strategische partner voor de directie.

Door deze strategische en vraaggestuurde aanpak versterkt de CISO niet alleen de controle over informatiebeveiliging, maar creëert hij ook een gezonde balans tussen verantwoordelijkheid en beheersbaarheid. Dit leidt tot een effectiever risicobeheer en draagt direct bij aan het behalen van bedrijfsdoelstellingen. Bovendien vergroot deze benadering de veerkracht van de organisatie, terwijl de persoonlijke druk op de CISO en het team wordt verminderd, wat bijdraagt aan een duurzamere en productieve werkomgeving.

De weg van verandering

Het succesvol implementeren van beveiligingsinitiatieven vraagt niet alleen om technische expertise, maar vooral om het vermogen om de directie en het senior management mee te nemen in het strategische belang van informatiebeveiliging. In veel organisaties wordt beveiliging nog te vaak gezien als een kostenpost of een operationele kwestie. De uitdaging voor de CISO is om dit gesprek te verschuiven naar de strategische waarde die beveiliging biedt op het gebied van bedrijfscontinuïteit, groei en concurrentiekracht; en daarmee de spagaat tussen operationele verantwoordelijkheden en strategische doelstellingen te overbruggen.

Wanneer de directie terughoudend is of onvoldoende zicht heeft op de kansen en risico's van informatiebeveiliging, kan educatie een krachtig middel zijn om bewustwording te vergroten. Het aanbieden van gerichte trainingen en workshops helpt om de impact van beveiliging op de bredere bedrijfsstrategie te verduidelijken. Wet- en regelgeving zoals Network and Information Security (NIS2)-richtlijn of de Artificial Intelligence (AI) Act bieden concrete ingangen om het gesprek aan te gaan. De nadruk moet liggen op de strategische implicaties van niet-naleving, zoals reputatieschade of verlies van marktaandeel. Voor multinationals is het daarbij essentieel om ook wetgeving buiten de EU in acht te nemen. De CISO speelt hier een sleutelrol door aan te geven wanneer de beveiligingsmaatregelen toereikend zijn en verdere stappen geen toegevoegde waarde meer bieden.

Het opbouwen van sterke samenwerkingsverbanden binnen de organisatie is eveneens cruciaal. Door samen te werken met afdelingen zoals compliance, legal en interne audit, kan de CISO ervoor zorgen dat informatiebeveiliging niet wordt gezien als een geïsoleerd IT-probleem, maar als een integraal onderdeel van het bredere risicomanagement en de governance-structuur van de organisatie. Dit versterkt de positionering van beveiliging op de strategische agenda en helpt de CISO om de spagaat tussen operationele betrokkenheid en strategische verantwoordelijkheid effectief te beheersen.

Het is daarnaast essentieel om beveiligingsdoelstellingen op een manier te presenteren die directie en senior management aanspreekt. In plaats van zich te richten op technische risico's en potentiële dreigingen, kan de CISO beter benadrukken hoe een robuuste beveiligingsstrategie bijdraagt aan de veerkracht en continuïteit van de organisatie. Dit helpt om beveiliging te positioneren als een strategisch voordeel in plaats van een verplichting. Tegelijkertijd blijft het belangrijk om in wederzijds vertrouwen met de directie te bepalen wanneer de beveiliging "goed genoeg" is om de risico's beheersbaar te houden zonder onnodige druk op operationele processen en budgetten.

Door educatie, samenwerking en strategische communicatie kan de CISO niet alleen informatiebeveiliging steviger verankeren binnen de organisatie, maar ook zichzelf positioneren als een betrouwbare strategische partner die directie en management ondersteunt bij het realiseren van bredere bedrijfsdoelstellingen. De CISO fungeert daarbij als een belangrijke adviseur en toezichthouder die de organisatie helpt risico's effectief te beheersen en zich voor te bereiden op toekomstige uitdagingen.

Als u dit artikel leest in uw rol als CISO en worstelt met het vinden van de juiste balans tussen operationele controle en strategische doelen, onthoud dan dat uw verantwoordelijkheid verder reikt dan het managen van beveiligingsmaatregelen. Uw waarde ligt in het vermogen om beveiliging te positioneren als een strategisch voordeel, dat direct bijdraagt aan de bredere bedrijfsdoelstellingen. Werk nauw samen met de directie, spreek hun taal, en gebruik regelgeving zoals NIS2 niet alleen om te voldoen aan de eisen, maar om uw organisatie sterker en veerkrachtiger te maken. Uiteindelijk wordt succes bepaald door uw capaciteit om beveiliging naadloos te verbinden met groei en continuïteit – en zo uw organisatie naar een hoger niveau te tillen.

Referentie

(1) https://www.gartner.com/en/articles/cybersecurity-leaders-are-burned-out-here-s-why

Auteurs: Marcel Spruit is Lector Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool in Den Haag. Hij is te bereiken via m.e.m.spruit@hhs.nl. Céline Kreffer was ten tijde van het onderzoek waarop deze publicatie is gebaseerd Onderzoeker Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool. Nu is zij Analist Bestuurlijke Informatie bij het Ministerie van Justitie en Veiligheid in Den Haag. Zij is bereikbaar via https://www.linkedin.com/in/céline-kreffer-71170212a/.

Informatie(on)veilig gedrag van medewerkers

Mensen maken fouten, ook ten aanzien van de informatieveiligheid. Om deze fouten aan te kunnen pakken is inzicht in menselijk gedrag nodig. Dit vraagt om een praktisch en wetenschappelijk gefundeerd gedragsverklarend model. Die modellen zijn gangbaar in de informatiebeveiligingswereld, maar hebben zo hun beperkingen. Daarom presenteren we hier een alternatief.

Mensen maken fouten en veroorzaken daarmee incidenten, ook met betrekking tot digitale data. In een organisatie hebben medewerkers zowel een negatieve als een positieve invloed op de informatieveiligheid, doordat zij enerzijds fouten kunnen maken en anderzijds oplossingen kunnen bedenken en uitvoeren die risico's voorkomen of beperken. Het is nuttig om vooral de negatieve impact te beperken door het aantal en de ernst van fouten te verminderen. Daarvoor is inzicht nodig in het gedrag van medewerkers en de mechanismes die leiden tot fouten. Het is weliswaar onmogelijk om bij medewerkers fouten ten aanzien van de informatieveiligheid helemaal te voorkomen, maar het terugbrengen van het aantal incidenten door fouten is niet te veel gevraagd. Inzicht in gedrag en gemaakte fouten kan ook aantonen dat veel fouten van medewerkers eigenlijk voortkomen uit organisatorische problemen. Zo maakt bijvoorbeeld een onervaren medewerker zonder goede begeleiding fouten die voorkomen hadden kunnen worden door wel goede begeleiding te geven.

Modellen

In de afgelopen decennia zijn heel wat modellen voorgesteld om menselijk gedrag te verklaren, of zijn oude modellen afgestoft. Enkele bekende modellen die in de informatiebeveiligingswereld worden gebruikt zijn Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Knowledge-Attitude-Behaviour (KAB), Capability Opportunity Motivation - Behaviour (COM-B) en Theory of Situation Awareness (TSA). De grootste gemene deler van deze modellen is dat ze nogal hoog over gaan en/of zich maar op een deel van de relevante gedragsbeïnvloedende factoren richten (1). Daardoor kunnen ze een onvolledige verklaring van informatieveilig gedrag geven. Een relatief uitgebreid model is in 2000 in een whitepaper gepubliceerd (2) en opgenomen in het boek Informatiebeveiliging onder controle (3), maar dat model is voor veel mensen te veel van het goede. Er is dan ook behoefte aan een handzaam, maar wel wetenschappelijk gefundeerd gedragsverklarend model dat alle belangrijke gedragsbeïnvloedende factoren bevat.

Met een gedragsverklarende model in de hand kunnen we niet alleen fouten in informatieveilig gedrag van medewerkers verklaren, maar ook organisatiefouten

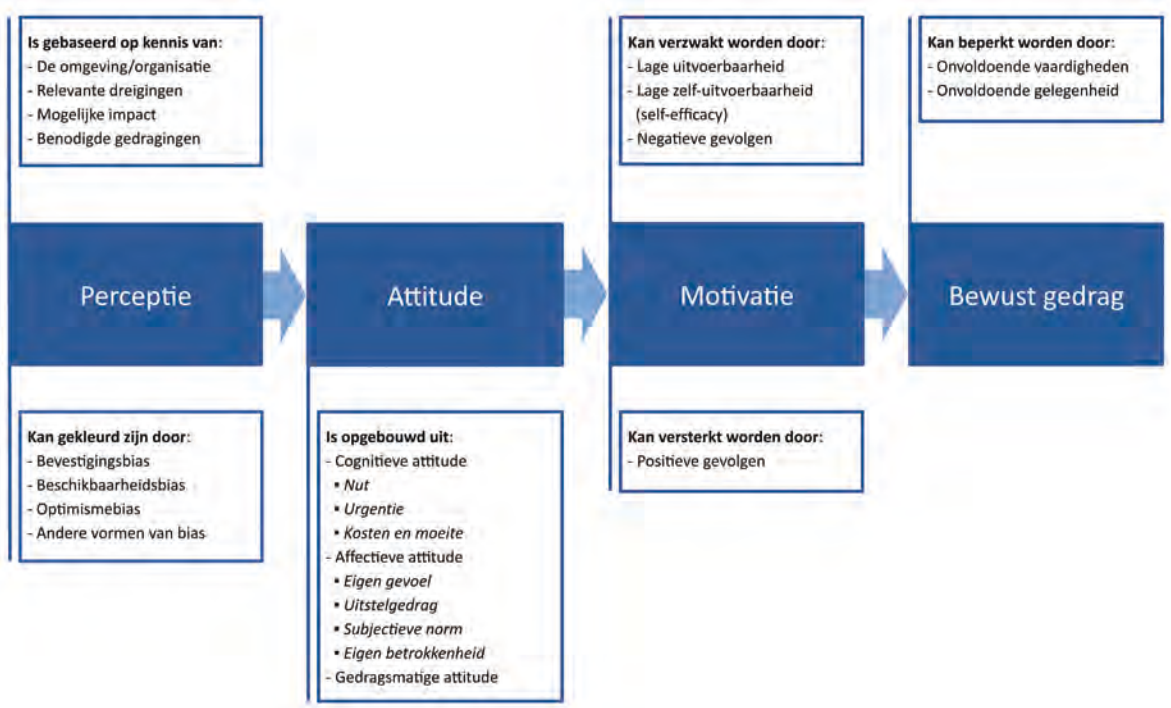
In een organisatie bestaat informatieveilig gedrag van een medewerker uit gedragingen die de betreffende medewerker onbewust of bewust uitvoert (3, 4, 5). Het onbewuste informatieveilig gedrag stoelt op automatismen en wordt bepaald door de omgeving, oftewel de organisatie. Fouten in het onbewuste gedrag moeten dan ook worden aangepakt door de organisatie zodanig aan te passen dat deze fouten niet meer worden gemaakt.
Het bewuste informatieveilig gedrag is gedrag waarvan de medewerker zich bewust is (3). Hieronder valt ook gedrag dat de medewerker uit onwetendheid, onoplettendheid, slordigheid, of nalatigheid uitvoert, waardoor de betreffende medewerker zonder opzet, oftewel per ongeluk, fouten maakt. Daarnaast kan de medewerker ook opzettelijk fouten maken, oftewel de regels overtreden. Dit kan de medewerker te goeder trouw doen, bijvoorbeeld in een uitzonderingssituatie waarin de regels niet voorzien zijn of te kwader trouw, bijvoorbeeld uit rancune. Het aanpakken van fouten in het bewuste informatieveilig gedrag is een complexe zaak. In deze paragraaf gaan we daarom in op het verklaren van het bewuste informatieveilig gedrag (1). Dit heeft betrekking op enerzijds het uitvoeren van handelingen ten aanzien van informatieveiligheid, bijvoorbeeld het afwijzen van cookies die niet nodig zijn en anderzijds het uitvoeren van informatiebeveiligingsmaatregelen, bijvoorbeeld door het gebruik van sterke wachtwoorden. Vanuit zichzelf doen veel mensen dit nog onvoldoende (6).

Gedrag

De belangrijkste voorspeller van bewust informatieveilig gedrag bij een medewerker is de motivatie, oftewel de intentie, om dit gedrag daadwerkelijk uit te voeren. Vanzelfsprekend moet de medewerker dan wel de benodigde vaardigheden bezitten. Verder mag de organisatie het informatieveilig gedrag niet te lastig of zelfs onmogelijk maken of anders gezegd, de organisatie moet de persoon wel de gelegenheid bieden om informatieveilig gedrag uit te voeren.

Een belangrijke invloedsfactor op de motivatie van de medewerker voor informatieveilig gedrag is diens perceptie (7). De perceptie is het beeld dat de medewerker in kwestie heeft van de betreffende situatie. Dit beeld steunt in belangrijke mate op kennis van de omgeving/organisatie, de relevante dreigingen, de mogelijke impact ervan en de benodigde gedragingen. Wanneer deze kennis bij medewerkers niet in voldoende mate aanwezig is, dan kunnen ze de risico's van de situatie niet goed inschatten en weten ze niet welk informatieveilig gedrag van hun wordt gevraagd.

