iB
INFORMATIEBEVEILIGING
jaargang 16 - 2016
#3

CISO EDITION

The 'Seven Habits of highly effective CISO's'

EU-US Privacy Shield: de vervanger van Safe Harbour

Grip op informatiedeling met derden

No-brainer-security-checks

SECURITY Academy

Unlock je carrièrepad bij de Security Academy

Studeren aan de Security Academy staat voor diepgang en kwaliteit. Voor zowel de security specialist als de business continuity en crisismanager bieden wij 28 certificeringen aan waarmee u zich, ongeacht uw instapniveau, verder kunt ontwikkelen. Benieuwd naar het geheel vernieuwde certificeringsprogramma? In mei vindt de officiële lancering plaats van dit internationale certificeringsprogramma.
Ga voor een sneak preview naar de **Security Academy Backstage FB** pagina

SecurityAcademy.nl

info@securityacademy.nl

+31(0)348-408061

Deze keer geen voorwoord van mij. In deze uitgave hebben we een gastredacteur aan het werk gelaten en ik vond het passend dat hij het welkomstwoord zou doen. Ik wens jullie veel leesplezier.

Lex Borger, hoofdredacteur

CISO SPECIAL

In 2015 typeerde CT Partners de CISO als "an IT and a business leader expert at anticipating, preventing and responding to cyber-attacks, and informing Board level executives as well as C-suite peers". Ook Accenture en Ponemon deden in 2015 uitspraken over de toegevoegde waarde van de CISO in relatie tot innovatie en differentiatie. Deze verantwoordelijkheid vergt andere zienswijze van de CISO, waarvan er in deze special een aantal worden behandeld. Mijn boek "Hoe veilig is mijn aandeel?" is de weerslag van ruim 6 jaar onderzoek naar, onder andere, de rol van de Chief Information Security Officer (CISO) als eindverantwoordelijke voor de security visie, missie en strategie van de organisatie. De CISO neemt daarmee een prominente plek in in de bestuurskamers. Nieuwe inzichten positioneren informatiebeveiliging zelfs als een factor voor marktdifferentiatie. Hunter en Westerman deden in 2007, op basis van wetenschappelijk onderzoek, al suggesties voor de CISO om zijn Board te helpen met een dergelijke positionering. In deze special krijgt de CISO handvatten om de organisatie mee te nemen om IB te gaan beschouwen als onderdeel van integraal management. Immers is het 'aandeel' van elke manager en directeur in het proces en cultuur van beveiliging van steeds directere invloed op de gepercipieerde waarde van de organisatie. Ik beschrijf in het artikel met CFO Hans Go en het artikel met Prof. Hans Mulder enkele voorbeelden waarbij adequate security invloed heeft op de gepercipieerde waarde van de organisatie.

Informatiebeveiliging is in de wetenschap een relatief nieuw vakgebied. Het is een zeer dynamische wereld waarin de ontwikkelingen elkaar snel opvolgen. Als je als CISO in staat bent je eigen vakgebied te ontstijgen en door adequaat risk- en security-management toe te passen aantoonbaar waarde kan toevoegen ben je mijn inziens van toegevoegde waarde voor je organisatie. Sterker nog, volgens CT Partners en Accenture wordt dit ook in toenemende mate van de CISO verwacht. Ik heb in deze CISO-special een aantal artikelen verzameld die andere zienswijze stimuleren en bijdragen in de "Key Board Advisor" die CT Partners schetst. Zelf ben ik in 2014 gestart met mijn onderzoeken toe te passen in de rol van CISO. In eerste instantie bij het UWV als ad-interim CISO en momenteel bij NN-Group als CISO. Deze empirie schijnt nieuw licht op mijn eigen wetenschappelijk onderzoek en geeft bovenal inspiratie om de wetenschap nog praktischer te benaderen. Ik hoop dat de artikelen in deze special ook jou de nodige nieuwe inzichten en inspiratie geven.

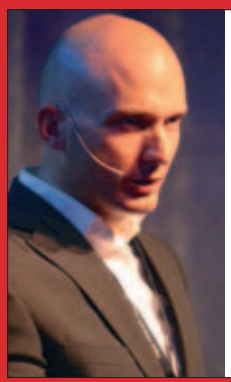
Yuri Bobbert, gastredacteur

In dit nummer

VERGADEREN OM TE BESLUITEN

Het gebruik van een Group Support System in Informatiebeveiliging

Besluitvorming tijdens vergaderingen is een ongrijpbaar fenomeen [1]. Zo definieerde Thomas Kayser vergaderingen als "a gathering where people speak up, say nothing, and then all disagree" [2]. Effectiviteit van vergaderingen is wereldwijd veel beschreven. Onder andere het gebrek aan zogenaamd "evidence trailing". Dit herleiden wie, wanneer en waarom een bepaalde beslissing heeft genomen blijkt complex en gezien de stand der technologie vandaag de dag niet meer nodig. Vergaderingen moeten besluitvormers juist faciliteren in het delen van kennis, het bespreken van complexe onderwerpen, het bewaken van voortgang van projecten et cetera en dit alles vaak onder grote tijdsdruk en onzekerheden [3].



Lec. Yuri Bobbert MSc RI CISM SCF startte in 2004 een beveiliging en risicomanagement advies en integratie organisatie. Parallel daaraan startte hij in 2008 zijn doctoraat onderzoeken naar organisatie transformaties met als rode draad "Maturing Business Information Security"(MBIS). Meerdere boeken, publicaties en een onlinekennisplatform (www.mbis.eu) zijn hiervan het resultaat. Met zijn ruime praktijkervaring bij meer dan 300 organisaties acteert Bobbert op het snijvlak van organisatietransformatie, advies, IT en management. Zo is Bobbert interim Chief Information Security Officer (CISO) van het UWV en momenteel als CISO bij Nationale-Nederlanden Group. Hij is daarnaast als lector Business Information Security verbonden aan Hogeschool NOVI en als onderzoeker zowel verbonden aan het Digital Security Institute van de Radboud Universiteit in Nijmegen als aan de Universiteit van Antwerpen. Zowel in zijn managementadviespraktijk als wetenschappelijk onderzoek gebruikt hij Group Support Systemen (GSS) om in groepsverband kennis te genereren en delen, consensus te bereiken en daarmee de strategische en tactische besluitvorming te bevorderen. Yuri is bereikbaar op y.bobbert@novi.nl.

Echter door het gebrek aan efficiënte sturing, evenwichtige betrokkenheid van deelnemers en de wet van de decibel, verlopen ze chaotisch en leiden ze tot frustraties. Bij complexe onderwerpen, die een bepaald kennisniveau vereisen, met een lange doorlooptijd is sturing op het proces net zo belangrijk als sturing op de inhoud [3]. Ook bij risicomanagement en informatiebeveiliging wordt nog té veel op de inhoud gestuurd in plaats van op het proces om te komen tot de gewenste uitkomsten [4]. Het informatiebeveiligingswerkveld wordt grotendeels gemanaged door inhoudelijke mensen die ook in vergaderingen in beperkte mate sturen op een gezonde balans tussen inhoud en het proces [5].

Vergaderingen zonder sturing op het proces leiden bij de deelnemers tot teleurstelling [6]. Om teleurstellingen te voorkomen, meer effect te realiseren met meetings en doelgerichter samen te werken kan vergadersoftware in combinatie met een ervaren facilitator een goede uitkomst bieden. Uit een studie onder maar liefst 900 vergaderingen komt naar voren dat er 56 procent besparing kan worden behaald op mensuren door de inzet van technologie in combinatie met een goede facilitator [6]. Dan te bedenken dat de gemiddelde manager 25 tot 80 procent van zijn tijd besteedt aan vergaderen is de besparingssom binnen een gemiddelde organisatie snel te maken.

56% besparing

"For example, IBM has documented, through a cumulative comparison of person-hours expended, a 56 percent savings attributable to GSS use....However, it is unlikely that a GSS, in and of itself, is sufficient to turn meetings into satisfying, productive events....
although the technology has matured to the point where it is very easy to use by almost anyone, our experience continues to confirm that the quality of the group session is predominantly dependent on the facilitator."

Informatiebeveiliging; een complexe en zorgvuldige zaak

Informatiebeveiliging is een goede maar lastige zaak, immers het vakgebied is continu in ontwikkeling. Wat gisteren een goede praktijk was, is vandaag achterhaald. Het is dus van belang om de actuele en juiste kennis op het gebied van informatiebeveiliging boven op tafel te krijgen. Maar hoe doe je dat?

In het kader van een onderzoek op de Universiteit Antwerpen en Universiteit Nijmegen blijkt dat Group-Support-Systemen (GSS) - ook wel vergadersystemen genoemd - complexe oordeel- en besluitvorming zoals die op het gebied van informatiebeveiliging kunnen vereenvoudigen en versnellen. Aan eenvoud en snelheid is binnen de informatiebeveiliging behoefte.

Iedereen aan het woord

Een GSS kan ingezet worden om de belemmeringen tussen de deelnemers, zoals hiërarchische verhoudingen of verschillen in opvatting, te doorbreken. Door de mogelijkheid anoniem aan de discussie deel te nemen is men meer bereid tot openheid. Immers ideeën worden in de bijeenkomst beoordeeld op hun inhoud en door de anonimiteit niet op hun herkomst. Het verschil tussen introverte en extraverte deelnemers verdwijnt. Daarnaast noodzaakt het maken van een elektronische agenda tot het vooraf analyseren van het vraagstuk, de groepsdynamiek, ofwel de achtergronden en belangen van de deelnemers, in relatie tot het proces en het product van de vergadering.

De versnelling komt doordat iedereen "gelijktijdig" aan het woord is, daardoor kunnen meer mensen deelnemen en duren vergaderingen korter. Een directe analyse onthult de meningsverschillen, waardoor de discussie gericht wordt op de kernpunten, wat tijd bespaart. Uiteraard worden de resultaten van het vergadersysteem direct in een leesbaar verslag gepresenteerd.

Cybersecurity in de boardroom

Cybersecurity is de wat populistische framing van alles wat buiten op het internet gebeurt en invloed kan hebben op onze kritische assets (kroonjuwelen). Dat de betrokkenheid van management en bestuur bij informatiebeveiliging wenselijk is niet nieuw [7]. Betrokkenheid gaat echter verder dan het alleen beleggen bij de CIO of IT-afdeling. Oprechte betrokkenheid gaat over kennis opdoen, hebben en delen – tijdens vergaderingen - zodat je als bestuurder een eigen mening kunt vormen en waarde kan brengen in de besluitvorming [4].

Het onderzoek in Nijmegen en Antwerpen toont aan dat door het gebruik van GSS, vergaderingen rondom het prioriteren van beveiligingsmaatregelen heel effectief kunnen verlopen.

"This paper describes the application of Group Support Systems (GSS) in the field of Business Information Security Governance (BISG). The focus is on longitudinal small team collaboration – for instance within Boards of Directors (BoD), Management Teams and groups of experts – with large amounts of items. It shows how GSS can play a facilitating role in small team collaboration with large amounts of data." [8]

Er bestaat steeds meer een wens en noodzaak om vanuit het bestuur meer richting te geven en grip te krijgen op dit in toenemende mate complexe onderwerp. Deze complexiteit en de hoeveelheid onderwerpen dat het behelst maken het noodzakelijk om op een eenvoudige en snelle wijze inzicht te krijgen en een gemeenschappelijke basiskennis te ontwikkelen [4].

Een voorbeeld-agenda van een CyberSecurity economics, gebaseerd op het Gordon Loeb-model, workshop met een GSS:

De officiële onderzoekpublicatie uit 2015 [9] over het gebruik van GSS in het selecteren Security Governance praktijken en kritische succesfactoren bestempelt GSS als een "krachtig" en vernieuwend middel in kennisdeling en besluitvorming binnen bestuurskamers.

"Information Security (IS) is increasingly becoming an integrated business practice instead of just IT. Security breaches are a challenge to organizations. They run the risk of losing revenue, trust and reputation and in extreme cases they might even go under. IS academic literature emphasizes the necessity to govern Information Security at the level of the Board of Directors (BoD) and to execute (i.e. plan, build, run and monitor) it at management level... GSS is a powerfull and novell instrument to discuss and prioritize complex items such as Information Security Practices. The paper ultimately identifies a list of 22 core principles. This list can function as frame of reference for Boards of Directors and Management Teams in order to increase their level of Business Information Security (BIS) Maturity. [9]

Naast het gebruik voor de wetenschap heeft GSS zichzelf in de praktijk meer dan bewezen. Honderden sessies bij organisaties waar kennisdeling en snelle besluitvorming, over veiligheid van belang is, hebben baat bij GSS. Daarbij is te denken aan organisaties als de Nationale Politie, Justitie, Woningbouw-coöperaties, Waterschappen, TNO, Clingendael en Schiphol.

Van strategie naar operatie

GSS laat zich ook uitermate goed gebruiken voor het analyseren en prioriteren van strategie-elementen. Denk aan strategische elementen van de beroemde Harvard Professor Michael Porter [10] [11]. Zijn modellen blijken uitermate geschikt om middels GSS-sessies de strategische kerndoelen van cybersecurity te bespreken en prioriteren en uit te zetten in een verbeterprogramma van maatregelen [12]. Door de economische waarde van de kroonjuwelen te kwantificeren en deze af te zetten tegen bestaande of nieuwe maatregelen breng je als bestuurder meer kwantiteit en kwaliteit in de financiële besluitvorming over cyber security-investeringen. Het wereldbekende "security economics"-model van Gordon & Loeb [13] geeft de elementen om in een GSS-sessie te komen tot een juiste informatiebeveiligingstrategie en de financiering ervan. Hun model is beschreven in diversen publicaties waaronder het Wall Street Journal [14], en wordt in een animatie [15] op het internet kernachtig toegelicht. Deze animatie is specifiek voor managers, bestuurders en toezichthouders. De animatie is een samenvatting van meerdere publicaties die aantonen dat een slimme strategie in Cybersecurity een positief

Prof. Dr. Ing. Hans Mulder MScBA startte na zijn studies HTS-informatica en Bedrijfskunde aan Nijenrode in 1995 een ICT- en organisatieadviesbureau. Gelijktijdig startte hij aan de TU Delft een onderzoek op het gebied van Enterprise Design, waarin hij onder andere Group Support Systemen (GSS) onderzocht. Na zijn onderzoek ontwikkelde hij het GSS MeetingWizard. Momenteel adviseert Hans diverse ondernemingen en overheden met de inzet van GSS en houdt hij zich als professor, verbonden aan de Universiteit Antwerpen en Antwerp Management School, bezig met bezig onderzoek en onderwijs. Hans houdt zich daarnaast als deskundige frequent bezig met geschillenbeslechting. Hij treedt regelmatig op als deskundige voor Arrondissementsrechtbanken en Gerechtshoven en heeft sinds 1996 meer dan 150 arbitrages, mediations, bindend adviezen en deskundigenonderzoeken uitgevoerd. Hans is auteur van diverse boeken, zoals Eenvoud in Complexiteit en Rapid Enterprise Design, en artikelen, die gepubliceerd zijn in vakbladen en internationale tijdschriften. Hans is bereikbaar via Hans.mulder@meeting-lab.nl

effect kunnen hebben op de gepercipieerde waarde van de organisatie [16]. Ook in dit geval brengen bestaande business modellen nieuwe invalshoeken in het security domein en wordt de GSS-methode gezien als instrument voor high-collaboration-teams om daarmee disruptieve innovatie te realiseren [2]. Het vertalen van - bijvoorbeeld de NCSC-dreigingsbronnen (zie kader) naar effectieve strategische maatregelen waar de organisatie haar kroonjuwelen op een duurzame wijze mee beschermd komen dus niet meer uit de theoretische boeken, uit hoofden van individuen, maar uit de hoofden van het slimme collectieve brein van de groep [17].

Dreigingsbronnen

- **Beroepscriminelen**
- **Staten**
- **Terroristen**
- **Cyber vandalen**
- **Hacktivisten**
- **Interne actoren**
- **Cyberonderzoekers**
- **Private organisaties**

bron: Nationaal Cyber Security Centrum NCSC
[bron: CBSN2015]

Door de inzet van kennisverhogende instrumenten zoals GSS leren bestuurders en managers op eenvoudige wijze hoofd van bijzaken te onderscheiden. Vergaderingen verlopen plezieriger, efficiënter en brengen inzicht in alle relevante bewijzen voor een slimme besluitvorming [18]. Dit geeft hen in een zeer kort tijdsbestek de essentiële kennis en handvatten om het gesprek met de security-professionals te ontdoen van complexe mystiek en jargon. Bewezen technologie en theorie, zoals double-loop-learning, geven zo meer grip om verantwoordelijkheid te kunnen blijven nemen.

Referenties

[1] S. Elsayed-Elkhouly and H. Lazarus, "Why is a third of your time wasted in meetings?," Journal of Management Development, vol. 16, no. 9, p. 672, 1997.

[2] T. Kayser, Mining Group Gold;Third Edition: How to Cash in on the Collaborative Brain Power of a Team for Innovation and Results, vol. 2, Illinois United States: Irwin, 2010.

[3] J. Altier, " Process Expertise - A Critical Managing Fundamental," Business Horizons, no. January, pp. 10-15, 1993.

[4] J. Pai, "An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP).," Management Decisions, Vols. Jan 1-44, no. Emerald Group Publishing Limited, pp. 105-22, 2006.

[5] S. Miranda en R. Bostrom, „Meeting Facilitation: Process Versus Content Interventions," Management Information Systems, vol. 4, nr. 15, pp. 89-115, 1999.

