INFORMATIEBEVEILIGING MAGAZINE

- Psychologie over CEO-fraude
- CISO @home
- Shared Research Programma Cybersecurity

JAARGANG 20 - 2020 - EDITIE 2

Vieze luchtjes

Nicole van Deursen

De redactie heeft een nieuwe hobby erbij: iB-Magazines snuiven. In 2019 was er namelijk een uitgave waar een 'vreemd luchtje' aan zat. De drukker heeft dit onderzocht. Het bleek inderdaad zo te zijn dat er iets aan de hand was: er zat een bacterie in het lakreservoir. Sindsdien snuffelen wij allemaal even aan de nieuwe uitgave om zeker te zijn dat alle processen nog steeds in orde zijn bij de leverancier. Informatiebeveiligers hebben blijkbaar een fijne neus voor afwijkingen.

Helaas kunnen we aan leveranciers van ICT-producten en diensten niet ruiken of ze hun zaken op orde hebben. Dat veel van ons daarmee worstelen bleek uit de grote opkomst van de PvIB-avond over 'Vendor risk management' op 5 februari. De presentaties gingen vooral in op het beheersen van risico's van leveranciers waar je al een relatie mee hebt.

Dat het een acuut en actueel onderwerp is, bleek ook begin januari weer toen de media met volle vaart doken op kwetsbaarheden in een veel gebruikte oplossing. Velen van ons werden met onze neus op de feiten gedrukt. Onze redactie bespreekt het in de rubriek 'Achter Het Nieuws'. Daarnaast denk ik dat het ook belangrijk is om kritisch te blijven kijken naar nieuwe producten en diensten die worden aangeboden. Verkopers proberen ons namelijk regelmatig wondermiddelen aan te smeren of ze presenteren gegevens in hun voordeel. Laat je dus niet bij de neus nemen en maak gebruik van de 'Bingokaart' in dit magazine als je iets hoort dat bijna te mooi is om waar te zijn. Soms ruikt iets moois gewoon niet goed.

Nicole

IN DIT NUMMER

Auteurs: Inge Wetzer & Elke Weijkamp zijn sociaal psycholoog Cybersecurity & Compliance. Zij ondersteunen organisaties door medewerkers weerbaarder te maken tegen cyberaanvallen, om zo informatieveiligheid te bevorderen.

Dit is het derde artikel van de drieluik 'Het meten van gedrag in de cybersecurity'

Psychologie over CEO-fraude

En waarom awareness niet voldoende is

Slachtoffer worden van CEO-fraude. Het is voor de meeste organisaties ondenkbaar en toch is het aan de orde van de dag. Er is eind 2019 zelfs een politieteam opgezet om deze vorm van criminaliteit te bestrijden. Niet alleen grote organisaties maar ook steeds meer kleine organisaties zijn hiervan namelijk de dupe. Schuldgevoelens en schaamte zijn vaak het resultaat. Vanuit de psychologie is te zien dat er verschillende factoren zijn die deze mogelijkheid van fraude in de hand werken.

In de eerste twee delen van dit drieluik werd uiteengezet dat er in de cybersecurity een kloof bestaat tussen awareness en gedrag. Ook werd toegelicht waarom vragenlijsten tekortschieten als het gaat over het meten van daadwerkelijk gedrag. Dit laatste deel van het drieluik richt zich op de specifieke casus van CEO-fraude. Het behandelt de verschillende aspecten die bepalen hoe kwetsbaar een organisatie is voor deze vorm van criminaliteit. Tevens laat het zien hoe groot het aandeel van de menselijke factor hierin is en wat een organisatie zou kunnen doen om zich hier beter tegen te wapenen.

Van awareness naar gedrag

Een recente overwinning voor psychologen: sinds een aantal jaren hoeven we geen lans meer te breken voor het belang van de mens in cybersecurity. Het nieuws en de ervaring hebben veelvuldig onderstreept dat een organisatie niet voldoende cyberveilig is wanneer er alleen aandacht wordt besteed aan het goed inrichten van het beleid en de techniek. Menselijk handelen veroorzaakt regelmatig datalekken, verstoringen of andere problemen. Nieuwer is het inzicht dat de initiatieven aan deze menskant verder moeten reiken dan alleen het bewust maken van de medewerkers, dus de 'awareness' verhogen (1). Zoals het eerste artikel uit dit drieluik liet zien, bestaat er een grote kloof tussen wat mensen wéten en wat ze daadwerkelijk doen (2). Om medewerkers daadwerkelijk weerbaarder te maken tegen cyberdreigingen, zal er dus gericht moeten worden op veilig gedrag als einddoel. Dat gaat verder dan bewustwording alleen. Gedrag is een stuk complexer dan awareness. De psychologische theorie van gedrag van MacInnis, Moorman & Jaworski (3) stelt dat gedrag bestaat uit motivatie, capaciteit en gelegenheid. Ofwel: gedrag vindt pas plaats als iemand het wíl doen, het kán doen en de kans krijgt om het te doen.

Het tweede deel van dit drieluik lichtte toe waarom vragenlijsten tekortschieten wanneer het gaat om het meten van cyberveilig gedrag (4). Dit liet zien dat de zelfrapportage in vragenlijsten vaak aangeeft wat iemands intentie is, maar dat daadwerkelijk gedrag nog iets anders is. Om het drieluik compleet te maken zal in dit laatste deel ingezoomd worden op een concreet geval van cybercriminaliteit: CEO-fraude. Dit voorbeeld onderstreept zeer duidelijk de standpunten uit het drieluik.

CEO-fraude

CEO-fraude is op dit moment één van de meest voorkomende vormen van internetcriminaliteit. Echter, wanneer mensen in een vragenlijst worden gevraagd of zij geld zouden overmaken naar een onbekende rekening, of geld zouden overmaken zonder dat hierbij gebruik is gemaakt van het vereiste vier ogenprincipe, antwoorden zij veelal 'nee'. Een mooie illustratie van het feit dat wéten wat veilig is en de intentie hebben om het goede te doen, niet voldoende zijn.

CEO-fraude is een misleidende term. Veelal wordt met behulp van social engineering een medewerker in de organisatie beïnvloed om een financiële transactie te verrichten of een rekeningnummer aan te passen. Het is dus niet de CEO die fraudeert, maar het lijkt alsof de CEO telefonisch of per mail een opdracht geeft om een dergelijke transactie uit te voeren. Hierbij wordt vaak zeer zorgvuldig te werk gegaan. Te denken valt aan vervalste (digitale) handtekeningen of een gespooft telefoonnummer. Recentelijk was zelfs in het nieuws dat een bedrijf

was opgelicht door een telefoontje met een stem die klonk als de stem van de CEO (5). Om tegen dergelijke aanvallen weerstand te bieden is technisch veel mogelijk, maar uiteindelijk gaat het erom hoe de medewerker handelt. De kwetsbaarheid zit dus voor een groot deel ín de eigen organisatie.

`CEO-fraude is een vorm van financieel economische criminaliteit die al decennia speelt. Toch is het tegenwoordig aan de orde van de dag en worden medewerkers op steeds geavanceerdere wijzen verleid tot het doen van onterechte betalingen. Er wordt voorafgaand aan de diefstal vaak uitgebreid onderzoek naar het slachtoffer alsook naar de organisatie gedaan. Het is volgens Hoffmann een van de meest voorkomende vormen van internetcriminaliteit. De gevolgen zijn veelal groot en onomkeerbaar, zowel voor het slachtoffer als financiële en imagoschade van de organisatie. CEO-fraude wordt door buitenstaanders vaak als onmogelijk en onbegrijpelijk bestempeld. Mensen durven er nauwelijks over te praten wanneer het hen is overkomen, verhalen worden niet of anoniem gedeeld. Bestuurders begrijpen het niet: hoe kan dit bij hún organisatie gebeuren? Toch vormen zij zelf veelal het grootste gevaar. Dit geeft problemen, maar net zoveel kansen om gewenst gedrag (preventief) te stimuleren en het gevaar tegen te gaan' (6).

Inmiddels zijn er meerdere grote zaken van CEO-fraude in de media gekomen en wordt er binnen organisaties aandacht aan besteed. Dat het gebeurt, weten veel mensen dus wel. Toch betekent dat bewustzijn niet dat CEO-fraude op zijn retour is. Sterker nog: Hoffmann ziet het aantal CEO-fraude gevallen nog altijd toenemen. Een toename die gepaard gaat met steeds geavanceerdere methoden. De wereldwijde schade wordt geraamd op zo'n 9 miljard dollar. Ondanks de grotere awareness moeten we toch verder gaan kijken naar de oorzaken.

De psychologie over CEO-fraude

De psychologie laat zien dat gedrag van medewerkers mede wordt bepaald door de cultuur en het voorbeeldgedrag vanuit het management. Wanneer gekeken wordt naar organisaties, blijkt dat onder andere cultuur en leiderschap een belangrijke bron vormen voor het kunnen en durven uiten van fouten, het open durven en mogen zijn en niet te handelen vanuit angst en stress. Tevens blijkt dat organisaties die te maken krijgen met CEO-fraude veelal internationaal georiënteerd zijn (waarbij er sprake is van verscheidene managementlagen) en dat hiërarchie een grote rol speelt. Kwetsbaarheid voor CEO-fraude is ook groter wanneer de beslissingsbevoegdheid hoog in de organisatie zit. Tevens vormen de benoeming van de CEO zonder inspraak van het MT en langdurige dienstverbanden van de CEO kwetsbaarheden. Dit kan er onder

andere toe leiden dat de objectiviteit ten aanzien van deze persoon verminderd is. Er wordt weleens gesproken over 'de gouden handboeien'.

Ook is er vaak sprake van een grote afstand tussen de (dominante) CEO en de rest van de organisatie. Dit is veelal terug te zien in de stijl van leidinggeven door de gehele organisatie: de organisatie kenmerkt zich door een machtige hogere hiërarchische positie van waaruit besluiten top-down worden genomen. Een machtsafstand kan normen van ongelijkheid benadrukken (7). De organisatie draait om het leveren van prestaties in een zo kort mogelijk tijdsbestek, krachtig zijn en laten zien dat je beslissingen durft en kunt nemen (ofwel onzekerheidsvermijding). In deze organisaties worden fouten niet openlijk gedeeld, kwetsbaarheid niet getoond en feedback nauwelijks gegeven. Tenslotte is men zich meestal niet of nauwelijks bewust van het risico dat zij zelf lopen op externe CEO-fraude, terwijl tegenwoordig eerder de vraag kan worden gesteld wannéer het gebeurt dan óf het gebeurt.

Voorspellende factoren

Wat kan een organisatie doen om zich beter te wapenen tegen CEO-fraude? De eerste stap bestaat uit het in kaart brengen van de kwetsbaarheden van een organisatie. Hierboven zijn al een aantal factoren aangehaald die een organisatie kwetsbaar maken. Door dergelijke kwetsbaarheden structureel in kaart te brengen, kan voor een organisatie worden ingeschat hoe groot de kans op CEO-fraude is. Tevens geeft het handvatten voor maatregelen die de organisatie weerbaar maken, omdat het blootlegt welke factoren deze kwetsbaarheid bepalen.

Wederom kan de psychologie ingezet worden om deze voorspellende factoren te definiëren. Het bekende model van Hofstede (8) over culturele dimensies is vertaald naar organisaties. Zo geeft het inzicht in zes dimensies die de cultuur van een organisatie definiëren, en daarmee ook de kwetsbaarheid voor CEO-fraude voorspellen (9)(10). Deze zes dimensies worden hieronder besproken.

1. Procesgericht versus resultaatgericht

Een procesgerichte organisatie legt nadruk op hoe de medewerkers met zaken omgaan. Een resultaatgerichte organisatie legt de nadruk op wat de medewerkers bereiken. In een resultaatgerichte organisatie is men geneigd om meer risico te nemen dan in een procesgerichte organisatie. Wanneer het gaat om CEO-fraude lopen resultaatgerichte organisaties meer risico om slachtoffer te worden. Immers, het resultaat telt en dan kan het dat men omwille van dit resultaat het risico neemt om van een bepaalde procedure af te wijken. Dit in tegenstelling tot een procesgerichte organisatie, waar men juist is gericht op het correct naleven van de procedure.

2. Mensgericht tegenover werkgericht

In de tweede dimensie staan mensgerichte organisaties ten opzichte van werkgerichte organisaties centraal. Bij mensgerichte organisaties heeft men het idee dat er rekening wordt gehouden met de persoonlijke omstandigheden van medewerkers en dat de organisatie verantwoordelijkheid neemt voor hun welzijn. Bij werkgerichte organisaties gaat het daarentegen voornamelijk om het werk dat af moet. Dit kan soms ook ten koste van het welzijn van medewerkers zijn. Deze dimensie is veelal gerelateerd aan de manier van leidinggeven en de algehele visie van de organisatie. Durft men twijfels te tonen? Organisaties die meer werkgericht zijn, zijn kwetsbaarder voor CEO-fraude omdat mensen zich als persoon minder gezien en gehoord voelen. Het draait om het werk dat men aflevert dat veelal gepaard gaat met een resultaatgerichte handelswijze.

3. Organisatiegebonden versus professioneel

Bij organisatiegebonden organisaties wordt de identiteit van de medewerkers sterk gekoppeld aan het onderdeel zijn van de desbetreffende organisatie, los van de invulling van de functie. Zij identificeren zich vaak sterk met de directeur en leidinggevenden. Deze medewerkers zijn veelal korte termijn gedreven en hebben een interne werkfocus. Daarbij is het vooral belangrijk om hetzelfde te zijn als de andere medewerkers van de organisatie. Dit maakt hen gevoelig voor CEO-fraude, omdat zij niet snel willen en zullen afwijken van de sociale norm. Als die sociale norm betekent dat men de CEO moet helpen, zal men hier veelal snel stappen in ondernemen. Voor medewerkers van professioneel ingestelde organisaties is deze kans kleiner, omdat zij hun identiteit veel minder koppelen aan sociale normen. De meer formalistische grondslag van deze organisaties maakt dat medewerkers zich meer richten op de daadwerkelijke taak/rol die zij vervullen waarin verwacht wordt veel zelf en vooruit te denken en actief wordt gevraagd om kritisch te zijn.