Maar het blijft niet bij kennis alleen. De perceptie van de medewerker kan namelijk vertekend zijn door bias (8). Hiervoor zijn meerdere oorzaken, maar voor informatieveilig gedrag lijken vooral de bevestigingsbias, de beschikbaarheidsbias en de optimismebias van belang. De bevestigingsbias ontstaat doordat mensen de neiging hebben om vooral de risico's te zien die ze verwachten te zien of die aansluiten bij hun mening. De beschikbaarheidsbias ontstaat doordat mensen risico's overschatten van dreigingen waarover ze veel gehoord of gelezen hebben en ze onderschatten risico's van dreigingen die ze niet goed kennen. De optimismebias ontstaat doordat mensen hun eigen kennis en vaardigheden overschatten en de risico's ten aanzien van hunzelf en hun organisatie onderschatten.
Zelfs als de medewerker een juiste perceptie van de situatie heeft, dan betekent dat niet per se dat de medewerker ook positief staat tegenover het voor die situatie benodigde informatieveilig gedrag. De medewerker weet dan weliswaar op basis van de perceptie welk gedrag nodig is,



Figuur 1: Gedragsmodel met de factoren die van invloed zijn op het bewuste informatieveilig gedrag van medewerkers (1).

maar vindt toch dat hij of zij ervan af kan of moet wijken. In dit geval is de attitude, oftewel de houding of mening, ten aanzien van het benodigde gedrag afwijzend. De attitude is opgebouwd uit drie componenten: cognitieve attitude, affectieve attitude en gedragsmatige attitude (9). Ieder van deze componenten kan positief of negatief zijn en zo de motivatie positief of negatief beïnvloeden.

De cognitieve attitude is een rationele attitude. Het is gebaseerd op de mate waarin de medewerker enerzijds vindt dat het beoogde gedrag nuttig (effectief en proportioneel) en urgent is en anderzijds vindt dat er geen onredelijke kosten en moeite voor worden gevraagd.

De affectieve attitude is een gevoelsmatige attitude. Het is gebaseerd op een combinatie van gevoelsmatige aspecten:

1) het eigen gevoel ten aanzien van het benodigde gedrag, bijvoorbeeld de angst om gehackt te worden;
2) het uitstelgedrag, vooral als het activiteiten betreft waar de medewerker niet blij van wordt;
3) de subjectieve norm, oftewel de druk die de medewerker voelt om zich te conformeren aan wat hij of zij denkt dat anderen wenselijk vinden, met name als dit gerelateerd is aan belangrijke groepen zoals relevante peer-groepen, belangrijke personen of influencers;
4) de eigen betrokkenheid, bijvoorbeeld als de medewerker heeft geparticipeerd in het formuleren van veilige gedragingen.

De gedragsmatige attitude richt zich op het afstemmen van de eigen mening op het eigen gedrag, om de verschillen ertussen glad te strijken. In het kader van dit artikel is deze component minder van belang, omdat deze component vooral uit gedrag volgt en veel minder de oorzaak van gedrag is. Als de medewerker een goede perceptie van de situatie heeft en een positieve attitude ten aanzien van het benodigde informatieveilig gedrag, dan heeft dat een positief effect op de motivatie voor dat gedrag. Maar dan moet de medewerker wel vinden dat het betreffende gedrag uitvoerbaar is, ook door haar- of hem zelf (self-efficacy) (10).

Verder kunnen positieve gevolgen vanuit de organisatie, zoals complimenten of beloningen, de motivatie voor het

benodigde gedrag versterken. Anderzijds kunnen negatieve gevolgen vanuit de organisatie, zoals straffen, de motivatie juist verzwakken. De hierboven beschreven factoren die het bewuste informatieveilig gedrag van een medewerker beïnvloeden, zijn geresumeerd in figuur 1.

Toepassing van het model

Op basis van het hierboven beschreven model kunnen we voor een organisatie de stappen aangeven die nodig zijn om het informatieveilig gedrag van medewerkers te verbeteren. Uit het model blijkt dat de perceptie van een medewerker invloed heeft op diens attitude, die weer invloed heeft op diens motivatie, die weer invloed heeft op diens bewuste gedrag. Diezelfde logica moeten we dan ook terugzien in de aanpak van fouten in het bewuste gedrag. Dus de perceptie zo nodig aanpassen zodat de attitude optimaal afgestemd is op de situatie. Vervolgens de attitude aanpassen zodat de motivatie optimaal gebruik kan maken van de positieve insteek van de medewerker. En dat leidt dan tot het gewenste gedrag van de medewerker, mits de medewerker de benodigde vaardigheden heeft en de organisatie zodanig meewerkt dat het benodigde informatieveilig gedrag ook goed uitgevoerd kan worden.

Toch laat de praktijk zien dat er in veel organisaties wel erg makkelijk vanuit wordt gegaan dat alle geconstateerde fouten worden veroorzaakt door incapabele medewerkers, die hoognodig een bewustwordingscampagne moeten krijgen. Vaak is dit uitgangspunt onjuist en bovendien doet het geen recht aan de variatie van mensen en functies binnen de organisatie. Daarom is het goed om eerst de geconstateerde fouten in het informatieveilig gedrag van de medewerkers te analyseren en de oorzaken te achterhalen.

Uit analyse van geconstateerde gedragsfouten blijkt dat het merendeel van de gedragsfouten van medewerkers wordt veroorzaakt door organisatiefouten. De organisatiefouten kunnen het gedrag van medewerkers ongunstig beïnvloeden door in te grijpen op de factoren die van invloed zijn op het bewuste informatieveilig gedrag van medewerkers, zie figuur 1.

Veelvoorkomende voorbeelden van organisatiefouten zijn:

- Er is geen adequaat informatiebeveiligingsbeleid of dit beleid is niet goed gecommuniceerd naar of uitgelegd aan de medewerkers. Dit heeft bij de medewerkers een negatieve invloed op de kennis van relevante dreigingen, mogelijke impact en relevante gedragingen. Van de medewerkers kan dan niet worden verwacht dat ze een goed beeld hebben van wat er qua informatieveilig gedrag van hun wordt gevraagd.
- Het hoger management geeft qua informatieveilig gedrag zelf niet het goede voorbeeld. Dit heeft bij de medewerkers een negatieve invloed op de mening over de urgentie van het gevraagde gedrag. De medewerkers veronderstellen dan dat het beoogde informatieveilig gedrag ook voor hun niet noodzakelijkerwijs nodig is en laten dit achterwege.
- Informatiebeveiligingsmaatregelen zijn ondoordacht, onsamenhangend, of te belastend voor de medewerkers, bijvoorbeeld niet actueel of ingevoerd zonder rekening te houden met de eigenaardigheden van de organisatie. Dit heeft bij de medewerkers een negatieve invloed op de mening over het nut van de maatregelen. De medewerkers verzinnen dan veelal workarounds.
- Informatiebeveiligingsmaatregelen zijn onvoldoende geïntegreerd in de organisatieprocessen. Voor de medewerkers komen de inspanningen voor informatiebeveiliging dan bovenop hun 'gewone' werk. Dit heeft bij de medewerkers een negatieve invloed op de mening over de redelijkheid van de benodigde kosten en moeite. De medewerkers omzeilen dan bij voorkeur de betreffende maatregelen.

Organisatiefouten eerst aanpakken

Een prettige bijkomstigheid van het aanpakken van organisatiefouten is dat hiermee in één moeite ook de oorzaken van fouten in het onbewuste informatieveilig gedrag kunnen worden aanpakt. Dat is dus nog een reden om te beginnen met het aanpakken van de organisatiefouten.

Als ná het oplossen van de organisatiefouten uit verdere

Figuur 2: Stappen in de aanpak van fouten in informatieveilig gedrag van medewerkers.

analyse van de geconstateerde fouten blijkt dat er toch nog het een en ander schort aan het informatieveilig gedrag van bepaalde groepen medewerkers, dan kan het nodig zijn om bij die medewerkers de gevonden lacunes in perceptie, attitude en/of vaardigheden aan te pakken. Dit moet dan wel doelgericht worden opgepakt bij de medewerkers die het betreft en niet bij de andere medewerkers. Organisatiebrede maatregelen, zoals postercampagnes of verplichte multiplechoicetests, hebben in het algemeen geen noemenswaardig positief effect. Figuur 2 resumeert de stappen waarmee het informatieveilig gedrag van medewerkers verbeterd kan worden.

Conclusie

Medewerkers in organisaties maken fouten en veroorzaken zo incidenten, ook met betrekking tot al dan niet digitale data. Voor het aanpakken van deze fouten is inzicht nodig in het informatieveilig gedrag van medewerkers en daarvoor is een geschikt gedragsverklarend model nodig. De gedragsverklarende modellen die in de informatiebeveiligingswereld gangbaar zijn, hebben zo hun beperkingen. Daarom hebben we in dit artikel een alternatief model gepresenteerd, zie figuur 1.

Met dit gedragsverklarende model in de hand kunnen we niet alleen fouten in informatieveilig gedrag van medewerkers verklaren, maar ook organisatiefouten. Voor het aanpakken van fouten in het informatieveilig gedrag van medewerkers kan een stapsgewijze aanpak worden gevolgd, zie figuur 2. De aanpak begint bij het vinden en oplossen van organisatiefouten, omdat daarmee al een flink deel van de fouten in het bewuste en onbewuste informatieveilig gedrag opgelost kan worden.

Referenties

(1) Spruit, M., Oosting, D. & Kreffer, C. (2023). Factors that influence secure behaviour while using mobile digital devices. Information and Computer Security. https://doi.org/10.1108/ICS-02-2024-0035.
(2) Spruit, M. (2000). Human Error and Information Security. Whitepaper, Technische Universiteit Delft, Delft.
(3) Van Houten, P., Spruit, M., & Wolters, K. (2023). Informatiebeveiliging onder controle. Pearson.
(4) Bernstein, D. A. (2016). Psychology. Cengage Learning.
(5) Robbins, S. P., & Judge, T. A. (2019). Organizational Behavior. Pearson.
(6) Cybersecurity monitor 2021. CBS.
(7) Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37(1), 32-64.
(8) Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.
(9) Ostrom, T. M. (1969). The Relationship between the Affective, Behavioral and Cognitive Components of Attitude. Journal of Experimental Social Psychology, 5(1), 12-30.
(10) Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191-215.


AI

INTERVIEW

AI bij Enovation: nieuwsgierig en voorzichtig, met de mens in de beslisboom

De inzet van AI bij Enovation groeit, maar blijft gericht op zorgvuldige toepassing en gecontroleerde omgevingen. Bertine Uithoven en Arjan van der Beek van Enovation bespreken hoe AI de kwaliteit van processen in de zorg kan verhogen, maar benadrukken dat volledige automatisering niet de enige oplossing is. De focus ligt op backend- en frontend-functionaliteiten, waarbij AI als hulpmiddel dient voor efficiëntie zonder in te boeten op menselijke betrokkenheid en dataveiligheid. Hun visie: AI kan bijdragen aan de zorg, mits gedoseerd, transparant en met aandacht voor de gebruiker.

Waar ligt de focus op AI bij jullie?

Arjan: "Enovation was oorspronkelijk gericht op backend-processen, maar in de afgelopen jaren kwamen er steeds meer producten met frontend-functionaliteiten bij. In frontend-applicaties kun je de gebruiker hints geven door middel van AI, zoals: 'Let op, ik merk iets op…,' wat de proces- en eindkwaliteit ten goede komt. Deze ontwikkeling maakt ons zeker nieuwsgierig. In de markt zien we voorbeelden van vergaande automatisering van achtergrondprocessen. Daar zijn we echter nog terughoudend in; eerst willen wij de technische belemmeringen goed begrijpen. De AI-hype leidt tot grote investeringen en ontwikkeling, maar zodra obstakels opduiken, kunnen deze processen vastlopen. In het verleden is de ontwikkeling van AI vaker voor langere tijd gestagneerd, een zogenaamde 'AI-winter'. Dit maakt ons behoedzaam: we zijn nieuwsgierig en voorzichtig. Als je begint met AI, voelt het als een grote stap om backend-processen te automatiseren. Wij benadrukken dat er altijd een mens in de beslisboom betrokken moet zijn ('human in the loop')."

Bertine: "We laten tooling binnen een strikt veilige en privacy bewuste omgeving draaien en niet via internet. Dus eigen interne ervaring versus openbaar, want dat compliceert het gehele proces. De evaluatie van de tooling doorlopen wij samen met ons security office. Wij zien als voorwaarden, dat AI goed getraind moet zijn, data beschikbaar is, duidelijk is waar AI plaatsvindt, privacy goed in acht genomen is en hoe goed het lerend vermogen is? Dat zien wij als een gradueel proces."

Enovation verbindt dus de AI-inspanning aan een gecontroleerde omgeving en de koppeling tussen AI en de techniek in huis?

Bertine: "Punt een klopt, punt twee is de logische consequentie van het eerste. Daarbij wil ik benadrukken dat backend- en frontend-applicaties voor ons niet hetzelfde zijn als interne versus externe gerichtheid. AI kan voor beide worden toegepast. Wij starten met product development binnen een gecontroleerde omgeving, dus buiten de cloud. Om vervolgens (Bertine: "Dit is de kwaliteit van Arjan") andere afdelingen daarbij te betrekken."

Arjan: "Waar het gaat om details zitten wij met producten veelal op koppelvlakniveau. AI is nog niet sterk in details, wel in het generatieve gedeelte. Een vraag als: 'Hier heb je het koppelvlak met leverancier X en daar het koppelvlak met leverancier Y, maak hiervan een perfecte koppeling', is een lastige vraag voor AI. Wij kijken vanuit eigen problematieken, uitdagingen en vraagstukken naar de bijpassende oplossingen."

