iB
INFORMATIEBEVEILIGING
jaargang 17 - 2017
#6

CYBER UPDATE

Cyberveilig gedrag: Wat is het ?

Enterprise control by design - deel 2

De (r)evolutie van digitaal bewijs

Bankoverval

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

Protect your company against cyber threats

Intelligent Cybersecurity Services

Find out more:

www.nl.capgemini.com/oplossingen-voor-cyberbeveiliging

SPRAKELOOS

Sprakeloos stond ik, toen ik op de afgelopen ledenvergadering hoorde dat ik tot erelid gekozen was van het PvIB. Letterlijk. Ik had dit niet verwacht en vind het een hele eer. Bedankt!

Een jaar geleden gaf ik bij het bestuur en de redactie aan, dat ik ging stoppen met het redactiewerk. Ik besefte de laatste weken, bij de voorbereiding van deze uitgave, wel degelijk dat dit de laatste keer is dat ik die cyclus meemaak. Een reeks aan activiteiten, die je niet alleen doet. De productie van de vierenvijftig uitgaven die onder mijn verantwoordelijkheid verschenen, waren niet mogelijk geweest zonder de mederedacteuren, een team dat door zijn diversiteit een goede bakermat is voor ideeën en ook een kritische spiegel voor kan houden waar nodig, de eindredactie bij MOS, die het proces ondersteunt en af en toe aanwakkert, de schrijvers die we af en toe inhuren, vormgever Dimitri en drukker VdR druk & print. De redactie gaat door met innovatie naar andere verschijningsvormen, de drukversie is en blijft een zeer gewaardeerde verschijning.

Mijn grootste dank gaat uit naar de vele mensen die creatieve input leverden om de content mogelijk te maken. Want als er iets is dat ik geleerd heb in de afgelopen jaren, is het wel dat je weliswaar een focus kunt hebben op een soepele productie, maar dat je nergens bent zonder auteurs die bereid zijn artikelen te leveren met een professionele boodschap. Dus aan alle auteurs: bedankt!

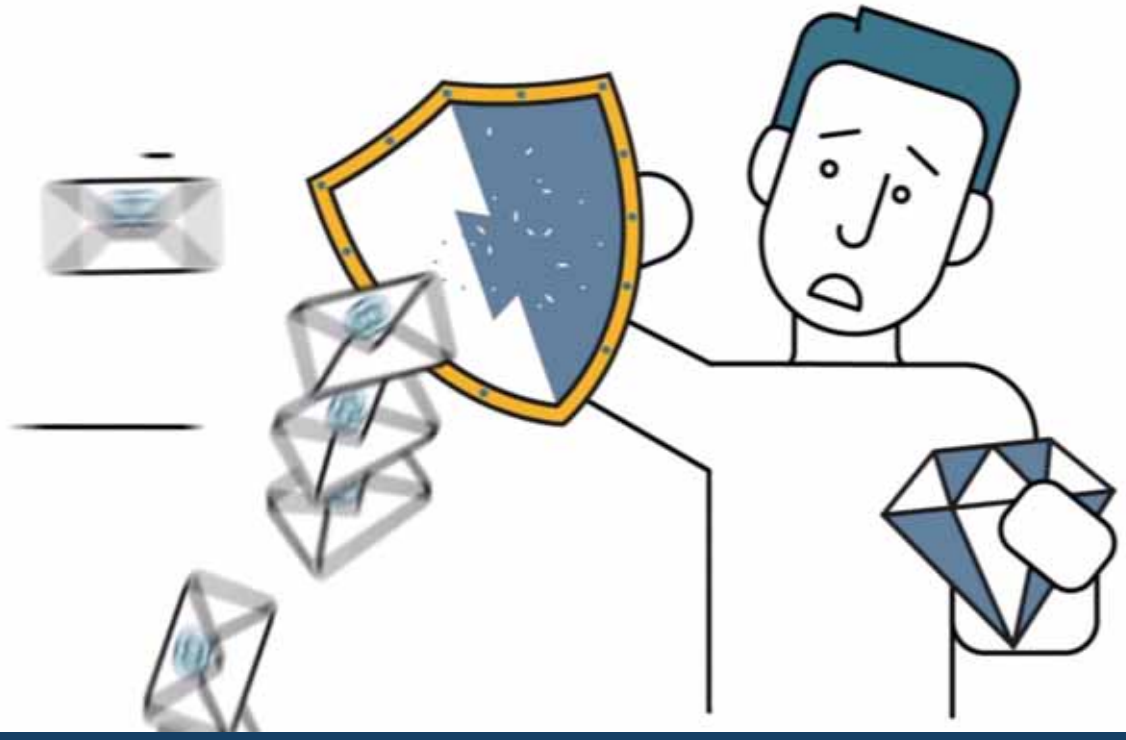
Bedankt voor de artikelen over beveiligingsraamwerken, -strategie, -beleid, -management, -risico's en -maatregelen. Er is geschreven over mensen, processen en techniek, waarbij de veelheid van toepassingsgebieden regelmatig geraakt werd. Of het nu over overheid, banken of industrie ging. Over landelijke regie, waakhonden, organisaties, netwerken of systemen. Over mainframe, Windows of Unix. Over wetten, standaarden of voorbeelden. Er is over geschreven!

En dat moet zo doorgaan. 'Cybersecurity', zoals we het zijn gaan noemen in de tijd van mijn redacteurschap, kunnen we alleen effectief aanpakken als we vanuit die veelheid van content kennis blijven delen. Daarmee en daardoor creëren we ook weer nieuwe kennis. Ik ga op zoek naar mijn nieuwe plaats in dat geheel.

Lex Borger

In dit nummer

Cyberveilig gedrag: meer dan alleen het locken van je beeldscherm - **4**
AVG in 6 maanden? - **8**
Workshop 'Artikel schrijven' - **10**
Enterprise control by design - deel 2 - **12**
Column Attributer - Cyber secured - **17**
De (r)evolutie van digitaal bewijs - **18**
Bankoverval - **22**
Column Privacy - AI een privacy professional geknuffeld? - **25**
Data veilig over glasvezel - **26**
Achter het nieuws - Dolle Dwaze Dingen - **28**
Column Berry - Vissen - **31**



CYBERVEILIG GEDRAG: MEER DAN ALLEEN HET LOCKEN VAN JE BEELDSCHERM

De menskant van cybersecurity krijgt steeds meer aandacht, naast de technische kant. En terecht. Immers, cybercriminelen maken steeds vaker gebruik van vernuftige social engineering technieken. Voor de meeste organisaties is daarom niet meer de vraag óf zij zich moeten bezighouden met het weerbaar maken van hun medewerkers, maar hóe. Een deel van deze menskant van cybersecurity bestaat uit het verhogen van awareness. Het uiteindelijke doel is echter niet alleen bewustzijn, maar ook het bewerkstelligen van cyberveilig gedrag. PVIB publiceert in de komende edities een drieluik omtrent cyberveilig gedrag, waarvan dit het eerste artikel is. In dit artikel wordt een breed inzicht gegeven in wat cyberveilig gedrag dan precies inhoudt. Waar hebben we het over als we praten over cyberveilig gedrag, welke gedragingen komen veel voor en hoe universeel of verschillend zijn die tussen organisaties?

Artikel 1 van Drieluik cyberveilig gedrag

Inge Wetzer, Hoffmann Cybersecurity

Steeds meer cyberaanvallen richten zich direct op de medewerkers van organisaties. Ransomware, door het aanklikken van een interessant ogende link; CEO fraude, door in te spelen op vertrouwen; of een trojan, door het openen van een bijlage uit nieuwsgierigheid, zijn aan de orde van dag. En dus volstaat het niet langer om met name de techniek veilig in te richten. Wat hebben we immers aan een goede virusscanner en firewall als vervolgens onze medewerkers telefonisch gevoelige informatie weggeven of op een link klikken en daarmee malware binnenhalen?

De groeiende aandacht voor de menskant van cybersecurity uit zich met name in de toenemende populariteit van awareness trainingen in de vorm van e-learning, workshops, games, et cetera. Belangrijk is echter dat niet bewustzijn het einddoel is, maar gedrag. Bij doorvragen blijkt al gauw dat organisaties willen dat de medewerkers zich cyberveilig gedrágen. Dit onderscheid tussen awareness en gedrag is belangrijk, omdat er vaak een kloof zichtbaar is tussen deze twee. Bijvoorbeeld medewerkers die wel wéten dat ze eigenlijk een lang en ingewikkeld wachtwoord zouden moeten gebruiken, dóen dat vaak toch niet omdat ze het teveel gedoe vinden. Of medewerkers zijn zich er wel van bewust dat ze hun laptop niet in de auto moeten laten liggen, maar doen dat toch wel, omdat dat even beter uitkomt.

Om de kloof tussen awareness en gedrag te overbruggen, is er vanuit de psychologie een programma voorhanden dat zich direct richt op het veranderen van gedrag (Wetzer, 2017). In dit gedragsprogramma worden inzichten vanuit de psychologie gecombineerd met die uit cybersecurity, om zo de cyberweerbaarheid van medewerkers van organisaties te verhogen. Een belangrijk uitgangspunt in het gedragsprogramma is dat gedrag, om veranderd te kunnen worden, heel specifiek gedefinieerd moet worden. Een breed begrip als 'cyberveilig gedrag' kan immers niet gemeten of veranderd worden. Bovendien is dit gedrag vaak afhankelijk van de context van een organisatie. De eerste stap in een gedragsveranderingsprogramma is dus om de gewenste gedragingen zeer specifiek te definiëren. Dit artikel zal meer inzicht geven in deze specifieke gedragingen.

Cyberveilig gedrag: Wat is dat eigenlijk?

Om organisaties te helpen hun medewerkers weerbaar te maken, heeft Hoffmann in de eerste helft van 2017 veelvuldig gedragsonderzoek gedaan binnen diverse organisaties. Door een team van psychologen is gesproken met medewerkers in functies verantwoordelijk voor informatiebeveiliging/cybersecurity, zoals (chief) information security officers, ICT'ers maar ook CFO's. Door het volgen van een speciale methodiek in workshopvorm, is voor deze organisaties benoemd welke doelgroepen binnen de organisatie kwetsbaar zijn als het gaat om cybersecurity. Vervolgens is in de workshops per doelgroep onderzocht welke specifieke gedragingen deze doelgroep in de ideale situatie zou vertonen. Deze doelgroepen en gedragingen vormden het startpunt voor een dieper onderzoek door de psychologen dat zich richtte op het in kaart brengen van de oorzaken voor het ontbreken van het gedrag. Deze inzichten geven vervolgens rechtstreeks handvatten over maatregelen die genomen kunnen worden om het gedrag te veranderen.

Doordat er voor een verscheidenheid aan organisaties workshops zijn gedaan, is er een breder inzicht ontstaan in de concrete gedragingen die onder de noemer 'cyberveilig gedrag' vallen: wat is dat nou eigenlijk precies? Deze inzichten zijn mogelijk interessant voor andere organisaties die zich willen richten op het verhogen van de weerbaarheid van hun medewerkers. Daarom beschrijft dit artikel een aantal van deze inzichten, die zijn gebaseerd op onderzoek naar in totaal 65 gedragingen bij diverse organisaties met betrekking tot informatiebeveiliging.

Doelgroepen

De doelgroepen voor een gedragsveranderingsprogramma bevinden zich in alle lagen van een organisatie. De kwetsbaarheden van deze doelgroepen verschillen echter wel van aard. Zo is bijvoorbeeld een HR-afdeling een belangrijke doelgroep, omdat zij veel persoonsgegevens van medewerkers gebruikt en regelmatig in contact staat met derden, zoals bedrijfsartsen of uitkeringsinstanties. Secretariaten, een andere veel onderzochte doelgroep, hebben vaak zeer veel toegang en autorisaties, waardoor zij erg zorgvuldig om moeten gaan met hun kennis en

Dr. Inge Wetzer is sociaal psycholoog cybersecurity bij Hoffmann Cybersecurity. Na haar studie economische psychologie is zij gepromoveerd in de sociale psychologie. Vervolgens heeft ze bijna tien jaar bij TNO gewerkt, waar ze gedragskundig onderzoek verrichtte en zich bezighield met gedragsverandering in het domein Defensie & Veiligheid. Sinds 2016 werkt zij bij Hoffmann. Haar opdracht is om haar kennis en ervaring op gebied van menselijk gedrag te koppelen aan het domein cybersecurity (en compliance), om zo werknemers van organisaties beter te beschermen tegen cyberaanvallen. Inge is te bereiken via i.wetzer@hoffmannbv.nl

CLUSTER	VOORBEELDEN GEDRAGINGEN
Wachtwoorden	Gebruik een sterk wachtwoord
	Zakelijk een uniek wachtwoord gebruiken (dus niet hetzelfde als privé)
	Wachtwoord niet delen met anderen
Clean desk	Sluit je ladeblok af, ook als je even weg bent
	Verstop je sleutel niet in een pennenbakje of andere logische plek
	Laat geen gevoelige informatie op je bureau liggen
Phishing mails	Verdachte mail herkennen
	Advies vragen voor je een verdachte mail/link/bijlage opent
	Melden van ontvangst verdachte mail (signaalfunctie)
Vertrouwelijke informatie delen in gesprekken	Controleer de identiteit van een beller voor je informatie weggeeft
	Spreek niet in het openbaar over vertrouwelijke onderwerpen
	Deel informatie alleen op basis van 'need to know'
Vertrouwelijke documenten	Vertrouwelijke documenten niet op een USB stick zetten (tenzij versleuteld)
	Vertrouwelijke documenten niet per e-mail delen (tenzij versleuteld)
	Veilig weggooien van vertrouwelijke documenten na gebruik
PC-gebruik	Lock je PC als je wegloopt van je plek
	Werk altijd onder je eigen account
	Bewaar bestanden op beveiligde schijven en niet lokaal

Tabel 1 - Clusters van gedragingen inclusief voorbeelden

informatie. Productiemedewerkers, op hun beurt, zijn juist weer een belangrijke doelgroep wanneer het gaat om informatie zoals recepturen en concurrentiegevoelige productiegegevens. De meeste gedragsveranderings-programma's richten zich dan ook op dit soort doelgroepen die een organisatie in een verticale doorsnede vertegenwoordigen. De belangrijkste resultaten omtrent de cyberveilige gedragingen worden hieronder beschreven.