4. Open versus gesloten organisaties

De vierde dimensie betreft de toegankelijkheid van een organisatie. Uit de praktijk blijken gesloten organisaties

gevoeliger te zijn voor CEO-fraude dan organisaties waar binnen een open organisatiecultuur van toepassing is. Bij een open organisatie is het eenvoudig voor nieuwkomers om zich snel thuis te voelen. Bij gesloten organisaties staat juist het tegenovergestelde centraal, voor nieuwkomers is het niet eenvoudig om tussen de andere medewerkers te komen. Collega's, inclusief management, handelen gesloten en soms zelfs geheimzinnig. Hierbij speelt ook hiërarchie vaak een prominente rol. Door deze manier van handelen is de kans op fraude groter bij gesloten organisaties, dan bij open organisaties waar eenieder geen belemmeringen voelt om zaken te bespreken.

5. Strakke controle ten opzichte van losse controle

Deze dimensie verwijst naar de mate van interne structuur en controle. Medewerkers van organisaties met een strakke controle hebben veelal een sterke mate van discipline, zijn zich bewust van de kosten en zijn punctueel. Zij spreken ook buiten het werk om serieus over het bedrijf en de bijbehorende werkzaamheden. Deze medewerkers staan in contrast met medewerkers van organisaties waarin losse, ofwel minder, controle de boventoon voert. Hier werken medewerkers niet volgens een vaste discipline en is men zich niet altijd bewust van kosten. Het gebrek aan voorspelbaarheid is veelal terug te zien in de improvisatie en verrassingen binnen de werkzaamheden van deze medewerkers. Uit de zaken van het verleden is zichtbaar dat organisaties met losse controles vatbaarder zijn voor CEO-fraude, juist door het gebrek aan controle en vaste structuren.

6. Pragmatisch versus normatief ingesteld

Bij de laatste dimensie komt ook het volgen van vaste procedures naar voren, maar speelt voornamelijk ethiek een belangrijke rol. Pragmatisch ingestelde organisaties zijn veelal gevoeliger voor fraude, omdat zij erg extern gericht zijn en tegemoet willen komen aan de wensen van de klant, waarbij resultaten belangrijker zijn dan het volgen van de juiste procedures. Dit gaat in veel gevallen gepaard met een flexibele handelswijze ten opzichte van ethiek. Dit heeft ook vaak te maken met de enorme concurrentie waarmee deze organisaties te maken hebben. Bij normatief ingestelde organisaties staat het correct toepassen van procedures juist centraal, die opgezet zijn vanuit de hoge normen van ethiek en eerlijkheid. Hierbij staat een nuttige bijdrage leveren aan de samenleving hoog in het vaandel. Zij hebben veelal minder concurrentie vanwege de wettelijk aan hen opgedragen taken.

Van inzichten naar maatregelen

Op het moment dat duidelijk is dat een organisatie een zwakke plek heeft voor CEO-fraude, kan dit worden omgezet naar maatregelen. Het specifiek analyseren van de verschillende dimensies voor een organisatie geeft inzicht in de kwetsbare factoren. Wanneer deze helder zijn, kan worden gekeken of en op welke manier deze kunnen worden veranderd. Concrete maatregelen kunnen leiden tot een vermindering van de kwetsbaarheid, zolang men maar zeer gericht weet waaróp men moet sturen. Dit betreffen maatwerkoplossingen op het gebied van de organisatie, de techniek én de mens.

Referenties

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

(2) Wetzer, I. M., & Weijkamp, E. (2019). Een psychologische benadering van awareness in cybersecurity: Medewerkers geven hun wachtwoord niet weg via de telefoon, toch? InformatieBeveiliging, 19(6), 26-29.

(3) MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

(4) Wetzer, I. M. (2020). Psychologen over het meten van gedrag in cybersecurity. En waarom vragenlijsten te kort schieten. InformatieBeveiliging 20(1), 4-8.

(5) BNR (2019, 3 september). Oplichters gebruiken nu de stem van je baas. Geraadpleegd van http://www.bnr.nl/nieuws/technologie/10388515/oplichters-gebruiken-nu-de-stem-van-je-baas

(6) Weijkamp, E. & Van Esch, M. (2019). Het grootste gevaar voor CEO-fraude vormt u als bestuurder zelf. 1-5.

(7) Fikret Pasa, S., Kabasakal, H., & Bodur, M. (2001). Society, organisations, and leadership in Turkey. Applied Psychology, 50(4), 559-589. MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

(8) Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Thousand Oaks, CA: Sage Publications.

(9) Sanders, G., & Neuijen, B., (1999). Bedrijfscultuur. Uitgeverij Van Gorcum.

(10) Hofstede, G., Hofstede G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind. Revised and Expanded 3rd Edition. New York: McGraw-Hill.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Toss a coin to your techie

Deze column is een ode aan de mensen die privacy echt mogelijk maken. De helden zonder cape die vaak in vergeten hoekjes in bedrijven hun eigen wereld hebben ingericht. Daar onverstoorbaar creatief zijn en er niet alleen voor zorgen dat alles blijft draaien. Maar zij vooral ook de rots in de branding te zijn als privacy-eisen allerlei praktische kopzorgen opleveren.

Met mijn team privacy officers ga ik over het WAT. Wij geven advies over de regels bij privacy. Welke spelregels in specifieke situaties gelden, welke voorwaarden gesteld moeten worden voordat je iets mag gaan doen of maken en zo nu en dan ook duidelijk en helder communiceren over wat nu juist niet mag. Het WAT is niet altijd heel makkelijk te vinden omdat de wet ruimte laat voor interpretatie of omdat de praktijk toch echt even wat anders in elkaar zit dan de wet 'zo makkelijk' doet voorkomen. Dat laatste komt natuurlijk ook vaak omdat schrijvers van de wet (net als de handhavers ervan) niet altijd weten hoe het er in de praktijk nu echt aan toe gaat. Maar dat terzijde.

Na het WAT zit onze taak er grotendeels op. Ik zeg grotendeels, omdat je als rechtgeaarde liefhebber van privacy natuurlijk niet zomaar iets over de schutting gooit. Dan weet je zeker dat de regel die je stelde niet opgevolgd gaat worden. Maar het HOE moet je toch echt uit handen geven aan de mensen die moeten zorgen dat de wet en de regel netjes geïmplementeerd worden. En daar, precies op dat punt, vind je de helden.

De techies. Het is een speciaal soort techie, die in staat is te luisteren naar de privacy officer (en misschien toch zelf ook wel veel van privacy houdt). En creatief meedenkt om ervoor te zorgen dat de regel goed in praktijk gebracht wordt met zo min mogelijk negatieve impact voor de bedrijfsvoering. Als dat er onverhoopt toch is, dan is deze techie in staat om het proces zo te begeleiden dat iedereen tevreden naar het eindpunt komt. Soms met prachtige kunstgrepen en als het echt niet anders kan, dan is deze techie in staat om de boel af te breken en opnieuw te beginnen. Deze keer wel de regels indachtig.

Deze column is voor jou Karen. Deze column is voor jou Dennis. Deze column is voor jou Jesse. Jullie zijn onmisbaar in elk bedrijf en jullie zijn de helden voor ons als privacypeeps. We zeggen het misschien niet vaak genoeg, maar zonder jullie kunnen we ons werk niet doen en we zijn jullie vreselijk dankbaar voor de praktische vertaling van onze privacyregels.

Rachel

Nicole van Deursen is hoofdredacteur van iB-Magazine. Nicole is bereikbaar via nicolevandeursen@hotmail.com

Bullshitbingo

Er is een cyberoorlog gaande, maar het aantal cybersecurityincidenten door aanvallen van buiten neemt af. Het is zelfs zo dat bedrijven steeds meer beveiligingsmaatregelen treffen: maar liefst 6 op z'n minst! De toekomst ziet er ook rooskleurig uit: er bestaan immers diverse oplossingen voor onze problemen, waaronder Time AI. In een tijd waarin sensatie, nepnieuws en pseudowetenschap snel verspreid worden en soms lastig te herkennen zijn, moeten we ons kritisch opstellen. De bullshitbingokaart kan je daarbij helpen.

In 2017 ging er een schok door onze wereld. Bill Burr, die in 2003 de richtlijn schreef voor NIST voor het hanteren van complexe wachtwoorden, liet in een interview met de Wall Street Journal weten spijt te hebben van zijn advies. In de tijd dat hij de richtlijn schreef, was er niet veel onderzoeksdata over wachtwoorden beschikbaar om daar enig advies op te baseren.

Omdat hij onder druk stond, baseerde hij zich op documenten uit de jaren 80, dus nog voor de massale omarming van het internet. Het zelfbedachte advies om hoofdletters, nummers en tekens te gebruiken en om deze elke 90 dagen te veranderen, werd wereldwijd overgenomen. Jarenlang bleef dit de standaard. Vandaag de dag is er veel meer onderzoeksdata beschikbaar over wachtwoorden. Op basis van die nieuwe kennis heeft NIST in 2017 de richtlijn aangepast. Toch zijn er anno 2020 nog steeds experts die vasthouden aan verouderd beleid voor wachtwoorden. Waarom prediken deze slimme mensen niet de nieuwste richtlijnen?

Een mogelijke verklaring daarvoor is dat overtuigingen moeilijk te veranderen zijn. Door jarenlange herhaling van het advies door invloedrijke personen krijgt het de status van waarheid. Mensen beoordelen de kwaliteit van nieuw en tegenstrijdig bewijs met argwaan. Bovendien zijn hoger opgeleide mensen vaak moeilijker te overtuigen van hun ongelijk. We krijgen last van een cognitieve illusie: we vertrouwen blind op wat we denken te weten, ook al is er genoeg bewijs van het tegenovergestelde. Maar onze natuurlijke argwaan kan in andere gevallen juist in ons voordeel werken om ons te beschermen tegen zeperds en charlatans.

Wondermiddelen

In augustus 2019 ontstond op de Black Hat-conferentie een relletje tijdens een presentatie van een commercieel bedrijf. Twitter ging los en er werd gejoeld in de zaal. Het bedrijf presenteerde een nieuw type encryptietechnologie, gebaseerd op eigen onderzoek en publicaties. De kritiek op de gepresenteerde oplossing was niet mals en Black Hat haalde de publicatie van de presentatie van hun website af. Hierop volgde een aanklacht door het bedrijf aan het adres van de Black Hat-organisatie. De partijen zullen dit in de rechtszaal verder gaan uitvechten.

Er waren diverse indicaties die de argwaan tegen de gepresenteerde 'Time AI' aanwakkerden. Bruce Schneier somt een aantal hiervan op in zijn blog (1). Wanneer een expert of een bedrijf bijvoorbeeld iets nieuws aanprijst en daarbij gebruik maakt van 'gobbledygook' (koeterwaals vol met onbegrijpelijke technische termen), dan kan dat een techniek zijn om iets leegs met ingewikkeld klinkende woorden te verhullen. De oplossing klinkt dan echt heel fantastisch. Als je op internet gaat zoeken, kun je zelfs 'gobbledygook generators' vinden. Die maken mooie teksten voor je zoals: 'We need a more contemporary reimagining of our dotcom relative contingencies.' Een Nederlandstalige generator heb ik nog niet kunnen vinden. Handig als afleidingsmanoeuvre om de luisteraar weg te trekken van de inhoud. Als je dit soort teksten hoort in een serieuze presentatie, moet je alert zijn. Wanneer een persoon niet op een begrijpelijke manier kan uitleggen hoe iets werkt, is dat hoogstwaarschijnlijk een indicatie dat a) het niet werkt, of b) hij niet begrijpt hoe het werkt.

Een andere indicator was de zogenaamde publicatie van wetenschappelijke papers. Wanneer een bedrijf zelf een paper publiceert, geschreven door wetenschappers, dan is dat geen wetenschappelijk paper. Een wetenschappelijk paper telt pas als het in een respectabele uitgave wordt gepubliceerd, na een grondig reviewproces door minimaal 3 andere wetenschappers. Aan de hand van het reviewproces wordt de methode die is gevolgd gecontroleerd en wordt de dataset nog nagekeken. Ook eerdere presentaties op wetenschappelijke conferenties zeggen niet altijd wat over de kwaliteit van een nieuwe uitvinding: er bestaan namelijk ook nepconferenties. Je kunt hierover op YouTube een vermakelijke presentatie uit 2018 terugkijken (2), waarbij journalisten een 'wetenschappelijk' paper lieten maken door een gobbledygook generator. De paper werd geaccepteerd door een 'wetenschappelijke' conferentie en de 'auteurs' mochten het komen presenteren. De conferentie bleek een oplichting te zijn, maar de journalisten hadden hierdoor wel een wetenschappelijke publicatie op hun naam staan. Tenslotte moet je ook altijd alert zijn wanneer je weet dat een bedrijf betaalt om hun product ergens te mogen promoten, zoals het geval was met de Time AI. Reclame heet dat, niet wetenschap.

Onderzoek

Wie gebruikt er niet wel eens een statistiek om indruk te maken of om een argument kracht bij te zetten? Een grafiek of een citaat met een percentage oogt vaak wel goed in de presentatie of managementrapportage. Statistieken kunnen nuttig zijn om een verschijnsel te verklaren, een verandering aan te tonen, beleidsbeslissingen te nemen of om financiële keuzes te maken. Binnen ons vakgebied kunnen statistieken gebaseerd zijn op data uit de eigen organisatie: KPI's, auditbevindingen, incidentenregistraties of logbestanden.

Statistieken gebaseerd op data uit meerdere organisaties worden vaak gepresenteerd door commerciële aanbieders van securitydiensten of -producten. De statistieken beschrijven vooral waargenomen gebeurtenissen en trends in staafdiagrammen en tabellen. Onderzoeksbureaus houden enquêtes of interviews, of combineren data uit verschillende onderzoeken. Bedrijven presenteren de waarnemingen uit hun klantenbestand vaak alsof deze voor alle organisaties in de wereld gelden en gebruiken de cijfers om aan te sporen tot actie op korte termijn. De brongegevens worden meestal niet gedeeld vanwege vertrouwelijkheidseisen en dus zijn de resultaten niet te controleren. Toch kun je door kritisch te kijken zelf je conclusies trekken over de betrouwbaarheid en relevantie van statistieken.

Recentelijk kwam ik enkele voorbeelden tegen waarin argumenten en statistieken als feiten werden gepresenteerd. In dit artikel gaat het erom de lezer mee te nemen in het kritisch lezen en niet om de betreffende organisaties en personen in een slecht daglicht te zetten. Daarom noem ik de bronnen niet. Elke gelijkenis met echte publicaties berust echter niet op toeval.