Bertine: "Een belangrijke trend is databeschikbaarheid. De basis voor deze ontwikkeling zijn de Europese normeringen en de positie van regio's. Die organiseren zich en komen tot onder andere CumuluZ-data (dat is data verzameld, gestapeld en gedeeld in silo's, die te ontsluiten moeten zijn voor de verschillende 'usecases' en zorgaanbieders). Daar zou AI een belangrijke rol in kunnen spelen. Het VWS houdt zich hier onder andere mee bezig: hoe kunnen wij onder meer AI in de zorg toepassen?! Zie de VWS-website (1). Aan alle kanten is er beweging en onderzoekt men of en hoe met elkaar daarin slagen te maken zijn."

Waar staat Enovation qua niveau in de data-waardeketen? (2)

Bertine: "Wij beschikken niet over veel data. Als 'man-in-the-middle' leven wij bij gratie van de gerealiseerde connecties met externe partijen. Veel zal in afstemming met onze relaties tot stand moeten komen. Dat bepaalt de complexiteit en de beschikbaarheid over databronnen. Oppervlakkig gezien is dat simpel, in werkelijkheid altijd een samenspel van actoren. Men waakt voor zwakke schakels. Enovation wil een veilig ecosysteem leveren. Het realiseren van een nieuw component in de 'pipeline', creëert evenwel een nieuw aanvalsvlak. Dat overdenken wij goed en vooralsnog is onze mening dat wij nu geen grote stappen zetten."

"Het toevoegen in de keten van AI-oplossingen is pas de laatste stap. Onze weg is: eerst intern, dan de gecontroleerde omgeving met één van onze producten en pas dan de keten. Dit pad kunnen wij verantwoorden. Het beleid is gecentreerd op: security, privacy, databeschikbaarheid, garanties en certificering. Dat is ons dagelijks bestaan: bescherming van de klantdata en dat is al meer dan veertig jaar ons bestaansrecht. Berekenend en afwegend opereren dus."

Als je kijkt naar de bedrijfslijn, is jullie AI-benadering strategisch georiënteerd?

Bertine: "Ja, dat klopt. De innovatiesnelheid is zo hoog dat dit niet eenvoudig bij te houden is. We moeten rekening houden met richtlijnen, registraties en standaardisatie. De zorg heeft te maken met steeds minder handen aan het bed en met meer kennisvereisten en hogere kosten. Meer efficiëntie moet, om de mens niet de belemmerende factor te laten zijn."

"Tijdens een samenwerking bij mijn vorige werkgever met het Nederlands Huisartsen Genootschap (NHG) en een derde partij, werd een model ontwikkeld waarmee opgedane wetenschappelijke kennis gegoten kon worden in een beslissingsondersteunende applicatie, bijvoorbeeld voor medicatiedosering, de substitutie van een medicament en/of een behandelplanaanpassing. Die innovatie vertaalde zich in een informatieve persoonsgerichte 'pop-up' op het computerscherm. Huisartsen reageerden daar in eerste instantie terughoudend op; zij zijn gewend om zelf de besluiten te nemen en de applicatie zou hen dat uit handen nemen. Gaandeweg omarmden ze de applicatie. Deze app was een voorloper van op AI-gebaseerde richtlijnen."

"Wij benaderen AI vanuit de beschikbare middelen en de regels, die stellen we vast voordat we AI testen en in productienemen. Wat wij inachtnemen, zoals: privacy (de notie van (persoonlijke) 'verantwoordelijkheid' en hoe wij de gedragsregels aanleren is intern vooral van grote waarde. Een onderwerp dat vooral bij Arjan ligt. Wij doen een stapje terug en vinden het belangrijk stil te staan bij deze nieuwe ontwikkeling."

Arjan: "Ik ga uit van de conceptgedragscode waarin één van de belangrijkste slogans luidt: nieuwsgierig en voorzichtig. Wat gaat of kan AI ons brengen? Wij zijn ons ook bewust van de AI-hypes. Wij kijken eerst intern wat AI ons kan brengen, waar AI sterk dan wel zwak in is. Ons pad ontwikkelt zich dan (of niet) op basis van ervaringen en gewonnen vertrouwen."

"Bij de realisatie van de gedragscode betrekken wij collega's. We moeten innoverend zijn, maar we moeten ook op de rem kunnen trappen als dat nodig is."

Waar zien jullie verbeteringskansen?

Arjan: "Welke efficiëntie en nieuwe risico's brengt AI met zich mee? Ik heb slechts één wetenschappelijk onderbouwd onderzoek gevonden met een uitspraak over de waarde van bijvoorbeeld een applicatie als Copilot. De bottomline van het rapport: het is moeilijk bepaalbaar of er een significant

McKinsey rapport: 75% van AI-resultaten bepaald door			
Proces		**Wereldwijde functionele bestedingsimpact**	**Detaillering**
1	zorg bij engineering voor de corporate-IT	31%	
2	zorg bij engineering voor product development	32%	
3	customer operations	38%	Sales Services: resolution during initial contacts, verkorte responstijden en toegenomen verkoopkansen
4	marketing	10%	Effectiviteit van content creation en efficiëntie
5	product, research and development	12%	
6	sales	4%	
Investeringsbedragen variërend van € 320 mrd tot € 490 mrd			

Overzicht 3 uit het McKinsey rapport (3).

efficiëntievoordeel wordt behaald dan wel van vermeende efficiëntie. Waar zit de hype en waar de efficiëntiewinst?"
Bertine: "Mee eens. De behoefte om te versnellen bestaat, men wil stappen zetten. Het gaat echter om gevoelige data waar wij vooral de transportpartij zijn en veelal níet de eigenaar, dus voorzichtigheid is vereist. Niet onze bronnen, maar data zijn onderdeel van ons systeem. Data-interpretatie zonder benutting van de bron is riskant. Niettemin, de roep vanuit de zorg om efficiëntieslagen te maken, is groot. Daar werken wij aan mee; lucht scheiden van de 'common ground' en bepalen wat bruikbaar is."
"Enovation is een grote partij en verantwoordelijk voor het veilig uitwisselen van data van gewone én bijzondere persoonsgegevens. Die laatste bevatten een hoog risicofactor. Wij zetten weloverwogen stappen en vragen daar intern continue aandacht voor. Dat doen wij explorerend, niet forcerend, en rekening houdend met mogelijkheden en beperkingen die passend zijn bij ons bedrijf."
"De zorgsector ondervindt een sterke toename van patiënten, wat leidt tot een groei in repeterende taken van zorgverleners. Door die repeterende taken volgens vaste criteria te automatiseren, kunnen we de basisprocessen efficiënter maken. AI voegt bovendien gezondheidskundige waarde toe door herkenbare patronen te analyseren, zoals het efficiënter dispatchen van ambulances naar de Spoedeisende Hulp (SEH) of andere zorgafdelingen. Door gebruik te maken van beschikbare data en werkdrukindicatoren kan AI de druk op de SEH verlagen. Implementaties hebben aangetoond dat het wegnemen van menselijke knelpunten in deze processen de doorstroom aanzienlijk vergroot, wat mogelijk is dankzij grote hoeveelheden betrouwbare data."
McKinsey stelt dat kenniswerkers zeker twintig procent van hun tijd besteden aan het zoeken naar relevante

informatie. Herkennen jullie jezelf in de daar te behalen efficiëntiewinst?

Bertine: "De vraag raakt de juiste snaar van waar wij staan en waarvan wij de waarde zien. Artsen zeggen: 'Zie AI niet als doel, maar als middel om de administratieve processen in beeld te krijgen'. De multidisciplinaire benadering en het goed begrijpen van de gebruikerscasus (McKinsey: genAI-waarde generatie: gebruikers specifieke casussen (3)) is de weg. Dat vereist van bedrijven visionaire en realistische technici, die met veldexperts (zoals artsen) om tafel gaan." "De arts benoemt het zorginfarct, de visionair presenteert zijn oplossing, en de realistische techneut (implementatiespecialist) bekijkt wat haalbaar is. Het is belangrijk om niet alleen onderzoek te doen naar oplossingen en technieken, maar vooral ook de gebruiker te ondersteunen en naar diens feedback te luisteren. Zorg is tenslotte niet gericht op economische winst, maar op de kwaliteit van leven. Dat blijft onderbelicht. Een chirurg moet conform procedures een patiënt-dossier doornemen, maar is dit altijd haalbaar? GenAI kan helpen door een samenvatting te geven van de recente ontwikkelingen rondom een patiënt, bijvoorbeeld wanneer je vraagt: 'Vat de belangrijkste gebeurtenissen samen van de afgelopen periode van persoon x'. Als GenAI in tien regels de hoofdlijnen kan weergeven, zou dit volgens artsen de kwaliteit van zorg aanzienlijk kunnen verbeteren, aldus reacties aan Arjan."

De nadruk ligt bij Enovation op research & development, maar is er ook een rol voor de supply chain?

Arjan: "Onze leerprocesinvesteringen kunnen we zeker vermarkten gezien het belang om de processen in de gezondheidssector te verbeteren. Nu we intern zijn opgestart en R&D hebben geëvalueerd, zijn wij beter in staat de voors en tegens met onze klanten en leveranciers te bespreken. We vertalen onze kennis naar consultancy over klant- en leverancierssprocessen, met mogelijkheden voor verbetering. Bij gebleken behoefte kan Enovation mee ontwikkelen."

Bertine: "Ten opzichte van vier, vijf jaar geleden staan wij op een andere positie. Wij waren de 'man-in-the-middle' en nu denken wij aan AI-oplossingen. Eerst interne realisatie, en dan via deze producten met de daarbij behorende klanten, nieuwe wegen inslaan. Het ligt logischer in de lijn die stappen nu te zetten in vergelijking met vijf jaar terug. De kennis is in huis, vroeger moesten wij van klanten veelal medewerking verkrijgen."

Creëren jullie later meta-data ten behoeve van overheidsbeleid en zorginstellingen?

Bertine: "Boeiende vraag. Het ligt niet in de aard van Enovation, maar tegelijkertijd sluit het dit ook niet uit."

Arjan: "Wij zijn heel dienstbaar, maar deze 'out of the box' gedachte past op dit moment niet in het beeld van Enovation. Als wij deze richting zouden uitgaan, dan moeten er aanvullende maatregelen tot stand komen. De vraag rijst of dit passend is voor ons. Wat Enovation niet wil zijn of worden is een 'Jack of all trades and a master of none' door te veel zaken naar ons toe te trekken zonder ons daarop te kunnen of willen specialiseren, zonder passende kennis of mentaliteit in huis te hebben en zonder een bepaalde 'change' of transformatievlak zoals een Denkwijzer."

Ter afsluiting, hebben jullie een boodschap voor jullie markt en onze lezers?

Arjan: "De gedachte vanuit nieuwsgierig en voorzichtig. Het zou mooi zijn als het verklaarbare AI zou worden in tegenstelling tot de zwarte-doos-AI, dat het nu te vaak is."

Bertine: "Ik sluit mij volledig aan bij Arjan."

Bertine Uithoven begon 7,5 jaar geleden bij Enovation als Product Manager ZorgMail en sinds 2,5 jaar is zij Portfolio Lead voor tevens vier andere producten in de gestructureerde gegevensuitwisseling, databeschikbaarheid en veilige mail. Mijn taak is vooral praktisch: organiseren en mensen meenemen naar de gewenste oplossingen; inhoudelijk en faciliterend. bertine.uithoven@enovation-group.com.

Arjan van der Beek kwam bij Enovation terecht na een overname. Hij is verantwoordelijk voor Product, Process and Quality en werkt op het snijvlak van techniek en zorg. Arjan was veertien jaar actief voor de Universele Meldbank Ontvanger (UMO), de oplossing voor zorgcentrales voor persoonsalarmering, telemonitoring en mobiele opvolging. Hij deed onderzoek naar de betekenis van AI, het risico bewustwordingsproces en de schaduwzijden daarvan. Universeel in de zin van merk-agnostisch. arjan.vanderbeek@enovationgroup.com.

Disclaimer: het interview is gebaseerd op een gesprek dat we hadden op 04.03.2024 en daarom op de kennis en technologie van dat moment. De snelle ontwikkelingen dienaangaande zouden inmiddels kunnen leiden tot nuancering.

Referenties

(1) https://bitly.cx/CCBbP Zie ook de site van het VWS: https://www.datavoorgezondheid.nl/ai

(2) Omvat o.a.: data-ontdekking, -invoer, -opslag, -beheer, -verwerking, -toegankelijkheid, -consumptie en -integratie.

(3) The economic potential of generative AI: the next productivity frontier, June 14, 2023

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Liefde is troef

"Ziek in je hoofd!", "Je douwt het door m'n strot", "Smerige pedofielen zijn jullie", "Ik heb serieus niks tegen homo/lesbies of welke naam dan ook, maar kappen nou!"

Zomaar een korte bloemlezing aan reacties die ik online krijg. En met mij vele anderen uit de LHBTI+ gemeenschap. RTL becijferde dat bij hun nieuwsberichten vrouwelijke queer personen 1 op de 5 keer dat zij actief zijn, haat terug ontvangen. Dat is 49% vaker dan bij anderen. Die onversneden haat is eng en daarenboven in extreme mate toegenomen, het maakt dat mijn eigen visie over anonimiteit, online reageren en privacy aan het schuiven gaat.

Laat me voorop stellen dat het verschuiven van de blik op privacy er ook wel een beetje bij hoort, van oorsprong gezien is het een fluïde begrip – wat wij als privacy definiëren is niet voor eens en altijd te vangen, het verandert met de tijd, de opvattingen en de cultuur mee. Voor RTL betekenen de uitkomsten van het onderzoek dat zij veel forser gaan ingrijpen – berichten verwijderen, of in het uiterste geval geen reacties toelaten.