Gedragingen

1. Er is een universele set van clusters van cyberveilige gedragingen

Een eerste interessante bevinding is, dat er in het domein van cybersecurity relatief veel clusters van gedragingen zichtbaar zijn die haast voor elke organisatie van toepassing zijn. Er is dus eigenlijk sprake van een universele set aan onderwerpen waar organisaties graag op het mensvlak mee aan de slag gaan.

Deze gedragingen kunnen worden geclusterd in de volgende zes onderwerpen.

- Wachtwoorden
- Clean desk
- Phishing mails
- Vertrouwelijke gesprekken
- Vertrouwelijke documenten
- PC-gebruik

Belangrijk hierbij is dat de clusters weliswaar universeel zijn, maar de gedragingen die organisaties graag willen zien van hun medewerkers, verschillen. Dit wordt hieronder toegelicht in de tweede conclusie:

2. Het belangrijkste gewenste gedrag binnen een cluster verschilt per organisatie

Ondanks de universaliteit op het gebied van overkoepelende clusters, valt wel op dat binnen deze clusters de specifieke gewenste gedragingen voor elke organisatie verschillen. Als voorbeeld nemen we het onderwerp wachtwoorden. Binnen dit cluster vallen verschillende gewenste gedragingen, zoals het gebruiken van een sterk wachtwoord, het gebruiken van een uniek wachtwoord voor de werkomgeving en het niet delen van het wachtwoord met collega's. Zo kwam in veel van de onderzochte organisaties het onderwerp wachtwoorden voor in de set van gewenste gedragingen. Echter welk van de specifieke gedragingen voor deze organisaties het belangrijkst werd bevonden, verschilde. Tabel 1 illustreert dit door voor elk cluster voorbeelden van gedragingen te beschrijven die binnen de clusters vallen.

3. Voor elke organisatie gelden tevens unieke gedragingen

Naast de universele clusters laten de resultaten van de onderzoeken zien, dat sommige gedragingen in het kader van cybersecurity zeer specifiek kunnen zijn voor een bepaalde organisatie. Naast gedragingen uit de universele set, is bij elk van de onderzochte organisaties sprake van unieke gedragingen die belangrijk zijn, bijvoorbeeld doordat de organisatie in een bijzondere branche werkt, een bijzonder

Motivatie: Wil iemand het gedrag vertonen; welk doel vindt iemand eigenlijk belangrijk?

Gelegenheid: De mate waarin de omstandigheden het gedrag bevorderen of belemmeren. Bijvoorbeeld fysieke omstandigheden, sociale omstandigheden en technologie.

Capaciteit: De mate waarin iemand in staat is om bepaald gedrag te vertonen, gegeven zijn eigenschappen, vaardigheden, kennis en instrumenten.

Figuur 1 – Gedrag = motivatie + gelegenheid + capaciteit

product verkoopt, of in een bijzondere fase (zoals overname) verkeert.

4. Een deel van de gedragingen is doelgroep-specifiek
Wanneer gekeken wordt naar de specifieke gedragingen die organisaties graag van hun medewerkers willen zien, valt te zien dat een deel van deze gedragingen uniek is voor een bepaalde doelgroep. Hierbij kan gedacht worden aan het verifiëren van iemands identiteit alvorens informatie over salaris te geven (voor HR), het dubbelchecken van facturen vanaf een bepaald bedrag (voor Finance) of het beveiligd versturen van contactgegevens van klanten (voor Marketing). Naast dit doelgroep-specifieke gedrag, zijn er ook gedragingen zichtbaar die doorgaans voor alle doelgroepen in een organisatie gelden, zoals het gebruiken van een veilig wachtwoord en het gebruiken van een afgesloten container voor het weggooien van vertrouwelijke papieren.

Hoe nu verder?

Op het moment dat het concrete gedrag duidelijk is, kun je aan de slag met gedragsverandering. Hiervoor is het belangrijk om eerst te begrijpen hoe gedrag in elkaar zit. De gedragstheorie van MacInnis, Moorman & Jaworski (1991) stelt dat gedrag kan worden gezien als resultaat van drie factoren: motivatie, capaciteit en gelegenheid. Met andere woorden: wíl iemand het doen, is hij in staat om het te doen en krijgt hij de kans om het te doen?

Als deze drie factoren alle drie in voldoende mate aanwezig zijn, zal gedrag plaatsvinden. Als één van deze factoren (deels) ontbreekt, is de kans op gedrag een stuk kleiner. Het verdelen van gedrag in deze drie componenten vergroot het inzicht in de maatregelen die een organisatie kan nemen om bepaald gewenst gedrag te laten optreden. Het inzicht dat gedrag uit meerdere componenten bestaat, maakt inzichtelijk waarom awareness programma's vaak niet tot het gewenste resultaat leiden. Awareness gaat over kennis en capaciteit. Dat gedrag niet optreedt vanwege een gebrek aan kennis erover is namelijk een aanname! Het kan net zo goed ontbreken aan motivatie of aan gelegenheid om het gedrag te vertonen. Daarom is het relevant om, voorafgaand aan het bedenken of implementeren van een interventie, te onderzoeken waarom bepaald gedrag niet of minimaal optreedt.

In de volgende editie van PVIB vindt u het tweede artikel uit het drieluik cyberveilig gedrag, dat ingaat op deze onderliggende redenen voor het ontbreken van gedrag en geeft antwoord op de vraag waaróm mensen het door CISO's gewenste gedrag soms toch niet vertonen. Het bespreekt resultaten van breed onderzoek naar een grote set van gedragingen in verschillende organisaties en geeft een beeld van de achterliggende oorzaken: willen de mensen het, kunnen ze het, en worden ze in staat gesteld om de cyberveilige gedragingen te vertonen? Het laatste artikel van dit drieluik zal ten slotte ingaan op de maatregelen die genomen kunnen worden om gedrag te veranderen, gegeven de onderzochte oorzaken.

Referenties

Wetzer, I. M. (2017). Voorbij awareness; grip op cyberveilig gedrag. InformatieBeveiliging,17(3), 24-26.

AVG IN ZES MAANDEN

Halen we dat?

De invoeringsdatum van de AVG komt met rasse schreden nabij. Bij publicatie van dit blad zijn er nog ongeveer zes maanden te gaan. Internationals, ondernemingen en rijksoverheden zijn allang bezig met de voorbereidingen voor de implementatie van de AVG, maar er zijn groepen die niet de lange adem hebben om hier zo lang van tevoren al mee bezig te zijn. Denk bijvoorbeeld aan de kleinere gemeenten en het MKB. En dan hebben we het nog niet eens over de ZZP-ers. Zij zijn nog bezig met de vraag wat de AVG voor hen inhoudt en waar ze dan zouden moeten beginnen.

Zie de AVG als een set kansen. Met de AVG wil Europa een gedragsverandering in de samenleving veroorzaken. In plaats van problemen in de verwerking van persoonsgegevens in de doofpot te stoppen, moeten we onze maatschappelijke verantwoordelijkheid nemen. Door respect te tonen voor onze klanten en ons tot doel stellen de kans op fouten te minimaliseren, laten we zien privacy serieus te nemen. Door tot op zekere hoogte openheid te geven over gemaakte fouten, kunnen we collectief leren van 'lessons learned'.

Organisaties verwerken persoonsgegevens als onderdeel van hun bedrijfsactiviteiten. Dit kunnen opgelegde taken of doelstellingen zijn of dienstverlening die dit ondersteunt. De AVG benadrukt simpelweg de noodzaak om daarbij een zorgvuldige omgang met persoonsgegevens in te richten. Voorkomen van privacy-incidenten die mogelijk als datalek gekwalificeerd moeten worden, is daarbij de koers. Maar dat was eigenlijk altijd al de kwalificatie van goed ondernemerschap. De echte kansen zitten in het uiteindelijke effect van het (opnieuw) beoordelen van de huidige bedrijfsprocessen en de persoonsgegevens die daarbij verwerkt worden. Hiernaar kijken met de AVG-bril op kan ook bij jouw organisatie tot interessante kansen leiden.

De AP probeert verwerkers in Nederland voor te bereiden door een 10-stappenplan op te stellen (1). Dit stappenplan biedt een aantal onderwerpen waar je aandacht aan moet geven, maar vergroot niet het draagvlak voor de AVG, door de manier waarop het geschreven is. Zo staat al in stap 1 de tekst "Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro ...". Met de focus op sancties blijft onderbelicht dat organisaties die voldoen aan de AVG daar zelf ook beter van worden.

De AVG geeft je, net zoals de Wbp, de mogelijkheid om gegevensbescherming op jouw manier in te richten. De AVG maakt de noodzaak om dat ook daadwerkelijk te doen echter tot een

serieus aandachtspunt. Pak deze kans dan ook en denk als bestuurder, functionaris en ondernemer zelf na hoe je het eigenlijk geregeld zou willen zien. Besef je ook dat er vaak al gerelateerde doelstellingen zijn gehaald door een andere discipline, zoals BCM. Zorg voor een goede afstemming met deze disciplines en bewaak de afspraken. Er zijn namelijk drie aspecten die je goed geregeld wilt hebben; Wie doet wat? Wat als het misgaat? Hoe beperk je de risico's?

Aspect 1: Wie doet wat?

Er zijn onder de AVG een aantal zaken die geregeld moeten worden. De activiteiten beginnen met het bepalen van degene die het gaat regelen. Hier volgt een lijst van de hoofdzaken voor kleinere bedrijven.

- Overzicht verwerkingen: Wie maakt een overzicht van alle gegevensverwerkingen die je zelf uitvoert of in opdracht van je bedrijf worden uitgevoerd? Wie beoordeelt de grondslag waarop die gegevens verwerkt worden?
- Functionaris gegevensbescherming: Sommige organisaties moeten een FG hebben, maar ook als het geen moeten is, kan het verstandig zijn om een FG te hebben. Wie beslist of er een functionaris gegevensbescherming wordt aangesteld?
- GEB (gegevensbeschermingseffectbeoordelingen): Wie bepaalt of de gegevensverwerking in je bedrijf waarschijnlijk een hoog risico oplevert? Want dan moeten er GEB's uitgevoerd worden. Wie gaat die uitvoeren? Wie bepaalt welke maatregelen genomen moeten worden? Wie overlegt met de toezichthouder als dat nodig is? Dit klinkt erger dan het is, je bent al een heel eind op weg met de risicoanalyse die je toch moet doen.
- Leidende toezichthouder: Voor de bedrijven die op meer plaatsen in Europa gevestigd zijn: Wie bepaalt welke toezichthouder de leidende toezichthouder is?
- Afhandelen van verzoeken: Mensen hebben het recht verzoeken in te dienen bij je bedrijf, zoals een verzoek tot inzage, correctie of verwijdering. Deze rechten bestonden al onder de Wbp. Nieuw is het recht op dataportabiliteit. Mensen mogen in specifieke situaties het verzoek indienen om hun gegevens te krijgen, in een vorm die het makkelijk maakt om die door te kunnen geven aan een andere organisatie. Dit zijn operationele processen. Wie is verantwoordelijk voor het opzetten daarvan? Wie is verantwoordelijk om deze processen uit te voeren?

Aspect 2: Wat als het misgaat?

Dit is eigenlijk niet anders. Een incident moet onderzocht worden. In het onderzoek bepaalt men of het ook een datalek betreft zoals bedoeld in de AVG (en Wbp). In dat geval moet bepaald worden of en hoe dit eventueel gemeld moet worden: bij de toezichthouder en in sommige gevallen ook bij de betrokkenen. Wie gaat dit doen, wat wordt er dan gedaan en wie ziet hierop toe?