`IoT device attacks up by 600%'

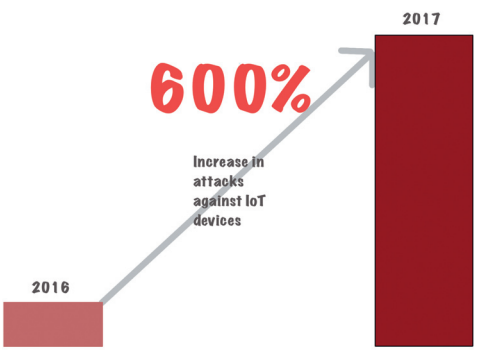
Bovenstaande uitspraak kwam ik tegen op een blog uit 2018. De blog was een review van een publicatie van een securitydienstverlener waarin een boel statistieken stonden. Een stijging van 600% klinkt indrukwekkend. Dat staat goed wanneer je het management wil overtuigen van het belang van IoT-securitymaatregelen. Maar wat staat hier nu echt?

Ten eerste kon ik deze uitspraak van de blogger niet terugvinden in het rapport waarover hij zei te schrijven. Waar haalt hij dat getal dan vandaan? Bij de blog staat geen auteur vermeld. Hierdoor is niet te controleren of de schrijver een goede reputatie heeft. Ook was het niet mogelijk om de schrijver te benaderen om te vragen waar hij die 600% vandaan heeft gehaald.

Dan is er de vraag wat de tekst precies betekent. Wat is een `attack'? Is dat elke poging om een IoT device te verstoren of alleen elke geslaagde poging? Bovendien weten we nooit zeker wat men bedoelt met een IoT device: gaat het hier om alleen een apparaat, zoals een thermostaat of beveiligingscamera, of gaat het om het totaal van componenten in een netwerk waarmee het apparaat is verbonden?

Een online zoektocht heeft me wel bij de bron gebracht van de 600%. Het was een jaaroverzicht van een andere securitydienstverlener. De blogger heeft dus een fout gemaakt in zijn bronvermelding: dit is de reden waarom je nooit een citaat van een citaat moet overschrijven.

Bovendien ging het om data uit een steekproef van één honeypot die het bedrijf zelf had opgezet, waarbij het dus nog maar vraag is of deze steekproef voldoende is om de data te generaliseren tot alle IoT-netwerken. Toch publiceert de organisatie het volgende: `(…) found a 600 percent increase in overall IoT attacks in 2017.' Er staat zelfs een grafiek bij om het argument visuele kracht bij te zetten. Echter, de grafiek laat helemaal geen cijfers zien en de tekst in het hoofdstuk geeft ook geen uitleg van deze berekening. In een poging om het getal van 600% te controleren heb ik het rapport over 2016 opgezocht. De data in het 2017 rapport zijn anders gepresenteerd dan die in het 2016 rapport, dus het is voor de lezer niet te achterhalen waar de 600% vandaan komt en hoe die moet worden geïnterpreteerd. Ook wordt niet uitgelegd of de honeypot sinds 2016 gewijzigd is en of de genoemde scans ook daadwerkelijk een aanval zijn waarbij (al dan niet succesvol) is geprobeerd om de systemen te beïnvloeden of dat het om `inventariserende' scans gaat.



Figuur 1 - Nagetekende versie van de originele grafiek.

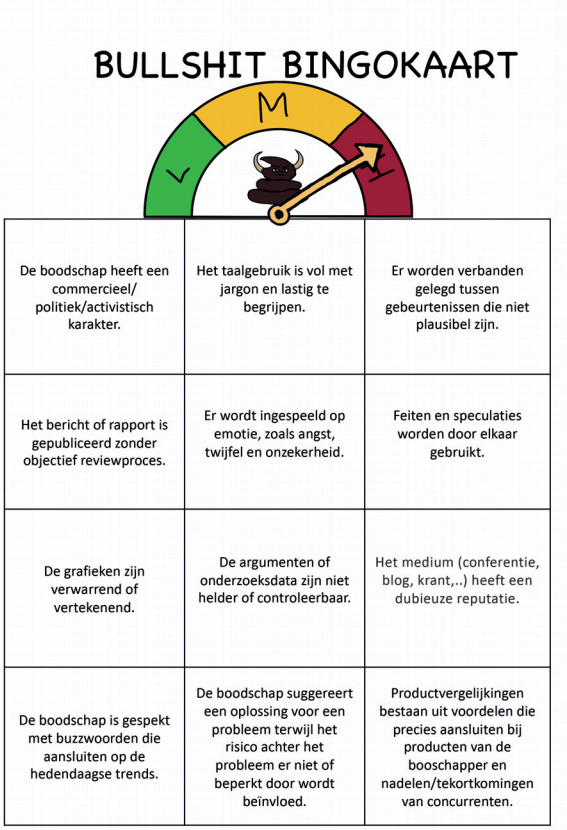
Een ander voorbeeld van onhandig gebruik van cijfers komt van een organisatie die in een persbericht enthousiast stelt dat het aantal ICT-veiligheidsincidenten door een aanval van buitenaf daalt. Dat is een interessante tegenhanger van het vorige voorbeeld waarin juist een 600% stijging van een specifieke soort aanval van buitenaf werd gerapporteerd. Het persbericht gaat over een nieuw onderzoeksrapport. Een opvallend punt in dit rapport zijn de gelegde

causale verbanden tussen cijfers en mogelijke verklaringen. Zo wordt bijvoorbeeld waargenomen dat grote bedrijven meer incidenten registeren dan kleine bedrijven. Dit wordt toegeschreven aan de complexere ICT-infrastructuur. Zij zijn daardoor een interessanter doelwit voor cybercriminelen. De auteurs gaan echter voorbij aan de mogelijkheid dat grote bedrijven meer ICT-middelen te beheren hebben en dat zij misschien professioneler zijn in het detecteren, registreren en rapporteren van incidenten dan kleine bedrijven.

Hetzelfde rapport jubelt ook dat bedrijven steeds meer maatregelen nemen om zich te weren tegen cyberaanvallen. Een kwart van de bedrijven neemt zelfs minstens 6 maatregelen. Maar hoeveel is eigenlijk '6 maatregelen'? Ben je met 6 maatregelen dan goed bezig? Als ik kijk naar de woorden die zijn gebruikt om de maatregelen te beschrijven, dan is men in dit rapport appels met peren aan het optellen. Een maatregel zoals 'encryptie voor het versturen van data' kun je niet optellen bij een maatregel die heet: 'risicoanalyses'. Een risicoanalyse is wellicht zelfs geen maatregel, maar eerder een instrument om over maatregelen te beslissen. Bovendien zegt het aanwezig zijn van een maatregel niets over het effectieve gebruik ervan binnen de organisatie. De maatregel die het beste scoort is 'anti-virussoftware'. In het rapport wordt verklaard dat dat mede komt omdat in Windows 10 de anti-virussoftware al is ingebouwd. Ook hier wordt een causaal verband gelegd waarvan het de vraag is of het plausibel is.

Emoties

Sommige publicaties of uitspraken over cybersecurity maken misbruik van het gebrek aan kennis bij het algemene publiek. Er wordt dan ingespeeld op gevoelens (zoals onveiligheid, angst en dreiging) om wederom een noodzaak te creëren. Emotie (denk aan angst of liefde) is vaak sterker dan logica. Dit zie je onder andere terug bij marketingcampagnes, phishingmails, persoonlijke adviseuses, politici, of in rapportages over cybersecurity-incidenten en -aanvallen. Gevoelens worden dan gepresenteerd als feiten of feiten en speculaties worden door elkaar gebruikt: 'We have groups wondering why the FBI never took the server. Why haven't they taken the server? I've been wondering that' (3). Andersom kunnen feiten op zo'n manier worden gepresenteerd dat maximale impact op het gevoel ontstaat: 'Klik nu hier anders sluiten we je account af!'



Figuur 2 – Bullshitbingokaart.

Waakzaamheid

Als vakmensen hebben wij veel kennis en staan we open voor nieuwe ontwikkelingen. Toch moeten we altijd waakzaam zijn bij het lezen van rapporten of het aannemen van adviezen. In dit artikel zijn enkele tips gegeven voor het beoordelen of een bericht nepnieuws, desinformatie of onzinnig is. Ik heb ze samengevat in een bullshitbingokaart. Hoe meer vakjes je kunt aankruisen, hoe groter de kans dat je gelijk hebt wanneer je instinctief twijfelt aan een bericht.

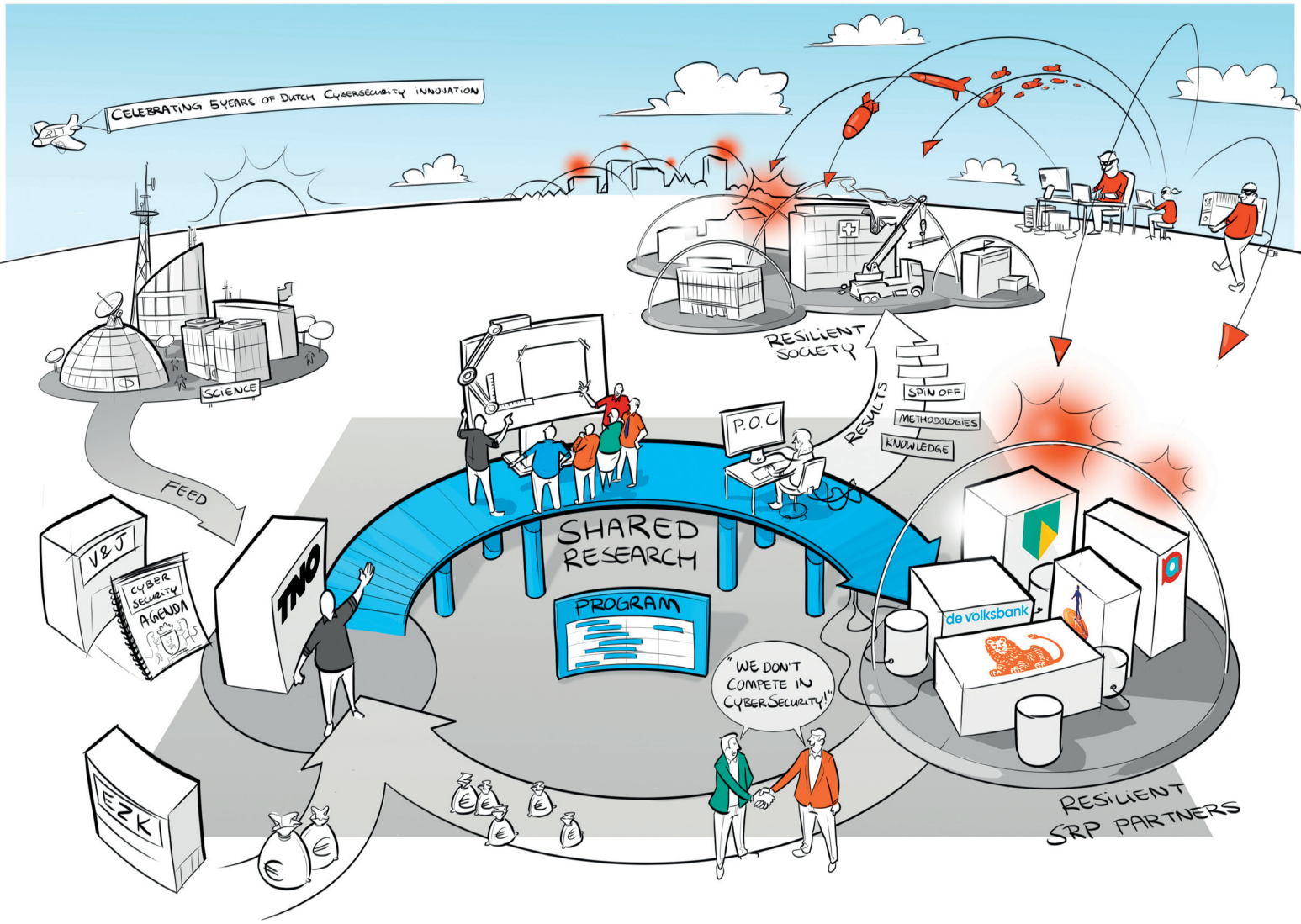
Referenties

(1) Bruce Schneier, The Doghouse. Blogpost op Schneier on Security, gepost op 5 september 2019: https://www.schneier.com/blog/-archives/2019/09/the_doghouse_cr_1.html

(2) DEF CON 26 - Svea, Suggy, Till - Inside the Fake Science Factory. Gezien op YouTube: https://www.youtube.com/watch?v=ras_VYgA77Q

(3) Trump/Putin Helsinki Press conference July 2018: https://www.youtube.com/watch?v=cwxqOolyWm0 (minuut 39:11)

Auteurs: Richard Kerkdijk is werkzaam bij TNO. Richard is bereikbaar via richard.kerkdijk@tno.nl. Maarten Jak is werkzaam bij ING. Maarten is bereikbaar via maarten.jak@ing.com. Reinder Wolthuis is werkzaam bij TNO. Reinder is bereikbaar via reinder.wolthuis@tno.nl. Rick van der Kleij is werkzaam bij TNO. Rick is bereikbaar via rick.vanderkleij@tno.nl. Bart Gijsen is werkzaam bij TNO. Bart is bereikbaar via bart.gijsen@tno.nl.



Shared Research Programma Cybersecurity

Het is alweer meer dan twee jaar geleden dat dit magazine aandacht besteedde aan het Shared Research Programma Cybersecurity (SRP). In 2019 is het eerste SRP-lustrum gevierd met een event in Utrecht en is het tweede SRP-magazine verschenen (1). Het is nu een goed moment om een update te geven over hoe het SRP zich heeft ontwikkeld en om een drietal projectresultaten toe te lichten.

Door: Reinder Wolthuis (TNO)

In 2018 heeft ook de Volksbank zich aangesloten. TNO werkt dus met drie grootbanken (Rabobank, ABN AMRO en ING), Achmea en de Volksbank samen om de Nederlandse samenleving te wapenen tegen cyberaanvallen van vandaag en morgen. Het doel is het creëren van een veilige en veerkrachtige digitale samenleving door innovatie op het gebied van cybersecurity. De belangrijkste voordelen van de samenwerking in het SRP zijn een 'shared workload', 'shared data' en 'shared funding'. Met andere woorden: de partners zijn actief in de projecten betrokken, delen (geanonimiseerde) data om ontwikkelde innovaties te evalueren en hebben een aandeel in de financiering. Ook de Nederlandse overheid levert een aanzienlijke financiële bijdrage.