Online anonimiteit en ook pseudo-anonimiteit hebben ontzettend belangrijke functies. Het maakt dat burgers zich kunnen uitspreken over onrecht, misstanden aan de kaak kunnen stellen en hun privéleven kunnen afschermen voor het grote publiek. En dat er grenzen zijn aan deze privacyaspecten, daarover zijn we het ook al tijden met elkaar eens. Niet alles kan of mag, zeker niet als het gaat om strafrechtelijk relevant handelen – denk aan discriminatie en haatzaaien.

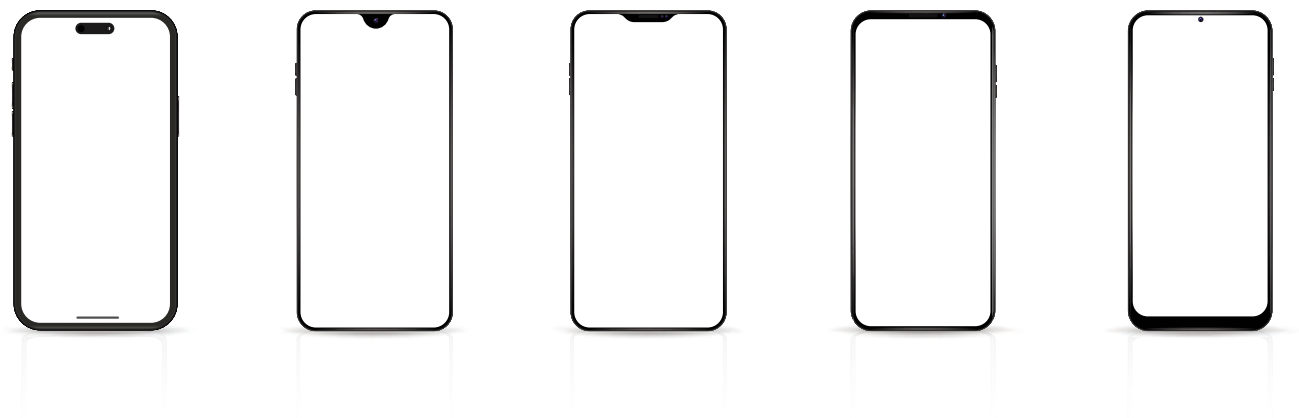
Zo'n 30 jaar geleden discussieerden we over waar het recht op privacy online ophoudt, of anonimiteit absoluut zou moeten zijn, of privacy überhaupt wel bestaat in een wereld waarin transparantie de 'default setting' is. Wellicht groener en activistischer was ik voorstander van die optie op absolute privacy door anonimiteit, maar geconfronteerd met een extreemrechtse regering en heel erg nare haatboodschappen aan mijn persoon, merk ik dat ik twijfel als ik mijn queer-zijn online laat zien. Want ik weet dat als ik de Gemeente Den Haag en onze Burgemeester dank voor hun steun aan de queer gemeenschap, dat ik berichten als bovenstaand krijg. En ik woon in Den Haag. En wie op mijn naam zoekt, vindt allerhande informatie over me. En ik heb een kind. En een kat. En die wonen ook in dat huis waar ik woon. En wat nou als ze me vinden?

Uit cijfers van de Rijksoverheid blijkt dat ongeveer zeven op de tien LHBTI+ personen in hun leven te maken krijgen met fysiek of verbaal geweld om wie ze zijn. Jaarlijks worden minder dan vijf daders voor LHBTI+ discriminatie veroordeeld. En uit recent onderzoek van de Erasmusuniversiteit blijkt dat daders bovengemiddeld vaak man zijn en bovengemiddeld vaak eerdere strafbare feiten op hun naam hebben, vergeleken met geweldplegers in het algemeen. De meeste van deze daders plegen geweld, omdat zij een afkeer hebben van LHBTI+ uitingen. Het gepercipieerde gevaar is dus niet denkbeeldig.

Toch blijf ik doorgaan met het normaliseren van niet-hetero zijn. Want ik besta en dat ga ik niet ontkennen. Maar wel iets voorzichtiger, en vooral ook met de hulp van anderen. Die vele anderen die niet LHBTI+ zijn maar nog wel in de stille anonimiteit leven. Aan hen vraag ik om uit die anonimiteit te komen, help mij en anderen door de haat online te overstemmen met liefde. Al is het maar door een hartje bij een LHBTI+ nieuwsbericht te plaatsen.

Rachel

Auteurs: Ronald Eygendaal schrijft sinds 1990 voor toonaangevende vakbladen in Nederland en België over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging. Hij is werkzaam als Advisor Information Security bij de Nederlandse Douane. Ronald is te bereiken via ronald@eygendaal.com



Bye bye Chinees, welkom Pool

Mijn privésmartphone begon de laatste tijd wat kuren te krijgen. Regelmatig kon ik het scherm niet meer bedienen en bleef de software hangen. Volgens mijn kinderen komt dit doordat pa veel opensource software en andere software 'troep' op zijn smartphone heeft. Pa, roepen ze dan, vergeet niet, het is een goedkope Chinese smartphone. Zelf hebben ze dure smartphones uit Zuid-Korea (Samsung) en Amerika (Apple), maar dat terzijde.

In de mondiale smartphonemarkt is China een heel grote speler. Het land maakt schitterende smartphones voor veel verschillende doelgroepen. Ik houd van een robuuste (ruggedized) smartphone die ook in zware omstandigheden werkt. Een smartphone die voldoet aan militaire testnormen voor bescherming tegen schokken, water, stof, extreme temperaturen en trillingen. En omdat ik soms wat onhandig ben, moet de smartphone waterbestendig zijn en een onderdompeling in water gedurende een bepaalde tijd kunnen weerstaan.

Maar Chinese smartphonemakers komen regelmatig in opspraak. Het bekendste voorbeeld is Huawei, dat sinds 2019 geen zaken meer mag doen met Amerikaanse bedrijven. De zorg over Chinese bedrijven als Huawei past in een breder beeld van het cybersecuritydreigingslandschap, dat continu in ontwikkeling is. Organisaties beveiligen hun ICT-apparaten en netwerken steeds beter tegen criminelen en statelijke actoren. Vaak bestaat deze beveiliging uit de implementatie van technische maatregelen, waardoor de actoren zich steeds meer richten op de werknemers in een organisatie. Als securityprofessional ben je daardoor ook op je privésmartphone kwetsbaar. Reden genoeg om na te denken over een Europese smartphone die aan mijn wensen en eisen voldoet.

Software of hardware probleem?

Terug naar mijn Chinese smartphone. De symptomen hebben

verdacht veel weg van een besmetting met een virus of malware. Het kan bijna niet, want alle smartphones in ons gezin zijn uitgerust met een 'F-Secure' antivirus- en internetbeveiliging en geüpdatet door KPN. Mijn Chinese smartphone is aangevuld met Hypatia, een opensource en gratis realtime malwarescanner voor Android en gebaseerd op de ClamAV-signatuur databases. Bij een virus- of malwarebesmetting had één van beide moeten piepen, maar ze blijven angstvallig stil. Als het geen virus of malware is, wat is het dan? Al jaren is mijn Chinese smartphone voorzien van RethinkDNS. Dit is een open source security-app met een firewall, die voorkomt dat apps ongeautoriseerd verbinding maken met internet. De app blokkeert spyware, malware, ransomware en meer. Ook is RethinkDNS voorzien van monitoring en houdt dus inkomend en uitgaand internetverkeer in de gaten. Daarnaast heeft RethinkDNS mogelijkheden om verdachte DNS te controleren. Maar ook de app signaleert geen verdachte zaken.
De internetverbinding dan misschien? Nu loopt mijn internetverbinding van mijn Chinese smartphone via een VPN van WireGuard over het internet naar mijn Fritz-box in het huisnetwerk en vanaf daar via KPN ADSL het internet op. Ook op deze verbinding is geen verdacht verkeer. Is dan toch de software kreupel geworden? Of Android? Of een vage app? Ik heb de Chinees teruggezet naar de fabrieksinstellingen, een verse Android 12 en de apps opnieuw geïn-stalleerd. Ook dit bracht geen soelaas... Nog maar eens wat getest en gerommeld, de apps één voor één geherïnstalleerd, getest, maar nog steeds de symptomen. Het lijkt toch op een hardwareprobleem.

Zonder bloatware of andere ongein

Dan maar een nieuwe smartphone. Een Android, maar welke smaak? Een kenmerk van Android is, dat de broncode beschikbaar is voor iedereen om te bekijken, te downloaden, aan te passen, te verbeteren en opnieuw te distribueren, zonder extra kosten of royalty's. Doordat andere programmeurs de broncode kunnen inzien, kunnen securityproblemen (vroegtijdig) worden ontdekt en verholpen, wat veiligheid biedt. Naast Android van Google zijn er andere opensource Androidplatformen zoals LineageOS, Replicant en CalyxOS. Deze platformen zijn veelal gebonden aan een beperkt aantal smartphones en soms zelfs aan één specifieke. Zoals het Android opensourceplatform Apostrophy, dat zich richt op perfecte privacy en security en alleen werkt op een smartphone van de Zwitserse fabrikant Punkt.
Dat maakt de zoektocht naar een vervanger voor de Chinees belemmerend. Dus is het selectiecriterium: Android van Google. Zijn we er dan? Nou nee, want veel smartphones worden geleverd met vooraf geïnstalleerde apps, die prestaties verminderen en de privacy kunnen schenden. Dit verschijnsel noemt men bloatware. We willen dus een 'kale' Android installatie – dus zonder bloatware of andere ongein – en dat is het belangrijkste softwarecriterium voor een rugged smartphone. Maar ook willen we een Androidversie 13 want deze biedt meer functionaliteit met betrekking tot security en privacy en valt daarmee uiteraard binnen het Europees verplichte patchbeleid. China kent veel producenten van rugged smartphones. Tot voor kort waren er in Europa ook behoorlijk wat producenten van dit type smartphones, maar sinds het wegvallen van de Britse Bullitt Group moeten we het nu stellen zonder merken als Cat, Land Rover en Motorola. Ook het Duitse Gigaset is na overname door Chinezen niet Europees meer. Blijven over: het Finse Nokia, het Franse Archos en Hammer uit Polen.

Fins, Frans of Pools?

Een middenklasse smartphone heeft tegenwoordig flink wat geheugen aan boord. Hoe meer werkgeheugen een smartphone heeft, hoe makkelijker het toestel zware apps en toepassingen draait. In het RAM (Random Access Memory) worden gegevens die applicaties nodig hebben tijdelijk opgeslagen zodat de smartphone ze snel kan ophalen. Zeker als men antivirussoftware en een firewall wil draaien naast de rest van de apps en toepassingen is een RAM van 8G een must. Mijn haperende Chinese rugged smartphone heeft ook een RAM van 8G en een opslag van 256G.
Reden genoeg om te kijken naar een Europese smartphone met deze specificaties. Hierdoor wordt het aanbod tot een aantal fabrikanten beperkt. Nokia heeft met de XR20 en de XR21 twee rugged smartphones en vallen af vanwege het te kleine werkgeheugen van 6G. De Franse Archos X67 rugged smartphone, draait nog op het stokoude Android 10 en is kansloos!
Blijft over de Poolse Hammer Blade V 5G. Deze heeft 8G werkgeheugen en de optie om virtueel op te schalen naar 14G werkgeheugen. Daarnaast heeft de smartphone een opslag van 256G. De Pool is gecertificeerd conform IP69 en MIL-STD-810J. IP69 wordt gezien als de ultieme standaard voor waterdichtheid en de MIL-STD-810J richtlijn specificeert de omgevingscondities waaronder het apparaat moet blijven functioneren.

Op de Hammer Blade V 5G is een kale versie van Android 13 geïnstalleerd. Ik heb daarmee geen last van bloatware. Het softwarematig inrichten van de Pool kan beginnen en dat betekent met alle opensource software.
We bellen of appen!

COLUMN LEX

Securityberoepsprofielen in de herhaling

In mijn column in iB-Magazine 3 van dit jaar gaf ik aan dat er beroepsprofielen ontbreken en dat het tijd werd dat we die een structurele plaats geven. Vrijwel meteen na publicatie kreeg ik twee rectificaties in mijn e-mail-inbox. De beroepsprofielen zijn er wel! Met dank aan Fred van Noord en Jan Wessels, hier een aanvulling op mijn column, met in de hoofdrol de nieuwgevonden profielen.

Enisa heeft een European Cybersecurity Skills Framework (ECSF) gepubliceerd (1), waarin twaalf cybersecurity beroepsprofielen zijn opgenomen. Wanneer je eenmaal deze referentie hebt, dan zie je dat hier best breed in de beroepswereld naar verwezen wordt. Ik noem even Isaca en SANS als degenen die mij schaamrood op de kaken geven, omdat ik die had moeten vinden. Alle beroepsprofielen uit de Nederlandse publicatie zijn uiteraard opgenomen in het ECSF, alle profielen die ik als ontbrekend had aangegeven ook, en dan nog vijf profielen meer.

Eerst wil ik de door mij genoemde ontbrekende profielen introduceren. Ik had het over de SOC-analist en het CSIRT/CERT-teamlid. Deze zijn gecombineerd genoemd als 'Cyber Incident Responder'. Deze functieprofielen liggen ook heel dicht tegen elkaar aan. De forensisch onderzoeker is een 'Digital Forensics Investigator', de security-onderzoeker is een 'Cybersecurity Researcher'. Allen komen goed overeen met de verwachting.
De vijf additionele zijn ook belangrijke rollen. De eerste die ik noem is 'Penetration Tester'. Dit profiel heeft een overlap in competenties met de 'Cyber Incident Responder', ook al zijn het qua taken en vaardigheden verschillende rollen. Daar heb ik wel een beeld bij, je hebt inzicht in de creativiteit van een aanvaller hard nodig in beide profielen.