Aspect 3: Hoe beperk je de risico's?

Er zijn een aantal doelstellingen waarvan het verstandig is om die na te streven. Als ze toegepast worden, kunnen ze de gevolgen van datalekken beperken. Denk hierbij aan:

- 'Privacy by design' en 'privacy by default': ga bij processen en systemen die persoonsgegevens verwerken na of de verwerking veilig is ingericht; het ontwerp, de implementatie, de opzet en de uitvoering. Denk hierbij na hoe de persoonsgegevens mogelijk misbruikt kunnen worden en door wie. Te vaak denken we alleen vanuit de scenario's waarbij alles goed gaat.
- Verwerkersovereenkomsten: zorg dat de afspraken met dienstverleners die je gebruikt om persoonsgegevens te verwerken op orde zijn en nageleefd worden. Je kunt wel diensten uitbesteden, maar dat ontslaat jou niet van je eigen verantwoordelijkheden. En verwerk je persoonsgegevens voor een ander? Wees je dan bewust dat een probleem ergens in de hele verwerkingsketen jouw probleem kan worden. Dit was al ingeregeld onder de Wbp. Je mocht er al niet meer vanuit gaan dat de leverancier de privacyzaken wel regelt. Onder andere de plaats van verwerking is belangrijk: als de verwerking binnen de EU plaatsindt, is het eenvoudiger te regelen.
- Toestemming registreren: In veel gevallen is de grondslag voor verwerking wettelijk geregeld. Maar als de grondslag van gegevensverwerking is, dat je toestemming hebt gevraagd en gekregen van de betrokkenen, dan zal je dit moeten registreren.
- Bewustwording: zorg dat de relevante mensen bekend zijn met de begrippen en regels uit de AVG en de keuzes die je bedrijf heeft gemaakt op basis van die regels. Als medewerkers nauwelijks weten wat een datalek is, kunnen ze ook niet helpen deze te voorkomen. Probeer hierbij zoveel mogelijk 'Jip & Janneke taal' te gebruiken.

Als deze drie aspecten geregeld zijn, kun je stellen dat je het goed genoeg doet, dat je 'in control' bent. En dat geeft de gelegenheid om weer te focussen op ondernemen.

Conclusie

Bedenk dat 25 mei 2018 slechts een datum op de kalender is waarop de regie over persoonsgegevens aangepast wordt. Er was al een Wet bescherming persoonsgegevens van kracht, er wordt gewoon een volgende stap gezet. Hoe hard je er ook aan werkt om klaar te zijn voor de invoering van de AVG, besef dat aandacht voor de zorgvuldige omgang met persoonsgegevens een voortdurend aandachtsgebied betreft. Je bent dus nooit klaar. Dat komt, doordat informatiebeveiliging en privacybescherming dynamische processen zijn, geen statische producten die je projectmatig kunt opleveren. De voorbereiding is dus geen sprint waarbij je voor 25 mei 2018 moet finishen. Zorg dat je daar ook naar handelt. Focus op de grootste risico's, maak bestuurders, managers en medewerkers enthousiast over de veranderingen die doorgevoerd worden, adem in en neem de volgende stap.

Links

(1) 10-stappenplan van het AP: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-biedt–10-stappenplan-voorbereiding-nieuwe-privacywet

Deelnemers workshop 'Artikel schrijven'.

WORKSHOP ‘ARTIKEL SCHRIJVEN’

AVG in zes maanden

Tijdens de viering van het tweede lustrum van het PvIB op 28 september 2017 heeft de redactie een workshop `Artikel Schrijven’ georganiseerd. Het voorgaande artikel `AVG in zes maanden’ is gemaakt op basis van deze workshop.

Voor de viering van het tweede lustrum van het PvIB werd de commissies gevraagd workshops te bedenken voor de avond, die zowel serieus als `for the fun’ mochten zijn. Daarover nadenkend, kwamen we bij een observatie die we als redactie regelmatig doen: IB-professionals voelen zich lang niet altijd prettig bij het idee een artikel te moeten schrijven.

Ik ken dat gevoel, ik was ook zo’n professional. Ik heb echter geleerd dat het grotendeels gewoon een kwestie van doen is. Je leert in de praktijk. En de praktijk kan intimiderend overkomen. Ik zie collega’s die zonder problemen een artikel kunnen schrijven. Ze weten welke boodschap ze willen brengen, welke insteek ze daarvoor kiezen en schrijven zo een artikel als ze daar even voor gaan zitten.

Voor mij is dat moeilijker. Ik moet concreet door een aantal stappen heen, waarbij ik een artikel langzaam laat ontstaan. Ik heb een grote lijst met mogelijke ideeën. Een aantal van deze ideeën werk ik uit, zodat het duidelijk is welke boodschap ik wil leveren. En als er dan een artikel moet komen, dan pak ik een uitgewerkt idee en maak een outline van het artikel. Die outline wordt soms nog een aantal keren bijgewerkt.

Aan het artikel `AVG in zes maanden’ hebben de volgende mensen meegewerkt:

Uit de workshop – eerste ronde

- Jasper Rappard <jasper.rappard@predictive.nl>
- Mark Verelst <mark@kuifjes.com>
- Jan Verschuren <jan.verschuren@hccnet.nl>
- Chris de Vries <impuls@euronet.nl>

Uit de workshop – tweede ronde

- Rijk Prosman <r.prosman@aspect-ict.nl>
- Kees van der Stelt <k.vanderstelt@aspect-ict.nl>
- Jan Wessels <jan.wessels@rabobank.com>

Uit de workshop – derde ronde

- Henk-Jan van der Molen <hjvdmolen@ziggo.nl>
- Ted Mos <t.mos@tbmgroep.nl>

Uit de redactie

- Lex Borger
- Lex Dunn
- Tom Bakker

Tot dit moment heb ik nog niet echt geschreven, dat is de volgende stap. Doordat ik met de outline een structuur heb, kan ik stukken van die structuur uitwerken, soms niet eens op volgorde. Loop ik ergens vast in een passage, dan ga ik elders door. Uiteindelijk krijgt het hele artikel zo vorm. Soms is het artikel zelfs anders van opzet dan wat de gedachte was bij het maken van de outline, dat is prima. Voortschrijdend inzicht noem ik dat.

Zo kwamen we tot de beslissing om te proberen een serieuze workshop op te zetten die tot doel had om deelnemers een deel van die reis tot een artikel te laten ervaren en ze achteraf het product te tonen. Afhankelijk van de interesse konden we tijdens de workshop één of meerdere artikelen laten ontstaan. Door deze vorm te kiezen; een estafetteconstructie in een beperkte tijd, kun je niet verwachten dat er een uitgebreid diepteartikel tot stand komt, maar ga je voor een kort artikel met een simpele boodschap. De workshop heeft uiteindelijk één artikel opgeleverd. Dat artikel is in deze uitgave opgenomen.

We staken de workshop pragmatisch in, in vijf delen, waarbij de laatste twee delen na de workshop zijn uitgevoerd:

1. **Ideeën opstellen;**
2. **Een idee uitwerken tot een outline;**
3. **De outline verfijnen;**
4. **Het artikel schrijven;**
5. **Terugkoppelen naar de deelnemers.**

Hierdoor is tijdens de workshop het fundament gelegd voor het artikel. We kozen er bewust voor om alles op papier vast te leggen. Deze 'old school' methode garandeerde dat kennis eenvoudig en volledig overgedragen werd van groep naar groep. Alle deelnemers hebben het uiteindelijke artikel nog kunnen inzien voor publicatie (stap 4) en konden er opmerkingen bij plaatsen (stap 5). Dat leidde nog tot enige aanpassingen. Bij stap 1 en 2 zijn sjablonen gebruikt om de workshop gestructureerd te houden. Deze sjablonen zijn te downloaden via de onlineversie van dit artikel (1).

Stap 1 – Idee uitwerken

In de eerste stap was het de bedoeling om zoveel mogelijk ideeën op papier te zetten, een eenvoudige, snel uit te voeren stap. We gebruikten daarvoor het ABC-model: Argument – Bewijs – Conclusie. Hiermee wordt een idee vastgelegd door een gedachte op te schrijven. Wat houdt je bezig? Waar wordt over gepraat bij de koffieautomaat? Dat is de 'A' – het argument. Waarom is dat zo? Geef kort het bewijs voor en/of tegen het argument aan. Dat is de 'B'. De hoeveelheid aan bewijs geeft aan hoe gemakkelijk het is om over het argument te schrijven. Het liefst wil je wat positief bewijs en een beetje negatief bewijs. Dan kun je een lekker lopend verhaal opzetten. Als laatste kun je een conclusie trekken– de 'C', over het argument naar aanleiding van het bewijs. De conclusie moet niet voor de hand liggen, want dan wordt het geen interessant verhaal, maar het moet ook geen vergezochte conclusie zijn.

De groep die stap 1 uitvoerde, kreeg de opdracht zoveel mogelijk ideeën in te brengen en uit te werken. Uiteindelijk zijn vier ideeën volledig volgens het sjabloon uitgewerkt.

Stap 2 – Van idee tot outline

De tweede groep kreeg de vier uitgewerkte ABC-tjes om hier een artikel uit te kiezen ter uitwerking. De groep koos 'GDPR in 6 maanden'. Vervolgens namen ze het idee tot zich en zochten hier een focus en scope bij, noemden de kernwoorden die in het artikel terug zouden moeten komen. Er bleek geen research nodig te zijn, het onderwerp stond bij de deelnemers voldoende op het netvlies. Het bewijs uit de vorige stap werd een slag dieper uitgewerkt naar kernachtige formuleringen van punten vóór en tegen. Idealiter worden deze formuleringen ook in een logische volgorde gezet, maar daar is de groep niet aan toegekomen. Vervolgens werd een insteek gekozen voor het artikel en werden de pakkende elementen van het artikel bepaald. Door tijdsnood was dit beperkt, maar de groep heeft wel wat ideeën opgeschreven.

Stap 3 – Het artikel verfijnen

Bij stap drie zat de redactie om de tafel met twee professionals met flink wat schrijfervaring. Dat hielp wel bij de verfijning. Op dat moment werd de structuur van de workshop losgelaten en voerde de redactie een gesprek met de deelnemers over de aangedragen elementen. Het uitgangspunt bleef om de aangedragen ideeën verder te brengen richting een artikel dat getrouw was aan de kaders die in de eerste twee stappen gezet waren.

Stap 4 – Het artikel schrijven

Na de workshop werkte de redactie het artikel uit. De opzet bleek prima geschikt om een artikel van twee pagina's te schrijven.

Stap 5 – Terugkoppeling

Het conceptartikel is daarna teruggekoppeld naar alle deelnemers. Hier kwamen nog wat opmerkingen uit, die vooral leidden tot herformuleringen om de leesbaarheid te verbeteren en hier en daar toevoegingen van informatie om de balans te houden.

De redactie vond de workshop een succesvolle activiteit. De deelnemers maakten een artikel, waarin zij hun inbreng ook herkennen. Dit stimuleren is één van de fundamenten van de redactie. We gebruiken deze aanpak in de toekomst graag nog een keer om tot één of meerdere artikelen te komen. We zoeken daarom vakgenoten die graag eens aan een artikel mee willen werken, maar nog wat aarzelend staan tegenover dat hele schrijfproces. We horen graag van jullie via ibmagazine@pvib.nl!

Links

(1) Onlineversie van dit artikel:
https://www.pvib.nl/actueel/blogs/workshop-artikel-schrijven

Lex Borger, hoofdredacteur IB magazine.

ENTERPRISE CONTROL BY DESIGN - DEEL 2

Met als sleutelbegrip business alignment schetste het artikel 'Enterprise Control by Design' (1) een gestructureerde aanpak voor het afleiden van control requirements. Beschreven is hoe, in een continuüm van verandering, vanaf Strategisch Plan, via Business Model, Business Capability Architectuur tot en met Business Capability Stories, control requirements afgeleid kunnen worden die aansluiten op strategische belangen en transformaties van een concern.

In dit artikel werken we dit onderwerp verder uit aan de hand van Information Security Control requirements die we schetsmatig koppelen aan Business Capability Stories om zodoende te komen tot een business-aligned raamwerk voor Information Security Risk Control.

Het vertrekpunt

Het vertrekpunt van dit artikel is gelijk het eindpunt van het vorige artikel (1), namelijk; Business Capability Stories. Deze stories leggen in essentie vast aan wie en onder welke voorwaarden stakeholders door middel van de capability touchpoints van een capability toegevoegde waarde bieden aan begunstigden. Zoals in het vorige artikel aangegeven, zijn Business Capability Stories in opzet analoog aan User Stories, zoals deze bekend zijn in de context Agile/Scrum en hebben ze de volgende structuur:
<Stakeholder> leverages <Capability Touchpoint> of <Capability> to deliver <Benefit> to <Recipient> under <Terms>
Een aantal voorbeelden worden in tabel 1 getoond.