Menselijke factor

Nieuw sinds 2017 is dat de menselijke factor uitdrukkelijker in het onderzoeksprogramma aan bod komt. Aangezien de mens een belangrijke rol speelt in de cyberverdediging is het belangrijk om meer inzicht te creëren in hoe de mens (in de rol van slachtoffer, verdediger dan wel aanvaller) denkt, handelt en kan worden beïnvloed.

Wat gebleven is, zijn de mooie projecten met mooie resultaten die over een breed palet van securitygebieden de beheersing over cyberrisico's en -verdediging tegen aanvallen verbeteren. Die resultaten bestaan uit nieuwe en betere inzichten, methodieken of tools.

Deze resultaten worden zo breed mogelijk gedeeld.

Er wordt op dit moment gesproken over de programma-invulling in de komende jaren. Daarin ligt nog meer de nadruk op open samenwerking met andere partijen, snel kunnen acteren op ontwikkelingen in de omgeving, een structureel en continu innovatiemanagementproces en veel communicatie naar en zichtbaarheid in de maatschappij. Nadrukkelijk worden hierbij ook partijen uitgenodigd om aan te sluiten, expliciet ook uit andere sectoren dan de financiële sector.

Hieronder drie inhoudelijke resultaten vanuit het SRP-cybersecurity:

- het cybergedrag van bankmedewerkers;
- self-healing;
- threat landscaping.

Meer informatie is op de website te vinden (2).

Door: Rick van der Kleij (TNO)

Cybergedrag van bankmedewerkers

Banken nemen geavanceerde technische maatregelen om cybercriminaliteit buiten de deur te houden. In het verleden is gebleken dat technische maatregelen alleen niet voldoende zijn om criminaliteit of cyberincidenten te voorkomen. Incidenten vinden hun oorsprong veelal in het gedrag van medewerkers. Zo is bekend dat een groot deel van medewerkers hun wachtwoorden hergebruiken (50-

Medewerkers maken vaak bewust de keuze om bestanden niet te versleutelen

60%) of delen (30-95%). Dit maakt de banksystemen kwetsbaar voor hacking. Om de digitale veiligheid van banken te vergroten is het dus van belang dat er ook wordt gekeken naar het gedrag van de eigen medewerkers.
De meest gebruikte manieren om medewerkers te motiveren om zich cyberveilig te gedragen zijn het opstellen van gedragsvoorschriften of het houden van bewustmakingscampagnes. Voorschriften bepalen de verantwoordelijkheden van werknemers bij het voorkomen van incidenten. Deze voorschriften zijn echter vaak gebrekkig van opzet. Bijvoorbeeld omdat de verantwoordelijkheden van werknemers niet goed zijn afgestemd op de productiviteitsdoelen van werknemers. Dit leidt ertoe dat werknemers procedures omzeilen of minder veilig maar productiever beveiligingsgedrag aannemen. Ook bewustmakingscampagnes zijn veelal onsuccesvol. Meestal omdat zij zijn gebaseerd op onjuiste veronderstellingen over waarom mensen zich wel of niet veilig gedragen. Bewustmakingscampagnes worden bijvoorbeeld vaak gelanceerd vanuit de veronderstelling dat kennis over cybersecurity ontbreekt. Terwijl in feite andere factoren leiden tot niet-naleving van het beleid, zoals slecht ontworpen beveiligingsmaatregelen of een hoge werklast.

Systematisch standpunt

Daarom moeten we eerst begrijpen waarom werknemers zich al dan niet veilig gedragen. Op basis van deze inzichten kunnen we dan interventies ontwikkelen die de oorzaken wegnemen van het onveilige gedrag. Het hebben van een systematisch standpunt over de verschillende soorten cybergedrag die werknemers wel of niet uitvoeren en de redenen daarvoor, is naar onze mening de eerste stap bij het tegengaan van incidenten en het bevorderen van cyberveilig gedrag op de werkvloer.
Samen met de SRP-partners hebben we gekeken naar het securitygedrag van hun medewerkers. Hiermee hebben we verschillende vragen beantwoord. Wat is cyber(on)veilig gedrag? Hoe (on)veilig gedragen medewerkers zich? Hoe meet je cyberveilig gedrag? Ook hebben we gekeken naar de bronnen die het cyberveilig gedrag van medewerkers frustreren. Dit met het oog op het ontwikkelen van interventies in een later stadium. De achterliggende vraag was: hoe kunnen we medewerkers helpen in het bereiken van hun zakelijke doelen op een veilige manier? Hierbij hebben we een gedragsmodel gebruikt dat stelt dat gedrag ontstaat door een samenspel tussen kennis van medewerkers, de gelegenheid voor veilig gedrag en de motivatie die medewerkers hebben om zich veilig te gedragen.
We hebben zeven clusters van cybergedrag geïdentificeerd via interviews en documentstudie. Een belangrijk cluster is 'omgaan met vertrouwelijke informatie'. Hierbinnen vallen specifieke gedragingen zoals 'het versleutelen van informatie met speciale software' en 'het waarborgen van correcte adressering van elektronische berichten'. We vroegen meer dan 2000 medewerkers binnen de banken vervolgens hoe zij omgaan met vertrouwelijke informatie. Daarnaast vroegen we ook naar hun kennis, motivatie en de gelegenheid die door de bank wordt geboden om op een juiste manier om te gaan met informatie.
Over het algemeen genomen zien we dat medewerkers zich veilig gedragen. Er zijn bovendien geen opmerkelijke verschillen tussen de banken. Alleen het versleutelen van vertrouwelijke informatie blijft achter. Medewerkers weten hoe ze dit moeten doen en encryptiesoftware is voor handen, maar, zo laten medewerkers ons weten, het versleutelen van bestanden is te moeilijk, het stoort te veel met het werk. Medewerkers maken vaak bewust de keuze om bestanden niet te versleutelen, bijvoorbeeld als deze gedeeld moeten worden met anderen. Een kansrijke oplossingsrichting lijkt dan ook te liggen in het (her)ontwerp van veiligheidsmaatregelen. Door security mensvriendelijker te maken kunnen we medewerkers helpen in het bereiken van hun zakelijke doelen op een meer veilige manier.

Door: Bart Gijsen (TNO)

Self-healing

Cybersecurityonderzoek zorgt ervoor dat organisaties beter bestand zijn tegen moderne cyberaanvallen. Dit neemt echter niet weg dat ook aanvallers hun technieken voortdurend vernieuwen. Ze ontdekken en misbruiken nieuwe

kwetsbaarheden (zero-day exploits) in de ICT-middelen van organisaties en maken steeds meer gebruik van geautomatiseerde aanvalstechnieken. Deze vicieuze cirkel van cyberaanval en -verdedigingstechnieken leidt tot een voortdurende toename van kosten en toenemende inzet van experts. Daarnaast vergen deze ontwikkelingen ook een steeds kortere reactietijd van de experts in de SOC's. In het SRP-onderzoek naar self-healing for cybersecurity (SH4CS) is daartoe de vraag op langere termijn geadresseerd op welke wijze deze vicieuze cirkel doorbroken zou kunnen worden.

De term self-healing werd geruime tijd geleden geïntroduceerd in een visie om ICT-systemen te ontwikkelen die autonoom (zonder menselijke interventie) in staat zijn om zich aan te passen aan factoren die de beoogde werking van het systeem verstoren. Inspiratie voor de ontwikkeling van self-healing-systemen komt voort uit de analogie met biologische mechanismen, zoals het menselijk immuunsysteem. In feite is het immuunsysteem ook verwikkeld in een vicieuze cirkel, vechtend tegen aanvallen van bestaande en muterende virussen, bacteriën, parasieten en schimmels. In het SH4CS-onderzoek is een parallel getrokken tussen het menselijk immuunsysteem en hedendaagse cyberdefensieve maatregelen. Daaruit zijn een aantal opvallende aspecten naar voren gekomen die nieuwe inzichten verschaffen hoe de cyberdefensieve maatregelen op een andere, meer autonome manier kunnen worden ingericht.

Een van deze inzichten is de constatering dat bij ICT-systemen en netwerken de disposability eigenschap ontbreken waarover menselijke cellen wél beschikken: een lichaam blijft gezond als (in beperkte mate) zijn cellen sterven. Het immuunsysteem gebruikt deze eigenschap door voortdurend cellen te vernietigen, met een voorkeur voor cellen die geïnfecteerd zijn of zich niet-lichaam-eigen gedragen. De meeste ICT-systemen missen deze disposibility eigenschap. Ze zijn niet ontworpen om voortdurend (en zonder specifieke reden) systeemonderdelen te termineren en nieuwe onderdelen op te starten. Dit strookt ook niet met de traditionele opvatting over ICT-beheer. Met recentere DevOps-methoden en -technieken dient zich echter wel de mogelijkheid aan om 'regeneratieve ICT-infrastructuur' te realiseren.

In het SH4CS-onderzoek is op basis van Kubernetes technologie een experiment ontwikkeld om het concept van regeneratieve containers (die gebruikt worden om IT-applicaties uit te voeren) te demonstreren en beproeven. Dit experiment demonstreert hoe het container-opstartproces en container-terminatieproces de verspreiding van malware-infecties van de containers kan beperken en de detecteerbaarheid kan verhogen (doordat de infectie steeds opnieuw verspreid moet worden naar 'geschoonde' containers). In geval van een detecteerbare infectie kan de verspreiding zelfs autonoom (dat wil zeggen: zonder betrokkenheid van experts) beëindigd worden door een versnelling van het container-terminatieproces.

Dit vooralsnog eenvoudige experiment is de eerste stap richting het ultieme doel om de benodigde, schaarse cyberdefensieve expertise in de vicieuze cirkel te minimaliseren. Uiteraard is SH4CS geen wondermiddel dat alle cybersecurityproblemen oplost, maar zal het eerder een bruikbare aanvulling zijn op andere oplossingen. Ook wordt momenteel onderzocht onder welke omstandigheden het middel wellicht erger kan zijn dan de kwaal, zoals er ook door het menselijk immuunsysteem gezondheidsrisico's op kunnen treden. Verder onderzoek zal uitwijzen of en hoe de toepassing van SH4CS zal bijdragen aan de 'battle of the cyber fittest'.

Door: Richard Kerkdijk(TNO) en Maarten Jak (ING)

Threat landscaping

Met de term 'threat landscape' (dreigingslandschap) wordt in essentie gedoeld op een naar prioriteit gerangschikt overzicht van (cyber)dreigingen waarop een organisatie zich moet voorbereiden. In dit project is een methode ontwikkeld om een dergelijk dreigingslandschap af te leiden uit (cyber)dreigingsinformatie en incidentgegevens die een organisatie in de loop der tijd heeft verzameld. Belangrijk uitgangspunt was om daarmee tot een dreigingslandschap te komen dat specifiek is toegespitst op de individuele organisatie die het samenstelt. Dit vanuit de filosofie dat organisaties als ABN AMRO, ING, Rabobank en Volksbank vanuit hun uiteenlopende bedrijfsprofielen een evenzo uiteenlopende waardering van (het belang van) specifieke dreigingen zullen hebben.

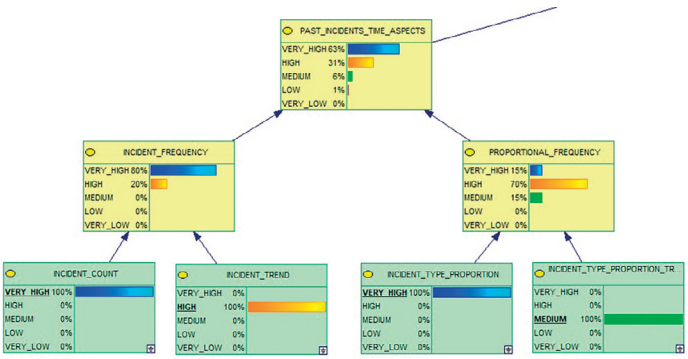
Het concept van een dreigingslandschap is niet nieuw, verscheidene leveranciers en ook organisaties als ENISA publiceren met enige regelmaat overzichten van (ontwikkelingen in) cyberdreigingen die zij belangwekkend achten. Dergelijke rapportages bieden weliswaar nuttige informatie, maar zijn in de regel te generiek om richting te geven aan de cybersecurityaanpak van een individuele organisatie. Bovendien is het begrip 'dreiging' niet altijd eenduidig afgebakend, hetgeen leidt tot inconsistente overzichten van actoren, aanvalsmethoden en meer algemene trends op het gebied van technologie en (cyber)security. Om hier meer lijn in te brengen, is vroeg in het project besloten om het top level dreigingslandschap met zogeheten campaigns (3) te bevolken en deze consis-

tent als (campaign) by (threat actor (type)) te formuleren. Deze ontwerpkeuze legt de focus op het eindspel van aanvallers en leidt tot items als (targeted ransomware) bij (Gogalocker) en (manipulation of payment applications) by (Carbanak Group). Onderliggende kenmerken zoals de capaciteiten en werkmethoden van een threat actor zijn daarbij uiteraard wel van belang, enerzijds om de ernst van een dreiging op waarde te schatten en anderzijds om in de informatiebehoeften van specifieke belanghebbenden te voorzien. Met het oog op het laatste zou het dreigingslandschap bijvoorbeeld ook een rangschikking van meest relevante aanvalsmethoden kunnen bieden.