Een 'Cyber threat intelligence specialist' vergt invulling door iemand die analytisch van aard is, kan overzien, goed kan afstemmen met verschillende stakeholders en goed kan documenteren. Het lijkt zo een behoorlijk brede rol. De 'Cybersecurity auditor' is een nuttig profiel binnen een grotere organisatie en cruciaal als je wilt certificeren tegen de ISO 27001. Zoals ik het lees hoeft het geen formele auditor te zijn, zoals een RA, RE of CISA, het gaat wel weer om de vergelijkbare vaardigheden. En dan is er nog de 'Cybersecurity educator'. Dit profiel is heel breed neergezet binnen de menselijke kant van informatiebeveiliging. Alles wat te maken heeft met kennis opdoen en vaardigheden trainen valt hieronder, of het nu een securityopleider/-trainer is, een awareness trainer binnen een bedrijf of een academische positie in het hoger onderwijs.

De 'Cyber legal, policy & compliance officer' is het laatste profiel uit het ECSF. Het lijkt heel erg op de CISO, maar dan meer gefocust op compliance, en wat meer afstand van risicomanagement. Hier valt de DPO (data protection officer) in, maar het dekt in mijn ogen ook het profiel van de CISO die aan de board rapporteert of er dicht tegenaan zit, vooral door de elementen business- en securitystrategie in het profiel.

Zo is er genoeg stof om over na te denken, vooral bij het opstellen en invullen van functieprofielen in de informatiebeveiligingsorganisatie, maar ook voor het toetsen van de effectiviteit van de huidige organisatie binnen bedrijven en overheid. Uiteindelijk verwacht ik dat zo ook de opleidings- en ontwikkelmogelijkheden van security professionals helder worden.

Referentie

(1) https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

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

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

COLUMN MARTIJN

Samen of alleen? Cyberincidenten worden complexer

Het aantal cyberincidenten stijgt elk jaar nog steeds. Ze zijn, net als onze IT-systemen, complexer geworden met meer impact op bedrijfsvoering. Dit raakt niet alleen de organisatie zelf maar ook klanten, partners en toeleveranciers. We krijgen steeds meer te maken met elkaar tijdens incidenten.

Een voorbeeld is de afhankelijkheid van de IT-dienstverlener, de MSP (Managed Service Provider). Soms leveren ze niet alleen de werkplekken en andere infrastructuur, maar dragen ze zelfs verantwoordelijkheid voor de security, zowel voor het inrichten daarvan als ook de monitoring. Als een incident optreedt is er dus een grote afhankelijkheid van de dienstverlener. Omdat de schade van een cyberincident aanzienlijk kan zijn, komt de vraag logischerwijs steeds vaker op of een IT-dienstverlener niet deels verantwoordelijk is voor het feit dat de security niet op orde was. Tijdens een incident kan dit contraproductief zijn, omdat een dienstverlener zich defensief kan opstellen, en erg gaat opletten op wat voor informatie gedeeld kan worden. Ook achteraf kan het vragen opleveren: ben je wel transparant op de hoogte gesteld van alle bevindingen?

Maar niet alleen het spanningsveld met de IT-dienstverlener wordt complexer, ook die met andere organisaties. Criminelen richten zich steeds vaker op toeleveranciers. Op die manier kunnen ze meerdere slachtoffers maken door een hack te plegen. Het kan zo maar voorkomen dat je daardoor met andere slachtoffers in hetzelfde schuitje zit. Communiceer je dan met elkaar? Ga je bevindingen uit onderzoek met elkaar delen, en misschien zelfs collectief naar de crimineel stappen om te onderhandelen als dat nodig is? De meeste mensen die ik spreek vinden dat een goed idee, maar in de praktijk zie ik dat de meeste organisaties geheim willen houden dat er een incident heeft plaatsgevonden. Hierdoor worden er echte kansen misgelopen.

Ook naar personen, intern en extern, is er meer aandacht voor persoonsgegevens die gelekt worden tijdens hacks. Stel: een e-mailaccount van een HR-medewerker is gehacked, en er is niet precies te zeggen welke mails zijn ingezien door de hacker. Ga je er dan vanuit dat alle e-mails zijn ingezien? Vaak betekent dat een flinke lijst met mensen die geïnformeerd moeten worden. Hoewel steeds meer organisaties een goed retentiebeleid op dit soort informatie voeren, zie ik toch steeds vaker gebeuren dat dit soort meldingen gewenst zijn. Personen zijn zich steeds vaker bewust van de risico's die dit met zich meebrengt, en verwachten ook meer van de organisatie om te helpen dit risico te begrijpen en mogelijk zelfs op te lossen. Het risico is dat dit een ingewikkelde toekomst teweegbrengt. Een toekomst waarbij we minder samenwerken met alle stakeholders die nodig zijn tijdens een incident, maar eerder tegenover elkaar zullen staan. Goed voorbereid zijn op incidenten, waarbij duidelijk is welke leveranciers allemaal nodig zijn en hoe er samengewerkt kan worden, is essentieel. Het vermijdt de defensieve en conservatieve reactie om andere stakeholders te zien als risico's in plaats van kansen.

Zorgen dat je in die voorbereiding de verantwoordelijkheden goed scheidt tussen die leveranciers, zoals IT en security apart beleggen, kan je een hoop wc-eend-situaties besparen in de toekomst!

Auteurs: Gerard Doeswijk werkt bij SkyKick Seattle in de functie van Vice President Cybersecurity & Data Protection met als aandachtsgebieden softwareontwikkeling op basis van agile, data protection by design en default principes. Daarnaast houdt hij zich bezig met certificering- en assurancetrajecten van de back-up, cloud management en security SAAS/PAAS-producten. Hij is ingenieur in de informatica, gecertificeerd in agile methodieken, gecertificeerd lead auditor voor ISO 27001, ISO 22301 en CISA. Hij is bereikbaar via https://www.linkedin.com/in/gdoeswijk/

NIS2 en de regie op orde in de (cloud-)keten

IT-supply chain, compliance, incident management, cloud- en business-continuity. Om maar even met de deur in huis te vallen met een paar prachtige 'Dunglish' krachttermen die vandaag de dag (weer) op de agenda (zouden moeten) staan van de bestuurders c.q. board die druk bezig zijn met de volgende (IT-)governance uitdaging.

Nu we eindelijk een beetje grip gekregen op de Algemene Verordening Gegevensbescherming – in de volksmond vaak GDPR genoemd – moeten we met zijn allen alweer vol aan de bak met de Network Information and Security 2 (NIS2)-richtlijn. En? Weet u al wat die NIS2-richtlijn in concrete zin voor uw organisatie moet gaan betekenen? Of bent u, net als ik, druk in gesprek met consultants, advocaten en leest u ook de summiere toelichting bij de richtlijn op de website van het Nationaal Cyber Security Centrum?

Van uitstel komt geen afstel

Gelukkig hebben we in Nederland een beetje respijt gekregen. Het is natuurlijk niet duidelijk of de val van het kabinet in 2023

hier iets mee te maken heeft gehad. Maar wat zou het. Wat we wel weten is dat het Ministerie van Justitie en Veiligheid heeft geconstateerd dat zij de deadline van 17 oktober 2024 niet zullen halen.

Net als met de AVG blijft natuurlijk de Europese deadline hetzelfde, en van uitstel komt zeker geen afstel. Dus als u nog niet bent begonnen met de voorbereiding dan… Nou ja, vult u zelf maar in of u meer van paniekvoetbal of een rustig potje schaken houdt.

Concreet zijn er wel al een paar zaken. Zo kunt u in ieder geval al (laten) vaststellen of uw organisatie zich moet registreren en of u dat als een essentiële of belangrijke NIS2-entiteit (1) moet doen. En dan is er de zorgplicht (2), een mooi eufemisme voor vereisten of gebruiken we tegenwoordig liever de term requirements? Want dat is toch vaak iets dwingender, zeker als het in een contract is opgenomen.

Want u zult een risicoanalyse doen, en beleid en procedures voor incidentenbehandeling hebben. Om nog maar niet te spreken van noodvoorzieningenplannen (een mooie voor het spel galgje), een back-up en nog meer van dat soort kostbare zaken.

De pijn verzachten

Maar de essentie zit hem, net als bij de AVG, toch weer in de keten. U zult, en ik kan dit niet hard genoeg benadrukken, móéten weten hoe de informatiebeveiliging van álle toeleveranciers in uw IT-supply chain is geregeld én of deze dan ook voldoet aan de vereisten van de NIS2-richtlijn. En hier zit natuurlijk de crux en de pijn. Want u leest het al, het is een richtlijn en de vereisten moeten nog worden vastgelegd in (nationale) wetten en regelgeving. En die zijn nu juist nog even uitgesteld!

Rollen de questionnaires, de zogenaamde secondparty-audits, en de eerste NIS2-overeenkomsten alweer gestaag bij uw IT- en juridische afdeling binnen? Of heeft u proactief uw inkoopafdeling op pad gestuurd om de pijn voor uw eigen organisatie iets te verzachten? Nu kunnen we natuurlijk, lekker nationalistisch gaan roepen dat deze onzin-EU-regelgeving nou weleens mag stoppen. En wellicht dat er een nieuwe minister Digitale Zaken komt die dat in Brussel kan gaan verkondigen of ook hier een 'opt-out' voor vragen. Maar dat zou toch een beetje gek staan in dit verregaand gedigitaliseerde land.

Haast

Dus wat nu? Toch maar 'een beetje voorbereiden' en al die cloudpartijen op hun verantwoordelijkheden gaan wijzen met een questionnaire? Of bent u nog één van de weinige organisaties in Nederland die alles zelf in beheer heeft in uw datacenter in de kelder? Wij houden het bij onze organisatie op de oude, vertrouwde ISO 27001 (cybersecurity), ISO 27701 (dataprotection), ISO 22301 (business-continuity) en ISO 20000 (servicemanagement). De certificering op de eerste twee heeft ons al de nodige inzichten gegeven in onze risico's en de delta tussen wat we hebben kunnen opmaken uit de richtlijn en die twee standaarden.

Afgezet tegen de Infosheet NIS2-verplichtingen is er nog wat werk te doen. En gelukkig maar, want een ISO-gecertificeerd managementsysteem brengt nu eenmaal de vereiste om aan continue verbetering te werken. En dat is en blijft natuurlijk hard nodig als het gaat om cybersecurity. Of wacht u liever op de certificering onder de Cybersecurity Act (EU Verordening 2019/881)? Eén daarvan is de European Cybersecurity Certification Scheme for Cloud Services (EUCS). Die is de in 'de ontwikkelingsfase', volgens de informatie op de website van de Cybersecuritycertificeringsautoriteit (3) (nóg eentje voor galgje!). Gezien de haast waarmee het certificeringsschema voor artikel 42 van de AVG is opgepakt, en dat dit kandidaat-certiferingsschema alweer van juli 2020 is, is het wellicht raadzaam om uw energie en middelen anders en wijzer te besteden.

Let wel, als bestuurder krijgt u ook nog eens te maken met persoonlijke aansprakelijkheid bij het niet naleven van de NIS2. Dus neemt u dat alstublieft mee in de risicoanalyse, dan is die paar ton voor een cybersecurityprogramma wellicht wat minder misselijk. En als er dan toch ergens een opt-out kan worden gezocht, is het te hopen dat de nieuwe ministersploeg de wedstrijd in Den Haag begint, voordat er naar Brussel wordt getogen.

Referenties

(1) Infosheet NIS2 verplichtingen: Registratieplicht Publicatie Nationaal Cyber Security Centrum www.ncsc.nl
(2) Infosheet NIS2 verplichtingen: Zorgplicht Publicatie Nationaal Cyber Security Centrum www.ncsc.nl
(3) Certificeringsschema's Cybersecurity certificering (NCCA) Rijksinspectie Digitale Infrastructuur (RDI)

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

BLOG

Supply chain stap: van droom naar daad

Supply chain is voor mij in het Nederlands: totstandkomingsproces voor producten en diensten in vooral het domein van de geautomatiseerde informatie- en communicatietechnologie. Supply chain is zo een traject van 'droom tot daad', waarbij de droom de allereerste gedachte: 'Ik zou voor dit probleem toch eens een informatiesysteem moeten bedenken' is, en de daad: 'de werkelijke toepassing van dat systeem door een voldoende opgeleide en over risico's voorgelichte gebruiker'. In het totstandkomingsproces van de supply chain is – natuurlijk, u kent mij - het IT-auditproces, gericht op het te ontwikkelen product of systeem, een van de belangrijkste stappen. Ik ga daarom verder in op de met (IT-)audit samenhangende risico's. Daarbij gebruik ik een voorbeeld over bedrijfsartsen, omdat ik overeenkomsten zie tussen hun werk en dat van security-officers & -consultants.

"Want tussen droom en daad..." hoor je bij kickoffvergaderingen. De daarbij veelbetekenende blik van de overduidelijk intellectuele spreker nodigt dan uit om dat aan te vullen met: "staan wetten in den weg, en praktische bezwaren". Deze zin van de Belgische auteur Willem Elsschot is een regel uit zijn schittterend gedicht Het Huwelijk, over een gruwelijk onderwerp. Omdat het zo gruwelijk prachtig is en er weinig gedichten in iB-Magazine staan, heb ik de tekst in een kader opgenomen. Aan het einde van dit artikel, om de clou niet te verraden en de sfeer hier niet te bederven.
Een Westerse arts heeft als doel zijn patiënt weer beter te maken en gebruikt daarvoor medicijnen en medische ingrepen. Een meer holistisch opgeleide arts past ook het gesprek en de analyse toe om mensen te genezen. Een aardige huisarts weet dat je met tijd, aandacht en goed luisteren (oogcontact, knikken, hummen, actief samenvatten) naar de klachten van een patiënt ook al heel ver komt. Correctieve maatregelen dus.