Constituenten van de Business Capability Stories zien we, afzonderlijk en ook in cartesische combinatie, als assets die aan een controleregime onderworpen zijn.

De assetportefeuille

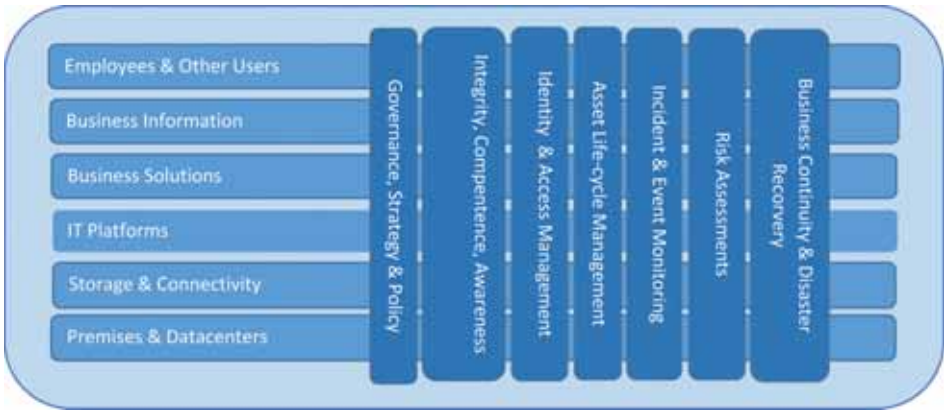
Voor het systematisch afleiden van control requirements is de verzameling te beschermen assets, om verschillende redenen, misschien wel de meest belangrijke resource en als samenstel natuurlijk ook een asset. Het is belangrijk te weten dat deze verzameling, die we de assetportefeuille noemen, aan voortdurende verandering onderhevig is.
Sommige van deze assets komen in beeld voor de beheersing van informatiebeveiligingsrisico's. Deze verzameling dopen we bij deze de assetportefeuille voor informatiebeveiliging (IB-assetportefeuille).
Nog eens wordt benadrukt dat assets in de assetportefeuille te correleren zijn met concrete constituenten van Business Capability Stories. Zodoende is alignment met de capability architectuur, het businessmodel en ook de business strategie gewaarborgd. Dit alignment is een kritische en kwaliteitsbepalende factor voor onder meer het creëren van plausibele dreigingsscenariomodellen, effectieve business impact analyses en het geavanceerd meten en kwantificeren van risico's en opportunity's is

Het controle requirements raamwerk

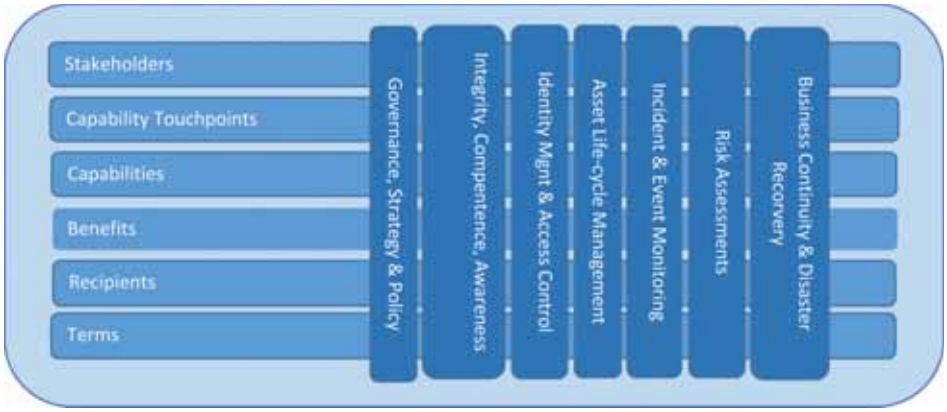
Geldende regelgevende en statutaire requirements vormen

Stakeholder	Touchpoint	Capability	Benefit	Recipient	Terms
HR Project Manager	Storage Mgnt Portal	Storage Mgnt	Storage Upgrade	HR	Silver-SLA
Storage Administrator	Storage Management Interface	Storage Mgnt	Allocated Storage	HR Project Management	Silver-SLA
Hiring manager	request resource	Internal Staffing	Project SME	Project x	standard-temp-hr
Sales Department	DR Advisory	BCM	DR Plan	Sales Department	standard-bcm
Retail products Dept	SIEM Services	SOC	SIEM Services	Consumers Portal	standard-24-7

Tabel 1 - Voorbeelden van Business Capabilities Stories



Figuur 1. Willekeurig gekozen controle model.



Figuur 2. Controle model versus assettypen.

op ieder moment een samenstel van organisatiespecifieke control requirements die van toepassing zijn op de assetportefeuille. Dit samenstel van controle requirements noemen we een controle raamwerk (engels: control framework). Ook hier kan de lezer er rekening mee houden dat het controle raamwerk aan verandering onderhevig is.

Het controle model en het controle regime

Enterprise Control by Design wordt gerealiseerd door de borging van een regime dat in opzet, inrichting en werking waarborgt dat een organisatie in staat is om de uitgestippelde strategische koers te varen, binnen gekozen toleranties en voor zover dat a priori mogelijk en gewenst is. Een controle model, of controle landschap definiëren we als het cartesisch product van de assetportefeuille en het controle requirements raamwerk. Zie het als een kaart die in specifieke zin definieert welke controle op welke assets van toepassing zijn.
In TOGAF termen uitgedrukt is een controle landschap een view op de organisatie die voor Control by Design meerwaarde biedt. Per stakeholder zullen andere viewpoints

Ing. Maurice Gittens, CRISC, CGEIT, CISA, CISM. Maurice werkt momenteel als Capability Architect bij de overheid. Hij is bereikbaar via maurice@gittens.nl.

op dit landschap bestaan.
We spreken van een controle regime als een controle model in opzet, inrichting en werking in een organisatie is geborgd als een collectie van plan-do-check-act cycli die op verschillende niveaus en voor verschillende soorten assets het controlebeleid uitoefenen. Doorgaans zal de effectiviteit van een controle regime door middel van periodieke audits getoetst worden.
Een abstractie van een willekeurig gekozen controle model (met uitsluitend high-level IB-gerelateerde control requirements) wordt in figuur 1 getoond.

Het voorbeeld in Figuur 1 toont horizontaal de constituenten van business capability stories uit de business capability map en verticaalt een aantal willekeurig gekozen high-level IB gerelateerde control requirements. Deze weergave helpt de consistentie en uniformiteit te visualiseren waarmee control requirements op assets van toepassing zijn.
Figuur 2 toont een verdere vertaling en concretisering van het voorbeeld controlelandschap naar assettypen die in het domein van IT-security herkenbaar zullen zijn.

Ik stel bijvoorbeeld, dat de effectiviteit van een managementsysteem voor informatiebeveiliging gebaat is bij een extensionele definitie van het controle model, ingezet om de operatie van de plan-do-check-act cyclus te ondersteunen. In latere vervolgartikel(en) probeer ik deze materie met enkele voorbeelden te concretiseren.
Voor nu is het belangrijk om te realiseren dat controle requirements vanaf concrete assets, zoals specifieke servers en applicaties, volgens de geschetste aanpak via business capability maps en businessmodels, met de business strategie te correleren zijn. Dit alignment biedt voordelen, ook als men de ambitie heeft om enterprise performance op discrete wijze te administreren (bijvoorbeeld in tijd, geld, materialen, risico-indicatoren) en maakt het mogelijk te rapporteren op basis van KPIs die effectief te aggregeren en consolideren zijn.

Het belang van identiteit en integriteit

Het aantonen dat een organisatie in control is, behelst het gestructureerd administreren van relevante informatie over het controle regime, het aggregeren en consolideren van deze informatie en het correleren van deze informatie aan strategische doelstellingen. Een belangrijk doel hierbij is om op verschillende niveaus in de organisatie, via passende rapportages, informatie te bieden die, met name de checkfase van continuous improvement (PDCA) cycli, van onderbouwde feedback voorziet. Die feedback geldt als stuurinformatie voor het managen van veranderingen.
Issues met de integriteit van deze gegevenshuishouding doen afbreuk aan de kwaliteit van deze feedback. Derhalve zijn sluitende requirements een verzameling voor identiteit en effectief management van identiteit in een controle regime van kritische succesfactoren.

Toegepast op Business Capability stories geldt dat de belangen van stakeholders en begunstigden (dit zijn de recipients) gebaat zijn bij effectieve identity management controls. Hoe zal men anders bijvoorbeeld kunnen waarborgen dat:

- Benefits bij de juiste begunstigden terecht komen?
- Stakeholders zich geen benefits toe-eigenen waar ze geen recht op hebben?
- Audittrails op integere wijze relevante business events vastleggen?
- Et cetera

Anders gezegd: issues met identiteit op het niveau van assets in bijvoorbeeld de IB-asset portefeuille, manifesteren zich in de kwaliteit van stuurgegevens op het niveau van business capability stories en hebben in cumulatieve zin negatieve impact op stuurgegevens op het niveau van de business capability map, het businessmodel en de strategie.
Voor het identificeren van issues met identiteit hanteer ik als vuistregel de volgende aforisme.
Identity is:

- the difference between 'this' and 'that'
- not subject to change
- absolutely necessary

Mijn poging dit in het Nederlands te vertalen is als volgt.
Identiteit is:

- het verschil tussen 'dit' en 'dat'
- niet aan verandering onderhevig
- een absolute noodzaak

Toepassingen voor dit aforisme in de context van b.v. Identity & Access Management zijn er vele.

FEEDback STUURT verandering

In artikel (1) is het schema uit figuur 3 gebruikt om alignment in de tijd en tussen requirements op verschillende niveaus te visualiseren. De essentie van de boodschap was dat het succesvol effectueren van een strategische visie, juist gegeven de realiteit van continue verandering, sterk afhangt van de alignment van requirements in de tijd en op verschillende niveaus.

Toevoeging aan dit artikel is het belang van de feedbackketen vanaf de operatie naar de strategie, zoals onderstaand aangegeven.

Op ieder niveau in een organisatie zijn verschillende PDCA cycli (en corresponderende managementsystemen) te onderscheiden. De checkfase van deze cycli worden gevoed door KPIs die tot Act, Plan en Do activiteiten voor verschillende stakeholders kunnen leiden. We herkennen in deze een Check, Act, Plan, Do cyclus, die natuurlijk, behalve het gekozen perspectief, niet wezenlijk anders hoeft te zijn dan een

Strategie	S:t+5	S:t+6	S:t+7	S:t+8	S:t+9	S:t+10
Business Model	B:t+4	B:t+5	B:t+6	B:t+7	B:t+8	B:t+9
Business Capability Architectuur	A:t+3	A:t+4	B:t+5	A:t+6	A:t+7	A:t+8
Capability Solution Design	O:t+2	O:t+3	O:t+4	O:t+5	O:t+6	O:t+7
Capability Increment Realisatie	V:t+1	V:t+2	V:t+3	V:t+4	V:t+5	V:t+6
Productie	P:t+0	P:t+1	P:t+2	P:t+3	P:t+4	P:t+5

Figuur 3 - Alignment in de tijd en tussen requirements op verschillende niveaus

Strategie	S:t+5	S:t+6	S:t+7	S:t+8	S:t+9	S:t+10
Business Model	B:t+4	B:t+5	B:t+6	B:t+7	B:t+8	B:t+9
Business Capability Architectuur	A:t+3	A:t+4	B:t+5	A:t+6	A:t+7	A:t+8
Capability Solution Design	O:t+2	O:t+3	O:t+4	O:t+5	O:t+6	O:t+7
Capability Increment Realisatie	V:t+1	V:t+2	V:t+3	V:t+4	V:t+5	V:t+6
Productie	P:t+0	P:t+1	P:t+2	P:t+3	P:t+4	P:t+5

Figuur 4 - Feedback stuurt verandering op hogere niveaus

standaard PDCA cyclus.
Een mogelijk denkmodel in relatie tot een Check, Act, Plan, Do cyclus is wat mij betreft goed uitgewerkt als de Observe, Orient, Decide, Act cyclus, of een OODA loop. OODA loops werden oorspronkelijk toegepast in militaire context en vinden inmiddels toepassing in steeds meer vakgebieden. Het is de moeite waard OODA loops in militaire context te bestuderen, maar in dit artikel gaan we hier niet verder op in.
Een voorbeeld van een security capability die als een OODA loop te zien is, is bijvoorbeeld een Security Operations Center. De Observe fase monitort events op potentiele dreigingen, op basis van additionele threat Intelligence bekijkt men of er daadwerkelijk actie noodzakelijk is. Een Decision wordt volgens een beslisboom genomen en vastgelegd en vervolgens wordt er tot Act(ie) overgegaan in lijn met het genomen besluit.
Anders dan bij plan-do-check-act cycli is het streven bij een OODA loop om de doorlooptijd zo klein mogelijk te houden. Zelf zie ik preventieve controls als goede kandidaten om via een PDCA cyclus te managen en detectieve controls als juist primaire kandidaten voor OODA loops. Is er geen urgentie bij en zijn correctieve maatregelen goed voorspelbaar? Dan volstaat een PDCA cyclus. OODA loops treden in werking als PDCA cycli niet effectief kunnen zijn, zoals waar incident response direct noodzakelijk is. Voor effectieve Enterprise Control by Design zijn wat mij betreft PDCA cycli en OODA loops bruikbare bouwstenen, juist omdat beiden feedback bieden die het control regime van belangrijk stuurgegevens kunnen voorzien.