[6] N. Romano and J. F. Nunamaker, "Meeting Analysis: Findings from Research and Practice," in 34th annual Hawaii International Conference on System Sciences, Maui Hawaii, 2001.

[7] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture.," Decision Science, Vols. 28-43, no. 4, pp. 615-60, 2012.

[8] Y. Bobbert and J. Mulder, "Group Support Systems Research in the Field of Business Information Security; a Practitioners View," in 46th Hawaii International Conference on System Science, Hawaii US, 2013.

[9] Y. Bobbert en J. Mulder, „Governance Practices and Critical Succes Factors suitable for Business Information Security," in International Conference on Computational Intelligence and Communication Networks, India, 2015.

[10] M. Porter, How Competitive Forces Shape Strategy, United States: Harvard Business Review, 1979.

[11] Y. Bobbert, „Porters' Elements for a Business Information Security Strategy," ISACA Journal, vol. 1, nr. United States, pp. 1-4, 2015.

[12] Y. Bobbert and A. Niet, "Cyber security in the boardroom," in Oracle Innovation in Government Day, Erasmus University Rotterdam, 2015.

[13] L. Gordon en M. Loeb, „The Economics of Information Security Investment," ACM Transactions on Information and System Security, vol. 5, nr. 4, pp. 438-457, 2002.

[14] L. Gordon en M. Loeb, „You May Be Fighting the Wrong Security Battles: How IT executives can determine the right amount to spend—and where to spend it," The Wall Street Journal, 2011.

[15] Gordon-Loeb Model for Cybersecurity Investments animatie op YouTube https://youtu.be/cd8dT0FuqQ4

[16] L. L. M. Gordon en T. Sohail, „"Market Value of Voluntary Disclosures Concerning Information Security"," MIS Quarterly, vol. 34, nr. 3, 2010.

[17] M. Turoff, S. Hiltz, H. Cho, Z. Li and Y. Wang, "Social Decision Support Systems," in Proceedings of the 35th Hawaii International Conference on System Sciences, Hawaii, 2002.

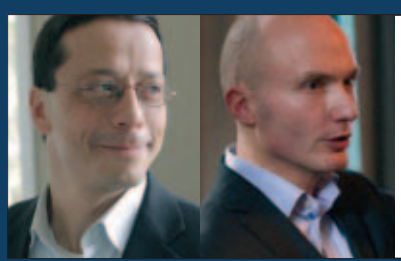
[18] J. S. R. Pfeffer, „ Evidence Based Management," Harvard Business Review, Vols. %1 van %2Pfeffer, J., Sutton, R.I.; (2006) Evidence Based Management, Harvard Business Review Jan 2006, nr. January, pp. 1-13, 2006.

[19] A. Riabacke, "Managerial Decision Making Under Risk and Uncertainty," IAENG International Journal of Computer Science, Vols. 32-4, no. IJCS_32_4_12, 2012.

The "Seven Habits of highly effective CISO's"

Een review vanuit een Chief Financial Officer (CFO)-perspectief.

In 2013 heb ik (Yuri Bobbert) een grootschalig onderzoek gedaan naar de CISO van de toekomst. Een deel van dit onderzoek wordt uiteengezet in dit artikel. Het onderzoek heeft geresulteerd in "Seven habits of highly effective CISO's". In lijn met de "Seven Habits of Highly effective People" van Stephen Covey. Ik heb Hans Go gevraagd zijn reflectie te geven op deze zeven gewoontes. Met name omdat de CISO in toenemende mate rapporteert aan de CFO of de CRO. Hans Go is als interim CFO werkzaam geweest bij Spyker Cars, Unilever en momenteel is Hans de interim CFO van De Koninklijke Nederlandse Munt. In deze functie heeft hij veelal IT en Security in zijn portfolio. De reflectie van Hans Go is in de kaders weergegeven.



Drs. Hans Go RA is Financial & Operational Interim Manager bij Pro Corporate. Hans is bereikbaar via hans.go@procorporate.nl.

Yuri Bobbert (CISO) Msc is PhD onderzoeker en lector op het terrein van bedrijfskritische informatiebeveiliging (Business Information Security). Bobbert combineert zijn lectoraat bij Hogeschool NOVI met zijn rol als CISO. Bobbert is bereikbaar via y.bobbert@novi.nl.

Data als kritische asset op de balans?

Met de intrede van security in de boardroom wordt de vraag actueel hoe dit onderwerp te duiden. Hoe specificeren we het? Wie is verantwoordelijk en aansprakelijk? Dit is noodzakelijk om greep op de materie te krijgen. Het duiden is vooral lastig omdat de kritische assets (in dit geval data) doorgaans niet als zodanig op de balans staan en dus ook niet in het jaarverslag terugkomen. Zelden wordt de goodwill van de data op de balans tot uitdrukking gebracht. Daarom staat dit onderwerp in de meeste gevallen ook niet op het netvlies van de bestuurder (Raad van Bestuur) of de toezichthouder (Raad van Commissarissen). De CISO, als strategisch adviseur van de directie, zal te allen tijde zijn RvB en RvC moeten voeden met feitelijke data over hoe het er aan toegaat binnen de organisatie en de keten(s) waar zij deel van uitmaakt. Om zich een volledig beeld te kunnen vormen, is het dan ook essentieel dat hij zijn eigen logging en monitoring en zijn eigen reporting lines up-to-date houdt. Dit proces kan manueel verlopen, maar deels ook automatisch via dashboard tooling. Alleen op die manier kan hij zijn RvB en RvC voorzien van de meest actuele informatie over risico's die worden gelopen ten aanzien van de stakeholder(s) en kan de RvB en RvC hierover proactief communiceren, onder meer in haar verslaglegging (integrated reporting).

> We kunnen hier de parallel met de CFO leggen. De CFO gebruikt zijn administratieve organisatie en interne controle veelal op basis van automatisch gegenereerde data om deze automatisch te kunnen vertalen naar kritische ratio's als solvabiliteit en liquiditeit. De CFO leunt in toenemende mate op geautomatiseerde tooling waarbij hij met een druk op de knop "fact based" een betrouwbaar beeld van de organisatie heeft. Ten einde zijn jaarverslag te kunnen samenstellen.

Het is anno 2016 nog steeds zo dat het lastig blijkt om grip te krijgen op het veelkoppige monster "Cyber Security". Een belangrijke oorzaak hiervan is dat de bestuurder nog steeds onvoldoende wordt gevoed met input om een gefundeerde discussie te kunnen voeren. De CISO zal hier in toenemende mate een belangrijke rol vervullen, enerzijds als adviseur en anderzijds als sparring partner van het bestuur [1]. Uit onderzoek van IT policy compliance [2] en Accenture [3] blijkt dat organisaties die de rol van CISO strategisch beleggen aanzienlijk beter presteren, in sommige gevallen realiseren deze 6.4% meer winst ten opzichte van het industrie gemiddelde. Dit vergt wel veel van de CISO in zijn rol als strategisch leider. De vraag is of de CISO van morgen wel de juiste kennis en kunde heeft en of de huidige opleidingen voldoende zijn toegerust op dat wat de CISO van de toekomst moet kunnen en kennen.

De CISO van vandaag

In 2013 heb ik een grootschalig onderzoek uitgevoerd om te verkennen wat de strategische kernvraagstukken zijn waar securityprofessionals mee te maken hebben. Ik wilde vaststellen over welke kennis en welke vaardigheden CISO's moeten beschikken om de zogenaamde 'knowing-doing-gap' [13] te overbruggen. De bevraagde security-experts geven aan dat security veelal wordt gezien als een project, maar meer moet worden opgevat als een proces. Dit wordt ook bevestigd door andere onderzoekers [4].
Net als boekhouden is security een proces en geen project. Opvallend is dat de ondervraagden bij de beantwoording van de vragen weinig 'zachte vaardigheden' aanreiken, zoals overtuigingskracht, communicatieve vaardigheden of sensitiviteit aangaande ontwikkelingen in de organisatie. Terwijl ze wel veel waarde bleken te hechten aan zulke 'soft skills' en deze zelfs als een belangrijke succesfactor aanmerkten. Ook verschillende onderzoekers geven deze softskills aan als succesfactor [5]. CISO's zitten ogenschijnlijk dus wat meer aan de hard-skills-zijde (kennis en ervaring) en minder aan de soft-skills-kant (vaardigheden en competenties). Dit is tegenstrijdig aan dat wat bestuurders en toezichthouders verwachten ten aanzien van de toekomstige ontwikkelingen van hun talenten. Zij zien een groeiende behoefte bij zichzelf en hun mensen aan onder andere; helikopterview, kritisch doorvragen, oordeelsvermogen, commitment, resultaatgerichtheid, ondernemingszin en strategisch inzicht [6] [7] [1].
Dit vraagt om een verschuiving binnen de CISO-capaciteiten en hedendaagse opleidingen. Inhoudelijke kennis zal moeten worden aangevuld met bedrijfsmatige, organisatorische en psychologische vaardigheden. Gericht op het aanzetten tot voorwaartse actie. Tenminste, als de CISO de verandering blijvend wil laten zijn en security als een continu proces wil borgen. Al met al kunnen we uit het onderzoek uit 2013 concluderen dat de CISO van vandaag beperkingen heeft. CISO's evalueren en adopteren maar deels de relevante krachten in hun strategie en beleid [8]. Ze weten dat security een continu proces is maar hebben moeite het daadwerkelijk als zodanig te effectueren. Een mogelijke blinde vlek kunnen de sociale vaardigheden zijn. Bijvoorbeeld vaardigheden om doortastend te zijn of meer eisend ten aanzien van het management.

	From…	To…
CEO	Visionary	Purpose-driven
Board Director	Protecting Shareholder value	Increasing shareholder value. Engaging, accountable, international and digitally savvy
CFO	Managing financial performance, compliance, risk and costs	Highly visible and accountable for growth and shareholder value
CHRO	Attracting and developing talent	Driving high-performance culture
CMO	Building awareness and demand	Predicting and delivering top-line growth
CISO	***Protecting and responding to cyber attacks***	***Anticipating, preventing, limiting and responding to attacks. Key Board advisor***
CIO	Managing back-office systems	Delivering competitive advantage
General Counsel	Managing risk	Proactively achieving goals through regulatory framework

Tabel 1 - De essentiële vereiste leiderschapsvaardigheden in 2020 in relatie tot de CISO (afgeleid uit het GET-rapport).

De CISO van de toekomst

De CISO van de toekomst zal doordrongen moeten zijn van het enorme effect dat het vertrouwen van de stakeholders heeft op de continuïteit van zijn organisatie. Hij zorgt verder voor de noodzakelijke verbinding van de governance (het richten) met het management (het inrichten van processen) en met de operatie (het verrichten van activiteiten). En als er stakeholderbelangen in het geding zijn, dan grijpt hij in. Steeds zal hij hun belangen op het gebied van security verbinden aan de belangen en doelstellingen van de organisatie. De CISO van de toekomst is een verbinder zo stelt ook het globale HRM-instituut GET [9] wat jaarlijks onderzoek doet naar C-level-functies en bijbehorende competenties. De CISO van de toekomst is in staat om met bestuurders in begrijpelijke bewoordingen over technische onderwerpen te communiceren. Hij/zij is een vaardige verandermanager die psychologisch inzicht paart aan organisatorische sensitiviteit. Hij beschikt over globale kennis van aanpalende disciplines zoals juridische zaken. Hij weet waar de grenzen van de wet liggen en waar die worden overtreden. Hij weet ook waar de aansprakelijkheden van de organisatie liggen. Hij heeft een inschatting gemaakt van de risico's die de organisatie loopt en is in staat om deze in financiële zin te kwantificeren.
Hij heeft verder globale kennis van HR-processen. Hij weet wat de regels zijn waar gebruikers zich aan moeten houden en zorgt ervoor dat deze niet strijdig zijn met hun wettelijke rechten, zoals bijvoorbeeld vastgelegd in arbeidsrecht en de privacywetgeving. Hij is verder toegerust met globale kennis van architecturen (business-systemen en IT-architecturen) en kan securityarchitectuurprincipes duiden. Ook heeft hij globale kennis van marketing in huis. Kennis die hij vooral intern benut om bij de medewerkers de juiste houding en het juiste gedrag te bewerkstelligen.

Niet in de laatste plaats heeft hij/zij feeling voor finance. Hij begrijpt waar de organisatie haar geld mee verdient, hoeveel er wordt verdiend en of het op een verantwoorde wijze wordt uitgegeven (security van investeringen in relatie tot risico's). Hij is in staat om business cases uit te werken en toe te lichten om de noodzaak van investeringen in security te onderbouwen. Hij maakt een gedegen afweging van security-uitgaven ten opzichte van te realiseren doelen en kan deze afzetten tegen de industriecijfers (benchmarks). De CISO van de toekomst weet bovenal wat hij niet weet. Daarom weet hij dat hij moet samenwerken en is hij daardoor in staat samen te werken in multidisciplinaire teams van experts. Hij waakt als een liaison over de juiste teamsamenstelling van kennis, vaardigheden en ervaring.

The Seven Habits of highly effective CISO's

Op basis van mijn onderzoeken en de inzichten die ik heb opgedaan in de praktijk ben ik tot een overzicht gekomen van de zeven gewoontes van de effectieve CISO voor de toekomst. Dit in lijn met de bekende "Seven habits of highly effective people" van Stephen Covey [10]. Hans geeft zijn kritische reflectie op deze zeven punten vanuit zijn rol als CFO.

The Seven Habits of highly effective CISO's

1. Know your Forces - Be prepared and proactive
2. Scientist - Be critical and curious to anybody
3. Put passion in your IS plan
4. Synthesize, hypothesize and prioritize in vulnerabilities, threats, risks, incidents and disasters
5. Listen, Summarize, Drill down (LSD)
6. Smart Coalitions (synergy)
7. Pump up you brains (sharpen the saw)

UITWERKING VAN KADER

1. Ken je krachten. Uit mijn onderzoek in 2013 wat verschenen is in ISACA journal in 2015 blijkt dat CISO's het vijf krachten model van Harvard Professor Michael Porter goed kunnen gebruiken in het formuleren van hun securitystrategie. En hen bovendien helpt om de mystiek van securityjargon te verlossen. Dit kan helpen in begripsvorming en de boodschap over te brengen aangezien Michael Porter en zijn managementmodellen een algemeen managementbegrip zijn in heden ten daagse bestuurskamer.

Een CFO heeft veel verschillende aandachtsgebieden. Het is onmogelijk voor haar/hem om in al deze gebieden bij te blijven. Daarom is een CISO die zijn vakgebied kent van groot ondersteunend belang. Zeker als deze de invloed van zijn expertise op andere CFO-issues kent (zoals bijvoorbeeld risico, compliance, kosten, business support, et cetera) en bovendien helder kan communiceren! Ik word nog te vaak bestookt met mystiek jargon.

2. Wees kritisch en nieuwsgierig. Don't take no for an answer. Onderzoeksvaardigheden zoals een goede probleemdefinitie kunnen maken, scherpe vragen stellen en waarheidsbevinding zullen de CISO helpen causale verbanden te leggen en daarmee beter onderbouwd de bestuurder van informatie te voorzien. Managementinformatie die van cruciaal belang is in de besluitvorming in het mitigeren van risico's [11] en onderbouwen van investeringselecties. Vragenstellen, probleem en impactanalyse helpt de CISO ook in de juiste prioriteiten te stellen en doelgerichter zijn inzet te verdelen.

Een CFO heeft gevraagd maar zeker ook ongevraagd een sparringpartner nodig op het CISO-gebied. Een goede CISO begeleidt de CFO hierin en behoedt deze voor zaken die van de rails kunnen lopen. Hij denkt mee met risicogebaseerde security-implementaties en kent ook "the basic economics". Ik bedoel daarmee dat de CISO mij ook moet kunnen uitleggen welke financiële rechtvaardiging ten grondslag ligt aan de security-uitgave, en wat de gevolgen zijn als we niets doen. Met andere woorden nadenken over alternatieven.

3. Passie. Geen enkele professional floreert bij passiviteit. De inspiratie die de CISO kan brengen met zijn passie voor het vak kan een groot verschil maken in de omarming van security door niet-vakbroeders. Denk aan leiderschap, voorbeeldgedrag, houding en andere zachtere kanten. Gedragswetenschap leert ons dat verandering succesvoller is als er een hoge mate van empathie en compassie is. Een meer intrinsiek ingegeven leidmotief, zoals goed huisvaderschap, om de securityverandering in te willen zetten [12].

Een CISO met passie voor het vak werkt aanstekelijk en vergroot de kans op acceptatie en omarming door de organisatie. Een CFO weet dit en zal gebaat zijn met een dergelijke persoonlijkheid op de CISO functie.

4. Synthese zorgt voor het onderzoeken en erkennen van de samenhang der dingen. Er zijn vaak verbanden te leggen in het risk- en security-vak. Op de juiste wijze relaties leggen tussen kwetsbaarheden, afwijkende gedragingen van systemen en mensen en incidenten vereist een gezonde vorm van paranoïde. In lijn met verbanden leggen is, timing, vaak komen investeringen in security nooit op een gewenst niveau, er ontbreekt soms een "sense of urgency". Wees je als CISO bewust dat timing "key" is om de juiste budgetallocatie te verkrijgen. Overspeel niet de hand en blijf streven naar gezamenlijk profijt.