Een traditionele Chinese arts heeft juist als doel om je gezond te houden en gebruikt daarvoor meer kruiden dan chemische medicijnen, maar ook het praten, voorlichten en luisteren van zijn Westerse evenknie. Dat alles echter, op een meer preventieve manier.

Bedrijfsartsen hebben juist tot doel om problemen op te lossen. Dit blijkt bijvoorbeeld uit het feit dat zij jou in hun gespreksverslagen geen patiënt noemen, maar medewerk(st)er. En als de bureaustoelen, eerder in het traject, al door de kantoorruimte vlogen eventueel zelfs betrokkene. De probleemgebieden waar de bedrijfsarts zich op richt zijn ruwweg de volgende:
1. medewerk(st)er doet in privétijd te weinig aan sport
2. medewerk(st)er heeft het te druk in het werk
3. medewerk(st)er heeft geen goede bureaustoel
4. medewerk(st)er begrijpt de leidinggevende niet
5. leidinggevende begrijpt medewerk(st)er niet

Het mooie van deze probleemgebieden is, dat de oplossing telkens enorm voor de hand ligt. Bedrijfsarts zijn, is daarmee een mooie tijdsbesteding voor iemand die wel medicijnen wil studeren, maar erg opziet tegen de extra vervolgstudies die zijn vereist voor huisarts én specialist.

Bij probleem 1 t/m 4 is het meestal een eigen keuze om naar de bedrijfsarts te gaan. Bij probleem 5 stuurt, in het algemeen, die leidinggevende de medewerk(st)er naar de bedrijfsarts. Daarom is mijn advies, voor medewerk(st)er of betrokkene, met haar/zijn verhaal en non-verbaal gedrag de bedrijfsarts te overtuigen dat vier van de vijf mogelijkheden in elk geval niet spelen. Er is namelijk ook nog een zesde, algemene oplossing: dat betrokkene, al dan niet financieel gecompenseerd, het bedrijfspand definitief verlaat. Dat moeten we met zijn allen niet willen, dus laat wel één van de vijf probleemgebieden voor de bedrijfsarts over.
Security-officers kunnen zich in hun loopbaan door deze rol/functiemodellen van artsen laten inspireren en hun gedrag en handelen zo vormgeven. Echter, gedrag afwisselen en afstemmen op veranderende situaties in de eigen werkomgeving.

Nuances over medewerker-problemen

Probleem: sport
Medewerk(st)ers die regelmatig sporten, zijn gezonder dan degenen die dat niet doen en alleen maar nachtenlang gamen, chips eten en cola of bier drinken. Méér sporten, is dus een veelgegeven advies. Hoewel iedereen vanzelfsprekend slanke, lenige (agile!), fitte, gespierde, afgetrainde medewerk(st)ers wil, kun je bij sporten helaas ook geblesseerd raken. Voor de werkgever tellen hierbij alleen de blessures waardoor u, beste lezer(es), (langere tijd) niet meer kunt werken. Soms is het daarom nodig een medewerk(st)er juist minder te laten sporten. De security-analogie is hier: BYOD (Bring Your Own Device). Of plat gezegd: elke lul, zijn eigen spul. Niet te weinig (nooit eigen apparatuur), maar ook niet te veel.

Probleem: drukte
Soms vertrekken er veel collega's vrijwillig of verdwijnen ze door reorganisaties. In sommige maanden zijn veel mensen fysiek ziek, door de heersende griep, of zijn ze 'niet in staat om te werken' verklaard door de bedrijfsarts, of hebben ze vakanties, ouderschapsverlof, pappa-dagen. Als de werkzaamheden dan toch in dezelfde grote kwantiteit en nauwkeurige kwaliteit moeten worden voortgezet, hebben de overblijvers het druk. Te druk, en dan zegt de bedrijfsarts tegen je, dat je de werkdruk moet gaan bespreken met je baas. En vaker 'nee' zeggen en proberen om activiteiten zoveel mogelijk te delegeren. Dat laatste woord lijkt trouwens op het Duitse acroniem: DELLE: durch einfach liegen lassen erledigt. Want veel problemen op je werk lossen zich vanzelf op, als je niks doet maar gewoon rustig afwacht. Ben je te druk met je werk, dan spreken we van burn-out of opgebrand. Wie graag met lucifers speelt, weet dat je een kaars aan twee kanten tegelijk kunt aansteken. Je hebt dan meer licht, maar de kaars is twee keer zo snel op. Dat snelle opbranden geldt ook voor 'human resources'. Aan de andere kant is er incidenteel iemand die zich verveelt, omdat hij het niet druk genoeg heeft. Hier wordt dan het etiket bore-out op geplakt. Deze personen lossen hun probleem, uit verveling, meestal zelf wel op. Ook op security-afdelin-

Verhogen security-awareness is als Haarlemmerolie voor alle securityproblemen waar we geen technische of organisatorische oplossingen voor kunnen bedenken

gen komt het voor (heb ik gehoord) dat er niet genoeg medewerk(st)ers zijn voor het oplossen van alle incidenten en het daarbij noodzakelijke uitzoekwerk (threat hunting of root cause analysis). Tegelijk zijn er soms securitymedewerkers van wie niemand precies weet wat ze de hele werkweek doen. Precies genoeg mensen inplannen voor de hoeveelheid securitywerk is het devies!

Probleem: ingezette hulpmiddelen

De 'stoel' staat voor alle ingezette hulpmiddelen. Er zijn ook medewerk(st)ers die problemen hebben met hun laptop of smarthone, meestal als ze NIET van Apple zijn, of die last hebben van het lawaai op kantoor; waar immers ook andere mensen zijn die bellen, praten of te luid ademhalen! Vaak vindt de bedrijfsarts hier een oplossing voor door de medewerk(st)er meer thuis te laten werken, waar de problemen met precies dezelfde apparatuur dan als sneeuw voor de zon verdwijnen. Komt een medewerk(st)er daarentegen bijna nooit op kantoor én klaagt zij/hij over 'gevoelens van vervreemding en afstand tot collega's', dan moet die persoon juist vaker op kantoor komen, om mee te vergaderen en (samen) te werken. Denk bij deze problemen aan alle technische securitymaatregelen die je (nog) kunt/moet implementeren, 'boys and their toys'. Lampjes, piepjes en grafiekjes. Ook het implementeren van 2 (of 3) factor authenticatie is eigenlijk puur een kwestie van meer of nieuwe/andere hulpmiddelen gaan gebruiken. Of je de muren van het bedrijfspand nu roze of lichtblauw verft maakt niet uit: de medewerk(st)ers gaan harder werken omdat ze het gevoel hebben dat er echt aandacht voor hun problemen is en dat het management er iets mee doet (Hawthorne onderzoek).

Probleem: "Ik begrijp de manager niet!"

Wanneer de medewerk(st)er bij de bedrijfsarts aangeeft, haar/zijn leidinggevende niet te begrijpen, vraagt de bedrijfsarts meteen én met nadruk: "Jij hebt dus een probleem met je huidige leidinggevende?" Dit lost bij goede verstaanders veel problemen al direct op. Als uit het verdere gesprek blijkt dat het werkelijk om niet begrijpen gaat, is 'een cursus volgen' het beste advies. Maar als blijkt dat de medewerk(st)er de leidinggevende gewoon een (ondeskundige, onbewame, onvriendelijke) eikel of mafketelin vindt, helpt een inhoudelijke cursus niet meer. De bedrijfsarts moet dan kiezen: óf hij gaat voor de 'mercy kill' oplossing óf hij biedt de medewerker een uitweg door te vragen naar vakantieplannen, een sport als hobby, de werkdruk in het algemeen, bijhouden van vakkennis op buitenlandse congressen. En natuurlijk de vraag: Zit je eigenlijk wel goed? Heb je wel een goede bureaustoel? Heeft men op kantoor al een goede stoel, dan kan het ook nog aan de stoel op de thuiswerkplek liggen. En een in hoogte verstelbaar sta-bureau op kantoor of in jouw huiskamer kan ook een tijdelijke uitweg uit de ontstane impasse zijn. Denk hierbij aan 'verhogen van de security-awareness' als Haarlemmerolie voor alle securityproblemen waar we geen technische of organisatorische oplossingen voor kunnen bedenken. Of niet willen of kunnen betalen.

Probleem: "Mijn leidinggevende begrijpt mij niet!"

Dit soort problemen zijn altijd lastig. De medewerk(st)er staat al met één been buiten, maar kan soms nog behouden blijven door na een goed gesprek in te zien, dat het eigenlijk een van de andere problemen betreft. Er zijn gradaties: de leidinggevende kan de afspraak met de bedrijfsarts voor de medewerk(st)er alleen in de agenda inplannen, maar zij/hij kan ook voorafgaand een intakegesprek doen waardoor de bedrijfsarts `alvast is inge-

Als in dergelijke werkomstandigheden de tegenpartij het puur zakelijk houdt, probeer er dan een persoonlijke draai aan te geven

praat over wat er allemaal speelt'. Extra moeilijk is het, wanneer de leidinggevende de werknemer wel degelijk begrijpt, maar hem/haar gewoon respectievelijk een eikel of mafketelin vindt. Dan valt er met meer sporten, een andere werkindeling of een (duurdere) nieuwe stoel weinig meer te redden.

Als in dergelijke werkomstandigheden de tegenpartij het puur zakelijk houdt, probeer er dan een persoonlijke draai aan te geven. Soms maakt de tegenpartij het te persoonlijk, zoals bij mobbing: het spelen op de vrouw/man, gericht op het beschadigen van de persoon door suggestief, irriterend, hinderlijk gedrag. Dan is het beter om het contact verder zakelijk te houden, dus mogelijk ook via advocaten.

Het is van belang de bedrijfsarts de gelegenheid te geven om uit de informatie die je verbaal en non-verbaal geeft, zelf de diagnose te stellen wat het probleem is. Vergelijkenderwijs: het is ook een goed idee dat een auditor samen met de auditee de actielijst met in te voeren verbeteringen opstelt óf dat een securityconsultant bij de eerste (project)bespreking vraagt: Wat denk je er zelf van, qua securityrisico's die hier spelen?

IT-audit proces risico's

Auditors moeten voor hun werk ieder jaar meerdere audits uitvoeren en maken daarom een jaarplanning. Om oppoets- of gladstrijkacties vlak voor de audits te vermijden, is het beter de planning niet af te stemmen met auditees. Auditees die veel problemen maken over de door de auditor geplande uitvoeringsperiode zijn een 'red flag'.

Bij een IT-audit wordt vooraf een normenkader opgesteld, dat moet worden geaccordeerd door de auditee. Tijdens het onderzoek worden de bevindingen vergeleken met het vooraf vastgestelde normenkader om tot een zo objectief mogelijk en door een ander toetsbaar oordeel te komen. Auditees die zogenaamd 'geen tijd hebben' om het normenkader te accorderen zijn een red flag, omdat ze zo het begin van de audit weten uit te stellen en dan kunnen gaan oppoetsen.

Als auditor begin je na veel wachten en smeken uiteindelijk dan toch maar aan jouw audit, met een niet door auditee geaccordeerd, maar wel succesvol eerder gebruikt normenkader. Omdat je toch je eigen jaarplanning moet uitvoeren. Wees dan niet verbaasd als diezelfde auditee jou vertelt dat jouw auditresultaten ongeldig zijn, omdat het normenkader niet vooraf is geaccordeerd. Dit gebeurt overigens alleen bij een negatief oordeel, maar goed, de meeste IT-auditrapporten hebben een negatief oordeel met aanbevelingen. Als de auditee het in de rapportbespreking op de inhoud niet van de auditor kan winnen, begint hij over fouten in het proces.

Bij een normenkader van 100 regels, waarbij er op 20 punten problemen zijn, kiezen de meeste auditors ervoor om de overige 80 regels niet op te nemen in het auditrapport. Dit om de rapportomvang te beperken en qua audit-uren (er is altijd te weinig ingepland voor rapportage) binnen budget te blijven. Er bestaan echter auditees die aanvoeren 'maar er gaat toch ook heel veel goed...' - en dan, nadat je een aantal van die punten (bijvoorbeeld 40) hebt toegevoegd, klagen dat het auditrapport veel te lang is om te lezen voor een drukbezette manager. En dat sowieso tweederde van de in het rapport behandelde punten voldoende zijn! Door alleen regels te tellen, gaan ze voorbij aan de ernst en omvang en daarmee het gewicht van de diverse tekortkomingen. Wees voorzichtig met toevoegen van tekst aan je rapport op verzoek van de auditee!

Veel tekortkomingen leiden ook tot veel aanbevelingen. Een auditee, wiens bonus afhankelijk is van het aantal opgeloste auditissues per jaar, zal de auditor vragen om 'behapbare' aanbevelingen, waarvan 'door de auditor gemakkelijk is vast te

stellen dat ze compleet zijn uitgevoerd'. Dat het er daardoor veel worden, is voor die auditee helemaal geen probleem. Andere auditees lopen hun bonus juist mis, als ze teveel openstaande issues hebben per 30 september, want in oktober start elk jaar de bonus-beoordelingsronde. Sommige van die auditees vragen daarom om grote, veelomvattende aanbevelingen en abstracter geformuleerde acties. "Want goed beschouwd hangen die problemen met elkaar samen!" en: "We moeten het goed en gestructureerd oplossen, desnoods kost het dan wat meer doorlooptijd", krijg je dan te horen als auditor. Red flag!

De risico's in de supply chain van auditrapporten liggen echter niet alleen aan de kant van de auditee als onderzochte partij. Een junior auditor voelt zich een jonge god, die alle tekortkomingen in het proces van de auditee waarneemt, ze allemaal foutloos en volkomen objectief interpreteert. Althans, dat denkt zij/hij zelf. Als

de junior auditor vaststelt dat in zes van de twintig onderzochte personeelsdossiers een geparafeerde kopie van een geldig identiteitsbewijs ontbreekt, en dat die persoon dus mogelijk helemaal niet bestáát, maar wel maandelijks salaris ontvangt; adviseert hij daar voortaan bij nieuwe medewerk(st)ers beter op te letten en om bestaande personeelsdossiers aan te vullen.

Een senior auditor heeft meer ervaring, maar wil graag god (lees: auditmanager) worden en abstraheert het advies van de junior tot 'verbeteren van de procedure persoonlijke identificatie'. Daardoor wordt helaas onduidelijk dat het probleem puur zit in de naleving van de op zich best redelijke procedure: vergelijk iemands gezicht met de foto op het identiteitsbewijs, maak een kopie voor het dossier en zet er een paraaf en datum op als teken dat je dit bewust hebt gedaan. Maar het abstracte advies klinkt veel professioneler dan: in zes dossiers alsnog een kopie paspoort stoppen.

Een auditmanager (weer een stapje hoger op de auditor-rots) denkt dat hij al god is en maakt van het advies 'verder verbeteren van de bestaande procedure persoonlijke identificatie nieuwe medewerk(st)ers'. Want zij/hij wil de auditee erkennen voor het vele goede werk dat er al is gedaan, het advies toespitsen op 'des Pudels Kern' en graag ooit overstappen als manager naar die afdeling.

Het hoofd van de auditafdeling weet in de tussentijd dat hij nooit echt god zal worden, maar dat poortwachter Petrus ook een zeer belangrijke en invloedrijke positie is. Hij leest alle auditrapporten die per maand verschijnen, kan ze onderling vergelijken, de grote lijn zien en past het advies daarom aan naar 'voldoende aandacht blijven houden voor naleving van de procedures en deze waar nodig actualiseren'. Daar kan je het als auditee moeilijk mee oneens zijn! En in een followup interview over de actielijst is het gemakkelijk naar waarheid aan de auditor te antwoorden dat je hier inderdaad en voortdurend aandacht voor hebt. Zodat deze actie snel afgerond kan worden.
Houd je haaks en blijf gezond!

Het Huwelijk
Toen hij bespeurde hoe de nevel van den tijd
in d'ogen van zijn vrouw de vonken uit kwam doven,
haar wangen had verweerd, haar voorhoofd had doorkloven,
toen wendde hij zich af en vrat zich op van spijt.

Hij vloekte en ging te keer en trok zich bij den baard
en mat haar met den blik, maar kon niet meer begeren,
hij zag de grootse zonde in duivelsplicht verkeren
en hoe zij tot hem opkeek als een stervend paard.

Maar sterven deed zij niet, al zoog zijn helse mond
het merg uit haar gebeente, dat haar tóch bleef dragen.
Zij dorst niet spreken meer, niet vragen of niet klagen,
en rilde waar zij stond, maar leefde en bleef gezond.

Hij dacht: ik sla haar dood en steek het huis in brand.
Ik moet de schimmel van mijn stramme voeten wassen
en rennen door het vuur en door het water plassen
tot bij een ander lief in enig ander land.

Maar doodslaan deed hij niet, want tussen droom en daad
staan wetten in den weg en praktische bezwaren,
en ook weemoedigheid, die niemand kan verklaren,
en die des avonds komt, wanneer men slapen gaat.

Zo gingen jaren heen. De kindren werden groot
en zagen dat de man dien zij hun vader heetten,
bewegingloos en zwijgend bij het vuur gezeten,
een godvergeten en vervaarlijke' aanblik bood.

Rotterdam 1910, Verzen
Willem Elsschot (1882-1960)

COLUMN NICOLE

Sterke wachtwoorden, zwakke regels: tijd voor vooruitgang

Het voelde als een verademing toen ik kennisnam van het advies van het National Institute for Standards and Technology (NIST) in de Verenigde Staten over wachtwoorden. In hun nieuw voorstel willen ze enkele hardnekkige, maar contraproductieve regels rond wachtwoorden loslaten. Een van de belangrijkste veranderingen: het verplicht wisselen van je wachtwoord om de paar maanden.
Deze regel stamt uit een tijdperk waarin de meeste mensen weinig besef hadden van digitale beveiliging en simpele wachtwoorden gebruikten, zoals de naam van hun hond of hun geboortedatum. Die waren makkelijk te raden. Tegenwoordig echter, hebben veel mensen sterkere wachtwoorden, vaak automatisch gegenereerd door wachtwoordmanagers. Zo'n wachtwoord is zó veilig dat het helemaal niet regelmatig vervangen hoeft te worden. Sterker nog, de oude regel kan de beveiliging juist verzwakken, omdat gebruikers geneigd zijn een eenvoudiger, makkelijker te onthouden wachtwoord te kiezen wanneer ze gedwongen worden steeds te wisselen. Het NIST stelt dan ook terecht dat wachtwoorden alleen vervangen hoeven te worden wanneer ze daadwerkelijk gecompromitteerd zijn.

Daarnaast bekijkt NIST ook kritisch de regel om specifieke karakters, zoals hoofdletters of speciale tekens, verplicht te gebruiken. Ook deze regel blijkt vaak overbodig, vooral wanneer een wachtwoord lang genoeg is. In plaats van de beveiliging te versterken, maakt het de keuze voor een goed wachtwoord alleen maar moeilijker en kan het gebruikers weer richting onveiligere keuzes duwen. Wat verfrissend is aan dit nieuwe advies, is dat het werkelijk rekening houdt met de praktijk. Het lijkt bijna revolutionair om af te wijken van traditionele adviezen die jarenlang onaangetast zijn gebleven. Maar het opvallende is dat dit NIST-advies helemaal niet 'nieuw' is. Wie wat verder terugkijkt ontdekt dat ze al jaren geleden aangaven dat periodiek wisselen van wachtwoorden eerder een zwaktebod is dan een vorm van beveiliging.

Ga je nóg verder terug, dan kom je bij de spijtbetuiging van Bill Burr, de man achter de oorspronkelijke NIST-richtlijnen uit 2003. In 2017 gaf hij in een interview met de Wall Street Journal ruiterlijk toe dat – met de kennis van nu – zijn advies destijds onjuist was. Toch heeft deze openlijke herziening weinig impact gehad, want veel bedrijven en instellingen hangen nog steeds vast aan die verouderde regels. Het is ronduit verbijsterend dat we in een tijd waarin iedereen schreeuwt dat de wereld sneller verandert dan ooit, zo achterlopen in het bijstellen van onze digitale veiligheidspraktijken. Het lijkt erop dat we op het gebied van wachtwoordbeleid zijn blijven haken in 2003, terwijl de dreigingen van vandaag om veel slimmere en flexibelere oplossingen vragen.

Laten we daarom eindelijk luisteren naar de aanbevelingen die al jaren op tafel liggen. Of nog beter: laten we luisteren naar adviezen die vooruitkijken naar de toekomst. Misschien kunnen we ons dan eindelijk losweken uit het verleden en écht vooruitgaan.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Auteur: Leo van Koppen is redactielid van iB-Magazine. Hij is bereikbaar via leo@es4cs.nl

BOEKREVIEW

Titel boek:	***Don't push me! Hoe je mensen wél beweegt***
Auteur:	Genieke Hertoghs
Taal:	Nederlands
ISBN:	9789082579925
Prijs:	paperback € 24,95, e-book € 13,99

Waarom drammen niet werkt

In ons vakgebied is het van groot belang dat je de organisatie meekrijgt in cyberveilig gedrag. We hebben altijd een overvloed aan goede adviezen voor securitymaatregelen beschikbaar. Het maakt niet uit of dat nu op het organisatorische vlak ligt van security-awareness of op het technisch vlak in het voorkomen van kwetsbaarheden in je softwareapplicatie. Het probleem is bijna altijd dat er onvoldoende opvolging of invulling wordt gegeven aan de voorgestelde maatregelen.

We weten het allemaal: bij de implementatie van maatregelen moet je als security-officer hard werken aan het draagvlak. Want dan krijgen jouw adviezen een kans te worden opgevolgd. Het echte probleem zit hem eigenlijk in het feit dat het creëren van een draagvlak zo verschrikkelijk lastig is. Dat onderwerp komt nu net weer niet aan de orde in het CISSP, CISM of Master programma. Vreemd eigenlijk, want speelt het een cruciale rol in het succes van de security-officer/consultant. Eigenlijk een essentiële soft skill die niet mag ontbreken in onze security opleidingen.

Brein kent twee systemen

Velen onder u hebben vast weleens gehoord of kennis genomen van het gedachtegoed van Daniel Kahneman. In zijn boek Thinking Fast and Slow legt hij uit hoe ons brein eigenlijk twee systemen bevat. Systeem-1 is onze automatische piloot en werkt vrijwel autonoom. Zonder er bewust over na te denken rijd je

bijvoorbeeld feilloos in druk verkeer of begrijp je non-verbale uitingen. Systeem-2 vraagt onze volledige aandacht en concentratie bij het oplossen van moeilijke vraagstukken en het nemen van beslissingen. Systeem-1 levert automatisch input voor je handelingen en ondersteunt daarmee ook systeem-2. Wellicht breng ik u nu in verwarring want de titel boven deze review is wel correct. Het boek dat ik in deze review wil bespreken gaat niet over Thinking fast and slow, maar maakt gebruik van het gedachtegoed van Kahneman. Met name hoe de ontvanger van de boodschap, jouw advies, verwerkt in systeem-1.

Don't push me van Genieke Hartoghs maakt op een heldere wijze duidelijk waarom het 'pushen' van adviezen niet zomaar het gewenste resultaat oplevert. Waarom mensen deze adviezen in eerste instantie zullen negeren en gewoon hun 'eigen ding' blijven doen. Het maakt aan de hand van zeer aansprekende voorbeelden duidelijk waarom mensen dit gedrag vertonen en wat je zult moeten doen om mensen zover te krijgen dat ze achter je plannen gaan staan. Wat jij daar voor moet doen lijkt heel simpel, namelijk de bijna kinderlijk eenvoudige vraag stellen: waarom? Kortweg, niet 'pushen' maar 'pullen'! Dat blijkt in de praktijk nogal lastig te zijn, omdat je voor het stellen van open en neutrale vragen geduld moet hebben en zeker niet moet proberen de ander met jouw argumenten te overtuigen. In de voorgestelde methode gaat het bij aanvang (nog) niet om het rationele. De kunst is om eerst 'in positie' komen in het onbewuste brein (systeem-1) van de ander, door het initiële afweermechanisme van de ander met eenvoudige vragen stap voor stap te ontmantelen. Van belang is ook om de antwoorden te voorzien van de juiste support zodat je 'in positie' geraakt. Pas dan kom je binnen bij de ander en is er een basis voor gedragsverandering en eigenaarschap gelegd.

Elk persoon heeft in systeem-1 een defensiemechanisme dat onbewust wordt ingezet bij het aanhoren van afwijkend gedachtegoed. Bij een push zal dit mechanisme in werking treden en zelfs worden versterkt. Het effect is dat het tegendeel wordt bereikt. In de eerste stap is het van belang het ego niet te laten gelden (en dat is voor sommige adviseurs wellicht heel lastig!). In een volgende stap gaat het om jezelf in een positie te brengen waarin je impact kan maken. Het gaat om de vraag: Hoe ziet de ander jou? Dat is een oplopende schaal met zes niveaus:

- **probleem(0)-zekerheid(1)-verrassing(2)-aandacht(3)-toegevoegde waarde(4)-goeroe(5)**
  Om impact te kunnen maken is niveau 3-4 het vereiste niveau om succesvol te kunnen zijn. De sleutel tot succes ligt echter in, wat de schrijfster noemt, de scope. Dat is een gelaagdheid in de manier zoals de ander de wereld waarneemt. Een gelaagdheid in de volgende niveaus:
- **buitenwereld(0)-activiteiten(1)-meningen(2)-belangen(3)-overtuigingen(4)-identiteit(5)**
  De kunst is nu om via vragen door te dringen in die gelaagdheid en op zoek te gaan naar hoe de ander tegen de wereld (het probleem/de kwestie) aankijkt. Bij het pullen is de regievraag van belang, dat is een open vraag die bepaalt welk gebied je activeert in het brein van de ander. Je regisseert als het ware welk gebied van het onbewuste brein bij de ander geactiveerd wordt. Die zal vervolgens een antwoord geven omdat hij jouw interesse wil belonen, je een antwoord gunt, een oplossing zal aanreiken of zich ongemakkelijk voelt als hij het antwoord schuldig moet blijven. Na de regievraag volgen de doorvragen waarbij je jouw eigen scope moet uitschakelen (lastig) en vooral via support en andere open vragen meer in positie kunt komen. Pas als je in positie bent gekomen kun je het advies, je boodschap, gaan pushen. Ook hier past enige bescheidenheid. Alleen dat deel dat minimaal vaststaat, het aanvullende deel, ingevuld vanuit jouw scope, is onderhandelbaar.