FAIR

De grootste uitdaging in dit onderzoek was om observatiegedreven en bij voorkeur rekenkundig vast te stellen welke prioriteit aan de verschillende dreigingen in het dreigingslandschap moet worden toegekend. De in het FAIR (4) (Factor Analysis of Information Risk)-raamwerk beschreven taxonomie voor cybersecurityrisico's bleek hier een geschikt vertrekpunt voor te bieden. In samenwerking met de betrokken banken zijn de verschillende elementen van FAIR vertaald naar de context van een (cyber)dreigingslandschap. Hiertoe is onder meer gekeken naar enkele historische campaigns en de factoren die verschillende banken mee hebben gewogen bij het beoordelen daarvan. Op basis hiervan is een eerste set van 26 threat metrics gedefinieerd aan de hand waarvan een algehele threat score voor specifieke campaigns kan worden bepaald. In lijn met de FAIR-structuur reflecteren deze metrics niet alleen de kans dat een organisatie met een campaign te maken zal krijgen (5), maar ook de mate waarin weerstand tegen die dreiging kan worden geboden (6) en de impact van een eventueel incident. Voor het berekenen van de threat score is een zogeheten Bayesian Belief Network (7) samengesteld (zie figuur 1). Veel van de gedefinieerde threat metrics hebben een organisatie-specifiek karakter, waarmee het doel om het dreigingslandschap op individuele organisaties toe te spitsen is gerealiseerd. In totaliteit is de structuur van threat metrics wel relatief complex geworden. Het idee is echter om kwantificeren van deze metrics verregaand te automatiseren, niet in de laatste plaats om de threat score met enige regelmaat te kunnen verversen. Veranderingen op specifieke metrics kunnen immers tot een herschikking van dreigingen en daarmee een heroverweging van prioriteiten leiden. Punt van aandacht is dat voor de hand liggende bronsystemen (denk aan CTI-platformen (8), incidentregistratiesystemen en SIEMs (9)) niet vanzelfsprekend op deze automatiseringsslag zijn voorbereid. In samenspraak met de betrokken banken zal moeten worden nagegaan hoe de benodigde brongegevens structureel en maximaal efficiënt verzameld kunnen worden.

Parallel aan dit SRP-project liep vanuit de grootbanken het zogeheten '1-FTNL-initiatief' om tot een eenduidig (cyber)-dreigingslandschap voor de financiële sector als geheel te komen. Met dit traject is nauw samengewerkt, onder meer om onderlinge consistentie in terminologie en formats te garanderen. De in SRP verband ontwikkelde structuur van threat metrics wordt naar alle waarschijnlijkheid ook door dit sectorale initiatief omarmd, hetgeen de onderlinge synergie nog verder kan verstevigen.



Figuur 1 - De figuur toont een selectie van de totale set aan threat metrics.

Referenties

(1) https://www.tno.nl/media/14237/srp_magazine_-_editie_2019.pdf).

(2) https://www.tno.nl/srpcybersecurity

(3) Met campaign wordt gedoeld op een set van activiteiten (feitelijk incidenten) die een threat actor met specifieke aanvalstechnieken verricht om een bepaald doel te bereiken

(4) Zie https://www.fairinstitute.org/

(5) Dit wordt onder meer afgeleid uit de (veronderstelde) doelstellingen van de threat actor en de frequentie en geografische kenmerken van recente incidenten.

(6) Deze metrics appelleren onder meer aan detectiemogelijkheden en de mate waarin sprake is van specifieke kwetsbaarheden die de threat actor kan misbruiken.

(7) Een wiskundige methode om met kansverdelingen te redeneren, zie https://en.wikipedia.org/wiki/Bayesian_network

(8) Cyber Threat Intelligence

(9) Security Information and Event Management

Accountable

It is exactly a year since The Attributer last visited this attribute. Then the issue was with the Board of Disney and its decisions over cyber security. A group of shareholders were unhappy with the Board position and the company was heading for a clash at the forthcoming annual stockholders meeting. This time we are dealing with the ongoing story of Boeing. Whilst the entertainment industry and the aviation industry are both multi-billion-dollar businesses, no-one ever got killed watching a movie, unless they were on a flight at the time. In the case of Boeing more than 340 people were killed in two crashes involving the ill-fated but hugely popular 737 Max airplane.

Let's once again look at the definition of 'accountable':
'Accountable: *required or expected to justify actions or decisions; responsible, liable, answerable, chargeable, to blame for failures. Examples: 'Ministers are accountable to Parliament.' 'The government was held accountable for the food shortage'.'*

Boeing has a complicated statement of its vision and mission, covering multiple points of view (1). Interestingly one of the points is about safety, as you would expect:

'Safety: *we value human life and well-being above all else and take action accordingly. We are personally accountable for our own safety and collectively responsible for the safety of our teammates and workplaces, our products and services, and the customers who depend on them. When it comes to safety, there are no competing priorities.'*

That's fairly clear, but the Board obviously failed to take account of its own vision statement. After much talking about the crashes as an 'unfortunate sequence of events', eventually Dennis Muilenburg, the Chief Executive of Boeing, has had to resign. To suggest that such accidents are nothing more than 'bad luck' is an outdated and offensive message. The Attributer has written about a safety engineering methodology called STPA (see a previous article entitled SAFE), systems theoretic process analysis. This new approach to safety engineering is the work of Professor Nancy Leveson and her team at the MIT department of Aeronautics and Astronautics. The so-called 'swiss cheese' model in which the holes in cheese slices line up accidentally from time to time is not part of this modern approach. David Calhoun, Mr. Muilenburg's successor, take note.
There are many parallels between STPA and SABSA, one of which being the essential presence of governance and accountability. Both frameworks deal with systems engineering. Both make huge reference to the need for good governance at every level of the system, including the high-level corporate system that produces the lower level systems. Whilst the 737 Max is a system, it is only a sub-system of the larger system: the Boeing Corporation. And Boeing is only a sub-system of the entire aviation industry.
The key to safe and secure operations of any systems is therefore embedded in the way they are engineered, and systems engineering demands governance at every level and accountability of the human players who hold responsibility for governing the systems. One of the essential first steps in engineering a system is to state the purpose of the system. What is it meant to do? According to most industry commentators, Boeing has clearly attempted to put profit before safety, violating its own vision statement. The Board saw the purpose of the system to make profits. They neglected to take account of the purpose also being to protect the safety of passengers and to maintain the confidence of the flying public at large.
Every organisation writes and publishes vision and mission statements, but if they don't actually use them as guiding principles for how they do business then it's all smoke and mirrors – merely window dressing in a world greedy for profit. If good systems engineering principles are applied, then those mission statements mean something. If not, then the words are empty. Both SABSA and STPA are clear about governance and accountability. If you follow and apply these frameworks, then you will not go far wrong in the world.

The Attributer

References

(1) www.boeing.com/principles/vision.page

Enterprise architecture versus digital architecture

Op 29 augustus 2019 richtten René Vleesschauwer, Daniël van Loon en Maurits van der Plas officieel de Association of Enterprise Architecture Netherlands Chapter op. De AEA Netherlands Chapter is de Nederlandse vertegenwoordiging van de globale vakvereniging van Association of Enterprise Architects (AEA), dat als doel het versterken van de toegevoegde waarde van de EA voor de organisatie en haar ketens heeft.

Maurits van der Plas, Bas van Gils en Chris de Vries.

De redactie van iB-Magazine (PvIB) heeft gevraagd om de door de AEA Netherlands Chapter nagestreefde rol in het landschap van architecten, vakverenigingen en ledenorganisaties te beschrijven. Met name binnen het kader van het recent gewijzigde beleid van het Nederlandse Architectuur Forum (NAF) om het Landelijke Architectuur Congres (LAC) om te zetten naar de Digital Architecture Design Day (DADD) (1).

Blauwdruk

De essentie van enterpise architecture is het vormen van een conceptuele blauwdruk die de structuur en operaties van een organisatie definiëren. Architectuur gaat om (het sturen op) samenhang. Architecten zijn goed in het in beeld brengen van de grote lijn en het nemen van beslissingen op hoofdlijnen. Daarmee worden verschillende doelgroepen bediend. Het management kan bijvoorbeeld beter en effectiever besluiten over de richting van organisaties. Teams krijgen (net genoeg) richting mee om aan de slag te gaan (en daarmee voorkom je dat teams met te veel vrijheid 'alle kanten' opstuiven).

Digitale transformatie

Deze huidige tijd wordt gekenmerkt door een toenemende digitalisering. Er wordt met recht gesproken over een digitale transformatie. In het 'nieuwe normaal' is digitaal de norm. Dit

betekent dat processen, data en systemen – zowel binnen als buiten de organisatie – steeds meer met elkaar verbonden zijn. Veranderingen volgen elkaar steeds sneller op en hebben een grotere impact in het hart van bedrijfsoperaties (waardoor organisaties voor complexere verandervraagstukken komen te staan). De architectuurdiscipline helpt bij het beheersbaar houden van deze complexiteit.

Digital architecture design

Het begrip 'design' kent verschillende interpretaties: soms gaat het om het 'verder verdiepen van de hoofdlijn van de architectuur' en soms gaat het om het creatieve aspect waarin naar nieuwe vormen wordt gezocht waarbij functie en vorm/structuur bij elkaar komen. In de digitale wereld van nu (b)lijkt de tweede interpretatie het meest relevant.

DAD kan vanuit dit inzicht staan voor drie acties:

1. samen aan de slag;
2. sturen op voldoende samenhang;
3. het vinden van creatieve vraagstukoplossingen waarbij functie en structuur bij elkaar komen.

Wat zijn de verschillen en overeenkomsten tussen enterprise architecture en digital architecture design? Ook hier delen architecten uiteenlopende visies. Het is echter de vraag of deze twee visies echt zo verschillend zijn. Het begrip 'EA' is al wat ouder. Er kleeft de connotatie aan van 'oud denken': grote plannen, meeslepende verhalen en vooral met de systematiek 'waterval' aan de slag. Plat gezegd: het tegenovergestelde van de agile mindset die in moderne organisaties nodig geacht wordt. Echter deze schijnbare tegenstelling is volgens ons slechts een wijze van beschrijving van software-architectuur.

Digital architecture design is een moderne naam. Wellicht komt het voort uit het begrip 'digital business design' (2). In essentie gaan beide begrippen om hetzelfde. DAD heeft echter meer een moderne/agile afdronk.

Digitale functies en digitaliseren als proces

Het digitaal architectuur ontwerp ambieert tot coördinatie te komen van de digitale functies en het 'digitaliseren als proces'. Daarbij zoekt men vanuit de verschillende specialisaties versterking, zoals met de beveiligingswereld. Deze coördinatie is van belang, omdat in een steeds complexere wereld het onmogelijk is dat één discipline alles overziet.
Naast de primaire bedrijfsvoering en de IT (kan daar überhaupt nog wel onderscheid tussen bestaan?) is er onder meer rekening te houden met: architectuur, risico, veiligheid, privacy en datamanagement. In veel organisaties zet men daar stappen in, omdat de diverse stafafdelingen onder één leidinggevende worden geplaatst. Ook de beweging naar agile helpt erg. Daar is goede samenwerking vereist.

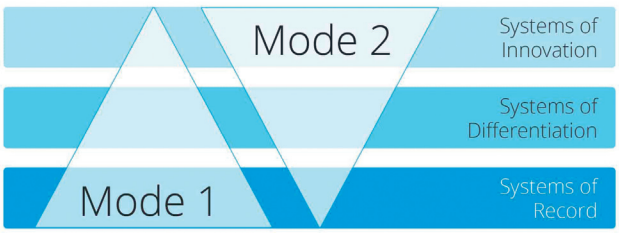
Koppeling digitale functies in digitaliseringsproces

Uiteindelijk gaat het om verandering en toepassen. Met de toepassing verdient de organisatie zijn geld. Het veranderingsproces zorgt ervoor dat de inrichting van organisaties met betrekking tot mensen, processen, data en systemen zo effectief mogelijk gerealiseerd worden in een snel veranderende context. Verder heeft het te maken met het spanningsveld tussen 'grip op verandering' en 'waardecreatie door verandering'.
Hier moet een balans worden gevonden: vanuit de architectuur- en ontwerpdiscipline tot op zekere hoogte grip houden op verandering versus waardecreatie door verandering. Als voorbeeld nastreven van synergie versus voldoende vrijheid voor de medewerkers en daartoe enablers aan te reiken. Hier doen teams hun voordeel mee.
Dit brengt de eerdergenoemde samenwerking tot stand. Spreekt men over 'grip' dan praat men ook over risico's en beveiliging. De securityprofessionals zoeken enerzijds naar die balans tussen maatregelen die de veiligheid garanderen en anderzijds de vrijheid om 'zinvolle dingen te doen'. Architecten, securityprofessionals en designers leren daarin van elkaar.
De nadruk ligt meer op de 'wisselwerking' dan op de 'versterking door input'. Concreet: architecten overzien de wereld en waar het heen zou kunnen gaan, securityprofessionals kunnen daarmee aan de slag en geven risico's en de noodzakelijke maatregelen aan. Dit stuurt dan weer de activiteiten van architecten (door terugkoppeling) die dan op de risico-aspecten net iets dieper kunnen gaan dan zij geneigd zullen zijn met betrekking tot minder spannende ontwerpvraagstukken.

EA- en DAD-uitdagingen

Enterprise architecture en digital architecture design staan dichtbij elkaar qua inhoud. De een heeft een moderne, de ander een wat meer 'old school'-connotatie met goed beschouwd een grote overlap. Organisaties leren steeds meer dat het niet een kwestie is van kiezen voor het ene of het andere. Het gaat er om 'de juiste aanpak binnen de gegeven context'.
Verglijkbaar introduceerde Gartner in 2014 Bimodal IT dat medio 2017 aan populariteit won (3), (4) en (5). Daar onderscheidde men een 'traditionele' aanpak waar grip en con-

trole van belang wordt geacht versus de agile aanpak waar wendbaarheid en vrijheid meer de boventoon voeren. Dit overlapt vrij goed de klassieke EA- en de modernere DAD-mindsetopvattingen. Ook hier geldt – zoals bij alle best practices – dat er goed vastgesteld wordt wat wel of niet bij een organisatie en diens omgeving het beste werkt.



Figuur 1 - Bimodal IT Gartner Model.

De uitdaging zit erin dat we onze kennis en ervaring moeten blijven delen. Niet alleen de successen, maar juist ook waar het minder goed ging. Acceptatie dus van een complexe wereld waar wel eens iets misgaat. We zullen moeten ervaren hoeveel architectuur/DAD je nodig hebt in een bepaalde setting.

AEA Netherlands chapter en haar collegae

In Nederland is het NAF een enorm sterke organisatie (wellicht zelfs al een merk?) als het gaat om architectuur. Met het Landelijk Architectuur Congres (LAC) had het NAF een goed congres. Dit was echter behoorlijk gericht op het traditionele EA-denken. Je zag eigenlijk nauwelijks mensen uit de DAD-wereld op dit congres. Het NAF heeft de dappere stap gewaagd om een nieuw dagcongres neer te zetten: DADD (5). Dit congres wil de bredere community aanspreken, het frisse thema sprak dan ook goed aan. Samen kom je verder. Dit klinkt afgezaagd, maar het is wel zo. Dit geldt ook voor AEA.