The enterprise gait: doubling the beat

Wie verandering in een (aligned) enterprise ziet als een complexe ritmische tred zal geïnteresseerd zijn in de repetitieve patronen die kenmerkend zijn. Bij verandering geeft het vaak inzicht om stil te staan bij de drivers voor verandering. Al snel kan men herkennen dat, in het algemeen, (stuur-)informatie gericht aan de juiste stakeholders en gremia, via bestemde besluiten, tot verandering leiden.
Is de alignment van requirements bij veranderingen bepalend voor de effectiviteit waarmee veranderingen worden doorgevoerd, dan zijn stuurgegevens bepalend voor wat er veranderd zal worden.
Eventuele verbeteringen die bij veranderingen gerealiseerd worden, zijn dus afhankelijk van de volledigheid, juistheid, tijdigheid, integriteit en beschikbaarheid van bestemde stuurgegevens. De rol van data governance, informatiemanagement en datamanagement zijn bij Enterprise Control by Design dus bepalend.

Links

(1) Artikel in Informatiebeveiliging: "Enterprise Control by Design", gepubliceerd in IB8 2016

Referenties

Economics of Organizations and Markets. S. Onderstal (2014)
Business Model Generation, A. Osterwalder, Yves Pigneur, Alan Smith, and 470 practitioners from 45 countries, (2010)
Balanced Scorecards & Operational Dashboards, Ron Person, Wiley Publishing, 2009
Artikel in Informatiebeveiliging: "Tethering Enterprise Interests", gepubliceerd in IB1 2014.
Artikel in Informatiebeveiliging: "Accual Based Risk Management", gepubliceerd in IB2 2012.
Artikel in Informatiebeveiliging: "Threat Scenario Modelling I", gepubliceerd in IB6 2015.
Artikel in Informatiebeveiliging: "Treating Risk Prospectively", gepubliceerd in IB1 2015.
Artikel in Informatiebeveiliging: "Requirements dependency analysis", gepubliceerd in IB3 2015

www.qsight.nl

Wij zijn QSight IT

de grootste 100% Nederlandse security specialist

Ons aanbod omvat, naast het leveren en integreren van IT technologie, een compleet scala aan IntelliServices: proactieve consultancy, support- en beheerdiensten. Om onze internationale klantenkring optimaal van dienst te zijn beschikken wij over een Security en Network Operations Center, 24/7 bemand. Onze teams van security- en netwerkprofessionals gebruiken technieken zoals Big Data, Machine Learning en Artificial Intelligence om cyberdreigingen vroegtijdig op te merken, af te wenden en IT kostenefficiënt te managen. Daarnaast helpt QSight IT organisaties te voldoen aan wet- en regelgeving en normenkaders zoals ISO 27001, NEN 7510, CobiT, GDPR (25 mei 2018!) en Logius.

Ons verleden ligt bij twee IT specialisten die binnen de vakgebieden security, storage, networking en cloud hun sporen verdiend hebben: Qi ict en Onsight Solutions. Met deze bagage creëren we een nieuwe werkelijkheid. Een dynamische en innovatieve wereld waarin we op een slimme en pragmatische wijze voorop lopen in het beveiligen en beschikbaar houden van informatie. Onze klanten kunnen hierdoor blijvend vertrouwen op hun primaire bedrijfsprocessen.

Wanneer mogen wij u van dienst zijn?

networking security storage cloud

QSight IT®

innovating your security

Arnhem
T 026 352 01 00

Delft
T 015 888 04 44

Veldhoven
T 040 291 31 31

info@qsight.nl
www.qsight.nl

CYBER SECURED

Two years ago, in the last article of 2015, The Attributer published this same title. So why choose the title again? This previous article examined the global geo-political threat landscape and the reasons to take it seriously. In the final paragraph of the article The Attributer wrote:
We need to shift into a different gear in our thinking and planning. The current approach of treating cybersecurity as a technical problem with local technical solutions will not serve us if (when) this future unfolds. We need end-to-end, wall-to-wall thinking, the type of thinking that SABSA practitioners use in developing business and technology architectures.
Two years on and we see the same struggle to create a paradigm shift in approach. We are still treating cybersecurity and cyberdefence as a purely technical issue with local solutions. It will never work. In this second article we examine the way in which SABSA can help to change the way we tackle cybersecurity.
Architecture often benefits from principles, so let's start with some:

1. Cybersecurity is as much a business issue as it is a technology issue. (If it didn't have a business impact, why would you care?)
2. Cyberspace is a deeply nested system of systems of immense complexity. Treating it as a set of discrete technical components is a systems engineering mistake.
3. Such complex systems exhibit emergent properties – behaviours that are not caused by component failure, but by unforeseen component interactions. Many cyberexploits rely on the attacker discovering an emergent property and using it against your system.
4. The human components; their behaviour and their interactions are the least predictable, and as such need to be addressed perhaps more carefully than the purely technical components.
5. Cybersecurity requires an architectural approach, not a collection of discrete components.

Figure 1 shows the SABSA Business Stack™. This is what The Attributer means by architecture – a series of interdependent, closely coupled layers. Note the Business Attributes Profile™ (BAP) at every layer of the stack and in People and Processes that cut across every layer. Every layer is a service consumer and a service provider (Everything-as-a-Service: EaaS). Attributes are inherited and interpreted at every layer by the layer below. There is an SLA between all layers with measurable performance targets for every Attribute.

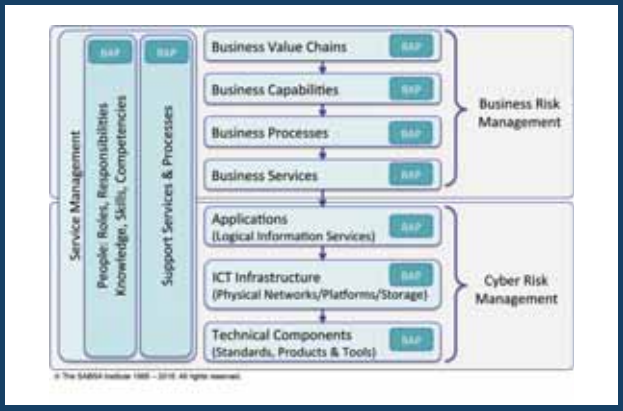


Figure 1: SABSA Business Stack

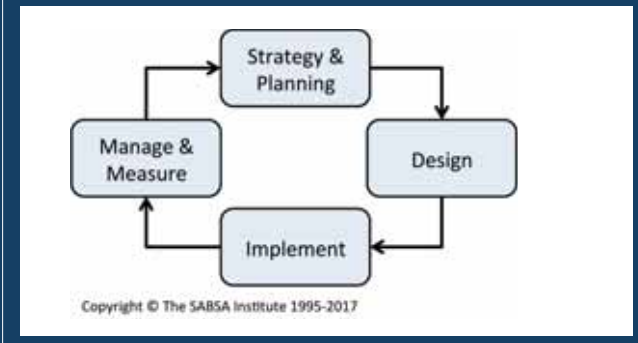


Figure 2: EaaS Supply and Demand Model

If you apply this stack model with rigour, you stand a chance of avoiding emergent properties by keeping a tight focus on each layer and its service interface. What is essential, is that the integrity of the layered supply and demand model is maintained throughout.
Disintermediation of a layer by skipping to a lower layer for a service request is forbidden. See Figure 2. Only service requests for services exposed in the service interface are allowed. For example, an application can measure the performance of the network for its latency, accuracy of delivery and sequencing, but it cannot measure whether confidentiality services are switched on in the network layer. Therefore it cannot (and must not) rely on that service being provided.

Architectural rigour will never guarantee that emergent properties are eliminated, but it will deliver significant improvements. It is time for the cybersecurity community to start taking a proper architectural approach. It is time for the adoption of SABSA as the framework of choice.

The Attributer

DE (R)EVOLUTIE VAN DIGITAAL BEWIJS

Digitaal bewijs gaat de komende 10 jaar revolutionair veranderen. In de afgelopen tien jaar werden ontwikkelingen in digitaal forensisch onderzoek gedomineerd door de opkomst van de sociale media, de smartphone en de cloud. Doordat smartphones steeds persoonlijker zijn geworden, wordt digitaal bewijs steeds vaker een aanvulling op traditioneel bewijs, zoals vingerafdrukken, voetsporen en DNA. Eigenlijk is de revolutie van digitaal bewijs al begonnen, maar we staan nog maar aan het begin. Op dit moment zijn er namelijk verschillende trends in de ICT die onomkeerbaar zijn en die naar verwachting een belangrijke rol zullen spelen in de revolutionaire ontwikkeling van digitaal bewijs.

Het internet of things

In de komende jaren zullen niet alleen computers en telefoons met hun gebruikers de online wereld bevolken. In het Internet of Things (IoT) wordt al onze apparatuur aangesloten op internet. Het zijn niet alleen apparaten die worden aangesloten, maar ook sensoren die gegevens vastleggen over van alles. Gegevens die veel meer over ons en onze omgeving vertellen dan we denken.
Langzaam begint door te dringen hoe afhankelijk we aan het worden zijn van het IoT en hoe gevoelig gegevens in het IoT kunnen zijn. Veel fabrikanten maken zich vooral druk over nieuwe businessmodellen en minder over veiligheid. Vlak voor het zomerreces werd door de Tweede Kamer met een overgrote meerderheid een motie aangenomen om iets de doen aan onveilige IoT-apparaten. In de VS is onlangs door senatoren een IoT Security Bill voorgesteld, die probeert standaarden af te dwingen om de beveiliging van het IoT te verbeteren.

DFRWS Conferentie

DFRWS is een organisatie van vrijwilligers die jaarlijks wetenschappelijke conferenties, technische werkgroepen en wedstrijden organiseert om de ontwikkeling van digitaal forensisch onderzoek te stimuleren en richting te geven (http://www.dfrws.org). Sinds de eerste DFRWS conferentie in 2001 in de VS komen wetenschappers en professionals jaarlijks bij elkaar in een informele omgeving. In 2014 werd voor het eerst de DFRWS EU georganiseerd in Amsterdam.
De wetenschappelijke research papers worden gepubliceerd in een speciale editie van het Journal of Digital Investigation. Naast wetenschappelijke bijdragen is er echter ook ruimte voor presentaties van best practices en worden workshops georganiseerd, waarin deelnemers ervaring kunnen opdoen met nieuwe technieken. Begin augustus van dit jaar werd de jaarlijkse DFRWS USA conferentie georganiseerd in Austin, Texas.
Naast deelnemers vanuit Hogescholen en Universiteiten zijn er ook deelnemers vanuit de grote bedrijven, zoals Google, Facebook, IBM, Deloitte, EY, en vanuit overheidsorganisaties zoals de Nationale Politie, FBI en de NSA. In Maart 2018 wordt voor de 5de maal de DFRWS EU georganiseerd. Ditmaal in Florence, Italië.

Kunstmatige intelligentie

Alles om ons heen wordt slim. Auto's, huizen, gebouwen en steden worden verweven met het IoT. Maar hoe slim is dat IoT nu eigenlijk? Wordt het slimmer dan wij zelf of worden we zelf ook slimmer? Zelfdenkende computers zijn nog ver weg, maar we staan nu wel aan het begin van een tijdperk van niet-denkende computers die veel slimmer zijn dan we tot voor kort voor mogelijk hielden. Vorig jaar heeft de computer met deep learning zelf geleerd hoe de beste menselijke GO speler verslagen kan worden. De slimheid van deep learning lijkt vooralsnog geen grenzen te kennen en bedrijven investeren op dit moment miljarden in kunstmatige intelligentie (AI). Deze technologie wordt nu klaargestoomd voor de zelfrijdende auto. Nvidia, de maker van de graphics processoren, liet begin dit jaar op haar jaarlijkse developers conferentie zien welke enorme ontwikkelingen er op dit moment gaande zijn om deep learning op grote schaal naar de consument te brengen. Daarbij is de zelfrijdende auto natuurlijk een inspirerend voorbeeld en tegelijkertijd ook een belangrijke stimulans om de technologie mobiel en betaalbaar te maken. Volgens Gartner zal er in 2020 nauwelijks nog software zijn zonder AI-functionaliteit.