Schriftelijke cursus

Don't push me! is meer dan een boek, het is eigenlijk een schriftelijke cursus. Het enige dat ontbreekt is de praktijk, maar die kom je elke dag in je werk tegen. Het boek kent een hele mooie structuur: het legt het probleem uit en neemt je op bijna meeslepende manier mee naar de oplossing. Het boek legt de belangrijke concepten zeer goed uit en belicht daarbij in het kort de onderliggende wetenschap zonder langdradig te worden. Daarnaast geeft het boek bij elk belangrijk onderdeel zeer aansprekende voorbeelden waardoor je het snel begrijpt. Dat wil niet zeggen dat je het zomaar even kunt toepassen. Daar wordt ook meerdere malen voor gewaarschuwd: het lijkt eenvoudig, maar is lastig in de uitvoering. Toch denk ik dat dit boek vele vakgenoten verder kan helpen. Als we ooit op het onderdeel, dat wij destijds de naam security awareness hebben genoemd, maar later de lading van gedragsverandering hebben gegeven, succesvol willen zijn, dan is de methode van pullen in plaats van pushen mijns inziens noodzakelijk. Dat is ook de reden van deze boekreview, vakgenoten bekend maken met deze methode. Ik wens jullie veel succes! Don't push me! biedt een heel goed inzicht in waarom drammen niet werkt en het boek leert je te pullen door je eigen ego opzij te zetten en via het onbewuste brein van de ander de gewenste gedragsverandering te bewerkstelligen. Wat mij betreft een must voor security-officers, met name met het aandachtsgebied van security-awareness, maar het kan ook voor securityconsultants een goed hulpmiddel zijn.

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.

De invloed van de wereld op onze leveranciers

In eerdere edities van iB-Magazine hebben we de risico's binnen de toeleveringsketen besproken, waarbij we recent focusten op de Europese Digital Decade-wetgeving. Deze regelgeving biedt kansen, maar roept ook vragen op over ethiek en verantwoordelijkheden binnen de informatiebeveiliging. Ondertussen spelen geopolitieke ontwikkelingen, zoals de handelsoorlog tussen China en de VS, een steeds grotere rol. Wat betekenen deze veranderingen voor onze aanpak in Nederland, en hoe houden we rekening met internationale leveranciers?

In de vorige editie van Achter Het Nieuws onderzochten we de juridische implicaties binnen de toeleveringsketen, met nadruk op Europese wetgeving en de kansen die deze voor informatiebeveiligers kan bieden. Naast deze interne ontwikkelingen vraagt ook het internationale speelveld om onze aandacht: denk aan de aanhoudende spanningen tussen de VS en China, met directe gevolgen voor bedrijven als ASML. Hoe beïnvloeden deze wereldwijde krachten ons werk, en wat betekent dit voor de samenwerking met leveranciers wereldwijd?

Fook Hwa Tan – Ketenrisico's omzetten in kansen

Geopolitieke uitdagingen dwingen Nederlandse bedrijven om zich aan te passen en veerkrachtig te zijn. Handelsoorlogen en strikte regelgeving veranderen het speelveld, maar in plaats van te focussen op risico's, kunnen we juist kansen benutten. De Nederlandse handelsgeest en openheid voor samenwerking met diverse partijen helpen ons om nieuwe kansen te grijpen en onze toeleveringsketen te versterken. Door overzicht en inzicht in de keten te creëren, kunnen we verbeterpunten identificeren en processen optimaliseren, wat leidt tot meer efficiëntie en een toekomstbestendig model waarin risico's vroegtijdig worden aangepakt.


Fook Hwa Tan


Leo van Koppen

Een cruciale uitdaging is het vinden van een balans tussen veiligheid, objectiviteit en inclusiviteit. Leveranciers uit complexe regio's kunnen risicovol lijken, maar een rigide benadering leidt tot uitsluiting. We moeten risico's beheersen zonder vooroordelen, door transparant en objectief te evalueren. Zo doen we recht aan zowel veiligheid als eerlijke kansen voor alle leveranciers, ongeacht hun herkomst. Culturele verschillen spelen hierbij een rol: intensief screenen kan in sommige Aziatische culturen als wantrouwen worden gezien, terwijl dit in westerse landen vaak als professionaliteit wordt opgevat. Begrip en respect voor culturele verschillen helpen ons effectiever te communiceren en duurzamere relaties met leveranciers op te bouwen.

Veerkracht vraagt vertrouwen en samenwerking. Laten we samen streven naar Digital Trust door transparantie en samenwerking. Alleen samen realiseren we een veilige, veerkrachtige en vertrouwde digitale toekomst.

Leo van Koppen – Polarisatie als risicofactor

Het antwoord op de gestelde vraag is natuurlijk een no-brainer, natuurlijk heeft het impact! Helaas moet ik constateren dat polarisatie op alle plaatsen in de wereld toeneemt. Ik ben daar niet van, het past niet bij mijn karakter, ben altijd op zoek naar harmonie, maar dat terzijde. Polarisatie wordt zichtbaar wanneer mensen uitgesproken meningen aan de uiterste kanten van een onderwerp innemen. Die discussie wordt in dit tijdperk met name via digitale middelen gevoerd en daarmee is de link gelegd naar het domein cybersecurity. Om je macht te kunnen tonen, je economie te versterken, je business te beschermen, je territorium uit te breiden, lijken alle middelen en methoden toegestaan. Nation state actors zijn daarbij de belangrijkste actoren.

De vraag heeft een nogal brede scope die ik omwille van de lengte van deze bijdrage maar wat kleiner kies. Ik beperk me dan ook tot deze threat actor en het nieuwe fenomeen van AI, dat zowel als maatregel of als bedreiging kan worden gezien. Voordat ik daar op in ga, eerst maar even de invloed van AI op de bedrijfsvoering beschouwen. Als die verwachtingen worden waargemaakt dan betekent dat de bedrijfsvoering, nog sterker dan het nu al het geval is, afhankelijk zal worden van informatievoorziening. Het gaat dan met name om de integriteit van de onderliggende data waarop AI is gebaseerd. We kennen deze relatie: toename in afhankelijkheden betekent in cybersecurity grotere risico's.

Artificiële Intelligentie heeft geen twee maar vier invalshoeken, althans zo stelt de AIVD in het onlangs verschenen document (3). Omdat ik het zelf niet beter kan verwoorden hierbij een ingekorte versie:

Aanvallen (dreiging)

1. Op generatieve AI, gericht op het verstoren of misleiden van AI-systemen, inclusief pogingen om de trainingsdata te beïnvloeden of de AI op ongepaste wijze te manipuleren
2. Met behulp van generatieve A, waarbij GenAI wordt ingezet als middel voor het uitvoeren van cyberaanvallen

Verdediging (maatregelen)

1. Van generatieve AI. Verdedigingsmaatregelen zijn gericht op het beschermen van AI-systemen tegen externe aanvallen en interne misbruiken. Dit omvat het veiligstellen van trainingsdata en het model, evenals het ontwikkelen van robuuste systemen die zichzelf kunnen verdedigen tegen aanvallen.
2. Met behulp van generatieve AI. AI wordt ook gebruikt als een hulpmiddel om te verdedigen tegen cyberaanvallen, door middel van realtime dreigingsdetectie en respons, of het combineren van en handelen op dreigingsinformatie uit verschillende bronnen.

Mijn conclusie bij het bovenstaande is dat er sowieso werk aan de winkel is, immers: de aanvallers beschikken door AI over meer geavanceerde tools. Hiervan kunnen we nog nauwelijks overzien welke impact het zal hebben, daarbij is ook het aanvalsoppervlak (data) verder uitgebreid. Natuurlijk komen er ook nieuwe tools beschikbaar waarmee we onze verdediging kunnen versterken, maar het beschermen van die complex AI-systemen en de bijbehorende data vraagt nieuwe expertise en veel tijd.

Drie effecten bij deze beperkte scope samengevat:

- State actors zullen een agressievere houding gaan vertonen om macht te behouden of uit te breiden
- Een sterkere afhankelijkheid van informatie en bijbehorende systemen ten gevolge van de toepassing van AI in bedrijfsvoering en economische bedrijvigheid
- En een sterk veranderend (complexer) speelveld door de komst van AI. Kortom de gevolgen van toenemende polarisatie op het wereldtoneel zijn enorm. Ik hoop, tegen beter weten in dat 'de wereld' gaat inzien dat polarisatie niets oplost. Een meer constructieve attitude zou ons veel verder brengen.

Referenties

(1) https://www.businessinsider.nl/topman-asml-kritisch-op-steeds-verder-gaande-exportbeperkingen-voor-china/

(2) https://nos.nl/artikel/2540868-asml-hard-onderuit-op-de-beurs-na-te-vroeg-verschenen-kwartaalcijfers

(3) https://www.aivd.nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity

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
Bianca Brooijmans
Alex Dingemanse
Marcel Feenstra
Maarten Hartsuijker
Fook Hwa Tan
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
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 2024 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

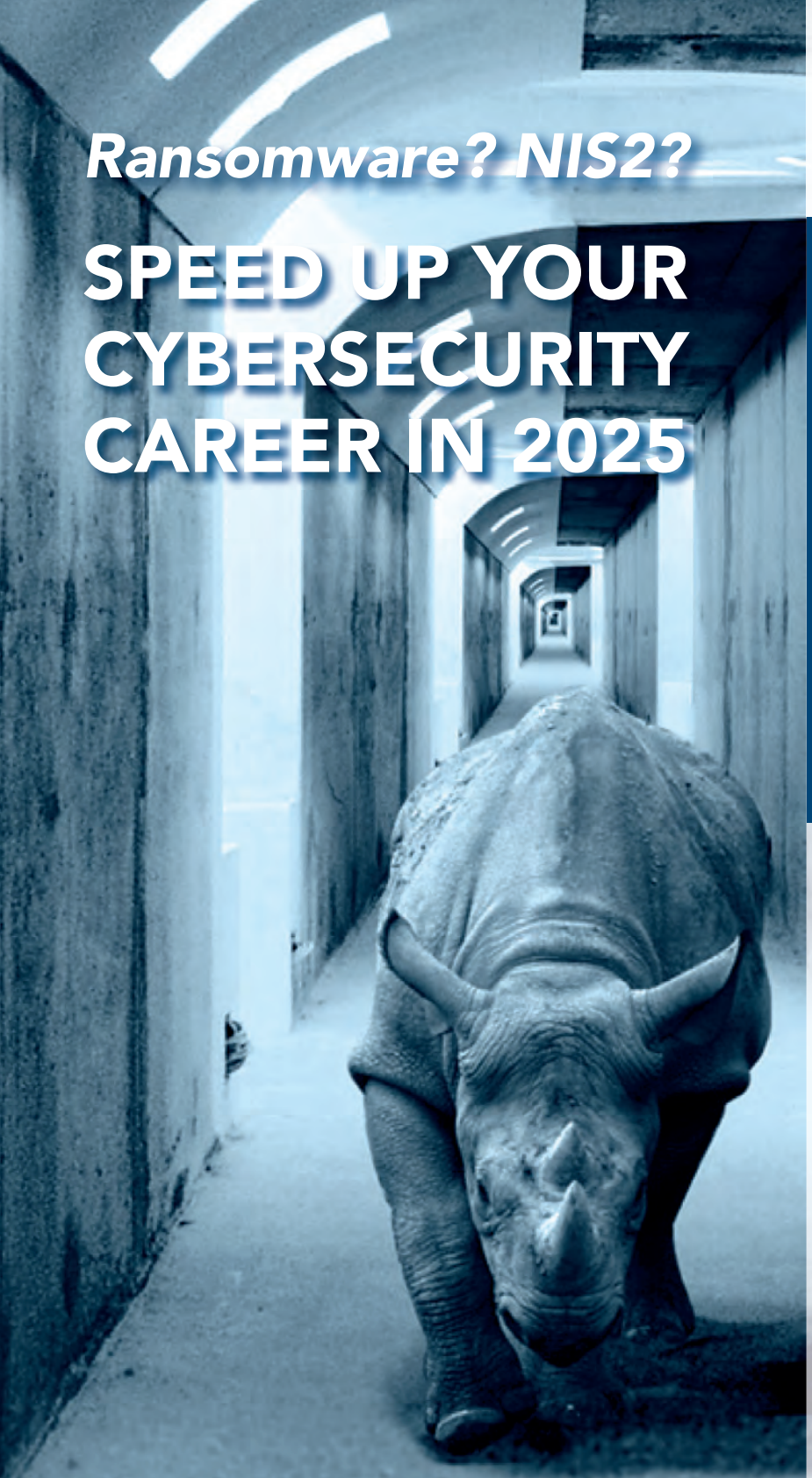
Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.

DNV



Ransomware? NIS2?

SPEED UP YOUR CYBERSECURITY CAREER IN 2025

Want security start bij mensen!!

TSTC
ICT en Security Trainingen

AIGP	Certified AI Governance Professional
CNIS2	Certified NIS2 Professional
BIO	Certified Bio Professional Foundation/Practitioner
OSCP	OffSec PEN-200
OSEE	OffSec EXP-401
CEH	Certified Ethical Hacker v13 AI

TSTC is een gerenommeerd IT opleidingsinstituut en erkend specialist in informatiebeveiliging en cybersecurity trainingen.

GET SKILLED
WWW.TSTC.NL

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 Offi cer

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 27001	Privacy Management

ONZE TRAININGEN ZIJN KLASSIKAAL OF LIVE ONLINE TE VOLGEN