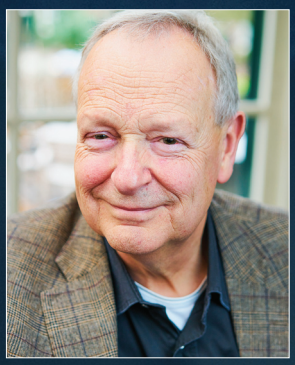
AEA en het NAF bouwen elk aan hun eigen community en zouden als concurrent van elkaar kunnen worden beschouwd. Beiden bieden echter hun respectievelijke communities een eigen toegevoegde waarde. Wij zien het digital architecture design als een verrijking van het landschap en vertrouwen erop aan datzelfde landschap een positieve bijdrage te leveren vanuit het AEA.
Binnen dit landschap zijn ook de andere verenigingen en organisaties te beschouwen als partners. Segmentatie is slechts goed tot op een bepaald niveau, het grote geheel is uiteindelijk bepalend voor het succes. Denk daarnaast ook aan het KNVI, ISACA en NOREA. Ook met hen zou een samenwerking van grote toegevoegde waarde zijn.

Referenties

(1) Interview met het NAF-bestuur, iB-Magazine jaargang 19 (2019) uitgave 5, pagina 16 t/m 19.
(2) 'Designed for Digital: How to Architect Your Business for Sustained Success'; Jeanne Ross (MIT).
(3) https://www.gartner.com/smarterwithgartner/how-to-innovate-with-bimodal-it/
(4) https://www.gartner.com/en/information-technology/glossary/bimodal
(5) https://www.researchgate.net/profile/Thomas_Keller12/-publication/316473387_BIMODAL_CORPORATE_IT_AND_ITS_IMPACT_ON_INNOVATION_ABILITY/links/5cc7058392851c8d220d4f6d/BI-MODAL-CORPORATE-IT-AND-ITS-IMPACT-ON-INNOVATION-ABILITY.pdf
https://www.researchgate.net/profile/Piet_Kommers/-publication/331174981_Edited_by_Piet_Kommers_and_Pedro_Isaias_Associate_Editor_Luis_Rodrigues_ISBN_978-989-8533-75-3/links/5c6ab38492851c1c9de7734d/Edited-by-Piet-Kommers-and-Pedro-Isaias-Associate-Editor-Luis-Rodrigues-ISBN-978-989-8533-75-3.pdf#page=224

Auteurs: Maurits van der Plas, voorzitter en medeoprichter van de Association of Enterprise Architecture (AEA) Netherlands Chapter alsook werkzaam in de functie van directeur Learning Solutions en Marketing & Sales bij van Haren Publishing. Maurits is bereikbaar via maurits@vanharen.net. Bas van Gils, ervaren Enterprise Architect & managing partner van Strategy Alliance. Bas is bereikbaar via bas.vangils@strategy-alliance.com. Chris de Vries is redactielid van iB-Magazine. Chris is bereikbaar via impuls@euronet.nl.

VOOR(UI)TGANG



Hoe gaat het met het PvIB? Het gaat heel goed, de activiteiten worden goed bezocht, het ledental groeit gestaag. Niks aan de hand zou je zeggen. Maar toch, je moet ook naar de toekomst kijken. Niets gaat vanzelf. In het algemeen staan verenigingen en clubs onder druk, ledentallen lopen terug, vrijwilligers zijn moeilijk te vinden, jongeren hebben weinig op met verenigingen. Over dat laatste: als je rondkijkt tijdens een PvIB bijeenkomst vallen de vele grijze hoofden wel op. Inventarisatie van het ledenbestand laat dan ook zien dat de meeste leden ouder zijn dan 45 jaar (62%). We hebben besloten daar wat aan te doen door meer jongeren (young professionals en studenten) binnen te halen. Daar zijn nu plannen voor in de maak.

Is het PvIB er alleen om onze leden te bedienen of hebben we ook een maatschappelijke rol? Tijdens bestuursvergaderingen is naar voren gekomen dat onze maatschappelijke rol zou zijn 'Nederland veiliger maken'. Dat klinkt erg filosofisch en abstract maar als je erover nadenkt is dit uiteindelijk toch waarom we als professionals dit werk doen. Die rol kun je voor de leden faciliteren door kennisdeling, netwerken etc. Gaan we nog een stap verder door PvIB te profileren als dé organisatie waar je moet wezen als deskundigheid gevraagd wordt over bijvoorbeeld een incident of IB/privacyvragen? Met andere woorden, ook verantwoordelijkheid nemen? Gaan we in de richting van een beroepsvereniging? Wat is het beroep dan? We hebben leden van allerlei pluimage: CISO's, FG's, ethical hackers, IT security experts, juristen, IT auditors etc. Best lastig. Allemaal vragen. Om enig zicht te krijgen in een aantal van bovenstaande vragen hebben we jullie recentelijk uitgenodigd om een enquête in te vullen.

In de enquête stelden we de vraag of we nog op de goede weg zijn met het magazine of dat het toch anders moet. Bijvoorbeeld, of we het magazine (alleen nog) digitaal uit moeten geven. Dat is een steeds terugkerende vraag tijdens de ALV. Andere enquêtevragen hebben meer betrekking op de inhoud en soorten van artikelen en een oproep of je bereid bent om een bijdrage te leveren door een artikel of column te schrijven. Dus graag nog even invullen via de PvIB website als je dat nog niet gedaan hebt.

De resultaten maken we in een van de komende nummers bekend. Nog even terug naar de profilering en bekendheid van het PvIB. Vorig jaar heb ik in deze column al gesproken over de mate van (on)bekendheid van het PvIB. Ik merk dat er nog steeds werk aan de winkel nodig is. We zijn bij veel bedrijven en instellingen best wel bekend. Maar hoe zit dat bij individuen die zich met informatiebeveiliging en privacy bezighouden? Door mijn vervroegde deeltijd pensionering kom ik nog wat vaker dan vroeger bij allerlei soorten bijeenkomsten, zoals bij CIO's, fysieke beveiligers, fraude preventie etc. Daar zijn we niet altijd bekend. Zelfs niet bij 'verdwaalde' informatiebeveiligers die ik daar tegenkom, maar ook niet bij (security)leveranciersbijeenkomsten. Die onbekendheid merk je ook op de jaarlijkse Infosecurity beurs waar men bij de stand komt met vragen over wie wij zijn en wat wij doen en waar studenten vragen of ze stage kunnen lopen bij het PvIB.

Maar ik moet zeggen dat er laatst wel een aangename verrassing was bij een leveranciers-symposium over cloudsecurity. Een van de sprekers liet een slide zien met een artikel over Zero Trust uit ons magazine van vorig jaar. Op de vraag of iemand in de zaal het al gezien had en het PvIB kende staken slechts een paar aanwezigen hun hand op. Waaronder ik natuurlijk. De spreker vroeg of ik het artikel kende? Mijn antwoord was: "Jazeker, ik ben de redacteur!" Ik heb meteen maar gereageerd met de opmerking dat men lid moest worden. Na de presentatie wilden aardig wat deelnemers meer informatie hebben. Ik ben in ieder geval druk bezig met het profileren van het PvIB.

Tom Bakker

Auteur: Erik Frambach is principal consultant governance, risk & compliance bij Strict BV.
Erik is bereikbaar via e.frambach@strict.nl.

CISO @home

Als je chief information security officer (CISO) bij een bedrijf bent, heb je vaak een zware taak. Je moet bijna overal verstand van hebben en voor iedereen werkbare en veilige oplossingen bedenken. Ook thuis liggen de risico's voor het oprapen. Hoe ga je om met smartphones, wifi, apps, router, firewall, smart TV, bluetooth, Google, enzovoorts? Er zijn opvallende overeenkomsten én opvallende verschillen tussen @work en @home die aan beide kanten te benutten zijn.

Thuis gaat CISO echt geen maatregelen opschrijven

Elk zichzelf respecterend bedrijf heeft een informatiebeveiligingsbeleid waar goed over nagedacht is, dat door de directie is vastgesteld en dat iedereen hoort te kennen en na te leven. Niet dat iedereen zich er altijd aan houdt. Daarnaast zijn er altijd mensen die zeggen dat ze het beleid nooit gezien te hebben. Dat is misschien ook zo, maar dan moet je je als CISO afvragen wat je kunt doen om de communicatie te verbeteren of het belang van informatiebeveiliging beter voor het voetlicht te krijgen.

Beleid

Thuis is er helemaal geen beleid. Toch zijn er (vaak impliciet) principes en (`excusez les mots') best practices die consequent worden gevolgd. Iedereen doet de deur op slot als hij of zij weggaat en iedereen heeft op zijn minst een pincode op zijn telefoon. Nu kun je stellen dat dit voorbeelden zijn van maatregelen, geen beleid. Dat klopt en dat zegt meteen iets over het volwassenheidsniveau van de informatiebeveiliging. Thuis gebeurt het meeste beveiligingswerk `ad hoc'. Niettemin is het voor de meeste huisgenoten evident dat je je wachtwoord voor je e-mail met niemand deelt. Als je vraagt waarom, blijkt dat nog best een lastige vraag te zijn. Dit is kennelijk een geval van `onbewust bekwaam'.

Zowel @work en @home moet je je afvragen: hoeveel beleid en hoeveel maatregelen heb je nodig en hoe helpt je dat om de boel veiliger te maken? Thuis gaat de CISO echt geen maatregelen opschrijven. Dan maar informeel, in de hoop dat voorlichting en bewustwording van risico's volstaan om het toepassen van adequate maatregelen voor elkaar te krijgen. Het voordeel @home is dat de omgeving heel overzichtelijk is: weinig mensen, veel contact en relatief weinig ICT.

In een bedrijf ligt dat anders. Er zijn (veel) meer mensen, je spreekt ze minder vaak, er is (heel) veel ICT (inclusief slecht beheerde IoT, net als @home). Ook scheelt het dat er contractuele verplichtingen zijn, die heel anders werken dan familiaire banden. Formalisatie van wat je wel en niet moet doen wordt dan belangrijker. Daarbij moet je op de steun van de directie kunnen bouwen.

Back-ups

Neem het maken van back-ups. Iedereen weet hoe belangrijk dat is. De CISO @home vraagt regelmatig: "Wat is ook weer het risico, wat zou je kwijt kunnen raken? O ja." In een werkomgeving zijn daar vaak professionele systemen voor geïnstalleerd. De meeste gebruikers (en vaak ook de beheerders) gaan ervan uit dat dat allemaal perfect werkt. Maar pas op: zowel @home als @work: assumption is the mother of all fuckups. Kun je echt al je foto's en al je apps terughalen als je je telefoon kwijt bent? Ook @work moet je regelmatig testen of je een bestand van een back-up terug kunt krijgen. De CISO @work zal aan de back-up-beheerder vragen om periodieke rapportages waarmee de goede werking wordt aangetoond. De CISO @home doet het anders: die zorgt dat hij of zij erbij is als een nieuw stuk ICT binnenkomt. Automatische back-ups worden meteen ingeregeld en van tijd tot tijd maakt deze CISO zelf (ongemerkt) een back-up van alle laptops. Als dan iemand in tranen is omdat hij 'alle kwijt' is, dan is de CISO @home de held die alles herstelt. Zowel @home als @work zijn zulke incidenten erg nuttig om de bewustwording te bevorderen en respect voor de CISO te kweken.

Risicomanagement

Waarom moet ik …? Hoezo mag ik niet …? Wat als ik (niet) …? Alles wat de CISO bedenkt, wordt ter discussie gesteld en dat legt meteen de basis voor risicomanagement. De CISO @work gebruikt vaak een risicoanalyse om vast te stellen wat een organisatie het beste kan doen om risico's te beheersen. Dat is vaak een tijdrovende bezigheid met als gevolg: een langdurig proces voor implementatie van maatregelen. En dan hebben we het nog niet eens over budgetten die bij elkaar gelobbyd moeten worden.

@home doen we niet zo moeilijk. We maken het heel persoonlijk: hoelang kun je zonder laptop? Wat kan er gebeuren als je Facebookaccount is gehackt? Wat is het je waard om dat te voorkomen?

Je bepaalt zelf je risicobereidheid en doet dat bewust. De kosten van maatregelen of de ellende in geval van geen maatregelen verdeelt de CISO @home naar draagkracht.

CISO @work besteedt veel tijd aan het beleggen van risico-eigenaarschap.

Natuurlijk speelt daarbij ook mee of risico's andere gezinsleden of de hele ICT @home-omgeving raken.

Eindverantwoordelijk

Risico's @home hebben dus in de regel een concrete eigenaar. Dat is @work vaak anders. Wie betaalt de rekening of krijgt op zijn kop als er iets misgaat? Wie bepaalt of een risico acceptabel is of niet? De directie is eindverantwoordelijk voor alles, maar moet vaak vertrouwen op inschattingen van anderen. De CEO wordt ontslagen als een afdeling grove fouten maakt. De minister moet opstappen als een overheidsdienst domme dingen doet. Maar het probleem zit vaak dieper in de organisatie, waar verantwoordelijkheden c.q. risico's verwateren, niet opgepakt, niet begrepen of niet belegd worden.

Elke beveiligingsmaatregel moet een onderbouwing hebben. Niet omdat het moet, maar omdat het nut heeft. De CISO @work realiseert zich dat ISO 27001 en andere normen er niet zijn om iedereen te plagen, maar om de organisatie vooruit te helpen. Als dat niet zo werkt, houd daar dan mee op, of begin er niet eens aan. De CISO @work besteedt daarom veel tijd aan het beleggen van risico-eigenaarschap. De CISO @home niet. Die stelt ook geen beveiligingsbeleid op, maar praat wel over wat er in de boze buitenwereld allemaal gebeurt. Daarmee heeft de CISO invloed op maatregelen die worden getroffen c.q. risico's die worden geaccepteerd of gemitigeerd. Zonder bewustwording en overtuigingskracht kom je nergens, zowel @work als @home. De CISO @work kan van de CISO @home leren om het vooral simpel te houden en voorbeelden te gebruiken uit de praktijk @home. De CISO @home kan van de CISO @work leren dat een lange adem en zachte persoonlijke beïnvloeding vaak meer succes oplevert dan harde maatregelen.

Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl. Sandra Kagie is freelance tekstschrijver (Sanscript Tekstproductie). Sandra is bereikbaar via info@sanscriptproducties.nl.