Als CFO wil je niet verrast worden. Een CISO die op tijd en realistisch de zaken aankaart, wordt serieuzer genomen dan een CISO die constant angst, stress, en urgentie creëert.

5. LSD; Luisteren, Samenvatten en Doorvragen. Een typische vaardigheid die technici niet altijd voorstaat. Het juist kunnen abstraheren van onderwerpen en tot een scherpe probleemdefinitie te komen vereist luister- en interpretatievaardigheden. Het samenvatten van de probleemstelling helpt je om de bevestiging te krijgen of we over het zelfde spreken en of de verwachtingen gelijk zijn. Doorvragen helpt ons om het probleem verder te ontleden en eventuele verbanden te leggen. Stephen Covey noemt deze gewoonte "aandacht voor andermans belangen". Jezelf bewust zijn van je eigen paradigma's (oogkleppen die de belangen van andere beperken) is een kunst. Hannah Nathans beschrijft dit mooi in haar boek "Adviseren als tweede beroep". Voor elke CISO die zichzelf als strategisch adviseur van de bestuurder ziet zou dit boek moeten lezen.

Een goede CFO wil graag het gehele speelveld overzien en dan op basis van informatie de risico's inschatten dan pas beslissingen nemen en acties initiëren. Een CISO die

dit begrijpt, zal altijd de dubbele bodem proberen op te sporen bij een oplossingsrichting. En tevens een plan B en plan C doordacht hebben mocht hier behoefte aan zijn. Een CISO die durft door te vragen en door te denken is dus van groot belang voor een CFO.

6. Slimme Coalities vormen door samen te werken met groepen en mensen die waarmee je een gezamenlijk belang hebt. De opkomst van samenwerkingsvormen tussen industrieën (CIP, CERT's) zijn een succesvolle aanzet hierin en hebben geleid tot vele succesvolle verbeteringen zoals Secure Software Development, Grip op datalekken, Beveiliging in inkoopcontracten.

Een CFO heeft vele stakeholders te managen, vaak met verschillende belangen en krachten velden. Een CISO die deze situatie snapt kan een CFO beter van dienst zijn en dit zal altijd worden gewaardeerd. Het kunnen voorsorteren voor bereiden met derden is dus van groot belang. Een CISO die zeer intelligent is maar alleen op zijn/haar kamer blijft zitten is echt van minder waarde voor een CFO dan iemand die vooral op pad gaat om structuren te smeden.

7. Onderhoud je zwaard zoals Covey het stelt. Zorg dat je constant bijblijft qua kennis en kunde. Door middel van permanente educatie de kennis en vaardigheden eigen blijven maken om de organisatie blijvend te kunnen (be)dienen. Voor het securityvakgebied, waarin veranderingen zich continu voordoen, zijn snelheid en doelgerichtheid van eminent belang. Interventies die nodig zijn om beveiliging naar een hoger plan te tillen kunnen niet uit louter theoretische zaken bestaan. Er is een voortdurende terugkoppeling vanuit de praktijk nodig. Snelle feedback-loops zijn essentieel. Daarom is 'action research & learning' zo'n uitermate geschikte methodiek voor ons vakgebied. Juist door deel uit te maken van het te onderzoeken object ontstaat 'levende kennis'.

Net zoals een CFO zijn permanente educatie moet onderhouden verwacht hij dat de CISO dat ook doet. Kwaliteit moet onderhouden worden. Je wilt geen mensen die de ontwikkelingen niet volgen maar er op anticiperen en deze mede vorm geven. Als CFO kan ik het waarderen dat securityprofessionals eens in de zoveel tijd bijpraten over trends en ontwikkeling, zeker als het gaat over fintech achtige ontwikkelingen waarbij onze expertisegebieden elkaar kruisen.

Referenties

[1] GET2020, „The essential C-suite leadership abilities required in 2020," CT Partners , United States, 2015.

[2] I. P. C. Group, „Best Practices for Managing Information Security," IT Policy Compliance Group, US, 2010.

[3] Accenture, „The Cyber Security Leap: From Laggard to Leader," Accenture , 2015.

[4] W. Flores, E. Antonsen and M. Ekstedt, „Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," computers & security, Vols. 1 van 22014-43, pp. 90-110, 2014.

[5] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture.," Decision Science, Vols. 28-43, no. 4, pp. 615-60, 2012.

[6] A. Klaassen en H. Rijken, „RvC moet meer proactief 'mee ademen' met bedrijf; Commissarissenonderzoek 2013/2014," GrantThornton, 2013.

[7] Forbes, „For Top CEOs, Culture Drives Value Creation," http://www.forbes.com/sites/robertreiss/2012/10/10/for-top-ceos-culture-drives-value-creation/, 2012.

[8] Y. Bobbert, „Porters' Elements for a Business Information Security Strategy," ISACA Journal, vol. 1, nr. United States, pp. 1-4, 2015.

[9] GET2020, "The essential C-suite leadership abilities required in 2020," CT Partners, United States, 2015.

[10] S. Covey, The Seven Habits of Highly Effective People, United States : Free Press; ISBN 9789047054641, 1989.

[11] D. Kahneman and A. Tversky, "Prospect Theory: An Analysis of Decision under Risk," Econometrica, vol. 47, no. 2, pp. 263-292, 1979.

[12] Luft, J.; Ingham, H., "The Johari window, a graphic model of interpersonal awareness," in Proceedings of the western training laboratory in group development, UCLA , 1955.

[13] J. Pfeffer and R. Sutton, "The Knowing?Doing Gap: How Smart Companies Turn Knowledge into Action," no. Harvard Business School Press, 2001.

Publicaties van de auteurs

Yuri Bobbert schreef in 2010 het boek *Maturing Business Information Security, a framework to establish the desired state of security maturity,* dat wordt gebruikt op verschillende universiteiten en hogescholen. Vanuit dit boek zijn de MBIS-methode en het MBIS-platform ontstaan (mbis.eu). In 2014 verscheen zijn tweede boek: Hoe Veilig is mijn 'aandeel'?, Het borgen van Reputatie, Vertrouwen en Continuïteit met de MBIS methode'.

Hans Go schreef in 2014 het boek *Wat zeggen die cijfers eigenlijk?* Tips & tricks voor niet-financiële professionals. Een boek voor niet-financiële mensen waarin op bijzonder toegankelijke wijze wordt beschreven hoe de financiële huishouding van een organisatie in elkaar steekt. EAN: 9789089652263

Leestips:

- http://www.forbes.com/sites/sungardas/2015/04/07/looking-for-a-practical-ciso-job-description-heres-a-day-in-the-life-of-the-ciso/
- http://infosecuritymagazine.nl/2015/03/24/de-chief-information-security-officer-van-morgen-op-zoek-naar-een-duizendpoot/
- https://www.pvib.nl/download/?id=17705208&download=1

- "Adviseren als tweede beroep", resultaat bereiken als adviseur. Auteur: Hannah Nathans.ISBN nummer: 9013028802.

STAKEHOLDERANALYSE; DE CISO'S GRIP OP INFORMATIEDELING MET DERDEN

Weet u als CISO welke informatie uw organisatie deelt met derden? In de praktijk blijkt uit onderzoek en nadere analyse dat organisaties geen compleet beeld hebben en onderschat wordt met hoeveel 'stakeholders' (al dan niet vertrouwelijke) informatie wordt gedeeld.

Zo bleek een organisatie, actief in de wereld van incassobureaus, al enige jaren aan bestandsverrijking te doen via een dataverrijkingbureau, waarvan de holding een concurrerend incassobureau bleek te zijn, tot schrik van één van de verantwoordelijke leden van de Raad van Bestuur.

Een zeer goed draaiende webwinkel maakte voor haar marketingacties gebruik van een extern bureau dat de mailing verzorgde. Ze ontdekten pas na een stakeholderanalyse dat nergens in het contract, noch in de SLA (Service Level Agreement) is vastgelegd dat de verstrekte data moet worden gewist na gebruik voor het beoogde doel. Ze hadden zomaar de 'kopie webwinkel' kunnen beginnen.

Een andere organisatie maakte vanuit de HRM-afdeling gebruik van een Arbo-dienst, die op haar beurt gebruik maakte van een inhuur Basisarts in opleiding, die parttime fungeerde als Arbo-arts, en volledige dossiers, inclusief medische gegevens, uitprintte en bewaarde op een studentenkamertje drie hoog achter in een studentenstad. Niet bepaald borging van de privacy van (zieke) medewerkers.

Stakeholderanalyse

Genoemde praktijkvoorbeelden zijn de resultaten van meerdere uitgevoerde stakeholderanalyses. Een aanpak overigens die zijn oorsprong kent vanuit Corporate Governance-principes [1][2] en verder is vormgegeven vanuit de wetenschappelijke wereld en door het combineren van bewezen methodieken zoals DEMO ('Design & Engineering Methodology for Organizations) [3]. Al jaren wordt op de Politie Academie bij rechercheonderzoek onderwijs gegeven in onder andere hypotheses en scenario's en de zogenaamde Criminaliteit Beeld Analyse (CBA) [4]. Op Technische Universiteiten is de DEMO-methodiek voor het ontologisch ontleden van enterprises niet onbekend. In 2009 is hiervan in het IB magazine een uitleg gedaan en voorbeeld gegeven aan de hand van het Electronisch Patienten Dossier [5].

De stakeholderanalyse is in feite een civiele variant van deze CBA, die vanuit een holistische benadering - die de DEMO-methodiek kenmerkt - heeft geleid tot een werkbare en pragmatische aanpak. In de praktijk worden alle stakeholders in beeld gebracht via een systematische analyse van de context van een organisatie.

na clustering kan 60% van deze kwetsbaarheden eenvoudig zelf opgelost worden

DEMO is the next generation methodology for modeling enterprises

It is a widely adopted international standard for designing and engineering 'extended enterprises'. The notation 'extended' indicates the broad variety of social interaction and interoperatibility between enterprises to accomplish a mutual benefit. Enterprises work together on all kinds of layers within the organization and therefore they cope with more and more extended inter(trans)actions that make use of information technologies –like the internet- to exchange business critical information.

Na nadere analyse bleek de informatie-uitwisseling vaak in één of meerdere opzichten substantiële risico's te bevatten, waarvoor actie en opvolging nodig was om die risico's te mitigeren, dan wel in ieder geval te reduceren.
Er werden verschillende typen risico's onderkend, namelijk:

- een organisatorisch afhankelijkheid (bijvoorbeeld van een beheerorganisatie)
- een contractuele afhankelijkheid (bijvoorbeeld van de kennis en kunde van een organisatie)
- een juridische afhankelijkheid (bijvoorbeeld via condities/randvoorwaarden in het contract/SLA)
- een technische afhankelijkheid (bijvoorbeeld van een schakel in de informatie bewerkingsketen)
- een ongewenst risico en/of kwetsbaarheid in termen van bedrijfscontinuïteit.

Binnen de zogenaamde Maturing Business Information Security (MBIS)-methodiek [6] wordt gebruik gemaakt van de stakeholderanalyse om bovenstaande risico's en afhankelijkheden inzichtelijk te maken. In feite stellen we bij de uitvoering van deze analyse de volgende vraag; wat betekent het voor uw organisatie in termen van Vertrouwelijkheid, Integriteit en Beschikbaarheid (CIA-triade).

Opvolging na een stakeholderanalyse

Uit ervaring blijkt dat na clustering 60% van deze kwetsbaarheden eenvoudig door de organisatie zelf opgelost kunnen worden. Voor de overige zullen (deel)projecten opgesteld moeten worden die gericht zijn op het mitigeren van de risico's. Hierbij valt onder andere te denken aan:

- Bewustzijnscampagne
- Vaststellen inkoopvoorwaarden
- Opstellen van SLA's

Hiermee geven we de CISO de juiste effectieve handvatten om grip te krijgen en houden op de informatiedeling van zijn organisatie met derde partijen in de digitale keten. Tevens helpt het de CISO verantwoordelijkheden voor controls op de juiste plaats te beleggen. Dit is relevant in het kader van governance en assurance over zijn digitale keten heen.

Referenties

[1] CACG. (1999). Guidelines principles for corporate governance in the commonwealth; Towards global competitiveness and economic accountability. Marlborough, New Zealand: Commonwealth Association.

[2] Mallin, C. (2010). Corprate Governance, Third Edition. New York: Oxford University Press.

[3] Meer informatie over DEMO: http://www.ee-institute.org

[4] Clarke, Ronald V. en Eck, John E. (2010). Probleemgericht werken en de rol van criminaliteitsanalyse in 60 kleine stappen. Rotterdam: Hogeschool INHolland; Apeldoorn: Politieacademie.

[5] Bobbert, Y. (2009). Use of DEMO as a methodology for business and security alignment. PvIB Magazine, 22-26.

[6] MBIS Methodiek: http://www.mbis.eu/

Drs. Hilko Batterink CISM CIPP/E is business/security consultant/beleidsadviseur bij DPA B-Able met veel expertise op het gebied van Security Governance en Security Assurance in zowel de business als IT omgevingen. Hij is daarnaast kernlid van de Domeingroep Governance en Normatiek van het CIP (Centrum voor Informatiebeveiliging en Privacybescherming) en tevens bestuurslid van de ISACA NL Chapter en daar actief als Government and Academic Relations Director.

COMPETENTIES MANAGEN OP BASIS VAN LEARNING-ANALYTICS

Hoe kan de CISO meer sturing geven aan de juiste kennis en competentiebalans binnen zijn security teams? In een snel veranderende omgeving zoals die van information-security, zijn vragen als deze aan de orde van de dag. Functieprofielen en de daarbij horende competenties, kennis, taken en verantwoordelijkheden zijn steeds minder statisch en lijken bijna dagelijks te veranderen door de dynamiek en de continue technologische ontwikkelingen in de omgeving van de securityprofessional. Het wordt daardoor steeds belangrijker om goed zicht te hebben op de aanwezige competenties en kennis van personeel, zodat je hier doelgericht op kunt sturen en kunt borgen dat medewerkers voldoende zijn toegerust om hun functie naar behoren in te vullen. Learning-analytics, analyse op basis van learning-data, kunnen hier in de toekomst een belangrijke rol in gaan spelen. Maar tot op heden wordt hier nog weinig gebruik van gemaakt in het bedrijfsleven.

Bij het verwerken van learning-data tot zinvolle statistiek, zogenaamde learning-analytics, kan men denken aan het collecteren, analyseren en interpreteren van learning-data van medewerkers en de omgeving waarin het onderwijs plaatsvindt. Op basis van deze data (data over de leerinspanning en resultaten van medewerkers), de interpretatie hiervan en de conclusies die je hieruit trekt, kun je doelgericht sturen op verbetering.

Je kunt bijvoorbeeld op basis van gedragsanalyse (gedragsfunnels, heatmaps, page-analytics) zien in welke mate/op welke wijze leercontent wordt gebruikt. Je kunt zien waar de medewerkers moeite mee hebben op basis van testscores. Je kunt zoeken naar een relatie tussen de tijd binnen de leeromgeving en toetsresultaten om een inschatting te maken in welke mate de content bijdraagt aan de leerontwikkeling.

Als je erin slaagt leerinspanningen accuraat te registeren en ook het rendement daarvan inzichtelijk te maken, kun je het management op alle lagen binnen de organisatie doelgerichte feedback geven op de individuele als ook collectieve competentieontwikkeling. Je kunt real-time laten zien in welke mate de medewerkers de kennis en het gedrag dat hoort bij hun functieprofiel adopteren en toepassen.

Kortom, de belangrijkste kernvoordelen van learning-analytics zijn:

1. Verkrijgen van inzicht in de performance en competentie-ontwikkeling van medewerkers (en de ROI van Learning & Development-inspanningen)
2. Verkrijgen van accurate en actuele stuurinformatie voor staf en management
3. Verkrijgen van inzicht in leerstijl, -voorkeur en rendement van medewerkers waarmee onderwijs effectief kan worden geïndividualiseerd

Learning-analytics als managementinformatie

Hogeschool NOVI experimenteert bij haar opdrachtgevers met het ontsluiten van dergelijke management informatie op verschillende niveaus. Zo laat NOVI teamleiders zien welke competenties individuele medewerkers beheersen en met welke zij nog moeite hebben op basis van toets- en assessment-resultaten. Op basis van geautomatiseerde mailberichten krijgt zo'n teamleider dan inzicht in de voortgang en leerresultaten van de medewerker en kan hij overwegen om een bepaald onderwerp toe te lichten aan zijn medewerker. Of bijvoorbeeld medewerkers met een complementair competentieprofiel met elkaar in contact brengen zodat ze van elkaar kunnen leren.
Hiermee krijgt de learning-data dus ook een sterke HR-functie voor staf en management en kan het eveneens ingezet worden om beter te kunnen sturen op teamdynamica, of de voortgang van bijvoorbeeld een reorganisatie.

Het 70:20:10-principe

Het "on the job"-leren en ontwikkelen is gebaseerd op het 70:20:10-principe [1]. Dit principe gaat ervan uit dat een werkende professional 70% leert via niet professionele trainers of docenten. Bijvoorbeeld door collega's, vrienden en relaties in de werksfeer. 20% leert via coaching en mentorschap en 10% door formele opleidingen en cursussen [2]. De balans van dat wat organisaties weten, vaak vertegenwoordigd in de hoofden van het individu, en dat wat ze kunnen, de mate waarin de 70% wordt benut en toegepast, is in het geval van security-effectiviteit van groot belang. In de theorie noemen we dit "het kennis-en-kunde-gat" (knowing-doing gap) [3]. Feitelijke kennis die wordt opgedaan blijft bij het toepassen van het 70:20:10-principe dus niet in de hoofden van de professional maar wordt actief gedeeld en komt zo de ontwikkeling van het individu als ook de organisatie ten goede [4]. Dit actief delen van kennis doet de effectiviteit van de security-organisatie toenemen [5]. Lector Yuri Bobbert van Hogeschool NOVI heeft onderzoek gedaan naar kennismanagement binnen Informatiebeveiliging en zogenaamd actiegericht Research, Learning and Development (RLD).

Voor de staf en het hoger management geeft Hogeschool NOVI feedback op meer abstracte KPI's, door de data van de gehele populatie te analyseren. Hierbij kan men denken aan zaken die relateren aan de voortgang van de reorganisatie, het gebruik van opleidingsbudget, de doeltreffendheid van de leercontent (ROI) en de competentieontwikkeling van de totale populatie of specifieke doelgroepen hierbinnen.

Ook voor de medewerker kun je de leerervaring aanzienlijk verbeteren door het gebruik van learning-data. Dat begint bij het accuraat inzichtelijk maken van leerprestaties, voortgang binnen een traject en de mate waarop dit aansluit bij zijn of haar doelen. Ook kun je op basis van bijvoorbeeld een functieprofiel, de keuzes voor specifieke content uit het verleden en behaalde resultaten de medewerker steeds beter relevante content aanbieden. Je kunt aan de hand van gekozen modules een aanname doen ten aanzien van zijn carrièreverloop/leerroute en op basis hiervan suggesties doen voor nieuwe en

George Vlug is Manager Business Development & Innovatie bij Hogeschool NOVI. Vanuit die rol is George verantwoordelijk voor alle business development, sales, marketing en innovatie-activiteiten van de instelling. Hogeschool NOVI leidt professionals in de Business en IT op en verzorgt hbo-opleidingen op het gebied van Bedrijfskunde, IT en Informatievoorziening. Dit studiejaar werd Hogeschool NOVI door de Keuzegids uitgeroepen tot beste deeltijdopleider van Nederland. Organisaties als het Ministerie van Defensie, ABN AMRO en Eneco behoren tot NOVI's klantenkring. George Vlug is bereikbaar via g.vlug@novi.nl

relevante modules. Doordat je ziet waar de medewerker goed of juist slecht op presteert kun je de service rondom het onderwijs personaliseren. Bijvoorbeeld door extra coaching op additionele content aan te bieden.

Een compleet zicht op ontwikkelingen

Organisaties, scholen en onderwijsinstellingen hebben moeite met het destilleren van de juiste data uit allerlei diverse activiteiten. Leerinspanningen en de concrete resultaten waar deze toe leiden zijn veelal lastig te vangen en duiden. Ook is de leerinspanning niet altijd direct tot een concreet rendement toe te schrijven en worden de inspanningen op verschillende plekken (offline of online) uitgevoerd.

Het gevolg hiervan is dat organisaties weliswaar over een enorme data-berg beschikken, echter dat deze diffuus verdeeld is over verschillende systemen, naar verschillende standaarden geordend, en zich moeilijk tot elkaar verhouden waardoor het lastig is de data te gebruiken ten behoeve van goede analyses.

Daarbij is essentieel om grip te krijgen op de totale leercurve van een individu. Ook wanneer iemand leert door bijvoorbeeld met een deskundige collega te spreken, informatie zoekt op het internet of een webinar volgt. De manier waarop mensen leren en waar zij hun informatie vandaan halen wordt steeds meer gefragmenteerd. Mensen zijn veel meer zelfredzaam doordat informatie veelal gemakkelijk toegankelijk is op het internet. De ontwikkeling die een medewerker doormaakt buiten een formele opleidingsomgeving wordt slechts zelden geregistreerd. Vaak omdat organisaties niet weten hoe dit moet of omdat de systemen die gebruikt worden voor het registreren van opleidingsinspanningen hier geen ruimte toe bieden.

Toch ontstaan er steeds meer mogelijkheden op dit vlak. Zo is het technisch beter mogelijk om de learning-data tussen verschillende databases uit te wisselen, zodat je deze data kunt samenbrengen op een centrale plek en het zo kunt gebruiken voor je analytics. Denk bijvoorbeeld aan de uitwisseling van data via de Tin Can xApi. Tin Can is een communicatiestandaard die je helpt leerinspanningen naar eenvoudige 'statements' te vertalen. Een statement beschrijft aan de hand van een aantal variabelen wie welke leeractiviteit heeft uitvoerd, op welk moment en met welk resultaat. Of dat nu het POP-gesprek met de manager, het lezen van vakliteratuur, het bezoeken van een congres of het volgen van een MOOC (Massive Open Online Course) was.

Voor het registreren van de activiteiten zijn tal van applicaties beschikbaar, en omdat Tin Can open source is, kun je er ook betrekkelijk eenvoudig zelf iets voor ontwikkelen. Hierbij is het belangrijk dat je de geregistreerde activiteiten, of dit nu een MOOC, POP-gesprek, of congres is, op zo'n manier registreert dat men de leerinspanning kunt relateren aan de variabelen waarop men wilt kunt managen, bijvoorbeeld de competenties, kennis en vaardigheden uit het functieprofiel.

Kennismanagement als onderscheidend vermogen in de "war on talent"

Wanneer je er als organisatie in slaagt om learning-data op een accurate wijze te registreren en structureren op zo'n manier dat je een compleet beeld krijgt van iemands ontwikkeling, kan je dit gebruiken om goede analytics te genereren ten aanzien van de competenties van een individu of groep. Dit geeft de juiste stuurinformatie in relatie tot het competentiemanagement, maar ook in relatie tot de ROI van Learning & Development inspanningen.

In een wereld die steeds dynamischer wordt en afhankelijker is van kennis en competenties van medewerkers krijgt kennismanagement een steeds prominentere plaats binnen organisaties. Niet alleen om de kennis uit de hoofden van het individu te delen met anderen, denk aan de 70% kennisadoptie, maar ook om een inspirerende omgeving te zijn. Werknemers "boeien en binden" met kennismanagementprogramma's wordt door diversen HR-organisaties naar voren gebracht als een middel om het intellectuele kapitaal van de onderneming te behouden en onderhouden. En in veel gevallen een unieke(re) arbeidsmarktpositie kan geven als het gaat om de "war on talent". Programma's waarbij de aandacht wordt gelegd op het structureel opbouwen van kennisdata over het individu alsook het collectief lijken onvermijdbaar en in toenemende mate van belang om constant aantrekkelijk te blijven voor medewerkers.

Conclusie

De veelzijdigheid van het securityvakgebied groeit. Door toenemende wet- en regelgeving, innovaties en stakeholder-eisen neemt ook de behoefte aan specifieke kennis en competenties toe. De CISO van de toekomst zal in toenemende mate zijn security-organisatie gerichter willen inrichten en sturen op kennis en competenties. De CISO kan dan terugvallen op learning-data die is verzameld binnen de organisatie.

Voor Hogeschool NOVI is learning-data een belangrijke driver in onderwijsvernieuwing. De eerste data-analytics-pilots bij verschillende organisaties zijn veelbelovend en de lessen die hieruit worden geleerd zullen een essentiële plek krijgen in doorontwikkeling van het onderwijs bij NOVI.
Hiermee kan NOVI zichtbaar bijdragen aan organisatiedoelstellingen, medewerkers beter individueel bedienen en onderwijs op een dynamische wijze invullen.

Referenties

[1] K. Kajewski en V. Madsen, „Demystifying 70:20:10," Corporate Education, nr. Deakin University, 2013.

[2] A. Tough, „Adults Learn: A Study of the Major Reasons for Beginning and Continuing a Learning," Ontario Institute for Studies in Education, vol. Toronto, 1968.

[3] J. Pfeffer and R. Sutton, "The Knowing?Doing Gap: How Smart Companies Turn Knowledge into Action," no. Harvard Business School Press, 2001.

[4] S. Cook and J. S. Brown, "Bridging Epistemologies: The Generative Dance between Organizational Knowledge and Organizational Knowing," Organization Science, vol. 10, no. 4, pp. 381-400, 1999.

[5] D. Feledi and S. Fenz, "Challenges of Web-Based Information Security Knowledge Sharing," in Seventh International Conference on Availability, Reliability and Security, IEEE, 2012.

SAMENZIJN

We zijn op weg naar Brussel als mijn dochter naast me in de auto zegt: "Mama, moeten we nu bang worden?" We praten over de aanslagen want juist die zijn aanleiding dat we nu naar Sint-Jans-Molenbeek (in de media afgekort tot "Molenbeek") gaan om onze familie te knuffelen. Ze kijkt me met een opgetrokken wenkbrauw aan en geeft zelf maar vast het antwoord: "Echt niet he!". Ik bewonder haar jeugdige doortastendheid. Zelf was ik namelijk best een beetje bang en voor het eerst in tijden voelde ik haarscheurtjes komen in mijn "privacy voor veiligheid"-adagium.

Op 22 maart besluit mijn zwager dat hij eens niet met de metro naar het werk aan de Rue de la Loi gaat, maar dat hij lekker op de fiets zal stappen. Een beslissing die hem later op de dag aan allen laat melden dat hij veilig is en "gaat straks vrouw, kinderen, buurman, bakker, diens vrouw en haar hond maar eens goed knuffelen want van stoere praat is niemand ooit beter, laat staan veiliger, geworden."

Direct na de eerste meldingen van aanslagen in Brussel, loop ik getergd rond door mijn huis. Tv aan (voor het eerst in 6 jaar kijk ik naar nieuws) en met de telefoon in de hand probeer ik mijn zus te bereiken om te vragen of een ieder gezond en wel is, wetend dat haar man zich "in dé zone" bevindt. We communiceren via WhatsApp, het mobiele netwerk ligt eruit en bellen is onmogelijk. Zodra het "iedereen is ongedeerd" me bereikt, stromen de tranen over mijn wangen. Opgelucht en tegelijk zo verdrietig en ook boos over wat er allemaal gebeurt.

In de dagen die volgen voel ik mijn eigen geloofssysteem op momenten wankelen. Zou het helpen om dit soort zaken te voorkomen als we wat privacy inleveren? Rationeel weet ik natuurlijk best dat het inleveren van privacy geen veiligheid oplevert, maar dat is makkelijk praten op emotionele momenten. Ik snap zo vreselijk goed dat angst, afschuw en boosheid leiden tot boude uitspraken en dat de behoefte tot het veilig voelen overheerst. En ik snap ook heel goed dat dit een uitgelezen moment kan zijn om allerlei privacyonvriendelijke maatregelen in te voeren. Hey, als zelfs een privacyfundamentalist zich onvast op haar voeten voelt…

Reden temeer dus om als één front op te staan tegen die privacyonvriendelijke maatregelen. Als het ooit tijd was om je sterk te maken voor privacy en andere grondrechten, dan is het nu wel. Kritisch zijn en blijven is juist nu onze kracht. Niet toegeven aan angst (ja, ook ik zeg het nu) en doe als die geweldige 8-jarige kleine Diva van mij. Kijk naar de wereld en diegenen die je liefhebt en geloof in het mooie en het goede van de mens. Terwijl ik in Brussel aan de tafel zit en om me heenkijk besef ik me dat er geen veiliger gevoel is dan met al je geliefden samen te zijn.

Mr. Rachel Marbus
@rachelmarbus op Twitter

BELEG SECURITY IN DE LIJN

Interview met Paul Oor, Security Manager Atos

Het Business Prevention Department. Met die woorden werd nog niet eens zo heel lang geleden de security-afdeling van menig bedrijf omschreven. Paul Oor, Chief Security Officer Benelux & The Nordics van Atos, kan het weten. Met woorden van dergelijke strekking kreeg ook hij te maken. Sinds enkele jaren is de situatie volgens hem compleet veranderd.

Het bijna standaardantwoord op security-vragen 'Nee, kan niet', wil Paul niet meer horen. Het is nu 'Ja' of 'Ja, mits'. "Voor ons als Atos is innovatie een steeds belangrijker thema, zowel intern als naar klanten toe. Dan kan en wil ik niet degene zijn die ontwikkeling tegenhoudt en daarmee de business in de weg staat", stelt hij onomwonden. Het sleutelwoord is wat mij betreft 'risicobereidheid'. Welke risico's ben je bereid te nemen om te komen tot succesvolle, veilige groei. Dat is de vraag die we ons als totale organisatie continu moeten stellen."
De tijd dat security van een bedrijf een ondoordringbaar fort maakte en dit vervolgens bewaakte, ligt wat Paul betreft dus in het verleden. Security levert wat hem betreft anno 2016 een bijdrage aan de business. Security is in zijn ogen dus veel meer geworden dan focus op audits, beleid en compliance alleen.

Interessanter en uitdagender

Een verandering die Paul absoluut niet terug zou willen draaien. Zijn vak is er veel interessanter en uitdagender op geworden. "Omdat er veel meer van ons wordt gevraagd", legt hij uit. "Vroeger bedachten we vooraf wat er allemaal mis kon gaan bij de implementatie van bijvoorbeeld een nieuwe tool of de introductie van een nieuwe techniek. Op basis hiervan stelden we regels op en hier moest iedereen binnen de organisatie zich aan houden."
Regels zijn wat hem betreft ook nu nog nodig, maar hij ziet ze meer als de witte lijnen op de snelweg waar je tussen moet blijven. "Bovendien kunnen er uitzonderingen zijn en kun je in bepaalde situaties de witte lijnen negeren. Zoals je dat op de weg ook mag doen in de spits wanneer de spitsstroken zijn opengesteld en je dus een doorgetrokken witte lijn mag passeren."
"Bij twijfel of er in bepaald geval sprake is van een 'spitsstrook-situatie' moeten collega's van allerhande afdelingen je als Security Officer weten te vinden", benadrukt Paul. "Die vertrouwenspositie moet je hebben om je vak anno 2016 op de juiste manier in te kunnen vullen. Heb je deze positie niet, dan vindt men een weg om je heen en dus ook om regels en voorzorgsmaatregelen heen", waarschuwt hij.

Rol als regisseur

Paul omschrijft zijn rol als Chief Security Officer gezien de genoemde ontwikkelingen als die van een 'regisseur' binnen de organisatie. "Formeel ben ik een minister zonder portefeuille. Ik heb geen eigen budget en geen mensen waaraan ik direct leiding geef."
"In feite zijn al mijn collega's mijn voelsprieten binnen de organisatie. Mijn ogen en oren. Iedereen moet mij weten te vinden wanneer ze ook maar de minste of geringste twijfel hebben. Of het nu gaat over een verdacht pakketje in de parkeergarage of een vermoeden van een datalek."

Deze vertrouwenspositie bouw je volgens Paul niet zomaar even op. "En het lukt ook niet iedereen", benadrukt hij. "Een moderne Security Officer moet in mijn ogen een echte netwerker zijn. Een vakkundig adviserende 'verkoper', noem ik het ook wel. Wat je wil bereiken binnen een organisatie is immers nadrukkelijk zelfsturend vermogen. Security moet anno 2016 ingebed zijn in de business zelf en niet alles zelf hoeven doen."

Eigen verantwoordelijkheid

Het feit dat hij geen eigen budget heeft, is voor hem precies om de hierboven genoemde reden geen probleem. Integendeel, hij ziet het als een voordeel. "Had ik een eigen budget dan roept iedereen tegen mij: 'Dan doet security het toch lekker zelf!' Nu dat niet het geval is, wordt de eigen verantwoordelijkheid voor security binnen de business veel meer gevoeld."
Security en in het verlengde daarvan privacy zijn binnen Atos dus nadrukkelijk zaken waar iedereen oog voor heeft en ook moet hebben. Niet voor niks worden nieuwe medewerkers vrij snel na binnenkomst door Paul geïnformeerd over het belang hiervan voor de organisatie als geheel. "Op die manier probeer ik direct awareness bij iedereen te kweken", legt hij uit.

Naast het intern bouwen aan een netwerk, noemt Paul het voor een moderne Security Officer ook van groot belang buiten de eigen organisatie contacten te leggen. Navelstaren past wat hem betreft niet in open wereld zoals we die anno nu kennen. "Je moet juist werken aan smart coalitions, zoals het Nationaal Cyber Security Center (NCSC), dit noemt. Om zo diegenen met verkeerde intenties tegen te houden. Als professionals kunnen we hierbij nadrukkelijk van elkaar leren. Vakverenigingen als PvIB, ISACA en ISC2 zijn hierin heel belangrijk", geeft hij aan.
"De techniek ontwikkelt momenteel zo snel. Om van de laatste stand van zaken op de hoogte te zijn, heb je deze externe contacten ook nodig. Je kunt simpelweg niet alles zelf bijhouden."

Sandra Kagie is freelance tekstschrijver/journalist (website: www.sanscriptproducties.nl; Twitter @SanScript). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'.

“De tijd dat security van een bedrijf een ondoordringbaar fort maakte en dit vervolgens bewaakte, ligt in het verleden.”

Zorg: snelheid van ontwikkelingen

De snelheid waarmee ontwikkelingen momenteel gaan én maatschappelijk worden geaccepteerd, verbaast Paul misschien nog wel het meest. “The internet of things, het feit dat de fysieke wereld en de cyberwereld of de logische wereld steeds meer in elkaar grijpen. De toegenomen waarde van allerhande data en informatie. Het zijn ontwikkelingen die we hebben voorzien. Maar het gaat allemaal wel heel snel. En dat beschouw ik als een belangrijke zorg.”
“Gebruikers halen informatie binnen zonder te weten wat het precies behelst. Ze maken gebruik van apparaten en applicaties zonder te weten wat ze precies gebruiken. En daarin schuilt wat mij betreft het belangrijkste gevaar.”

“Eerdere lifechanging-ontwikkelingen zoals het industrieel en later ook huishoudelijk gebruik van elektriciteit, gingen veel geleidelijker. Het duurde decennia voordat dit ‘normaal’ en ‘veilig’ was. Hetzelfde geldt voor de introductie van de auto. Terwijl we nu bij nieuwe ontwikkelingen amper de kans krijgen om te snappen wat er precies gebeurt.”

Een punt van zorg dus wat Paul betreft. “Maar zeker geen reden om op de rem te gaan staan”, haast hij zich te zeggen. “We moeten ons echter wel bewust zijn van de risico’s. En hierop anticiperen door bijvoorbeeld in ons onderwijs aandacht te besteden aan de ontwikkeling van nieuwe competenties: samenwerken, oplossingsgericht denken, risico’s en initiatieven durven nemen”, somt hij op.
Om de uitdagingen van de 21e eeuw het hoofd te kunnen bieden, moeten we geen ‘nee-zeggers’, maar ‘ja, mits’ers’ opleiden. Want dat zijn wat Paul betreft de mensen die over enkele jaren die vraagstukken kunnen oplossen waarvan we het bestaan nu nog niet eens weten.
“Sociale- en netwerkvaardigheden moeten daarom in security-opleidingen veel dominanter worden”, stelt hij. “Duidelijk en effectief communiceren is essentieel.” Een opleidingstaak waarbinnen hij ook voor zichzelf en zijn collega’s een belangrijke rol ziet weggelegd. Reden voor hem om bijvoorbeeld geregeld gastcolleges aan security-studenten te geven.

‘Bangst voor wat ik niet zie’

“Ik ben het bangst voor wat ik niet zie”, gaat Paul verder. “Dus niet voor de DDoS-aanvallen en het klinkt misschien raar, nu Brussel nog maar zo kort geleden is. Maar ook dit soort aanslagen, hebben we allemaal voorzien. En daar kun je je dus op voorbereiden. We hebben er helaas ook al vaker mee te maken gehad. Checklists liggen dan ook al klaar, ook binnen een organisatie als de onze.”
Terrorismedreiging is dus zeker iets waar een Chief Security Officer zich volgens Paul anno 2016 mee moet bezighouden: “Veiligheid van je mensen en continuïteit van je dienstverlening zijn immers essentieel.” Waarbij je je volgens hem vooral moet proberen te verplaatsen in de tegenstander. “Wat is zijn belang? We zijn als CISO’s nog te vaak puur techniek gedreven. Systemen draaien weer en dan hebben we de situatie onder controle. Maar dat is in de huidige maatschappij altijd een tijdelijke situatie”, benadrukt hij.
“We moeten ons realiseren dat er over heel de wereld continu mensen actief zijn voor wie het hun nine-to-five-job is de maatschappij te ontwrichten door aanvallen op onze fysieke en digitale wereld voor te bereiden. Iets dat nog niet genoeg in onze mindset zit.”

‘Reasonable endeavour, geen garantie’

Een honderd procent veiligheidsgarantie kun je als Security Officer volgens Paul nooit geven. Terwijl klanten hier volgens hem wel naar vragen. “Wat we kunnen bieden, is een ‘reasonable endeavour’ (redelijke inspanning)”, legt hij uit. Waarbij kwaad kunnen denken, je kunnen verplaatsen in de tegenstander, en meedenken in vernieuwingen wat hem betreft dus cruciale eigenschappen zijn waarover elke CISO zou moeten beschikken.

“Als het je als Security Officer vervolgens ook nog lukt deze sense of urgency in de organisatie in te bedden, door het creëren van awareness op alle niveaus ben je wat mij betreft geslaagd in je opdracht. Je hebt vanuit security-oogpunt de voorwaarden gecreëerd voor innovatie en succesvolle, veilige groei”, besluit hij.

Fotografie Paul Oor: Atos

SAFE

In this article we pick up the thread of the previous article on the attribute 'emergent' with regard to system properties and follow it through on a specific path – that of systems safety. By 'safety' we mean not being injurious or dangerous to human life and health. Safety and security are closely related concepts. In the French language they share a single term – 'sécurité', and in English language these terms are often found together in single phrases, such as 'safe and secure'.

The unwanted emergent property related to systems safety is known as 'hazardous', being the opposite of 'safe'. The safety industry has its own set of professional experts whose main job is safety design and safety engineering in systems of all types.

Those of you familiar with SABSA will know that the main uniqueness of the SABSA methodology is Business Attribute Profiling, and that much of the remainder of the framework is synthesised from a mixture of concepts borrowed from other frameworks, methods and standards. So it seems a good idea to examine the concepts and practices of the safety engineering community and see what additional wisdom we might learn from them and perhaps enhance SABSA thinking by adopting and aligning with these ideas. The SABSA Institute is now embarking on this line of enquiry as part of its endeavours to broaden the understanding and practice of risk management.

One of the most eminent thought leaders on safety engineering is Nancy Leveson from MIT, USA. Her book, Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, published in 2012 is currently the most up-to-date definitive work on the subject. It departs from previous safety methodologies, such a chain-of-events analysis, by taking a systems-engineering view rather than a component view. The method described in the book for hazard analysis is known as STPA (Systems-Theoretic Process Analysis) and builds on an accident-modelling technique known as STAMP (Systems-Theoretic Accident Model and Process) and an analytic technique for accident investigation known as CAST (Causal Analysis using Systems Theory).

Given the fact that the safety and security professional communities are hardly aware of one another and do not as a rule intermingle, there are surprising conceptual similarities between STPA and SABSA. The potential for enhancing SABSA by cross-fertilising with STPA thinking seems to be a very good prospect. To demonstrate that, here are some key points that both frameworks share. Both are focused on:

- Systems engineering as the underlying methodology
- Holistic systems analysis versus component analysis
- Top-down decomposition from the highest level value statements
- Layered (tiered) systems analysis to reduce complexity and enhance simplicity of design
- Treating unwanted events as a control problem not a failure problem
- Modelling control systems and analysing the models
- Nested and embedded feedback control loops
- Organisational governance as being a critical success factor in achieving the objectives, both in systems development and in systems operations, and applied at all governance levels – regulatory, management and technical
- Seeing requirements definition as essential to a successful mission and flawed requirements as being the root of many problems
- Seeing people and process as an integral part of a system – not just technology
- Drawing on finite state machine theory (FSM) to determine safe/secure states and unsafe/insecure states and the events that trigger transition from one finite state to another
- Seeing that the interaction between systems components, each working to specification, can be the source of unwanted systems behaviour without any single component failing. (A system property, not a component property)

From the point of view of The SABSA Institute, these similarities mean there is a rich seam of safety knowledge and know-how to be mined to find new aspects of analysis that can strengthen SABSA. The Institute will therefore be initiating a research project in the near future to investigate the possible advantages of adopting and/or aligning with some of the STPA thinking. Anyone with an interest in participating in this project should let us know by sending a message on www.sabsa.org/contact or by emailing to info@sabsa.org.

The Attributer

EU-US PRIVACY SHIELD: DE VERVANGER VAN SAFE HARBOUR?

Op 2 februari 2016 is overeenstemming bereikt tussen de Europese Unie (EU) en de Verenigde Staten (VS) over een nieuwe overeenkomst voor doorgifte van persoonsgegevens naar de VS. Deze overeenkomst, het EU-US Privacy Shield, moet binnen 3 maanden geïmplementeerd worden. De overeenkomst stuit echter al direct op kritiek.

Dit artikel gaat in op die kritiek en ook op de vragen: waarom is Safe Harbour ongeldig verklaard, wat lost het EU-US Privacy Shield op en wat niet, en hoe zit het met de implementatie van het EU-US Privacy Shield?

Korte achtergrond Safe Harbour[1]

De huidige Europese Richtlijn bescherming persoonsgegevens (95/46/EG) is zo opgezet dat vastgesteld moet zijn dat er bij verwerking van de persoonsgegevens, adequate maatregelen zijn genomen ter bescherming van deze persoonsgegevens. Dat geldt ook bij verwerking van persoonsgegevens buiten de EU. Dit laatste wordt gerealiseerd door verwerking buiten de Europese Economische Ruimte te verbieden tenzij een land erkend is als adequaat. Adequaat wil zeggen dat het niveau van bescherming van persoonsgegevens gelijkwaardig is aan dat binnen de EU. De Europese Commissie (EC) is bevoegd om dit adequaatheidsbesluit te nemen. Zo'n adequaatheidsbesluit stelt bedrijven uit erkende landen onder meer in staat om Europese persoonsgegevens te verwerken.

Voor de VS geldt dat zij door de EU niet als een land met adequate privacywetgeving wordt beschouwd. Dit komt omdat de betreffende wet- en regelgeving binnen de VS anders is dan in de EU. De VS kent sectorspecifieke wetgeving, maar een algemeen kader dat vergelijkbaar is met onze Richtlijn bescherming persoonsgegevens is er niet.

Het gevolg was dat er afspraken moesten worden gemaakt tussen bedrijven in de VS en Europa om verwerking van Europese persoonsgegevens in de VS mogelijk te maken.

In 2000 heeft de EC een "executive agreement" gesloten met de VS: Safe Harbour. Amerikaanse organisaties die zich (vrijwillig) aansloten bij het Safe Harbour Framework, werden gezien als organisaties die veilig omgingen met Europese persoonsgegevens. De dekking van de overeenkomst betrof puur de deelnemende organisaties. Uitgangspunt was het voldoen aan de zeven principes van deze richtlijn (notice, choice, onward transfer, security, data integrity, access and enforcement). Doorgifte van persoonsgegevens vanuit de EU naar een bij Safe Harbour aangesloten organisatie was met het Safe Harbour-verdrag toegestaan.

Waarom een nieuwe overeenkomst?

In een eerdere publicatie in Informatiebeveiliging[2] wordt uitgebreid ingegaan op oorzaken van het ongeldig verklaren van Safe Harbour. Hieronder kort nog wat punten.

Data is (toch) opvraagbaar

In de VS wordt onderscheid gemaakt over hoe om te gaan met de privacy van Amerikaanse en niet-Amerikaanse burgers. Dit heeft te maken met het al dan niet toepasselijk zijn van de Fourth Amendment van de Bill of Rights in de Amerikaanse grondwet. In het Fourth Amendment is het recht op bescherming tegen onredelijke doorzoekingen en inbeslagnames opgenomen. Het Fourth Amendment kan alleen door Amerikaanse burgers worden ingeroepen en door buitenlanders die zodanige banden met de VS hebben ontwikkeld dat ze deel uitmaken van de Amerikaanse samenleving. De gemiddelde Europeaan kan daardoor geen aanspraak maken op bescherming onder de Bill of Rights.

Er bestaat echter een risico dat Europese (persoons)gegevens door de Amerikaanse overheid worden opgevraagd bij bedrijven die een werkterrein in de VS hebben. Dit is versterkt door de implementatie van de USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) welke in 2001 werd ingevoerd.

De Amerikaanse overheid kan op basis van deze Patriot Act (inmiddels Freedom Act) gegevens vorderen ongeacht of Safe Harbour van toepassing is. Dit in combinatie met eerder genoemd verschil van bescherming van Amerikaanse en niet Amerikaanse burgers is een gevoelig punt bij de verwerking van persoonsgegevens in de VS.

Zelfregulering

Het Department of Commerce (DoC) beheerde de lijst met Safe Harbour-bedrijven. Er was echter geen sprake van echt beheer. In de praktijk certificeerden en controleerden bedrijven zichzelf. [3]
Uit evaluaties van de EU in 2002 en 2004[2] bleek al dat het systeem van zelfregulering niet werkte. Vier jaar later, in 2008, was er niets verbeterd en kwam het onafhankelijke onderzoeks- en adviesbureau Galexia in een rapport [4] tot een vernietigend oordeel. Van de 1.597 organisaties op de Safe Harbour-lijst voldeden er slechts 348 enigszins aan alle zeven principes[2].

Safe Harbour ongeldig

Het waren onthullingen van klokkenluider Edward Snowden over NSA-activiteiten die ervoor zorgden dat binnen Europa minder vertrouwen ontstond aangaande de vertrouwelijkheid van data getransporteerd naar en/of opgeslagen in de VS.
Deze onthullingen waren aanleiding voor een rechtszaak tussen de Oostenrijker Max Schrems en Facebook. Schrems vroeg de Ierse privacytoezichthouder om een oordeel over de legaliteit van de gegevensuitwisseling van Facebook Ierland met Facebook USA. Op basis van de onthullingen van Snowden zag hij een risico met betrekking tot de bescherming van privacy in de VS. De zaak is verwezen naar het Europese Hof en deze heeft op 6 oktober 2015 besloten om een streep door het Safe Harbour-verdrag te zetten, op grond van de volgende redenen:[2]

1. Safe Harbour voorziet niet in een goede procesgang voor personen die zich benadeeld zien.
2. Er bestaan geen mogelijkheden voor personen om toegang te krijgen tot hun persoonsgegevens en om deze te laten wijzigen of wissen.
3. Safe Harbour verhindert Data Protection Agencies om onderzoek te doen naar privacy-inbreuken door Amerikaanse bedrijven.

Stappen en status

Op 2 februari 2016 hebben de EU en de VS overeenstemming bereikt over een nieuwe overeenkomst: het EU-US Privacy Shield. Deze overeenkomst kan, indien nodig, elk jaar worden aangepast. Eén en ander is echter nog niet geformaliseerd.

Op 29 februari 2016 heeft de Europese Commissie de voorlopige tekst[3] gepubliceerd. Deze wordt nu door de Artikel 29-werkgroep (de gezamenlijke Europese privacytoezichthouders) beoordeeld om na te gaan of er een adequaat beschermingsniveau wordt gerealiseerd met deze overeenkomst.
De Artikel 29-werkgroep zal naar verwachting half april haar advies uitbrengen.

Het Artikel 31-comité zal vervolgens naar verwachting in mei 2016 een bindend advies geven. In dit Comité (dat genoemd is naar artikel 31 van richtlijn 95/46/EG) hebben ambtelijke vertegenwoordigers van de lidstaten zitting. Het staat onder voorzitterschap van de Commissie. Het Comité heeft tot taak de Commissie te adviseren over voorgenomen besluiten inzake het toereikend zijn van het gegevensbeschermingsniveau in derde landen. Na het bindende advies kan de beslissing omtrent het al dan niet adequaat zijn van het EU-US Privacy Shield door de Europese Commissie worden genomen.

Als de EC akkoord gaat met het EU-US Privacy Shield, start het DoC met het accepteren van certificatie van bedrijven onder het EU-US Privacy Shield Framework. Om aan te sluiten bij dat Framework, zal een in de VS gevestigd bedrijf een zelfcertificering moeten doorlopen en voorleggen aan het DoC. Het verschil met Safe Harbour is dat er nu wel controles plaats zullen vinden.

Zolang het akkoord omtrent het EU-US Privacy Shield programma er nog niet is, zal gekeken moeten worden naar alternatieven voor doorgifte van persoonsgegevens naar de VS, zoals: het Europees Modelcontract of Binding Corporate Rules.

Menno Arentsen is Audit Manager bij Capgemini Nederland. Hij is te bereiken via menno.arentsen@capgemini.com.

Sinds het schrijven van dit artikel is bekend geworden dat de Artikel 29-werkgroep haar (niet bindende) advies heeft afgegeven, vanwege de nog steeds te grote toegang voor de Amerikaanse overheid is dit advies negatief. ***Redactie IB***

Een belangrijke ontwikkeling naast het Privacy Shield is het feit dat president Obama op 24 februari de Judicial Redress Act heeft getekend. Als deze geëffectueerd is, dan hebben EU burgers toegang tot de rechtbank in de VS voor privacyzaken gerelateerd aan naar de VS getransporteerde persoonsgegevens.

De Judicial Redress Act geeft EU burgers dezelfde rechten als Amerikaanse burgers en inwoners. De wet is van toepassing op landen aangemerkt door het US Department of Justice (DoJ). Deze landen moeten dan aan de volgende voorwaarden voldoen: 1) passende beveiligingsmaatregelen hebben voor privacygevoelige informatie welke gedeeld wordt met de VS; 2) toestaan dat persoonsgegevens worden gedeeld met de VS voor commerciële doeleinden en 3) gebruik maken van door DoJ gecertificeerde data-transfer-policies die de beveiligingsbelangen van de VS niet belemmeren.[5]

Belangrijkste verschillen tussen Safe Harbour en EU-US Privacy Shield[7][8]

In welk opzicht is het EU-US Privacy Shield een verbetering ten opzichte van Safe Harbour? Wat zijn de belangrijkste verschillen?

Jaarlijkse aanpassing

De overeenkomst kan, indien nodig, elk jaar worden aangepast.

Lijst gecontroleerde deelnemers

Amerikaanse bedrijven moeten zich aanmelden voor het EU-US Privacy Shield-programma. Er komt een EU-US Privacy Shield-lijst met deelnemers. Dit lijkt op de oude Safe Harbour-lijst, alleen is er geen sprake meer van zelfregulering, want er vinden onafhankelijk controles plaats. Aan de hand van vragenlijsten wordt vastgelegd hoe men Europese data behandelt en hoe het doorgeven ervan moet plaatsvinden. De toepassing wordt gecontroleerd en bedrijven die hier niet aan voldoen worden van de lijst verwijderd.

Op het moment dat een bedrijf aansluit bij het EU-US Privacy Shield Framework, moet zij publiekelijk bekendmaken dat ze voldoet aan de (meer specifieke) eisen van het Framework. Dit zorgt ervoor dat de gedane toezegging afdwingbaar wordt door de US Federal Trade Commission (FTC) binnen het wettelijke kader van de VS.

Amerikaanse bedrijven kunnen door het DoC samen met de Europese privacytoezichthouders worden gecontroleerd om vast te stellen of ze aan de regels voldoen.

Geen mass-surveillance

De Amerikaanse overheid heeft de EU schriftelijk toegezegd dat toegang tot data door de Amerikaanse overheid in het kader van veiligheid beperkt zal worden en aan specifieke eisen zal voldoen. Er worden geen grootschalige surveillance-operaties uitgevoerd op data van Europeanen die naar de VS worden getransporteerd.

Mogelijkheid export van gegevens te stoppen

Een ander verschil met de oude situatie is dat Europese nationale privacytoezichthouders kunnen beslissen dat een bedrijf de export van gegevens moet stopzetten. Ze kunnen hiertoe overgaan als ze van mening zijn dat er geen adequaat beschermingsniveau voor persoonsgegevens aanwezig is.

Klachtafhandeling

Voor burgers zijn voorzieningen getroffen om misbruik van gegevens door commerciële bedrijven te laten behandelen, te weten:

- Een klacht indienen bij het bedrijf zelf. Deelnemende bedrijven moeten toezeggen binnen 45 dagen te reageren. Ieder (Amerikaans) bedrijf dat Europese persoonsgegevens verwerkt onder het EU-US Privacy Shield moet voldoen aan adviezen die in dit kader gegeven worden door Europese privacytoezichthouders;
- Een klacht indienen bij de eigen nationale privacytoezichthouders. Deze zal de klacht doorgeven aan het DoC (reactie binnen 90 dagen) of, als het DoC het probleem niet kan oplossen, aan de FTC;
- Gebruik maken van "the Alternative Dispute Resolution". Een tool waarin per bedrijf (deelnemend aan de EU-US Privacy Shield) is aangegeven bij welk onafhankelijk orgaan klachten gemeld en afgehandeld kunnen worden.
- Ten slotte, als bovenstaande niet werkt, het arbitragemodel. Individuen kunnen zich richten tot het Privacy Shield Panel welke bindende beslissingen kan nemen van toepassing op zelfgecertificeerde bedrijven in de VS.

Voor privacyklachten waarbij een Europeaan vindt dat de overheid van de VS de beveiliging van persoonsgegevens onrechtmatig heeft geschaad, kan hij of zij terecht bij een Amerikaanse ombudsman. Deze gaat na of de zaak goed onderzocht is, of de wet- en regelgeving van de VS is toegepast en, daar waar van toepassing, correcte herstelmaatregelen zijn getroffen.

Het EU-US Privacy Shield lost zo een aantal problemen op die het Safe Harbour-verdrag kende. Het EU-US Privacy Shield adresseert daarbij zowel de 13 aanbevelingen die de Europese Commissie heeft gedaan in 2013 [10] en adresseert de aangehaalde punten in het oordeel van het Europese Hof van 6 oktober 2015, doordat: 1) het geen model van zelfregulering meer is; 2) er een procesgang is voor personen die zich benadeeld zien; 3) men toegang kan krijgen tot de eigen data; 4) er een wettelijk kader is; 5) privacytoezichthouders onderzoek kunnen doen naar privacyinbreuken door Amerikaanse bedrijven en 6) grootschalige surveillance-operaties op data van Europeanen die naar de VS worden getransporteerd niet meer mogen worden uitgevoerd.

De kritiek

De eerste reacties op de gepubliceerde tekst waren echter niet lovend. Max Schrems noemde het verdrag: "Lipstick on a pig". De overeenkomst ziet er mooi uit, maar in essentie verandert (te) weinig.

Op 16 maart 2016 heeft een coalitie van 27 belangrijke organisaties een brief[9] gestuurd aan Europese staatshoofden en de Artikel 29-werkgroep waarin zij aangeven dat het EU-US Privacy Shield niet sterk genoeg is.

Belangrijkste kritiekpunt is dat het probleem dat leidde tot het ongeldig

verklaren van het Safe Harbour-verdrag, namelijk surveillance van Europese data door de Amerikaanse overheid, niet volledig is weggenomen[11][12]. De Amerikaanse overheid behoudt nog steeds het recht de data te gebruiken voor onderzoek in een aantal specifieke gevallen. De tekst verwijst naar een recente Directive van president Obama: richtlijn Presidential Policy Directive 28 (PPD-28). Deze geeft aan dat er 6 'specifieke' gevallen zijn waarin de gegevens kunnen worden (op)gevraagd door de Amerikaanse overheid, te weten: 1) het detecteren en tegengaan van spionageactiviteiten van buitenlandse mogendheden, 2) het bestrijden van terrorisme, 3) cybersecurity, 4) het tegengaan van de verspreiding van massavernietigingswapens, 5) het detecteren en afslaan van bedreigingen voor het Amerikaanse leger en dat van zijn bondgenoten en 6) het bestrijden van grensoverschrijdende criminele activiteiten.

De EC is het niet eens met bovenstaand kritiekpunt. Zij vindt dat de bevoegdheden van de Amerikaanse inlichtingendiensten wel degelijk voldoende worden beperkt. Haar interpretatie is dat de VS schriftelijke garanties hebben gegeven dat hun geheime diensten alleen data van Europese burgers aftappen en verwerken als daar noodzaak voor is. Er zijn 'duidelijke beperkingen, waarborgen en toezichtmechanismen' ingesteld voor deze activiteiten door de NSA.

Er is daarnaast kritiek op het feit dat niet helemaal duidelijk is hoe sancties die wij in Europa kennen, worden opgelegd. Het is bijvoorbeeld onduidelijk hoe een bedrijf in de VS zijn schade kan claimen na een datalek bij een bewerker in de VS, waarbij het betreffende bedrijf in Europa in problemen komt met de toezichthouder. Om dit alsnog goed te waarborgen moet men in de bewerkersovereenkomst hier duidelijke afspraken over maken.

Ander punt van kritiek is de opzet van het arbitragemodel daar waar het gaat om hoe Europeanen vanuit Europa een beroep kunnen doen op de Amerikaanse rechter. Iedereen kan een beroep doen op de Amerikaanse rechter, maar dat kan in principe alleen vanaf Amerikaans grondgebied.

Hoe verder?

Op dit moment vindt de beoordeling plaats van het EU-US Privacy Shield door de Artikel 29-werkgroep. Hoewel het een verbetering is ten opzichte van Safe Harbour zijn de problemen die leidden tot het ongeldig verklaren van Safe Harbour niet volledig opgelost. Er is vanuit verschillende kanten kritiek geuit op deze uitwerking. Anderzijds laait door recente gebeurtenissen juist weer de discussie privacy versus veiligheid op, waardoor Europeanen bereid lijken toch wat meer privacy op te willen geven als dat de veiligheid (bescherming tegen terrorisme) vergroot. Ook een aspect als het belang van vrij gegevensverkeer tussen de VS en EU voor bedrijven zal zwaar wegen in de besluitvorming over acceptatie van het EU-US Privacy Shield.

Als het EU-US Privacy Shield niet geaccepteerd wordt, speelt de vraag wat een goed werkbaar en door alle partijen acceptabel alternatief zou zijn. Is het überhaupt mogelijk om in een verdrag het spanningsveld van de verschillende zienswijzen ten aanzien van privacy en veiligheid te overbruggen? Zienswijzen kunnen ook veranderen: daags na de aanslag in Brussel werd in de Belgische Media al aangegeven dat gevreesd wordt dat de strijd tegen terreur ten koste zal (moeten) gaan van de privacy[13].

Voor nu moeten we de ontwikkelingen rondom het EU-US Privacy Shield nauwlettend blijven volgen.
Of het EU-US Privacy Shield het haalt, is op het moment van schrijven onzeker. Ik heb de antwoorden niet. Wel ter afsluiting een aantal voor mij nog onbeantwoorde, hiermee samenhangende vragen:

- Geven de alternatieven van dit moment (EU modelcontracten en/of Binding Corporate Rules) betere garanties dan het EU-US Privacy Shield?
- Is er sprake van een datalek (in het kader van de Wet bescherming persoonsgegevens) als de Amerikaanse overheid data opvraagt?
- Zijn de VS werkelijk het enige land waar wettelijke kaders misbruikt worden voor het uitvoeren van gegevensopvragingen door overheden of is de VS het enige land waarvan we het zeker weten?

Referenties

[1] Justitia.nl, Safe Harbour <http://www.justitia.nl/privacy/safe-Harbour.html>

[2] Mr. Rachel Marbus, Informatiebeveiliging nr. 8 2015: Na de veilige haven.

[3] Export.gov, U.S.-EU SAFE HARBOUR LIST <https://safeHarbour.export.gov/list.aspx>

[4] Chris Connoly (Galexia) The US Safe Harbour - Fact or Fiction? (2008), <http://www.galexia.com/public/research/assets/safe_Harbour_fact_or_fiction_2008/safe_Harbour_fact_or_fiction.pdf>, 2 December 2008.

[5] The National Law Review, Obama Signs Judicial Redress Act—Will It Move EU–U.S. Privacy Shield Forward, <http://www.natlawreview.com/article/obama-signs-judicial-redress-act-will-it-move-eu-us-privacy-shield-forward#sthash.IV7YAmXz.dpuf>, 27 februari 2016.

[6] European Commission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, <http://europa.eu/rapid/press-release_IP-16-433_en.htm>, 29 februari 2016.

[7] Justitia.nl, EU-US Privacy Shield, <http://www.justitia.nl/privacy/privacy-shield.html>

[8] European Commission, EU-U.S. Privacy Shield: Frequently Asked Questions, <http://europa.eu/rapid/press-release_MEMO-16-434_en.htm>, 29 februari 2016.

[9] Brief van coalitie van 27 belangrijke organisaties inzake de EU-US Privacy Shield, <https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf>, 16 maart 2016.

[10] European Commission, Communication from the commission to the European Parliament and the Council
on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf>, 27 november 2013.

[11] Europe vs Facebook, First reaction on: European Commission presents EU-US „Privacy Shield" < http://europe-v-facebook.org/PA_PS.pdf>, 29 februari 2016.

[12] AutomatiseringsGids, Jelle Wijkstra, Details nemen vraagtekens bij Privacy Shield niet weg. <http://www.automatiseringgids.nl/nieuws/2016/09/details-nemen-vraagtekens-bij-privacy-shield-niet-weg>, 1 maart 2016.

[13] bijvoorbeeld: De Standaard, Christof Vanschoubroek, Privacy moet kunnen wijken voor veiligheid. <http://www.standaard.be/cnt/dmf20160322_02196819>, 22 maart 2016.

ONLINE PRIVACY – DANSEND NAAR DE CRYPTOPTICON

In de laatste maand van vorig jaar was ik in de bijzonder bevoorrechte positie om deel te nemen aan een klein panel bij de Nyenrode Business Universiteit. Het panel had als onderwerp online privacy en computerethiek, met als bijzondere gast professor Deborah Johnson [1]. Professor Johnson is met name bekend vanwege haar auteurschap van de boeken Computer Ethics en Technology & Society: Engineering our SocioTechnical Future. Na een relatief korte introductie en het bespreken van wat stellingen en concepten rondom computerethiek werd al snel duidelijk dat haar werkveld geenszins van louter filosofische aard is. Het Business Prevention Department. Met die woorden werd nog niet eens zo heel lang geleden de security-afdeling van menig bedrijf omschreven. Paul Oor, Chief Security Officer Benelux & The Nordics van Atos, kan het weten. Met woorden van dergelijke strekking kreeg ook hij te maken. Sinds enkele jaren is de situatie volgens hem compleet veranderd.

Er ontstond al snel een levendige discussie die op veel fronten illustreerde in hoeverre de adoptie en integratie van (met name internet-) technologie in het dagelijks leven een vergaand effect heeft op onze privacy. Hierbij niet doelend op bijvoorbeeld de buitensporige en privacygevoelige verzameldrift van een enkel bedrijf á la Facebook, maar over het enorme potentieel tot 24/7-monitoring van absoluut alles en iedereen door middel van passieve elektronische surveillance. De enorme digitaliseringsgolf waarbij steeds meer systemen met elkaar verbonden worden, is inmiddels vanzelfsprekend geworden. Vrijwel iedere organisatie, van commercieel tot overheid, is dagelijks bezig met het toevoegen van systemen en data. Waar digitalisering en automatisering van nieuwe processen vroeger als innovatief en vernieuwend beschouwd werden, is het vandaag de dag vanzelfsprekend.

De openbaringen van Edward Snowden tonen aan dat er niet alleen partijen zijn die toegang zoeken tot (delen van) deze informatie, maar dat hierin een enorme macht verscholen gaat. Zonder meteen een aluminium hoedje te willen gaan vouwen, is het nadenken over de potentie van deze immer groeiende berg data naar mijn mening een sociaal-culturele plicht van ons allemaal. Jeremy Bentham en Michel Foucault spraken al over de Panopticon [2]; het vermogen om groepen te controleren, disciplineren, bewaken en te bestuderen door middel van constant toezicht. Indien een enkele partij -zoals een inlichtingendienst - volledig toegang heeft tot genoeg online data, kun je stellen dat de staat van panopticon al is bereikt. Experts spreken zelfs al van Cryptopticon [3], waarbij je niet alleen constant geobserveerd wordt, maar tevens geobserveerd wordt op manieren waar je geen weet van hebt.

Mooie voorbeelden van hoe veel potentiele privacygevoelige issues er nu al zijn, zijn er te over. Het fenomeen Facebook is vanzelfsprekend een mooi voorbeeld. Voor wie er niet bekend mee is: Facebook heeft enige tijd geleden heimelijk onderzoek gedaan naar het beïnvloeden van de gemoedstoestand van Facebook-gebruikers [4]. Wat men ontdekte was dat indien ze gebruikers maar genoeg negatieve nieuws-feeds toonden, deze gebruikers depressiever werden. Hoewel er relatief weinig ruchtbaarheid aan het onderzoek gegeven werd, kunt u zich afvragen of alle Facebook-gebruikers wel op de hoogte waren dat ze middels de EULA toestemming hadden verleend om ongevraagd op dergelijke wijze proefkonijn te zijn.

Een ander voorbeeld van de moreel-ethische kant van big data en online privacy zijn mobiele apparaten zoals de mobiele telefoon en de 'wearables' zoals de Apple Watch. De Apple Watch heeft namelijk sensoren waarmee de hartslag en het activiteitsniveau van de drager gemeten kan worden. Dit roept een aantal interessante vragen op. In Nederland is iedere burger namelijk bij wet verplicht om hulp te verlenen 'naar vermogen' als iemand onwel wordt [5]. Hoewel dit voor sommigen niet verder gaat dan 112 bellen, ben je strafbaar als je dit niet doet. De Apple Watch is in staat om bijvoorbeeld een hartstilstand snel te detecteren. Doet het horloge dit standaard ook? Zo ja, betekent dit dat het apparaat in zulke situaties melding maakt bij 112 of een andere hulpverlenende instantie? Zo niet, is Apple dan onder de Nederlandse wetgeving strafbaar? Zouden ze dat moeten zijn?

Dat Apple al het nodige doet aan 'profiling' van haar klanten zal de meeste gebruikers van de nieuwere iPhones al wel duidelijk zijn. Zo heeft mijn mobiele telefoon inmiddels al uitgevogeld waar ik woon, waar ik mijn boodschappen doe en wanneer, en lijkt het een

aanzienlijk overzicht te hebben van regelmatig terugkerende afspraken. Hoe ik dit weet? Wanneer ik niet thuis ben en ik stap in de auto, is mijn telefoon zo vriendelijk om aan te geven hoe het verkeer richting huis is. Op zaterdagochtend geeft het mij ongevraagd de verkeerstoestand richting de lokale supermarkt, en op momenten waarop ik standaard ga sporten geeft mijn telefoon mij informatie over het verkeer richting de sportschool. Geen van deze zaken heb ik zelf aangezet; dit waren blijkbaar standaardfuncties. Of deze data gedeeld wordt met Apple of met derden is me eerlijk gezegd niet duidelijk, maar ik vrees van wel. Het is voor de politie relatief eenvoudig om personen op te sporen aan de hand van de positie die hun telefoon weggeeft, maar Apple kan hen op voorhand al vertellen waar ik zal zijn op basis van de eerder verzamelde informatie.

Zoals gezegd is het niet mijn intentie om samenzweringstheorieën aan te zwengelen. Maar er zijn wel degelijk vragen die interessant zijn om nu al te stellen, zodat we nog een kans maken om als globale, sterk onderling aan elkaar verbonden samenleving, maatregelen te nemen die ons als individu in staat stelt échte privacy te kennen.

Tijdens het debat werd al snel verwezen naar Orson Wells' boek 1984, daarbij de parallel trekkend met een extreme politiestaat van constante observatie. Het is echter de moeite waard om te benadrukken dat in dat boek deze constante observatie opgelegd wordt. Men heeft geen keus in het geheel, en lang niet iedereen is er dan ook even blij mee. Op dit moment doen wij het echter allemaal zelf. Wij als consument bouwen zelf driftig mee aan onze eigen staat van onzichtbare monitoring, meestal omwille van het hebben van het nieuwste snufje. Daarnaast verwachten we veel van onze dienstverleners, maar mag het niet te veel kosten. Zaken zo veel mogelijk automatiseren had men zeer waarschijnlijk toch al wel gedaan, maar om de kosten te drukken is dit inmiddels ook wel noodzaak; de concurrent doet het immers ook. Het is dus eerder een ontspannen dans dan een gedwongen mars richting Cryptopticon.

Dat het actueel probleem betreft, zien we ook nu weer door de open brief van Apple [6] waarin zij aangeven dat de Amerikaanse overheid, hierin vertegenwoordigd door de FBI, hen probeert te dwingen toegang te geven tot de iPhone van een terrorist die betrokken was bij de zogeheten 'San Bernardino case' in december jongstleden. Zij geven aan dat de FBI Apple vraagt om een geheel nieuwe versie van het besturingssysteem van de iPhone te creëeren die voor de FBI te kraken is middels een achterdeur. Al snel vielen WhatsApp, Google en Microsoft hen bij, en nadat de diverse nieuwszenders zich mengden in de discussie was het circus compleet. Aan het eind van de dag ontstond zelfs een heuse coalitie met de titel "Reform Government Surveillance" [7] met daarin vertegenwoordiging van bedrijven zoals AOL, Apple, Dropbox, Facebook, Google en LinkedIn.

De Amerika-kenners onder u zullen zich overigens niet verbazen dat Fox News met name blijft vasthouden aan het verhaal dat de FBI slechts toegang vraagt tot de telefoon van de terrorist in kwestie. Dit is echter niet juist, en het argument dat Apple zich bijzonder onpatriotisch opstelt is dan ook bijzonder venijnig. Zij hebben de FBI voorzien van een stappenplan waarmee zij toegang tot het specifieke toestel konden krijgen, maar dit is blijkbaar niet goed aangepakt en daarmee zijn de simpele oplossingen ogenschijnlijk van de baan. De site VentureBeat heeft inmiddels een zeer nuttige pagina opgezet met daarin een timeline [8] van de hele zaak.

Zoals wel vaker lijken de betrokken partijen nauwelijks stil te staan bij de implicaties van deze discussie buiten Amerika. Wie er uiteindelijk zal winnen, bepaalt tevens of er überhaupt nog gesproken kan worden van enige gegarandeerde privacy voor iPhone-bezitters over de hele wereld. Geallieerd of niet, overheden over de hele wereld hebben een belang bij wat hier speelt. Het is daarom hoog tijd om ook hier aan te geven wat wij, Nederlandse burgers, nu eigenlijk willen. Zijn we het dansen al beu?

Referenties

[1] http://batten.virginia.edu/school/people/deborah-johnson

[2] https://nl.wikipedia.org/wiki/Panopticum_(architectuur)

[3] "Panopticon to Cryptopticon" Zie http://www.datajustice.org/blog/panopticon-cryptopticon-or-how-scary-surveillance-gave-way-invisible-data-driven-exploitation

[4] "Experimental evidence of massive-scale emotional contagion through social networks" A. Kramer, J.Guillory, J. Hancock. Zie: http://www.pnas.org/content/111/24/8788.full

[5] Een goede uitleg staat hier: http://ikehbo.nl/eerste-hulp-bij-ongelukken/hulpverlenen/verplicht-of-niet.php

[6] De open brief van Apple: http://www.apple.com/customer-letter/

[7] http://reformgs.tumblr.com/post/139513553507/reform-government-surveillance-statement

[8] Zie http://venturebeat.com/2016/02/19/apple-fbi-timeline/

Don Eijndhoven is Principal Cyber Security Architect bij Argent Consulting B.V.
Don is bereikbaar via d.eijndhoven@argentconsulting.nl.

NO-BRAINER-SECURITY-CHECKS

Hoe veilig zijn de online servers van jouw organisatie?

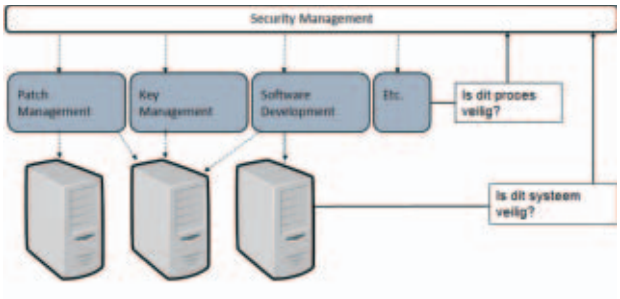
Beveiliging van servers kan worden uitgedrukt in termen van aanwezige kwetsbaarheden. Deze worden gerapporteerd door gespecialiseerde tools. Maar, helpt het gebruik van deze tools wel om tot voldoende beveiliging te komen? In dit artikel wordt een simpele, internetgebaseerde security-check geïntroduceerd die eenvoudige security-metrics levert en die organisaties helpt om langetermijnbeveiligingsdoelen te realiseren. Deze check is uitgevoerd op tien banken en tien academische ziekenhuizen in Nederland en België. De resultaten laten zien dat zelfs in de strenggereguleerde bancaire wereld deze goedkope en simpele methode nog een toegevoegde waarde heeft.

Een gangbare manier van werken bij het beveiligen van informatiesystemen is om de kwetsbaarheden op systeemniveau te inventariseren. Denk aan een Nessus-scan. Als eenmaal de kwetsbaarheden geprioriteerd zijn, wordt van de beheerteams verwacht dat ze de prio-1-kwetsbaarheden direct oplossen. Vanuit een tijdsperspectief zijn dat puntoplossingen: op één punt in de tijd voldoen alle servers aan het beveiligingsbeleid, welke geen prio-1-kwetsbaarheden accepteert.

Het probleem met deze systeemcentrische benadering is dat het afvinken van de kwetsbaarhedenlijst het doel is geworden, in plaats van het verbeteren van het beveiligingsniveau van de omgeving. Het oplossen van alle prio-1-kwetsbaarheden verbetert niet de ontwikkel- of beheerprocessen. Hierdoor zal het beveiligingsniveau door de tijd eroderen en nieuwe servers zullen dezelfde prio-1-kwetsbaarheden bevatten.

Onlangs kreeg ik het rapport onder ogen van een penetratietest op een web-applicatie. Het maakte melding van 25 cross-site-scripting-issues en elf SQL-injection-mogelijkheden. Het was duidelijk dat het ontwikkelteam niet bekend was met enige secure-programming-principes, en evenmin van het dreigingenlandschap rond web-applicaties. Hoe dan ook, de genoemde issues uit het pentest-rapport werden opgelost. Het rapport deed daarnaast een aanbeveling om een generieke maatregel tegen cross-site-scripting-aanvallen te implementeren. In mijn beleving een valide aanbeveling, omdat zoveel cross-site-scripting-issues waren gevonden tijdens de penetratietest. Hoeveel zouden er nog in zitten die nog niet gevonden waren? De reactie van de ontwikkelaar was echter dat deze generieke maatregel niet nodig was, omdat de applicatie immers geen cross-site-scripting-kwetsbaarheden meer bevatte! Wat we hier zien is dat het voldoen aan een kwetsbaarhedenlijst een vals gevoel van veiligheid geeft. Ik vertrouwde die web-applicatie voor geen cent, omdat de penetratietest duidelijk had aangetoond dat het software-ontwikkelproces onveilig was.

Wat als de veiligheid van servers niet over kwetsbaarheden in elke server ging, maar over de kwaliteit van de processen die het ontwikkelen en onderhielden. In dat geval zou het beveiligen gaan over het aanpassen van deze processen, in plaats van het afwerken van een kwetsbaarhedenchecklist en het fixen van de server. Het resultaat zou een duurzaam hoger niveau van systeembeveiliging zijn. Het zou leiden tot een omgeving waar risico's adequaat werden beheerst.



Figuur 1 - Security-rapportage gebaseerd op een proces of op een systeem

Voor een duurzame verbetering van beveiliging dient het beveiligingsniveau van de processen die het beveiligingsniveau voortbrengen te worden gemeten. Het verschil tussen een procescentrische en een systeemcentrische benadering is geïllustreerd in figuur 1. Voorbeelden van deze processen zijn Patch Management en Software Development. Een simpele en goedkope manier om hun security-kentallen te inventariseren wordt in de volgende paragraaf geïntroduceerd. Het heet 'no-brainer-security-metrics'.

No-brainer-security-metrics

Als je beveiliging goed implementeert, zul je niet eindigen met beveiligingsblunders in je systeem. Dat is het idee achter no-brainer-security-metrics. Enkele voorbeelden:

- Als je patch-management goed uitvoert, draait de server geen Apache-versie die end-of-life is.
- Als je SSH juist configureert, zal het geen cryptografische sleutel hebben die zo kort is dat deze eenvoudig kan worden gekraakt.
- Als je de server goed beheert, zal deze niet voorkomen op een blacklist voor malware-distributie.
- Als een gebruiker zich bewust is van informatiebeveiliging, zal ze haar wachtwoord niet aan een ander geven.

Pascal de Koning is cybersecurity consultant bij i-to-i en vervult een project-voorzitterschap bij de Open Group. Pascal kan bereikt worden via p.de.koning@i-to-i.nl.

Proces	No-brainer
Patch Management (P)	Het gebruik van End-of-Life softwareversies
System Maintenance (B)	Het IP-adres is aangetroffen op een blacklist voor malware (niet spam)
Key Management (S)(H)	Het ondersteunen van een 'deprecated'-encryptie-protocol, zoals SSLv2
Webserver Configuration (W)	Ondersteuning van de TRACE-method in een productieomgeving
Nameserver Configuration (N)	Ongeauthenticeerde zonetransfers toegestaan
Technical Design (D)	Inlog via een onversleutelde verbinding

Tabel 1 - Security-no-brainers per proces.

Kortom, een security-no-brainer is het ergste wat je kunt vinden tijdens een security-check. Het is van belang dat deze no-brainers eenvoudig en geautomatiseerd kunnen worden vastgesteld. Ten slotte leven we in een wereld die in toenemende mate digitaliseert en om dit bij te houden dient ook informatiebeveiliging te digitaliseren. Een goede security-no-brainer is er een die eenvoudig kan worden vastgesteld, die onontkenbaar een security-issue is, en die kan worden gelinkt aan een proces wat het systeem ontwikkelt of onderhoudt.

Figuur 2 - Voorbeeld van een security-no-brainer

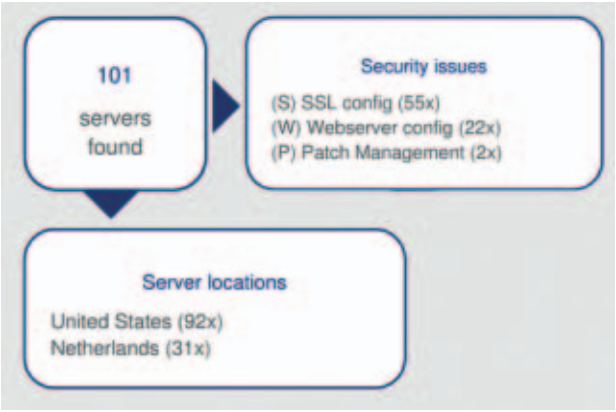
Verschillende ontwikkel- en beheerprocessen zijn verantwoordelijk voor de kwaliteit van de systemen. Bekende voorbeelden zijn:

- Software-ontwikkeling: het zorgdragen voor inputvalidatie, veilige manieren om databases te benaderen, etc. In één term, het toepassen van de regels voor veilig programmeren.
- Configuratiebeheer: het bijhouden van de lijst met servers die door de organisatie gebruikt worden.
- Systeem-hardening: ervoor zorgen dat de aangeboden functionaliteit vanaf de server geminimaliseerd is en dat deze functionaliteit zodanig is geconfigureerd dat misbruik niet mogelijk is.
- Key-management: het geheel van het toepassen van cryptografie, inclusief het opstellen van het crypto-beleid, het genereren van veilige sleutels, het vertrouwelijk houden van de sleutels gedurende hun levensduur en het up-to-date houden van crypto-hard- en -software met de laatste ontwikkelingen.
- Patch-management: het toepassen van security-patches voor firmware, platformen en applicaties binnen een acceptabel en haalbaar tijdsframe.

Het meten van de beveiliging van een server

Om de beveiliging van een server te meten, zijn zes processen geselecteerd. Voor elk proces zijn er één of meerdere no-brainers gedefinieerd. Om een idee te geven is een selectie van de gebruikte no-brainers in tabel 1 opgenomen. De letters tussen haakjes komen later terug in de detailrapportage.

Aan het begin van de meting krijgt iedere server een score van honderd punten. Voor elke no-brainer worden punten afgetrokken. Als een kwetsbaarheid niet kan worden vastgesteld gingen geen punten verloren. De security-score is dus gebaseerd op falsificatie: er wordt aangenomen dat de server veilig is, tenzij bewijs van het tegenovergestelde wordt aangetroffen. Figuur 3 toont een voorbeeld.



Figuur 3 - Voorbeeld security-metrics-rapportage

Ik verwachtte dat alleen kleine organisaties security-no-brainers zouden hebben. Wat zat ik ernaast!

network name, owner and location	IP-address	dns-name	score
NL-XYZ-NETWORK NL-XYZ Netherlands	111.111.111.0 – 111.111.111.255		
	111.111.111.22	www.organization.com	96
	-	webmail.organization.com	96
	111.111.111.24	login.organization.com	100

Figuur 4 - Fragment van de test-output. Servers van een organisatie en hun beveiligingsscore.

Figuur 4 toont de rapportage van de test bij één organisatie. Iedere unieke combinatie van een IP-adres en een DNS-naam wordt een 'server' genoemd. Als een website bijvoorbeeld is gehost op zes verschillende IP-adressen, dan telt dit als zes servers. En als tien domeinnamen uitkomen op hetzelfde IP-adres, dan telt dit als tien servers. De servers zijn in de rapportage gegroepeerd als ze op dezelfde IP-range staan, geregistreerd door dezelfde eigenaar. Als een server niet benaderbaar is, is geen security-score gegeven (wit vakje). De security-scores zijn gekleurd conform het stoplichtmodel. Groen is OK (geen of één no-brainer(s) gevonden), rood is een hoog risico (vijf of meer no-brainers gevonden).

Toen ik voor het eerst nadacht over deze security-no-brainers, verwachtte ik dat de meeste organisaties geen enkele no-brainer-kwetsbaarheid op hun servers aan internetzijde zouden hebben. Omdat het zo eenvoudig is om ze te vermijden. Omdat de interne beveiliging wel erg zwak zou zijn als de internetbeveiliging al no-brainers zou bevatten. Omdat het implementeren van informatiebeveiliging toch wel zo'n (vergeef me) no-brainer was als je e-business wilde doen. Mijn verwachting was dat het alleen deze delen van een organisatie zou doen oplichten die aan de aandacht van de security-officer ontsnapt waren. Ik verwachtte ook dat alleen kleine organisaties die voor hun bedrijfsproces niet afhankelijk waren van het internet deze security-no-brainers in hun servers zou hebben. Tjonge, wat zat ik ernaast!

De test: security aan internetzijde van banken versus ziekenhuizen

Voor de test zijn twee groepen organisaties geselecteerd. De eerste groep bestaat uit tien banken. Een bank opereert in een hooggereguleerde branche, heeft een sterke focus op risicomanagement en ICT is een zeer belangrijk deel van het primaire proces. De andere groep bestaat uit tien academische ziekenhuizen. Academische ziekenhuizen zijn er om levens te redden; hun focus is niet op informatiebeveiliging. Er is veel autonomie binnen de ziekenhuizen, resulterend in een wildgroei aan online servers. Alle twintig organisaties in de test zijn gevestigd in België en Nederland. Het aantal online servers per organisatie varieert tussen de tien en honderdvijftig.
Bedenk dat een gevonden security-no-brainers niet automatisch betekent dat de server kwetsbaar is. Het geeft wel aan dat de server aandacht nodig heeft. Als een gedetailleerde inspectie aantoont dat de server niet kwetsbaar is of dat het risico acceptabel is, mag de no-brainer blijven bestaan. Een voorbeeld is de versie-informatie die een webserver kan geven. De webserver-versie kan compleet verzonnen zijn, of de server kan gepatcht zijn zonder dat dit zichtbaar is in het versienummer. Een ander voorbeeld is een webserver die zwakke SSL-encryptie toestaat om te kunnen communiceren met klanten die oude browsers gebruiken. Dat zou een geaccepteerd business-risico kunnen zijn. Ergo, net als iedere security-check bevat ook de no-brainer-check false positives.

Figuur 5 - De security-status van servers aan internetzijde bij banken en ziekenhuizen

De resultaten van de test zijn weergegeven in figuur 5. De score van iedere online server is weergegeven met een kleur conform het eerder uitgelegde stoplichtmodel. Per regel zijn alle online servers van één organisatie weergegeven. De servers zijn gegroepeerd als ze in dezelfde IP-range zitten. De details gaan verloren in deze figuren, maar de grote lijn wordt wel zichtbaar.

Niet verrassend lijken de servers van de banken veiliger te zijn dan die van de ziekenhuizen. Oorzaak hiervan is dat in de bancaire sector de beveiliging meer gereguleerd is, waardoor er meer aandacht en geld aan informatiebeveiliging worden besteed. Het gevolg is dat onze spaarrekeningen beter beveiligd zijn dan onze medische dossiers. Voor een beter begrip kijken we naar de figuur 6.

Figuur 6 - Percentage servers met security-no-brainers bij banken en ziekenhuizen

Van de servers bij de banken heeft 95 procent geen of slechts één no-brainer. Dat percentage goedscorende servers was bij de ziekenhuizen veel lager, namelijk 72 procent. Andersom geredeneerd, bij 28 procent van de online servers van de ziekenhuizen zijn twee of meer security-no-brainers aangetroffen.
Bij de banken heeft 75 procent van de security-issues te maken met SSL/TLS-configuratie. Patch-management en webserver-configuratie telden elk voor tien procent van de security-issues. In de academische ziekenhuizen was SSL/TLS-configuratie ook het grootste probleem (50 procent), gevolgd door patch-management (33 procent). Het lijkt er dus op dat SSL/TLS-configuratie één van de moeilijkste dingen is om goed te doen. Van de tien banken waren er acht met één of meer security-no-brainers op hun online servers. Bij de ziekenhuizen was dit bij alle tien het geval. Het is interessant om te zien dat zelfs in de hooggereguleerde bancaire sector het aantal no-brainers niet nul is. Sommige banken halen deze score, maar zeker niet alle banken.

Conclusie

Een belangrijke toegangspoort tot de informatiesystemen van een organisatie is de internetzijde. De servers aan de buitenkant zouden moeten zijn ontwikkeld en onderhouden door veilige processen. Om een idee te krijgen welke processen onvoldoende veilig zijn is een no-brainer-check nuttig. De test toont aan dat dit voor 90 procent van de organisaties al voldoende informatie geeft om actie te kunnen ondernemen. Het stelt de security-manager in staat om te focussen op de gebieden met de hoogste risico's en om de beveiliging van ontwikkel- en beheerprocessen op niveau te brengen. Als dit eenmaal bereikt is zal de no-brainer-check minder issues rapporteren en is het risico gereduceerd voor de langere termijn.

Benieuwd naar de security-status van de webservers van je eigen organisatie? Bezoek internet-security-scan.com.

ARTIKEL VAN HET JAAR 2015

Ook dit jaar kreeg de jury (Renato Kuiper van VKA, Ellen Wesselingh van de Haagse Hogeschool en Jurgen van der Vlugt van Maverisk) weer artikelen met een breed scala aan onderwerpen voorgeschoteld. Op basis van een voorselectie door de redactie, heeft de jury uit een longlist van tien artikelen een top drie shortlist samengesteld. Dit hebben we gedaan door alle artikelen grondig door te nemen en op een aantal harde en zachte criteria te scoren. Vervolgens is de jury met elkaar in discussie gegaan over de gemaakte keuzes en tot een top drie gekomen.

Winnaars

1) Advanced Business Impact Analysis
M. Janec en E. Verweij

2) CSIRT Maturity Kit
M. de Hamer en D. Stikvoort

3) Veiliger met voorkennis
H.J. van der Molen

ARTIKELCRITERIA

Bij het jureren is onder andere gekeken naar de volgende criteria:

1. Opzet artikel – Is de opzet van het artikel juist voor de soort (inhoudelijk of opiniestuk)?
2. Leesbaarheid – Is het artikel helder en begrijpelijk geschreven, met passende illustraties? Is de stijl consistent, zoals serieus of satirisch? Of het nu een praktijkbeschrijving is of een wetenschappelijke beschouwing betreft, is de leeservaring prettig?
3. Benadering van de doelgroep – Is het duidelijk wat de doelgroep is voor het artikel? Is het artikel te volgen voor een lezer buiten de subgroep?
4. Vernieuwend gehalte – Heeft het artikel aspecten die getuigen van visie bij de auteur en/of nieuwe gezichtspunten op een onderwerp? In het Engels noemen we dit "thinking out-of-the-box".
5. Zet het de doelgroep aan het denken? – Ook als de auteur verslag legt van een gezamenlijk gedachtengoed of misschien zelf rapporteert over unieke gedachten van anderen, in hoeverre slaagt hij of zij er in om de lezer aan het denken te zetten?

JURYRAPPORT

Als juryleden hebben we afzonderlijk een kwalitatieve beoordeling gemaakt en op basis daarvan een volgorde aangebracht. In een uitgebreide en open discussie hebben wij vervolgens onze argumenten naast en tegenover elkaar gezet, en zijn wij op basis daarvan tot een eensgezinde conclusie gekomen over welke artikelen op welke plaats in de top drie zijn geëindigd.

Wat opviel bij een aantal artikelen is dat de auteurs minder aandacht bleken te hebben gegeven aan een methodologisch verantwoorde grondslag voor hun verhaal; kort door de bocht kwam weleens de vraag op: klopt het verhaal wel? Verder bleek het voor de meesten lastig om de analyse om te zetten in concrete handvatten voor de doelgroep als die in de praktijk met de materie aan de slag moet gaan. Oplossingen werden wel breed genoeg geformuleerd om in meerdere bedrijfstakken toepasbaar te zijn, maar bleven soms hangen in wat te veel algemeenheid, te veel 'open deur'. De balans hiertussen bleek een lastige afweging.

Ook varieerde de kwaliteit van het schetsen van een duidelijke context en analyse van het probleem. Het artikel Cybersecurity in de boardroom van Yuri Bobbert geeft een helder gestructureerd voorbeeld van hoe dat moet en is daarmee goed voor een eervolle vermelding voor de heldere structuur en schrijfstijl.

Het winnende artikel van dit jaar is een tweedelig artikel waarvan de jury vindt dat het onderwerp methodisch grondig is aangepakt en uitgewerkt. Het gaat over een actueel onderwerp, dat relevant is voor een verscheidenheid aan bedrijven. Hoewel de uitwerking naar concrete maatregelen in het tweede deel wat achterbleef bij de scherpe analyse in het eerste deel was het een duidelijke winnaar: Milena Janec en Eldine Verweij hebben met hun artikel Advanced Business Impact Analyse het thema Business Impact Analyse naar een hoger niveau getild en de jury ziet met belangstelling een vervolg tegemoet.

Een goede en duidelijke tweede plaats is er voor Martijn de Hamer en Don Stikvoort met een artikel over de CSIRT Maturity Kit. Sterke punten aan dit artikel waren de combinatie van verschillende invalshoeken en de holistische kijk op het thema incident-response. Ook hier ziet de jury uit naar een vervolg op dit actuele thema dat voor velen relevant is.

Nummer drie is geworden Henk-Jan van der Molen met het artikel Veiliger met voorkennis. Een goed leesbaar algemeen verhaal waarin verschillende invalshoeken samenkomen, waaronder ook de PDCA-kwaliteitscirkel van Deming. De jury had in deel twee graag een uitwerking naar praktijkervaringen gezien, zodat de lezer handvatten krijgt om de zeer relevante analyse uit het eerste deel naar de eigen praktijk te kunnen vertalen.

Aan alle auteurs en lezers: hartelijk dank, blijf schrijven en lezen en hou het veilig.

Renato Kuiper, namens de jury van het "Artikel van het Jaar", 1 april 2016. Renato is te bereiken via renato.kuiper@vka.nl.

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

DE AUTO ALS RIJDENDE ICT-KWETSBAARHEID

Onlangs is een proef uitgevoerd met zelfrijdende auto's op de A2 tussen Amsterdam en Beesd [1]. De moderne auto is niet meer denkbaar zonder ICT, niet alleen nodig voor de vele functies, maar ook als ondersteuning van de gebruiker van de auto (wellicht moeten we in dit verband inderdaad niet meer spreken van "bestuurder"). Maar welke risico's brengt dat met zich mee? De FBI heeft recentelijk een informatiebulletin uitgegeven, specifiek gericht op de mogelijkheid dat uw auto "gehacked" is [2]. Moet u in de nabije toekomst 's morgens niet meer naar de file-informatie kijken (dat heeft uw auto al voor u gedaan), maar op de website van het NCSC de lijst met actuele bedreigingen voor uw auto raadplegen? De redacteuren van IB geven hun mening, zoals altijd zijn deze stukjes op persoonlijke titel geschreven, en geven zij niet noodzakelijkerwijs het standpunt van PvIB of van de werkgever van de redacteur weer.


Bart van Staveren


Lex Borger


Maarten Hartsuijker

Bart van Staveren

De FBI waarschuwt terecht voor het risico van gehackte auto's. Niet alleen de bekende phishing pogingen vormen een risico, maar ook de in de naar alle waarschijnlijkheid in de software opgenomen backdoors vormen een mogelijkheid voor het overnemen van de auto. Het is eigenlijk niet bekend wat de kwaliteit is van de software die in de auto is opgenomen. De sjoemelsoftware van onder andere Volkswagen is daar maar een voorbeeld van. Dit geldt niet alleen voor auto's, maar voor alle software die in allerlei apparaten, die wij onder de verzamelnaam "Internet of things" aanduiden, opgenomen is. Het koppelen van "things" aan onze bedrijfsnetwerken brengt risico's met zich mee, die nog onvoldoende verkend zijn.

Maarten Hartsuijker

Een auto is steeds meer een computer op vier wielen geworden. Als er iets stuk gaat zit ligt daar steeds minder vaak een mechanische oorzaak aan ten grondslag. En om autoproblemen op te lossen is er niet zelden een software-update nodig. Steeds meer auto's zijn toegankelijk met apps. Soms zijn deze apps via Bluetooth aan de auto gekoppeld en soms via een UMTS SIM. En via het managementsysteem van de auto reiken die koppelingen tot diep in het technische hart van de auto. Gas geven, remmen, starten en stoppen... in diverse auto's zijn dit soort functies al computergestuurd of -ondersteund. Beveiligingsproblemen met auto's zijn niet meer dan een simpele optelsom van deze kenmerken. Als je de auto met de computer bestuurt en deze computer aan internet koppelt, dan is het een gegeven dat je beveiligingskwetsbaarheden introduceert. En dat er hackers zijn die gaan zoeken hoe ze deze kwetsbaarheden kunnen misbruiken. Zelf onderzocht ik de afgelopen jaren diverse connected-car-oplossingen en kwam tot de conclusie dat het type beveiligingsfouten dat we overal tegen komen, ook gewoon in de connected car wereld aanwezig is. Encryptiefouten, updatefouten, autorisatiefouten en SQL-injection: ze passeerden allemaal de revue. Dit soort fouten is prima op te lossen: het beschermen van een auto is in de basis geen rocket-science. Maar als je als berijder je auto beschermt met het wachtwoord "12345" dan moet je niet vreemd staan kijken als er ergens in Europa iemand op de claxon van jouw auto in Sillicon Valley staat te drukken.
Daar waar het "connected" maken van auto's op IT-vlak vooral voor beveiligingsproblemen zorgt, levert het op een ander vlak juist veiligheidspotentie op. Computergestuurde auto's kunnen zich immers feilloos aan de verkeersregels houden. Het feit dat de passagier haast heeft, zal er bij de computer niet toe leiden dat hij nog even met een dot extra gas tussen twee klaar-overs door schiet. Of al append een fietsend kind over het hoofd ziet. En juist door dat verschil leidt de computerisering van auto's hopelijk tot een significante afname van het aantal verkeersslachtoffers.

Lex Borger

Het is duidelijk dat de techniek functioneel in staat is dit te doen. En dat zal de komende tijd met grote stappen snel beter worden. Er is al voldoende bewijs dat zelfrijdende auto's beter functioneren dan bestuurders van vlees en bloed. En laten we wel wezen, wie wil er nu investeren in het halen van een rijbewijs in Nederland? Dat we in de nabije toekomst geen bestuurder meer zijn lijkt me prima. Dus we kunnen en we willen zelfrijdende auto's.

Dan krijgen we als vervolg de vraag: 'is het veilig?' Bij auto's is het beantwoorden van deze vraag nóg belangrijker dan bij andere apparaten, omdat het een gevaarlijke machine is. Als ik de mogelijke kwetsbaarheden langs ga, dan denk ik dat systeemfouten een veel grotere kans hebben dan cyberaanvallen. Maar ik besef mezelf ook dat ik waarschijnlijk de criminele aanvalsscenario's niet kan verzinnen. Zelfs als we alleen naar foutscenario's kijken, is het heel duidelijk dat veiligheid (safety & security) topprioriteit moet zijn. Dus we moeten meetbaar weten dat het veilig is, en hoe veilig het is.

Kunnen we het veilig maken? Ik denk het wel. Eigenlijk zijn de enige componenten die we toevoegen sensoren en software. De sensoren doen wat ze doen, die geven ruwe informatie door. De software zet dat om in actie. Wat we nodig hebben is kwaliteitssoftware. En we weten hoe we dat krijgen: We kennen de ISO 9126 en ISO 25000 standaarden, we hebben het CISQ [3] als organisatie die zich daarvoor inzet.

Wat mij wel regelmatig verbaasd, is dat dit bij software ontwikkelaars en de financiers daarvan lang niet altijd bekend is. Dit is dé reden dat we nog steeds crappy software de wereld in sturen. Bewustwording is dus de grootste uitdaging. En dan volgen er meer: training, budgetten, testen... En met elkaar delen van de belangrijke zaken die we leren. Dan hoef ik als rijder in een auto me niet druk te maken of de auto wel up-to-date is en niet gehacked is. Zullen er incidenten zijn? Zeker. Wordt autorijden dan veiliger? Zeker.

Links

[1] http://www.anwb.nl/auto/nieuws/2016/maart/praktijkproef-zelfstandig-rijden-a2-verloopt-zonder-incidenten

[2] http://www.automatiseringgids.nl/nieuws/2016/11/fbi-waarschuwt-voor-auto-hacks

[3] http://it-cisq.org/

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
Rachel Marbus (NS)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2016
De abonnementsprijs in 2016 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

VERBAASD?

Berry gaat weer eens een ergernis van zich afschrijven. Zoals wellicht bekend heeft de computerindustrie een enorme gang voorwaarts gemaakt. Moore voorspelde dat ieder jaar de snelheid van een computer zou verdubbelen, miniaturisatie heeft ervoor gezorgd dat de huidige telefoons de ENIAC ver voorbij geschoten zijn. Deze computer zag in 1946 het levenslicht en was dermate groot dat er diverse klaslokalen noodzakelijk waren om het apparaat te bergen. Invoer in de ENIAC was zeer bewerkelijk en niet vergelijkbaar met de opdrachten die we onze smartphones nu met onze stem geven.

Onvoorstelbaar veel data kunnen we op onze telefoons kwijt en ook zeer privacygevoelige gegevens reizen dagelijks mee in onze broekzak of handtas. Er wordt veel geld verdiend in de smartphone-industrie en de leveranciers struikelen over elkaar heen om de nieuwste modellen op de markt te brengen. De consumentenbond was het opgevallen dat Samsung-telefoons slechts twee jaar na de lancering van de telefoon nog updates krijgen en daarna niet meer. De bond vindt dat vreemd en eigenlijk niet kunnen en stapte naar de rechter om de beveiligingsupdates af te dwingen.

Het toestel dat je kocht voor een groot bedrag is mogelijk niet meer veilig en alle data op het toestel ook niet. Je creditcardgegevens, je wachtwoorden, je lieve sms'jes, je mooie foto's kunnen ineens de wereld gaan rondzwerven omdat een jongetje met jeugdpuistjes je telefoon heeft gehackt. Samsung geeft aan dat het niet realistisch is om alle 1324 modellen (bij benadering) van Samsung te voorzien van beveiligingsupdates. Dat zou veel te kostbaar worden. Samsung is het natuurlijk niet met de consumentenbond eens. Updates zouden de toestellen trager maken en dat wil de koper niet. Natuurlijk is er weleens een klein lekje geconstateerd (bijvoorbeeld Stagefright) maar dat is eigenlijk nooit misbruikt, volgens Samsung, en de consumentenbond overdrijft toch alles. Ik heb er natuurlijk niet heel veel verstand van maar het lijkt mij dat de consumentbond echt wel de beste papieren heeft.

In Amsterdam heeft een rechter de zaak toegewezen gekregen en hij heeft zich erover gebogen. De rechter is het met Samsung eens, de consumentenbond kan niet aantonen dat Stagefright misbruikt is. Daarom kan Samsung niet verplicht worden updates uit te brengen voor alle modellen die ze geleverd hebben omdat het uitbrengen van updates voor oudere toestellen tot 'enorme kosten' zouden kunnen leiden, die 'binnen de reikwijdte van het kortgeding niet voldoende zijn te overzien'. Dus Samsung mag wel bergen geld verdienen aan de smartphones maar hoeft geen investeringen te doen in het veilig houden van de toestellen.

Ik lees het een aantal keren door en doe vervolgens mijn PC uit, loop naar beneden en mijn vrouw ziet onmiddellijk dat ik mij weer eens heb opgewonden en vraagt voorzichtig hoe het gaat. Ik besluit haar niet het hele verhaal te vertellen maar ik pak haar telefoon. "Kun jij je voorstellen dat iemand jouw telefoon kan lezen zonder je vingerafdruk te gebruiken?" Nee, dat kon ze zich niet voorstellen want als de FBI er niet eens in kan hoe kunnen anderen dat dan wel?

Nee, gelukkig kan niemand in onze toestellen, maar dat geldt niet voor alle telefoons die momenteel gebruikt worden. Ze kijkt me aan en haar ogen zeggen mij dat ze zich niet kan voorstellen waarom ik me zo druk maak. Ik zucht en denk dat ze gelijk heeft.

Berry

TSTC

ICT en Security Trainingen

C|CISO

Certified Chief Information Security Officer

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

9-13 mei, 5-9 september, 12-16 december

Join the New Generation of Information Security Leaders

EC-Council

Accredited Training Center

WWW.TSTC.NL

T 0318 581480