Versmelting

Aansprekende successen van de toepassing van AI werden tot nu toe nog geboekt met data die door mensen op het internet zijn gezet. Denk aan de foto's op facebook, teksten en vertalingen op Wikipedia en de kennis die is vastgelegd in het semantische web. Dankzij het IoT kunnen computers nu rechtstreeks data uit sensoren ontvangen en kan de computer letterlijk voelen wat er gebeurt. Dit gevoel, in combinatie met deep learning en internet, gaat veel verder dan het automatiseren van alledaagse activiteiten. Automatische systemen zullen steeds meer autonomie krijgen, waarvan de zelfrijdende auto misschien wel het beste voorbeeld is.

Hans Henseler is lector Digital Forensics & E-Discovery bij de specialisatie Forensische ICT aan de Hogeschool Leiden en algemeen directeur en medeoprichter van Tracks Inspector. Op 21 november hield hij zijn lectorale rede in Leiden getiteld 'De (R)evolutie van Digitaal Bewijs'.

Dit artikel is eerder verschenen in 'AG Connect', oktober 2017

Onze fysieke wereld en cyberspace zullen versmelten. Spraakgestuurde assistenten luisteren onopvallend met ons mee, beantwoorden vragen en voeren opdrachten uit. Augmented reality-brillen projecteren hologrammen om ons heen en herkennen gebaren. Met eyetracking en haptische interfaces wordt de integratie steeds natuurlijker en worden onze zintuigen uitgebreid met de sensoren in het IoT. En het blijft niet bij onze zintuigen alleen. Elon Musk is vastberaden om met het bedrijfje Neuralink een interface te bouwen die het menselijke brein in staat stelt om nog veel sneller met computers te communiceren. Uiteindelijk worden onze natuurlijke intelligentie en waarnemingsvermogen daardoor groter en verandert augmented reality in augmented intelligence.

Digitaal forensisch onderzoek

Digitaal forensische onderzoekers zullen op zoek moeten gaan naar nieuwe technieken. Om wetenschappers en professionals uit te dagen is tijdens de DFRWS USA 2017 conferentie (zie kader) voor 2018 een nieuwe challenge gepubliceerd, waar wereldwijd teams van kennisinstellingen en bedrijven aan mee doen. De nieuwe challenge bevat IoT bewijs dat verzameld is in een fictieve moordzaak. Deelnemers worden uitgedaagd om forensisch bewijs uit de apparaten en uit de cloud te extraheren en te analyseren. Nederland is goed vertegenwoordigd in het DFRWS netwerk met deelnemers van het NFI, bedrijven, universiteiten en hogescholen. Het laboratorium van de afdeling Digitale Technologie bij het NFI heeft een sterke internationale reputatie. Ook bedrijven doen het goed. In 2011 wisten digitaal forensische onderzoekers van Fox-IT de DFRWS challenge te winnen. De gereedschappen en kennis van deze instellingen zijn echter slechts voor hun eigen medewerkers en een klein aantal stagiaires toegankelijk. Om dit soort kennis beter toegankelijk te maken, is onlangs op de campus van The Hague Security Delta een digitaal forensisch laboratorium geopend voor onderwijs en toegepast onderzoek (zie kader).

Revolutie

Het IoT, de opkomst van kunstmatige intelligentie en uiteindelijk de versmelting van cyberspace en de fysieke wereld, passen in het bredere perspectief van de vierde industriële revolutie. De vierde industriële revolutie bouwt voort op de derde revolutie, de digitale revolutie, en wordt gekenmerkt door samensmelting van verschillende technologieën, waardoor de lijnen vervagen tussen de fysieke, digitale en biologische domeinen.
Tot voor kort lieten we sporen achter, doordat we bewust gebruik maken van computer of smartphone. Als cyberspace en de fysieke wereld samensmelten, is de computer niet meer een hulpmiddel, maar wordt het een verlengstuk van onszelf. Onze menselijke 'footprint' zal steeds meer sporen nalaten in cyberspace en digitaal bewijs zal in alle vormen van opsporing en forensisch onderzoek een cruciale rol gaan spelen.

IoT Forensic labs

Voor digitaal forensisch onderzoek binnen IoT is gespecialiseerde apparatuur, kennis en software nodig. Denk hierbij aan chip-off, een speciale hardware techniek om geheugens uit te lezen als een apparaat beveiligd of zwaar beschadigd is, bijvoorbeeld door brand of water. In Nederland is dit soort apparatuur en kennis alleen beschikbaar bij gespecialiseerde labs van opsporingsdiensten, bij het NFI en bij bedrijven die die elektronische beveiligingen evalueren, bijvoorbeeld voor elektronische betaalsystemen van banken.
Dit soort organisaties en hun laboratoria zijn erg gesloten en alleen toegankelijk voor de eigen medewerkers en enkele stagiaires. Soms is er ook een screening nodig voor stagiaires, waardoor de instroom lastig is, zoals op dit moment het geval is bij de Nationale Politie. Daarom heeft Hogeschool Leiden per 1 september een IoT Forensics Laboratorium geopend op de campus van The Hague Security Delta (HSD). De totstandkoming van dit lab volgt op de opening vorig jaar van een onderzoeksruimte van het lectoraat Digital Forensics & E-Discovery van de specialisatie Forensische ICT. Doel van het nieuwe lab is om nauwer samen te kunnen werken binnen het werkveld van digitaal forensische onderzoekers.
Studenten kunnen, dankzij het lab, nu ook tijdens hun stage ervaring opdoen met geavanceerde digitale forensische technieken in opdracht van bedrijven die zelf niet over de kennis en geavanceerde apparatuur beschikken die nodig is voor forensisch onderzoek aan IoT apparaten. Specialisten van de afdeling Digitale Technologie van het NFI, Politie, FIOD, Defensie en van het bedrijfsleven zullen adviseren bij de inrichting en zullen op de HSD instructies en gastcolleges geven aan studenten, docenten en professionals over het uitvoeren van IoT forensics. Door deze samenwerking wil de Hogeschool Leiden haar onderwijs vernieuwen en de samenwerking met het werkveld intensiveren.
De focus van de HSD op Security en Forensics heeft op de campus tot een verscheidenheid aan bedrijven, overheidsorganisaties en kennisinstellingen geleid. Daarmee is een goede basis gelegd voor het aanvragen van subsidies voor toegepast onderzoek. Zo werkt Hogeschool Leiden momenteel samen met het Cyber Threat Intell lab van TNO en het Cyber Expertise Centrum van de Haagse Hogeschool aan de oprichting van een Nationaal IoT Security & Forensics Lab om startups en MKB bedrijven te adviseren bij innovaties op het gebied van IoT security en forensics.

(advertorial)

De laatste strohalm voor data protectie: ENCRYPTIE EN SLEUTELBEHEER IN COMBINATIE MET ACCESS CONTROL

De groei van nieuwe technologieën en innovaties verandert onze maatschappij de komende jaren radicaal op het gebied van digitalisering, cloud, big data en IoT. Het creëren van vertrouwen in het digitale tijdperk is daarom meer dan ooit essentieel en is de huidige uitdaging voor veel ondernemingen. Data en privacy beveiligingsstrategieën zullen daarom de komende jaren veelvuldig het onderwerp van gesprek zijn van bestuurders. Dit wordt ook grotendeels afgedwongen door nieuwe wet -en regelgeving de Algemene Verordening Gegevensbescherming (AVG of GDPR).

Huidige beveiligingsstrategieën voor protectie in het algemeen zijn gericht op preventie.
Dit is logisch, omdat beveiligingsstrategieën vaak gebaseerd zijn op het uitgangspunt: "voorkomen is beter dan genezen". Maar is dit nog steeds voldoende? Uit onderzoeken blijkt dat er op securitygebied veel wordt geïnvesteerd. Onderzoek van Juniper Research voorspelt dat de investeringen in cyber security in 2022 wereldwijd naar 135 miljard dollar zal stijgen. Dit bedrag was volgens Gartner in 2015 wereldwijd 75,4 miljard dollar. De verwachting is dat de kosten wereldwijd als gevolg van cybercriminaliteit in 2022 tot 8.000 miljard dollar zullen stijgen! De kosten van cybersecurity nemen toe maar staan niet in verhouding met de exponentiële stijging van de schade en kosten als gevolg van cybercriminaliteit. Typisch eigenlijk, omdat we de afgelopen jaren duidelijk hebben geleerd dat datalekken er altijd zullen zijn, ongeacht onze preventieve beveiligingsstrategieën. Met andere woorden; beveiligingsstrategieën enkel gebaseerd op het voorkomen van datalekken zijn onvoldoende gebleken om cybercrime het hoofd te bieden. Eén van de grootste denkers uit de wereldgeschiedenis, Albert Einstein, leerde ons: "We cannot solve our problems with the same thinking we used when we created them".

Hoe zou de beveiligingsstrategie eruit komen te zien als we de denkwijze van voorkomen van een data lek naar beveiliging van het data lek zouden verleggen?
Welke vragen zou je jezelf moeten stellen wanneer data gecompromitteerd werd:
Is mijn data encrypt? Is deze encryptie voldoende? Wie heeft toegang tot mijn data?
Deze vragen kunnen allemaal ondervangen worden door de toepassing van encryptie, sleutelbeheer in combintatie met access control. Deze 'nieuwe verrijkte' beveiligingsstrategie brengt de security dichter bij de data en de gevolgen van een inbreuk worden hierdoor significant verkleind. Organisaties die dit proces goed ingericht hebben kunnen ervan uit gaan dat de data onleesbaar is voor onbevoegden, maar vooral ook blijft wanneer deze gecompromitteerd is.

Gökmen Kiremit
Directeur Avensus
High Grade Security

De combinatie van deze nieuwe beveiligingsstrategie maakt dat het een sterke oplossing is voor data protectie en verkleint de gap tussen de beveiliging en de bedreiging significant. Daarnaast heeft deze denkwijze positieve gevolgen voor de organisatorische en technische inrichting van de wetgeving AVG.

Laten we vertrouwen creëren in onze digitale toekomst.

Avensus
HIGH GRADE SECURITY

BANKOVERVAL

Lessons learned voor een SOC

Toen ik tien jaar oud was, liep ik een keer vanuit school naar het huis van mijn grootouders om daar te gaan theedrinken. Ik passeerde het café, de slijterij, de banketbakker en de sigarenwinkel in het laatste rijtje huizen. Ja, mijn opa woonde daar op die hoek heel mooi! Net toen ik de hoek van zijn huis wilde omgaan, zag ik een vrouw met kinderwagen midden op de weg stilstaan en aandachtig naar het postkantoor kijken. Dat lag, ongeveer veertig meter verder, schuin tegenover het huis van mijn opa. Over die Tilburgseweg denderde de hele dag, dwars door het dorp Goirle, veel zwaar vrachtverkeer en ook veel personenauto's stoven voorbij. Die vrouw viel mij daarom op. En die auto met draaiende motor, aan mijn kant van de weg met de neus naar België gericht, was ook opvallend. Want je mocht daar vlak voor de onoverzichtelijke bocht niet parkeren. En de bestuurder in de auto stond bovendien vlak naast het meest stinkende urinoir van het dorp. Dat wist elke Goirlenaar. Op dat moment kwam een man het postkantoor uitgerend. Je kon daar geld storten en opnemen wist ik. En omdat de man een geweer in beide handen droeg, realiseerde ik me ook direct dat er een bankoverval gaande was en dat nog een tweede rover zou volgen met de buit. In mijn dorp! In die tijd waren er regelmatig fysieke bankovervallen (cyber crime was nog niet uitgevonden). Er waren toen ook meer afzonderlijke banken dan nu: de Amsterdamsche en Rotterdamsche Bank waren nog niet samen, laat staan samen met de Algemene Bank Nederland. De Coöperatieve Centrale Raiffeisen-Bank en de Coöperatieve Centrale Boerenleenbank moesten nog fuseren tot Rabobank. En al die banken "steunden op een flinke kluit poen", om het maar eens in het Bargoens te zeggen…

In de zijmuur van mijn opa's huis zaten nog granaatscherven en kogels van de Duitse soldaten uit de Tweede Wereldoorlog. Maar het huis stond er nog steeds en zou mij ook tegen die paar kogels uit dat oude geweer met houten kolf van die bankrover wel kunnen beschermen. Daarom besloot ik snel het huis in te gaan. Ik rende het steegje naar de tuin in en herinnerde me dat, volgens krantenartikelen over bankovervallen, omstanders vaak vergaten om het kenteken van de vluchtauto te noteren. Ik keek nog even om het muurtje, onthield het nummer en liep door naar de keuken. Mijn oma had daar op een vaste plaats een blocnote met pen op het aanrecht liggen. Zo was er altijd genoeg eten en drinken in huis. En ze kon steeds haar inspiratie kwijt, waardoor ze regelmatig prijzen won met slagzinnen voor producten en winkels. "Zij die het weten…. Gaan bij Borger's Steakhouse eten!", dat soort werk.