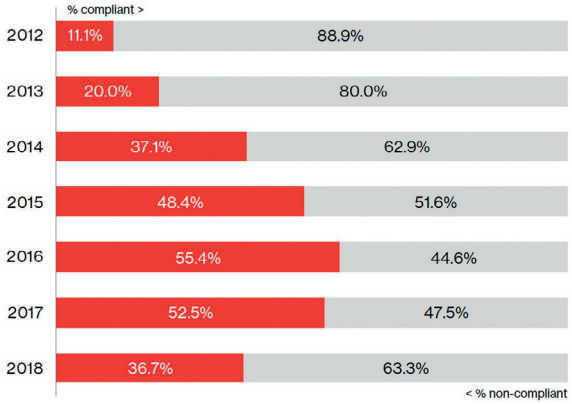
INTERVIEW

PCI compliance daalt verder: hoe keren we 'zorgelijke' trend?

"PCI DSS compliance is geen project, maar een continu programma." Dat is de hartenkreet van Gabriel Leperlier, senior manager security consulting EMEA van Verizon. Een jaar geleden hamerde hij in een gesprek dat we met hem hadden al op de noodzaak van meer duurzame aandacht binnen organisaties voor de Payment Card Industry Data Security Standard (PCI DSS). Na het uitkomen, afgelopen november, van het 2019 Payment Security Report (PSR) herhaalt hij deze oproep nog nadrukkelijker.

Uit onderzoek van Verizon, dat jaarlijks uitmondt in het Payment Security Report (PSR), blijkt namelijk dat het percentage bedrijven dat volledig PCI DSS compliance is, wereldwijd is gedaald van 52,5 procent in 2017 tot 36,7 procent in 2018. Terwijl in 2016 wereldwijd nog 55,4 procent van de bedrijven voldeed aan de internationale beveiligingsstandaard. Een tweede daling op rij dus.

Een forse daling die volgens Leperlier onder meer is te verklaren door een nieuw aspect in het onderzoek. Voor het eerst zijn in het onderzoek namelijk behalve data van Verizon ook data van QSA's (Qualified Security Assessors) van vier andere bedrijven gebruikt.
Ter geruststelling: veruit de meeste bedrijven die bij een tussentijdse assessment niet-compliance blijken te zijn, zijn dit volgens Leperlier bij de jaarlijkse 'final compliance validation' wel. Dat is belangrijk om te weten, omdat het hier gaat om de bescherming van gevoelige creditcardgegevens. Hij vergelijkt het met een APK-keuring: "Blijkt bij de keuring een band van je auto niet goed te zijn, dan komt de auto alsnog door de keuring wanneer de band vervangen is."



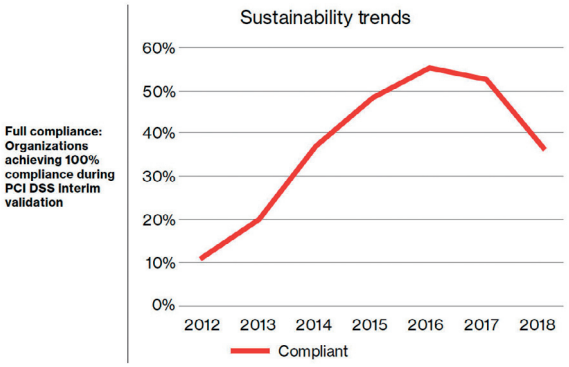
Figuur 1: PCI DSS Full compliance history.

De Payment Card Industry Data Security Standard (PCI DSS) is de internationale beveiligingsstandaard die is opgesteld door een samenwerkingsverband van creditcardmaatschappijen. PCI DSS helpt bedrijven die betalingen met creditcards accepteren hun betaalsystemen te beschermen tegen datalekken en diefstal van gegevens van kaarthouders. Elk bedrijf dat creditcardbetalingen accepteert, dient jaarlijks PCI DSS compliance aan te tonen. Ondernemingen met meer dan zes miljoen kaarttransacties per jaar moeten elk jaar een audit op locatie laten uitvoeren door een QSA, Qualified Security Assessor. Dit geldt ook voor bedrijven die door een creditcardmaatschappij zijn aangemerkt als 'Level 1 merchant'. Voor andere bedrijven geldt dat zij een online vragenlijst (self-assessment) in moeten vullen in combinatie met netwerkscans om zo aan te tonen dat ze compliant zijn.
Meer informatie is op de website te vinden (1).

De wijze waarop compliance door organisaties moet worden aangetoond, verschilt dus. Dit op basis van de rol die een bedrijf heeft: 'payment service provider' (PSP) of 'merchant'. En ook afhankelijk van het volume van transacties per jaar. De consequenties van het niet-compliance zijn, verschillen ook van bedrijf tot bedrijf. Voor merchants geldt volgens Leperlier dat ze contact moeten opnemen met hun bank wanneer ze niet-compliance zijn. Dit om uit te leggen wat de reden voor het niet-compliance zijn, is. De bank zal vervolgens een risicoanalyse maken en op basis daarvan bepalen of een bedrijf op zoek moet naar een andere bank of niet.
Voor PSP's ligt het heel anders, waarschuwt Leperlier. "Voor hen dreigt direct een verlies aan klanten wanneer ze niet-compliance zijn. Hun rating zal worden aangepast en klanten zullen het vertrouwen in een PSP verliezen."

Zorgelijk

Leperlier noemt de dalende trend wat betreft PCI-compliance van de laatste jaren 'zorgelijk'. De afname van het aantal bedrijven dat volledig PCI-compliance is, laat volgens hem namelijk zien dat bedrijven worstelen met het structureel op peil houden van het niveau van beveiliging.
Terwijl in 2004 (toen de PCI DSS werd geïntroduceerd) deskundigen er juist van uitgingen dat organisaties binnen vijf jaar structureel aan de regels zouden voldoen. De grafiek van de 'Sustainability trends' geeft echter iets anders aan. "Gegevensbescherming en naleving ervan zorgen voor dagelijkse uitdagingen", stelt Leperlier. Hij en zijn collega's adviseren daarom gegevensbescherming te benaderen als een schaakspel. "Met een degelijke strategie die het beoordelen van risico's en het plannen van verschillende stappen vooruit omvat." Chief information security officers (CISO's) richten zich volgens Leperlier in veel gevallen op het handhaven van de minimum beveiligingscontroles. "Terwijl ze dus oog zouden moeten hebben voor de groeiende competentie en volwassenheid van hun organisatie als het gaat om gegevensbescherming."



Figuur 2 - Sustainability trends.

Invloed GDPR?

Een jaar geleden sprak Leperlier nog de hoop uit dat onder invloed van de GDPR (de General Data Protection Regulation) de aandacht voor PCI DSS een boost zou krijgen. Een ontwikkeling die niet is terug te zien in het nieuwe rapport. "Veel bedrijven benaderen GDPR vanuit juridisch oogpunt, waarbij de focus ligt op contracten", geeft hij aan. Zo sluiten steeds meer bedrijven volgens hem bijvoorbeeld een verzekering af die de kosten dekt wanneer er onverhoopt sprake is van een datalek.
Zo'n verzekering kun je wat hem betreft afsluiten 'als extra geruststelling', maar een robuust compliance programma waarbinnen doorlopend toezicht en regelmatige meting zijn geborgd, moet wat hem betreft vooropstaan. De volgende conclusies uit het rapport maken duidelijk dat er op dit vlak nog een wereld is te winnen:

`Nearly one-fifth of organizations (18%) had no defined compliance program, according to approximately 55 organizations we surveyed for the 2018 PSR. Only 20% of organizations rated their Data Protection Compliance Programma as advanced. None of those organizations (0%) rated their program maturity as optimized.'
`Only 18% measured their PCI DSS controls more frequently than what PCI DSS requires across their entire environment. About one-third (32%) use control effectiveness and operational performance metrics. Only 7% use program impact metrics to measure program performance.'

Programma op papier

Bedrijven beschikken volgens Leperlier op papier vaak wel over nalevingsprogramma's voor gegevensbescherming. "Maar dat is slechts een begin. Je moet incident response trainen en testen," benadrukt hij. Dit op basis van gedegen risico-inventarisatie en daaruit volgende scenario's. Om snel te kunnen reageren en, nog beter, om te kunnen anticiperen op dreigingen moet je goed weten wie je vijand is, wat potentiële bedreigingen zijn en waar je zwakke plekken zitten. Deze `threat intelligence' wordt nog te weinig toegepast."
Eind dit jaar wordt de PCI DSS-standaard 4.0 geïntroduceerd. Leperlier noemt het `een revolutie'. Omdat de nieuwe standaard veel meer een `risk based approach' in zich heeft. "Dit om aan te geven hoe belangrijk het is om te evolueren van een reactief naar een proactief compliance programma."

Ondersteuning middels framework

In eerdere Payment Security Reports ontwikkelde Verizon methodes om organisaties te helpen hun Data Protection Compliance Programma's DPCP's te beheren. Deze zijn in het meest recente rapport gecombineerd tot het Verizon 9-5-4 Compliance Program Performance Framework. Het framework helpt het prestatievermogen en de procesvolwassenheid van DCPC's te ontwikkelen en verbeteren.

De belangrijkste vragen die middels het framework kunnen worden beantwoord, zijn:
- Is een compliance programma goed ontworpen?
- Wordt een compliance programma goed gemanaged?
- Werkt een compliance programma in de praktijk?
- Hoe robuust is een controle-omgeving?
- Weet een organisatie beperkingen en gebreken van een compliance programma op te sporen?

Continue aandacht voor compliance werkt

The 9-5-4 Compliance Program Performance Evaluation Framework

Evaluate and report the 9 Factors and each of the 5 Constraints across all 4 Lines of Assurance

Lines of Assurance:
1. **Individual accountability**
2. Risk management and compliance teams
3. Internal audit
4. External audit, regulators

Factor	Capacity	Capability	Competence	Commitment	Communication
1. Control environment	■	■	■	■	■
2. Control design	■	■	?	■	■
3. Control risk	■	■	■	■	■
4. Control robustness	■	■	?	?	■
5. Control resilience	■	■	?	?	■
6. Control lifecycle management	■	■	■	■	■
7. Performance management	■	■	■	■	?
8. Maturity measurement	■	■	■	■	?
9. Self-assessment	?	■	?	?	■

Figuur 3 - The 9-5-4 Compliance Program Performance Evaluation Framework.

Datalekken

Het nieuwste rapport bevat ook gegevens van het Verizon Threat Research Advisory Center (VTRAC). Gegevens waaruit blijkt dat het niet voldoen aan de standaard de kans op een datalek vergroot. "We hebben het al jaren over de nauwe correlatie tussen het gebrek aan PCI DSS-naleving en de kans slachtoffer te worden van een cyberaanval", aldus Leperlier. "In het huidige rapport hebben we daarom nog meer gegevens van het VTRAC-team, de auteurs van Verizons Data Breach Investigation-serie, gebruikt. En uit deze gegevens blijkt dat we nog nooit een datalek hebben vastgesteld bij een organisatie die compleet voldeed aan de PCI DSS-normen. Continue aandacht voor compliance werkt, kun je dus stellen."
Het complete 2019 Payment Security Report, met als titel `Navigating compliance programs toward maturity', is te vinden op de website van Verizon (2)

Referenties

(1) Www.Pcisecuritystandards.Org
(2) Www.Enterprise.Verizon.Com/Resources/Reports/Payment-Security/

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

BLOG

In der Beschränkung

Tijdens mijn studie Bestuurlijke informatiekunde leerde ik dat betrouwbare informatie uit een anekdote behalve juist ook volledig is. De paus bezocht New York en werd bij aankomst geïnterviewd. Een journalist vroeg: "Nachtclubs waar minderjarige meisjes topless bedienen, wat vindt u daarvan?" De paus schrok en vroeg: "Zijn hier nachtclubs waar minderjarige meisjes topless bedienen?" De volgende dag stond op de voorpagina: 'De paus arriveerde gisteren in New York. Zijn eerste vraag was: zijn hier nachtclubs waar minderjarige meisjes topless bedienen?' Door weglating van belangrijke details ontstaat dus een verkeerd beeld, hoewel het getoonde deel wel juist en waar is.

Ik heb dit voorbeeld goed onthouden. Daarom beantwoord ik mondeling of schriftelijk een vraag soms uitgebreider dan de vraagsteller had gehoopt. Een manager wilde ooit mijn gedrag aanpassen door op te merken: "Door de beperking toont zich de meester, zei Goethe." Een mooie spreuk, soms zelfs ingekort tot: 'Door de beperking ...' Daarmee suggereert men dat 'less is more' en dat een goed antwoord altijd kort is. Maar wanneer we kijken naar het hele citaat en de context, blijkt dat Johann Wolfgang von Goethe iets anders schreef en bedoelde.

'Natur und Kunst, sie scheinen sich zu fliehen
Und haben sich, eh' man es denkt, gefunden;
Der Widerwille ist auch mir verschwunden,
Und beide scheinen gleich mich anzuziehen.

Es gilt wohl nur ein redliches Bemühen!
Und wenn wir erst in abgemeßnen Stunden
Mit Geist und Fleiß uns an die Kunst gebunden,
Mag frei Natur im Herzen wieder glühen.

So ist's mit aller Bildung auch beschaffen:
Vergebens werden ungebundne Geister
Nach der Vollendung reiner Höhe streben.

Wer Großes will, muß sich zusammenraffen;
In der Beschränkung zeigt sich erst der Meister,
Und das Gesetz nur kann uns Freiheit geben.'

Goethe zei het niet in het Nederlands, maar schreef het als conclusie van een titelloos sonnet uit 1800. Het volledige citaat is: 'In der Beschränkung zeigt sich erst der Meister.' Dit betekent: binnen de beperking toont zich pas (dus voor het eerst) de meester. Dit verwijst naar het eeuwenoude opleidingstraject van de meester met zijn gezellen in een gilde. De gezel doet, na uitgebreid te zijn opgeleid door de meester, zelf zijn meesterproef en laat daarmee zien tot meesterniveau te zijn gekomen. Denk aan de huidige masteropleidingen, in het bijzonder aan de juridische faculteiten. En bij een gilde gaat het dakpansgewijs, omdat de ex-gezel daarna nieuwe gezellen gaat opleiden.
Goethe schrijft 'in' en niet 'durch'. De meester toont niet door een beperking dat hij vakman is, maar laat het zien in (dus binnen) een beperkende situatie. Een beperking die hij zichzelf bewust oplegt. Je opleiding opent de wegen die je op kan gaan en de uitdaging is om één kant op te gaan, wetende dat je daarmee tegen veel andere opties kiest. Wie alles wil kunnen, kan overal maar een beetje aan doen en zal nooit een kampioenschap bereiken. Goethe doelt erop dat men een keuze moet maken voor een bepaald beroep – en daarmee ook kiest om andere beroepen niet te doen. Alleen zo is het mogelijk in dat ene 'goed' te worden.
Het citaat gaat er dus niet over dat een boodschap in zo weinig mogelijk woorden en zinnen moet worden gevat. Gezien de eigen tekstproductie van Goethe zou dit tamelijk ongeloofwaardig zijn.
Goethe koos ervoor de zin te schrijven in een sonnet, een dichtvorm met strenge vormregels. Het rijmschema is ABBA, CDDC, EFG, EFG. Daarnaast mag het onderwerp pas in de tweede helft duidelijk worden. In eerste instantie lijken die regels de vrijheid van de auteur te beperken, maar doordat de zorg over de vorm is weggenomen, is de auteur juist 'vrij' om zich te concentreren op de inhoud van de over te brengen boodschap.
De volgende zin is de laatste van het sonnet en zoals het hoort de conclusie: 'Und das Gesetz nur kann uns Freiheit geben.' Beginnend met 'en' is dit het tweede en noodzakelijke deel van het citaat. Het gedicht geeft aan dat de mens zich beperkingen moet opleggen door een bepaald beroep of - zoals in dit sonnet - een uitingsvorm te kiezen en daarna binnen die ruimte zijn meesterschap moet tonen. En dat alleen die wettelijke beperking een kader biedt waarbinnen in vrijheid gewerkt en bewogen kan worden.
Met andere woorden: alleen iemand die overtuigd kiest voor een bepaald specialisme, daarmee een roeping volgt en dat vak met geestdrift (passie, hart en ziel) en ijver uitvoert, kan komen tot een waarlijk meesterschap. En bij die uitvoering moet de wet worden gehanteerd als kader en leidraad. Juist door de vorm waarbinnen het werk moet passen te fixeren, creëert de specialist zijn eigen vrijheid om als professional inhoudelijk goed zijn taak te doen. Bijvoorbeeld de AVG en de wet Computercriminaliteit bieden aan security- en privacyprofessionals zo'n kader. En ook de ISO27001-norm als code voor informatiebeveiliging is met enige dichterlijke vrijheid als een 'wet' (Gesetz) te interpreteren. Het is dus geen ballast, maar houvast.

Zo gaat dit sonnet uit 1800 over natuur, kunst en educatie dus ook over informatiebeveiliging. Johann Wolfgang toont ons daarmee opnieuw zijn ver vooruitziende blik. Dat deed hij immers ook in zijn bekende Faust boek. Daarin gaat het - in zekere zin - over de moderne neiging om ten bate van je voortdurende zucht naar likes je complete ziel en zaligheid te verkopen aan social media (zoals Fa..Bo..), maar daarover een andere keer meer.

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.

Afhankelijkheid van leveranciers

Terwijl we volop bezig zijn met het verzamelen voor artikelen voor deze uitgave van iB-Magazine, blijkt dat er een ernstige kwetsbaarheid (CVE-019-19781) zit in de Citrix Application Delivery Controller (NetScaler ADC) en Citrix Gateway (NetScaler Gateway). In Nederland zou het om 713 gebruikers gaan (1). Het NCSC gaat over tot het geven van een dringende waarschuwing aan gebruikers voor deze kwetsbaarheid met een ernst van 9,8 op een schaal van 1 t/m 10 (2). Wat volgt lijkt op een disaster recovery-programma: thuiswerkomgevingen worden afgesloten, medewerkers op de hoogte gesteld, extra monitoring op de omgeving ingesteld en ga zo maar door. Inmiddels zijn er Kamervragen gesteld vanwege het grote aantal (semi-)overheidsinstellingen en gemeenten die werken met Citrix.

Het is belangrijk om te leren van incidenten als deze. Als deze Citrix-kwetsbaarheid ons iets toont, is het de afhankelijkheid van een leverancier voor (technische) oplossingen. Bij de bekendmaking van de kwetsbaarheid lag de eerste prioriteit van geraakte organisaties uiteraard bij het nemen van maatregelen om het incident op te lossen. Nu is het tijd voor de evaluatie: deze situatie maakt (pijnlijk?) duidelijk hoe afhankelijk de organisaties die we proberen te beschermen zijn van leveranciers. Is dat een slechte zaak? Welke maatregelen kunnen we nemen? De redacteurs van iB-Magazine geven hun visie.

Fook Hwa

Ik heb in de eerste paar weken veel conference calls gehad over Citrix. Er was veel discussies over wat er allemaal in het verleden had moeten gebeuren. Dat punt zijn we voorbij en we moesten in een korte tijd inzicht krijgen in wat werd geraakt en wat niet. Dat is allemaal gelukt.

Het incident met Citrix laat weer eens zien dat je voor alles in je IT-landschap eigenlijk een back-up of alternatief zou moeten hebben. Vaak ontbreekt het echter aan inzicht in dit landschap om te kunnen bepalen wat en/of je zaken dubbel zou willen uitvoeren.

We worden echter wel steeds afhankelijker van technologie om überhaupt te kunnen werken. Dit betekent het dubbel uitvoeren om continuïteit te kunnen borgen. Of moet je afspraken maken, dat de leverancier dat regelt?

Fook Hwa Tan | Chris de Vries | Maarten Hartsuijker

Ik realiseer me heel goed, dat organisaties naar een business case zoeken die niet heel snel gemaakt kan worden. Het wordt veel te duur. Denk terug aan de Diginotar in 2010, waarbij we hebben geleerd om van twee Certificate Authorities (CA)-certificaten te kopen. Dat doen we nog steeds, toch? Nee, vaak niet meer.

Wat moet je wel doen: identificeer wat de kritiek is en overleg met leveranciers wat de alternatieven zijn, voordat het te laat is!

Maarten Hartsuijker

Kwetsbaarheden in software zijn aan de orde van de dag. De leverancier maakt ze bekend. Je neemt actie of geen actie. En in het laatste geval zit je op de blaren als je te laat bent met het treffen van maatregelen. Toen de exploits bekend werden, zaten helaas veel organisaties in Nederland op de blaren. Soms omdat ze in december hadden nagelaten om maatregelen te treffen, maar soms ook omdat ze na de vele (soms tegenstrijdige) berichten voor de zekerheid de stekker er maar uit trokken.

Citrix bezweerde dat de in december aangeraden work arround werkte, MITS je beide maatregelen om de path-traversal te detecteren en blokkeren implementeerde. Dit gold echter alleen voor up-to-date software. Er was namelijk eerder door Citrix in sommige versies een bug in de rewrite module gepatcht. En de work arround voor de kritieke kwetsbaarheid had een goed werkende rewrite module nodig om effectief te zijn. Hier werd het vermoedelijk voor velen complex. Er ontstond een bug-op-bug situatie, de juiste werking van de work arround werd onzeker en met veel berichtgeving in de landelijke nieuwsmedia wilden veel CEO's en IT de zekerheid dat hun organisatie geen risico's liepen. Je moet dan heel zeker van je zaak zijn om een memo te schrijven met de boodschap: we hebben het probleem geanalyseerd en de juiste maatregelen getroffen. Onze organisatie is hier niet kwetsbaar voor. Het belangrijkste leerpunt van het Citrix-incident is wat mij betreft dat veel organisaties na tientallen jaren oefenen nog steeds erg laat zijn met reageren op beveiligingsadviezen. Als we niet willen dat de geschiedenis zich herhaalt, moet de reactietijd van organisaties op kwetsbaarheden met een CVSS score van 9 of hoger naar 48 uur of lager.

Chris de Vries

Is het de duivel die ermee speelt of is er synchroniciteit in het spel? Op dit moment speelt het Citrix-probleem en we zien dat vele organisaties opeens twijfelen aan zichzelf (en liever nog aan hun leveranciers). Meteen denkt men dan terug aan de 'wet' van ketenveiligheidsrisico's, oftewel: de ketting is zo zwak als de zwakste schakel. Lees hierbij de buitenstaander of voor de goede verstaander: de leverancier.

Laat ik nu net vandaag (5 februari) bij een bijeenkomst zitten waarin kennisuitwisseling voor ecosysteembouwers opgelost worden in de 21e eeuw door massasamenwerking. Een van de 'slides' ging over drie inzichten van 'collectieve engineering':

1. 'De meesten onder ons eisen radicale simpliciteit, waarbij dit niet tegenovergesteld staat aan veiligheid, maar juist essentieel is voor die veiligheid.
2. De meesten onder ons reageren op actuele problemen, bijna nooit anticiperende op risico's.
3. Het menselijk geheugen is extreem gebrekkig.'

In de presentatie kwamen wat Dilberts tekeningen voorbij. Twee daarvan zou ik even willen omzetten naar het Citrix-probleem:

1. Wanneer wij ons maar hard genoeg concentreren, dan kunnen wij vergeten dat apparatuur wellicht niet goed functioneert en kunnen wij voortgaan met deze te gebruiken.
2. Wij vinden altijd wel de wezenlijke oorzaak van dit soort problemen: de mensen!

Herkenbaar, toch? En daarmee gaan wij over tot de orde van de dag.

Referenties

(1) https://www.security.nl/posting/639015/Honderden+Nederlandse+Citrix-servers+kwetsbaar+voor+aanvallen

(2) https://nos.nl/artikel/2318528-waarschuwing-voor-hacks-bij-citrix-servers-na-beveiligingslek.html

COLOFON

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

PvIB Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

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

BLADMANAGEMENT
MOS bv
José Broekhuizen
Lisa Petersen
E ibmagazine@pvib.nl

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

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

ABONNEMENTEN
De abonnementsprijs in 2020 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN Berry

Twijfels, twijfels en twijfels

Bij mijn werkgever werd besloten over te gaan naar Office 365. Gezien mijn verleden in de informatiebeveiliging werd mij gevraagd daar advies over te geven. Na wat gelezen te hebben over Office 365 en de wijze van implementatie kwam ik tot de conclusie dat het zowel prijstechnisch als beveiligingstechnisch een goede oplossing lijkt te zijn. De implementatie was inderdaad een fluitje van een cent en al snel was iedereen tevreden.

Een paar weken later kreeg ik in de avond een whatsappje van een collega die mij vroeg welk PDF-bestand ik hem had gezonden. Ik kon snel antwoorden dat ik beslist niets had gezonden, maar mijn collega bleef volhouden dat hij een PDF-bestand van mij had gekregen. Inmiddels kwam nummer 2 met eenzelfde opmerking. Ik begon onraad te ruiken en dacht: het zal toch niet zo zijn dat mijn Office 365-account gehackt is? In mijn mailbox zag ik geen bijzonderheden, behalve dat ik al een dag geen mail had ontvangen. Dat is eigenlijk niet mogelijk. Op de telefoon en iPad zag ik ook geen vreemde zaken, dus ik besloot de volgende morgen met onze techneuten te gaan praten.

Na een uurtje kwamen ze tot de conclusie dat mijn mailaccount gehackt was en niet meer beschikbaar was omdat Microsoft (MS) het account had geblokkeerd. Maar waarom informeren ze mij niet? Ze hebben mijn adres, mijn mobiele nummer en er zijn nog wel meer mogelijkheden om mij te bereiken.

Na twee uur bellen en query's gemaakt te hebben op mijn mailbox bleek inderdaad dat iedereen een mail had gehad met een PDF-bestand die een uitnodigende bestandsnaam had, maar die beslist helemaal niets met mijn werk of belangstelling te maken hadden. Om het document te openen hoefde je alleen maar even je Office-accountnaam en -password in te voeren. Ondanks het feit dat de site er 'profi' uitzag, kon je zien dat het nooit een site van MS zou kunnen zijn. Toch was het aantal relaties dat erg nieuwsgierig was naar mijn PDF schrikbarend hoog. En ja, ook hun account was in zeer korte tijd gehackt. Al mijn relaties kregen een mail met een waarschuwing dat ze de PDF niet moesten openen en met mijn verontschuldigingen. Mijn baas vond dat ik het moest melden bij de Autoriteit Persoonsgegevens. Mopperend heb ik de nodige formulieren ingevuld. Zou ik er ooit iets van horen? Ben bijna zeker van niet.

Nu blijft voor mij de vraag hoe het kon gebeuren dat ik gehackt werd. Ik maak gebruik van zeer complexe wachtwoorden, geen bestaanbare woorden, gebruik geen wachtwoorden meerdere malen voor verschillende sites, enzovoort. Voor mij was het voor het eerst in mijn 25-jarige internetcarrière dat er iets gebeurde met mijn gegevens wat ik beslist niet wilde. Natuurlijk weet iedereen wat ik fout deed, alleen ik weet het niet.

Berry

TSTC

ICT en Security Trainingen

Start 2020 goed met 20% PVIB korting op deze trainingen:

TSTC bestaat 20 jaar en geeft dit jaar PVIB leden 20% korting op geselecteerde trainingen op basis van hun lidmaatschapsnummer.
Vermeld dit nummer bij uw inschrijving.

PECB certificeringen

- ISO 27001 Lead Implementer
- ISO 27001 Lead Auditor
- ISO 27701 Privacy Lead Implementer
- CDPO Certified Data Protection Officer

ISC2 certificeringen

- SSCP - Systems Security Certified Practitioner
- CISSP - Certified Information Systems Security Professional
- ISSAP - Information Systems Security Architecture Professional
- CSSLP - Certified Secure Software Lifecycle Professional
- CCSP - Certified Cloud Security Professional

EC-Council certificeringen

- CEH - Certified Ethical Hacker
- ECSA - Certified Security Analyst
- C|CISO - Certified Chief Information Security Officer
- CSA - Certified SOC Analyst
- CTIA - Certified Threat Intelligence Analyst
- CASE - Certified Application Security Engineer JAVA/.NET

ISACA certificeringen

- CISM - Certified Information Security Manager
- CISA - Certified Information Systems Auditor
- CRISC - Certified in Risk and Information Systems Control
- CGEIT - Certified in the Governance of Enterprise IT

Divers

- Linux LPIC 3 security
- Security+
- (Web)Application Security Assessment based on OWASP

www.tstc.nl