Mijn ouders zaten al aan de thee met mijn grootouders. Met de koekjes hadden ze nog op mij gewacht. Ik noteerde snel het kenteken en draaide me langzaam om. "Wat schreef je op?", was hun logische vraag. Ging die kleine nu óók al strijkijzers winnen? Terwijl ik de rechtermouw van mijn denkbeeldige politie-uniform straktrok, zei ik zo nonchalant mogelijk: "Ze hebben net het postkantoor aan de Tilburgseweg overvallen. Minstens één van de mannelijke daders is zwaarbewapend met een geweer, vermoedelijk een Lee Enfield. De vluchtauto, met kentekennummer 12-34-XY, verdween met hoge snelheid in zuidelijke richting. Vermoedelijk naar Poppel, de eerste plaats over de Belgische grens, ongeveer tien kilometer verderop."
Dat van de Lee Enfield was een best guess. Als jochie wist ik wel schrikbárend veel over de wapens die – aan beide kanten – werden gebruikt in zowel het Wilde Westen als in de Tweede Wereldoorlog, maar ook weer niet alles. Maar het was zeker geen modern wapen. Mijn vader stond op, pakte het briefje, streek over mijn haar en complimenteerde me. "Goed gedaan jongen", zei hij, "maar je kunt dit beter niet tegen de politie zeggen. Voor je het weet, staan die daders bij ons als getuige op de stoep." Hij verdween uit de keuken. Ik pakte mijn kop thee en 'enkele' koekjes en ging in de huiskamer, zoals elke week, Avro's Televizier en de Panorama lezen. Totdat ik met mijn vader en moeder weer naar huis zou gaan. Na enige tijd keerde mijn vader terug in de keuken, we namen afscheid en reden naar ons eigen huis, ook in Goirle.

De volgende dag stond in het krantenartikel over de bankoverval, dat een jonge moeder met de schrik was vrijgekomen en dat de gevaarlijke daders waren aangehouden bij de Belgische grens. En dat dit allemaal was dankzij een oplettende sigarenboer, die de tegenwoordigheid van geest had gehad om het kenteken te noteren. Weliswaar in een kinderhandschrift, maar wel juist. Ik was licht teleurgesteld over de gang van zaken, maar wel blij dat mijn vader me in bescherming had genomen. Zeker toen enige tijd later de bewuste sigarenboer werd overvallen in zijn eigen winkel.

Mijn gedrag van toen is te vergelijken met de diverse noodzakelijke activiteiten van een Security Operations Center nu.
Ik kwam plotseling in een voor mij onverwachte situatie terecht. Maar ik wist al wel uit de krant dat bankovervallen bestonden (opleiding), hoe het eraan toe ging met wapens en snelle vluchtauto's en dat die gevaarlijk waren voor omstanders (scenario-analyse). Ik wist dat er een bank met geld was tegenover het huis van opa en oma (kroonjuwelen in kaart). Ik kende de normale verkeersstromen goed genoeg om de vrouw en de vluchtauto als opvallende zaken te signaleren (anomaliedetectie). Ik kon door mijn wapenkennis de ernst van het incident inschatten (threat analysis). Ik kon zelfs door de combinatie van het wapen, het parkeren naast het urinoir en de rijrichting van de vluchtauto, een globale daderanalyse (attributie) doen. Ik paste een lesson learned toe (uit evaluatie van eerdere incidenten), door in de drukte wèl op het kenteken te letten. Ik deed aan risicobeperking (containment, of salvage) door mezelf eerst in veiligheid te brengen. Er was een logboek beschikbaar, waarin alle informatie (hoofdzaken, maar ook belangrijke details) gemakkelijk konden worden vastgelegd en dat deed ik ook echt. Mijn vader, als manager, nam mij als boodschapper in bescherming. Ik gaf een korte, zakelijke omschrijving van het waargenomen incident (situational awareness). Mijn vader en moeder en opa en oma als "hogere managementlaag" geloofden mij meteen. Ze begonnen niet over "Wéét je dat, of denk je dat?" of "Nu doe je een aanname, misschien ging hij wel heel vlug naar de schietvereniging en was hij zijn foedraal vergeten?". Dat vertrouwen was voor hen ook gemakkelijk te geven, omdat ik als waarnemer expliciet aangaf wat ik zeker wist (een bankoverval) en waar ik over twijfelde (exacte type geweer en dus het mogelijke aantal kogels) (intelligence reporting). En ze beseften dat ik, ondanks mijn jonge leeftijd, inderdaad veel over wapens wist en voelden na tien jaar samenleven ook wel aan, dat ik dit niet zomaar zou verzinnen, compleet met een autokenteken (trust your expert). Daarna werd ik als waarnemend agent (of analist) bewust met rust gelaten, zodat de betreffende experts (de politie) aan het werk konden om de zaak op te lossen. Ook dat laatste geef ik als tip aan security operation centers: wanneer je al je SOC-medewerkers specialist noemt, accepteer dan ook dat ze ieder één ding hebben waar ze heel goed in zijn. Gebruik dat specialisme (waarnemen, aanvoelen, inschatten, benoemen, duiden et cetera) en zet andere uitvoerders en experts in om alle specialismen, zo effectief mogelijk, breed in uw organisatie in te zetten. Vanuit een TEAM-gedachte: Together Everyone Achieves More.

Robert Metsemakers is Enterprise Security Officer bij Achmea IT. Robert is bereikbaar via metsemakers@live.com

HEB JIJ VANDAAG AL EEN PRIVACY PROFESSIONAL GEKNUFFELD?

Op mijn iPad prijkt een prachtige sticker met de tekst: "Have you hugged a privacy pro today?". Gewoon leuk, een geintje. Maar, de afgelopen tijd kijk ik daar – na de zoveelste lange en zware dag – toch wat anders naar. Ik zie om mij heen de collega's massaal toewerken naar het einde van het jaar (je weet wel: 24 december). Iedereen trekt sprintjes en iedereen is een beetje moe aan het worden. Maar het einde is in zicht! Zo niet voor de privacy professional. Het einde van het privacy-jaar is pas op 25 mei 2018. Alhoewel, het einde… eigenlijk begint het dan pas echt. Maar goed, het is wel een eerste eindstreep om naartoe te werken.

Ik kijk naar mijn team en ben dankbaar dat ik ze om me heen heb. Jennifer die als een pro het programma voor de implementatie van de AVG in goede banen leidt. Jeroen die altijd maar door blijft gaan om de kwaliteit van onze inhoud te bewaken. Dennis met zijn onmisbare technische blik op privacy. En JP die weet wat er in commerciële hoofden leeft en telkens maar weer de meest politiek gevoelige dossiers tot een goed einde weet te brengen. Ze zijn geweldig, maar ze zijn ook moe. We hebben veel te veel werk want de "normale" caseload loopt gewoon door. En eerlijk is eerlijk, dat hield ons altijd al dagelijks royaal van de straat. De laatste tijd hebben we ook steeds vaker een beetje een kort lontje. Vergeef het ons alstublieft. We bedoelen het niet rot. Logisch ook wel, want er staat behoorlijk wat druk op de ketel. Het implementeren van alle eisen uit de AVG is een forse taak, niet in het minst omdat je aantoonbaar moet maken dat je in overeenstemming met de eisen uit de wet persoonsgegevens verwerkt.

Ik spreek deze dagen veel privacy professionals in allerhande organisaties. We proberen elkaar te helpen met kennis en praktische kunde. Maar ik zie daar ook exact eenzelfde beeld. Het moeten rennen om alles te halen met toch te weinig mankracht en te weinig resources. Nu weerhoudt dat geen van ons om ongelooflijk hard en inventief te werken om de eerste deadline van de 25e mei te halen met een opgeheven hoofd en prachtige aantoonbare privacy zaken in plaats. Want naast de vermoeidheid en de korte lontjes hebben we een ander ding gemeen met elkaar. Wij houden van privacy. Wij houden van de privacy van iedereen. Wij zullen dan ook alles doen wat we kunnen om die privacy te waarborgen.

Maar goed. Terug naar dat knuffelen. Mocht u een dezer dagen een privacy professional tegenkomen, wilt u haar/hem dan even knuffelen? Let wel: dat hoeft natuurlijk niet fysiek (en mag alleen als je voorafgaande aan de knuffel toestemming krijgt, net zoiets als met gegevensverwerken dus - #metoo). Maar we vinden het best heel fijn als je even vraagt hoe het met ons gaat, een beetje luistert en misschien zelfs wel een beetje helpt.
Met een dikke knuffel van mr. Rachel Marbus

Mr. Rachel Marbus
@rachelmarbus op Twitter

OPINIE

DATA VEILIG OVER GLASVEZEL

Optisch bedrog en onderbelichte kans

Met de inwerkingtreding van AVG/GDPR (1) in aantocht ligt er nu nog meer focus op het voorkomen van datalekken dan in de aanloop naar de Meldplicht datalekken (2) vorig jaar. In een steeds meer verbonden wereld is het belangrijk dat hierbij ook goed naar de netwerkinfrastructuur wordt gekeken en de manier waarop de wijze van communicatie met de buitenwereld de kwetsbaarheid vergroot of juist vermindert.

Terwijl glasvezel steeds vaker wordt ingezet om aan de bandbreedte behoefte van bedrijven en consumenten te kunnen voldoen, worden de specifieke security-eigenschappen en mogelijkheden van optische netwerken vaak over het hoofd gezien. En daarmee gaan organisaties voorbij aan zowel een mogelijk gat in de beveiligingsstrategie, waarbij gevoelige data kan lekken, als aan een even reële mogelijkheid om het risico op en de impact van datalekken te verkleinen.

Glasvezel als onzichtbare point of failure

Glasvezel heeft de reputatie veilig te zijn, een aanname waar helaas het nodige op af te dingen is. Via internet zijn eenvoudig en tegen een schappelijke prijs hulpmiddelen en instructies te verkrijgen voor het hacken van een glasvezelkabel. En met een beetje kennis is toegang krijgen tot deze kabels eenvoudiger dan wellicht gedacht. Denk bijvoorbeeld aan de putdeksels op straat in de buurt van uw lokale winkelcentrum. Gekleed als straatwerker kan een cybercrimineel eenvoudig een apparaatje op de glasvezel aanbrengen zonder dat iemand vragen gaat stellen. Het aftappen van de data die er overheen lopen, is met zo'n apparaatje een kwestie van minuten. Het resultaat is een perfecte kopie van de data. Omdat de kwaliteit van het signaal nauwelijks wordt aangetast, merken monitoringoplossingen vaak niet op dat er iets aan de hand is. Op deze manier kan het aftappen van het dataverkeer lange tijd ongemerkt plaatsvinden. Was dit twee jaar geleden al genoeg reden tot zorg, met de potentiële repercussies vanuit de AVG/GDPR in het vooruitzicht is het ondervangen van deze kwetsbaarheid een absolute noodzaak geworden.

Is latency de prijs die wordt betaald voor security?

Data op netwerken kunnen steeds minder effectief worden beveiligd met firewalls en antivirus/malwareoplossingen. Daarom worden steeds meer applicatie specifieke encryptieoplossingen aangeboden. Dit type oplossingen kent wel een aantal mogelijke bijwerkingen. Zo vergen ze vaak intensief beheer en beperken ze de bandbreedte die beschikbaar is voor de applicaties. Bovendien veroorzaakt het per apparaat versleutelen en ontcijferen van data latency, wat vooral voor financiële dienstverleners en content gerichte ondernemingen ingrijpende gevolgen kan hebben voor het bedrijfsresultaat. Zo rapporteerde Amazon (3) één procent omzetgroei per elke 100 milliseconde verbetering van de snelheid van de website.

Security by design

Tegenwoordig beweegt de infrastructuurmarkt zich naar security by design. Als je vanuit dit concept kijkt naar glasvezelnetwerken, is het logisch om data op het laagst mogelijke niveau, de optische transportlaag, te versleutelen. Zo implementeerde Telindus eind 2016 in-flight wire-speed encryptietechnologie bij een onderneming in de financiële dienstverlening, waarmee zowel de gewenste uitbreiding van de bandbreedte als de benodigde beveiligingverbetering werden gerealiseerd. Deze in-flight encryptie camoufleert het dataverkeer, zodat gegevens niet kunnen worden uitgelezen of gewijzigd (AVG/GDPR-auditer blij!). De encryptie is 'always on' en komt met een gebruiksvriendelijke dedicated encryptie-gebruikersportal (IT-manager blij!). Als de technologie voor in-flight encryptie in de hardware is ingebouwd, bedraagt de latency nanoseconden of microseconden in plaats van enkele milliseconden bij encryptie op hogere lagen. Bovendien beïnvloedt encryptie op de optische laag de bandbreedte niet en blijft 100 procent verwerkingscapaciteit beschikbaar (gebruiker blij!).

De beveiliging van glasvezel is, net als bij beveiliging van wat dan ook, zo sterk als de zwakste schakel.

De beveiliging van glasvezel is, net als bij beveiliging van wat dan ook, zo sterk als de zwakste schakel. In-flight encryptie op de transportlaag van het netwerk vermindert het risico van het lekken van data die over het glasvezelnetwerk loopt. Dat is een geruststellende gedachte in een wereld waarin data steeds intensiever worden ingezet en dus vaker onderweg zijn.

Links

(1) Autoriteit Persoonsgegevens – Algemene informatie AVG: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

(2) Autoriteit Persoonsgegevens – Meldplicht datalekken: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

(3) Website Speed: The Power of One Second: https://www.lireo.com/website-speed-the-power-of-one-second-infographic/

Patrick Scully P. Eng. MBA, heeft al meer dan 20 jaar R&D-ervaring op het vlak van optische netwerken. Als Product Line Manager bij netwerkstrategie- en technologiebedrijf Ciena ontwikkelt en introduceert hij netwerksecurity- en mediaoplossingen voor bedrijven en dienstverleners. Patrick is bereikbaar via pscully@ciena.com

Achter Het Nieuws

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.

DOLLE DWAZE DINGEN

Een jaar na de Mirai aanvallen op KrebsonSecurity en Dyn is er Reaper (1). Bij dit schrijven heeft Reaper nog niets aangevallen, maar het is al een veel groter IoT-botnet dan Mirai ooit was. Een botnet met miljoenen dingen, klaar om elke opdracht uit te voeren die het krijgt. Voeg hier Roca (2) aan toe; de kwetsbaarheid in de RSA sleutels gegenereerd door een software library van Infineon. Deze software zit ingebakken in honderden miljoenen toegangstokens, andersoortige dingen. Uit de publieke sleutels van een RSA-sleutelpaar is relatief eenvoudig de privésleutel terug te rekenen, wat het mogelijk maakt de toegangstokens te klonen op basis van publieke informatie. Je kunt zeggen dat IoT nooit ontworpen was om veilig te zijn, maar security software ingebakken in hardware tokens was ooit het schoolvoorbeeld van goede security. Nu zitten bedrijven die daarvan afhankelijk zijn met een grote hoofdpijn. Je vervangt niet 1–2–3 miljoenen tokens.

Wat kunnen we hieruit concluderen? Zijn dingen niet veilig te krijgen? Wat kunnen we wél aan deze problemen doen? Moeten we dit op een hele andere manier aanpakken? De redactie reflecteert…

Lex Dunn

IoT is het nieuwe goud voor hackers. IoT devices zijn (over het algemeen) low-cost, dus is er niet veel geld beschikbaar tijdens de ontwikkeling om meer te doen dan de gewenste basisfunctionaliteit bouwen. Bovendien staat er vaak vanuit de sales grote druk op het project om het device snel (en liefst in grote aantallen) op de markt te krijgen. We weten allemaal wat er dan als eerste geschrapt wordt! En doordat de functionaliteit vaak hardwarematig is ingebakken, is het later uitvoeren van updates zo goed als onmogelijk. Als er al resources beschikbaar zijn om een update te maken, want vaak werken deze al aan een nieuw device, met nog meer functionaliteit, om de argeloze gebruiker ertoe te verleiden een nieuwe versie te kopen. Hopelijk wordt er dan wel (door druk vanuit de markt) voldoende aandacht aan de beveiligingsaspecten gegeven.
Maar hoe kunnen we dit nu structureel oplossen? Het begint natuurlijk met 'security by design'; neem al beveiligingsmaatregelen mee in het basisontwerp. Gebruik vervolgens een goede programmeertaal en maak gebruik van standaard bibliotheken met functies die al in de praktijk getest zijn. Geen absolute garantie natuurlijk (denk aan OpenSSL), maar wel beter dan zo maar in het wilde weg zelf wat aanrommelen. En een hele botte maatregel kan zijn om kleine series te maken (denk aan de hardware tokens), want dan is de impact van een gevonden kwetsbaarheid gewoon kleiner (vooropgesteld natuurlijk dat je niet dezelfde programmatuur gebruikt, en die slechts aanvult met nieuwe functionaliteit).
Gaan we het echt ooit helemaal veilig krijgen? Er zullen altijd 'handige Henkies' zijn, die een device op een andere manier gebruiken, waardoor het mogelijk wordt om het te misbruiken. Dus wat moeten we doen? Meer in 'abuse' cases denken, scenario's bedenken hoe het mis kan gaan, en dan alvast passende tegenmaatregelen inbakken als het zover komt. En natuurlijk die ultieme bescherming inbouwen: "If everything else fails, fail safely (and switch off)".

Bart van Staveren

Het grootste deel van de gebruikers van IoT apparaten heeft geen idee van het bestaan van Reaper of Mirai. Een kleine rondgang bij familie en vrienden maakt duidelijk dat frequent gebruik gemaakt wordt van IoT apparaten en speelgoed. Bijna unaniem zijn ze van mening dat die dingen veilig zijn en dat de fabrikant daarvoor gezorgd heeft. Updates van firmware (hoewel ze niet weten wat dat is) hebben ze nooit ontvangen en zeker niet uitgevoerd. "Geen idee hoe dat moet", is in het algemeen


Maarten Hartsuijker


Lex Dunn


Bart van Staveren


Lex Borger

het antwoord.
Voor mij is de conclusie dat er nog heel wat gedaan moet worden aan de security awareness van de consumenten. Vanuit de consumenten zal de druk moeten ontstaan op leveranciers van IoT apparaten om deze ook veilig te ontwerpen, op een zodanige manier dat dit ook op termijn gegarandeerd kan worden. Wetgeving op dit gebied zie ik als noodzakelijk en wellicht dat het nieuwe kabinet hier prioriteit aan kan geven. De verdeling van ICT-onderwerpen over de verschillende portefeuilles maakt echter dat ik daar niet heel optimistisch over ben.

Maarten Hartsuijker
Als we kijken naar het Mirai botnet dat vorig jaar werd ingezet, zien we dat je geen IT studie hoeft te hebben gevolgd om te voorkomen dat producten onderdeel van het botnet uit gaan maken. Het botnet kon ontstaan door het gebruik van standaard inlognamen en wachtwoorden. Zo'n kwetsbaarheid valt prima te voorkomen, maar bestaat nog steeds, omdat producenten in groten getale nalaten om hun producten van willekeurige en onvoorspelbare wachtwoorden te voorzien.
Bij een cryptografisch product ligt dit anders. Het is verschrikkelijk moeilijk om toekomstvaste technieken te ontwikkelen die niet gekraakt kunnen worden. Daarnaast schrijdt de techniek voort en liggen implementatiefouten op de loer (bijvoorbeeld als er onvoldoende willekeurigheid zit in de priemgetallen die bij een RSA certificaat horen). Ook is de kennis die nodig is om betere cryptografie te ontwikkelen en bestaande te toetsen niet ruim voor handen.

Daarnaast zie je dat leveranciers (zeker als de hardwarecapaciteit beperkt is, zoals op een smartcard of in een ander klein IOT device) regelmatig veiligheid ten koste van functionaliteit laten gaan. Zware cryptografische functies zijn dan een te grote overhead en gaan ten koste van de gebruikersbeleving of de mogelijkheden van het product. Met als resultaat dat producten met zwakkere protocollen of algoritmen worden uitgerust.
We ontkomen er niet aan dat in de techniek die wij gebruiken voortdurend nieuwe kwetsbaarheden worden gevonden. Maar we kunnen de kans op misbruik met elkaar wel verkleinen door continu de laatste stand van de techniek toe te passen. En dat wordt nog erg vaak nagelaten. Dus: weg met de standaard wachtwoorden, generieke certificaten, 3DES verbindingen, SSLv2 en 512bits RSA keys! En: hallo goede RNG's, 4096bits RSA sleutels, Elyptic Curve cryptografie, TLS1.2 en willekeurige, unieke wachtwoorden!

Lex Borger
Het is geen kwestie van veilig krijgen, maar veilig houden. Je hebt sowieso last van encryptierot - het effect dat aanvallen op een encryptiealgoritme met een bepaalde sleutellengte alleen maar sneller en beter worden. Soms zelfs met sprongen beter. Een ding statisch inrichten werkt niet, al wordt het nog zo veilig gebouwd. Dus heb je twee mogelijkheden: of je ontwerpt de dingen met de mogelijkheid automatisch firmware te updaten, of je isoleert ze, waardoor de beveiliging buiten het ding komt te liggen, met duidelijke aanwijzing in de (bijgewerkte, online) documentatie dat je dat moet doen. Beide patronen hebben hun voor- en nadelen en alleen daardoor zullen er toch wel weer geslaagde aanvallen zijn. Dit is niet praktisch. Moeten we het wiel dan helemaal opnieuw uitvinden? Wellicht wel. Op dit moment werkt het economisch model niet. De bezitters van goedkope, slecht beveiligde dingen hebben daar zelf nauwelijks last of besef van, maar die apparaten kunnen wel ingezet worden in aanvallen. Je kunt uitgaan van het principe dat de vervuiler betaalt, maar ook dat geeft moeilijkheden. Dan moet de kwaliteit van beveiliging vooraf vast te stellen zijn, liefst voor de verkoop. Zo kom je toch in een cirkelredenering en ik kom dus tot de conclusie dat het voorlopig een wedloop blijft, waarbij de aanvaller het voordeel heeft. Jammer. Ik ben niet graag de pessimist, maar dit lijkt wel een onmogelijke positie van waaruit een verbetering moet komen.

Links

(1) KrebsonSecurity blog, Reaper: Calm Before the IoT Security Storm? - https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/

(2) NCSC UK, ROCA: Infineon TPM and Secure Element RSA Vulnerability Guidance - https://www.ncsc.gov.uk/guidance/roca-infineon-tpm-and-secure-element-rsa-vulnerability-guidance

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
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
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 2017
De abonnementsprijs in 2017 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

VISSEN

Ik sta niet bekend als iemand die altijd even gelukkig is met de wijze waarop bedrijven omgaan met de gegevens die ze links en rechts verzamelen. Ook is het voor mij weleens lastig om te onderkennen of ik nu een suikeroom in Amerika verloren heb of dat ik te maken heb met een phishing mail. Ik zal beide voorbeelden toelichten.

Gegevensbeheer
Mijn werkgever verwerkt veel gegevens van klanten en besparing op IT is een belangrijk onderdeel van het beleid van het bedrijf om de kosten behapbaar te houden. Zoals bij zoveel bedrijven draaien de werkplekken op Windows en daar wil weleens een update noodzakelijk zijn om de systemen waterdicht te houden.

Het probleem van deze update voor de IT-afdeling is, dat alle bedrijfsapplicaties getest moeten worden voordat de updates doorgezet kunnen worden. Als ik u aangeef, dat er meer dan tweehonderd applicaties zijn en dat die allemaal even belangrijk zijn, dan kunt u zich voorstellen dat het testen van de beveiligingsupdates een enorme klus is. Die moet met zeer grote regelmaat uitgevoerd worden, want het aantal beveiligingsupdates is aanzienlijk.

Ik hoef u niet te vertellen welke gevolgen het heeft als een besturingssysteem niet meer ondersteund wordt en in zijn geheel vervangen moet worden. Het is voorstelbaar dat, gezien deze problematiek, bedrijven het upgraden even laten voor wat het is en op de oude software doorgaan. Maar dat doen ze dan toch niet echt? Want als ze dat zouden doen, is het mogelijk dat persoonsgegevens lekken en in handen komen van duistere figuren, die dan met die gegevens bijvoorbeeld gaan phishen.

Suikeroom
Kort geleden werd ik verblijd met een mailtje van een notaris uit Amerika die een aangename mededeling had voor mij. Ik was erfgenaam van iemand die ik persoonlijk niet ken, dus de verassing was groot. Opgewonden vertelde ik mijn vrouw dat we erfgenaam waren. Zij keek mij aan en ging verder met waar ze mee bezig was. Verwonderd herhaalde ik wat ik zei. Haar reactie was nu: "Denk toch even na!"

Ja het was inderdaad wel vreemd. De vraag van de notaris om mijn creditcardgegevens even toe te zenden, zodat hij kon storten, maakte mij nu iets onrustig. Ik ging naar de website van de notaris. Dat zag er professioneel uit. Ik dacht na en besloot om de notaris maar even te bellen voordat ik mijn gegevens op de mail zou zetten. Ik probeerde een aantal keren het nummer dat in de mail stond, maar het lukte mij niet om de man (of vrouw) aan de lijn te krijgen. Mijn vrouw was kort en duidelijk: "Vergeet het maar en gooi die mail nu maar weg." Ik twijfelde nog. Ze had natuurlijk wel een punt, dat het vreemd was dat ik de man niet aan de telefoon kreeg, maar toch, stel dat het wél waar was.

U merkt dat ik best wel goed oplet bij het lezen van mijn mail, maar dat de mail soms zo bedrieglijk echt lijkt, dat het moeilijk is er niet op in te gaan. Ik heb er echt wel begrip voor dat sommige mensen een phishing mail niet als zodanig zien.

Mocht u informatie hebben dat notaris Johnson toch echt bestaat? Laat u het mij dan nog even weten? De mail is waarschijnlijk nog uit mijn prullenbak te halen.

Berry

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers