iB

INFORMATIEBEVEILIGING

jaargang 18 - 2018

#6

Metadata: een onbekend risico

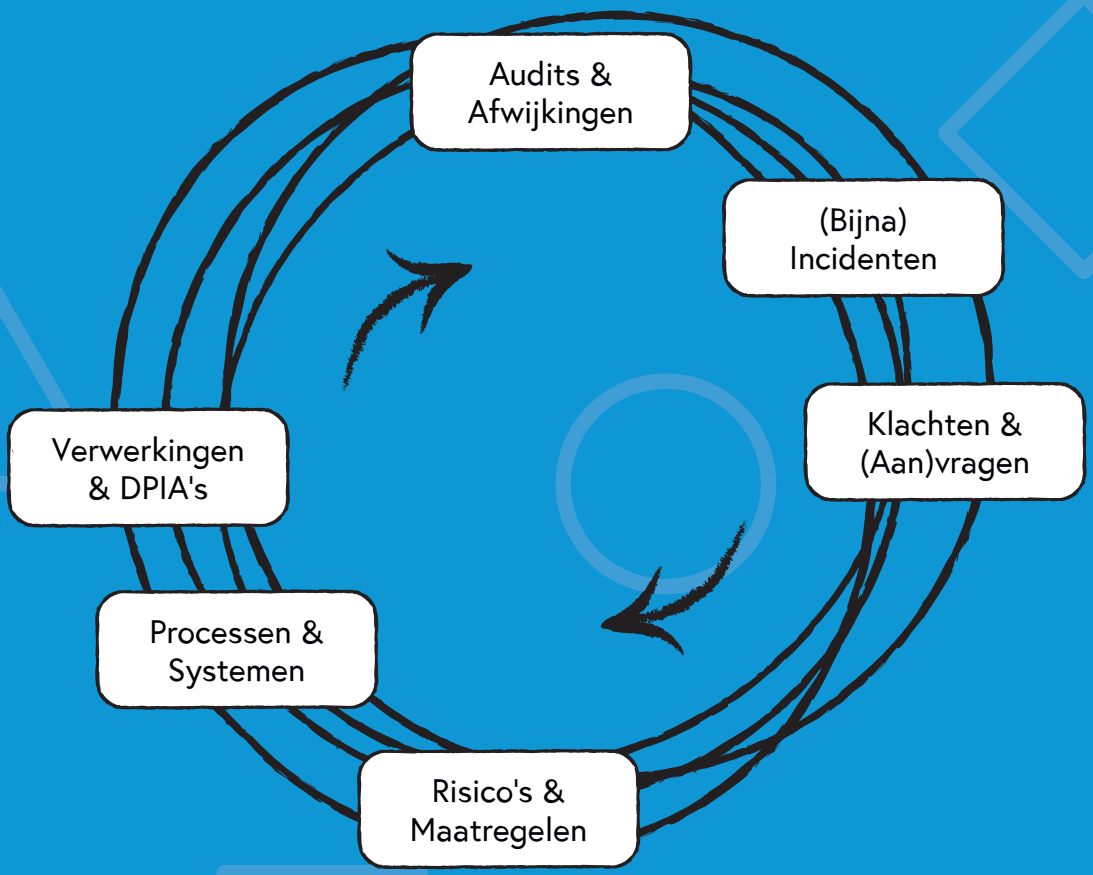
Smart Risk Management

Iemand heeft iets fout gedaan

PvIB: meer slagkracht en zichtbaarheid in 2019

De meest complete Privacy / AVG / GDPR Software

smile



- Makkelijk en veilig in gebruik
- Voor en door gebruikers ontwikkeld
- Juridisch beproefd
- Completer dan andere systemen
- SaaS en OnPremise geleverd

Start nu gratis! Kijk snel op: privacysuite.eu

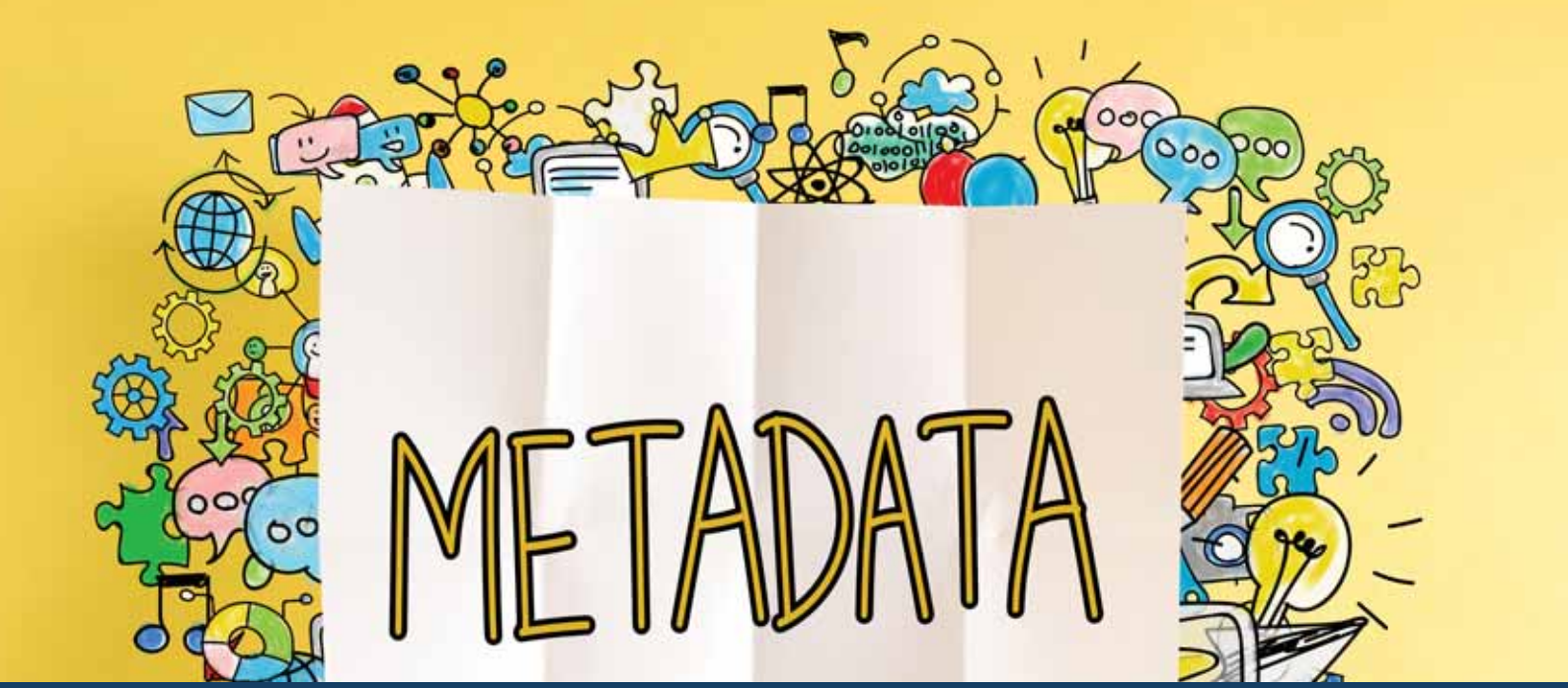
AFSCHEID

Lex Dunn: Aan alle goede dingen komt een einde en voor mij is nu het moment gekomen om afscheid van u als lezer te nemen. Zoals u wellicht weet, heb ik een bijzondere band met Zuid-Frankrijk. In de eerste helft van het nieuwe jaar gaan mijn vrouw en ik ons daar dan ook definitief vestigen. Daarom zijn dit mijn laatste woorden als redacteur van iB, maar u bent nog niet van mij af! In het eerste nummer van het nieuwe jaar blik ik terug op mijn rol als redacteur. Vanaf deze plek wens ik de redactie, en in het bijzonder de nieuwe leden, veel succes en wijsheid toe.

Nicole van Deursen: Het afgelopen jaar heeft de redactie afscheid genomen van een aantal zeer gewaardeerde redacteuren. Van de namen die in december 2017 op de redactielijst stonden, zijn er na dit nummer nog maar 3 over. De nieuwe redactie kent maar liefst 7 nieuwe gezichten en in dit nummer stelt een aantal zich weer aan u voor. Deze redactieleden hebben, zoals ze in het Engels zeggen, 'some big shoes to fill'. Maar met een team vol energie en inspiratie ziet de toekomst van dit blad er fris uit.
In de weken voor het drukken van dit magazine begint ook de marketingmachine voor de feestdagen op stoom te komen. Winkeliers kunnen in deze periode een kwart van hun jaaromzet halen. Geldt dat ook voor cybercriminelen? Halen zij deze periode ook een kwart van hun omzet binnen? Nicole ging op zoek naar aanknopingspunten voor het antwoord. In dit nummer hebben we naast de vaste columns een artikel over mens als sterkste schakel; een boekbespreking over Agile Secure Software Lifecycle Management; Lex en Tom waren bij de uitreiking van de Joop Bautz Information Security Award; er is een artikel over de Wbni; en een artikel over de hoeveelheid informatie die je ongewenst uit de metadata van documenten kunt halen. Kortom, een super diverse uitgave dus die het oude jaar waardig afsluit en het nieuwe laat beginnen. We kijken uit naar 2019 en wat het zal brengen.

Lex Dunn en Nicole van Deursen

In dit nummer



METADATA: EEN ONBEKEND RISICO

Lekt uw organisatie onbedoeld persoonsdata?

Als u op `opslaan als' klikt, is het niet alleen het bestand zelf dat wordt opgeslagen. Naast de inhoud van het bestand zelf wordt namelijk in bijna alle gevallen ook zogenaamde metadata opgeslagen. Metadata zijn niets meer dan `data over data' en bevatten bijvoorbeeld het precieze tijdstip waarop een document gecreëerd, gewijzigd of opgeslagen is.

In 2017 heeft Auke Zwaan een grootschalig onderzoek gedaan om te kijken of Nederlandse overheidswebsites dit soort metadata uit hun bestanden halen, voordat ze deze op hun websites publiceren. Wat bleek? Bij geen van de meer dan 1500 onderzochte websites was sprake van het stelselmatig wissen van metadata. Sterker nog: in 85 procent van de onderzochte documenten werden één of meerdere gebruikersnamen van de auteurs aangetroffen. Door deze informatie in een dashboard samen te voegen, werd gedemonstreerd hoeveel informatie een hacker hiermee tot zijn beschikking kan krijgen.

Sociale netwerken

Metadata bestaat uit `tags' die een waarde hebben. Voorbeelden van dit soort tags zijn `create date', `page count', `title' enzovoort. In documenten van Microsoft Office (.docx, .xlsx, .pptx, etc.) wordt daarnaast standaard de gebruikersnaam van de auteur opgeslagen. Dit gebeurt in de `creator'-tag. Opent een collega hetzelfde bestand hierna en slaat hij het op, dan verschijnt ook de gebruikersnaam van deze gebruiker in de metadata, in de `last modified by'-tag. Zo kun je van een bepaald document zien dat er twee mensen aan samengewerkt hebben.

In het onderzoek is op basis van deze informatie per overheidswebsite een 'samenwerkingsnetwerk' gemaakt. Hierin is te zien wie met wie heeft samengewerkt, wanneer en hoe vaak. Zo ontstaat een compleet beeld van de sociale contacten binnen en buiten een organisatie. Voor een hacker kan dit waardevolle informatie zijn voor het opstellen van een spearphishing-mail. Stelt u zich bijvoorbeeld de volgende situatie voor:

- Een hacker weet dat Mark en Sandra samengewerkt hebben aan een document met de titel 'Jaarrapportage 2018'.
- De hacker weet ook dat ze beiden samengewerkt hebben met een andere gebruiker met de naam 'John'.

Hij zou dan de volgende phishingmail op kunnen stellen (met malware in de bijlage):

"Hoi Mark,

Ik heb wat wijzigingen aangebracht aan de jaarrapportage (zie bijlage); John was het niet helemaal eens met de versie die nu op de website staat, was te verwachten.....
Kun jij je licht hier even over laten schijnen? Zie je bij de borrel!

Groet, Sandra."

Denk heel even na over bovenstaand voorbeeld. Zou u, als u Mark was, de bijlage openen, wetende dat u inderdaad samengewerkt heeft met Sandra en dat John uw manager is?

Tijdlijnen

Een volgende stap in het onderzoek was het maken van tijdlijnen. Door voor alle documenten van een auteur alle 'create date'-tags op te slaan, kon precies bekeken worden wanneer deze persoon het meest actief was. Hieruit ontstonden patronen die bijvoorbeeld een indicatie gaven van de gemiddelde werktijden (als iemand alleen tussen 8:00 en 16:00 documenten creëert), een vaste vrije dag (als er op vrijdag bijna nooit documenten aangemaakt worden), of een vaste vakantieperiode (als er ieder jaar de eerste 2 weken van augustus geen documenten gecreëerd worden).

Een hacker zou deze informatie kunnen toevoegen aan zijn spearphishing-mail. Bij de al aanwezige informatie over de samenwerkingsnetwerken, kunnen nu ook zinnen worden toegevoegd als:

"(...) toen je op vakantie was hebben John en ik document X gepubliceerd, kun je er toch nog even naar kijken?"

Op zichzelf staand zijn deze stukjes informatie misschien niet van grote waarde, maar alle beetjes informatie bij elkaar kunnen leiden tot een spearphishing-mail die zo goed is dat een slachtoffer niet eens twijfelt of deze nep is.

Kwetsbare software

Naast metadata-tags over auteurs bestaan er ook specifieke tags die informatie bevatten over gebruikte software. Hoewel deze tags vaak niet van grote waarde waren (vaak komt bijvoorbeeld 'Microsoft Office Word 2016' terug, maar zonder specifiek patch-level), waren er situaties waarin verwijzingen stonden naar bijvoorbeeld Windows Server 2003 (out-of-support sinds 14 juli 2015). Het behoeft weinig uitleg dat dit voor een hacker een belangrijke indicator is.

Externe bedrijven

Recentelijk is gebleken hoe snel malware en ransomware zich kunnen verspreiden via verschillende bedrijven (denk bijvoorbeeld aan WannaCry, NotPetya, etc.). Voor een hacker is daarom de 'company'-tag interessant. Soms blijkt hieruit namelijk dat een bepaalde externe partij documenten creëert voor een bepaalde organisatie. Door bij een phishingmail misbruik te maken van deze bestaande vertrouwensrelatie tussen de twee organisaties, wordt de kans dat een slachtoffer klikt alleen maar groter.

De huidige situatie

Na het onderzoek van 2017 is in 2018 door Dutch Crown IT een soortgelijk onderzoek uitgevoerd. Dit keer met als scope meer dan 250 grote tot zeer grote (internationale) organisaties. De uitkomst? Bijna precies hetzelfde. In een

Auke Zwaan (links) is ethisch hacker in de financiële sector. Hij is bereikbaar via auke.zwaan@os3.nl.
Wiebe Zwaan is werkzaam als Privacy Officer bij een groot handelshuis. Hij is bereikbaar via wiebe@dutchcrownit.nl.

enkel geval bleek dat een organisatie daadwerkelijk stappen had ondernomen om metadata te verwijderen van haar publieke documenten, maar in alle andere gevallen was hiervan geen sprake. Op het eerste gezicht lijkt er dus weinig veranderd. Wat sinds het onderzoek in 2017 echter wel veranderd is, is de komst van een nieuw hot topic: de Algemene Verordening Gegevensbescherming (`AVG', of `GDPR'). Deze brengt namelijk nieuwe uitdagingen voor organisaties met zich mee.

Grondslag

Persoonsgegevens (zoals bijvoorbeeld de `author'-tag) mogen alleen worden verwerkt als daar een grondslag voor is. Bij het verwerken van metadata zal dit vaak het `gerechtvaardigd belang' zijn. Er is sprake van zo'n belang als de afweging tussen de ernst van gevolgen voor de persoonlijke levenssfeer van de betrokkene en het belang van de organisatie doorslaat in het voordeel van de organisatie. Een voorbeeld:

"Een advocatenkantoor houdt door metadata-opslag (`author'-tag) bij welke advocaat op welk moment aan een dossier heeft gewerkt. Mocht er wat fout gaan, dan weet het kantoor wie hiervoor verantwoordelijk is."

Hier is een grondslag om metadata op te slaan. Immers, het kantoor heeft er belang bij te kunnen controleren wie wanneer aan welk document heeft gewerkt. De inbreuk op de persoonlijke levenssfeer van de medewerker is daarbij minimaal. Het belang is daardoor `gerechtvaardigd'.
Vaak is dit echter niet het geval:

"Een onderzoeksinstelling publiceert onderzoeken over maatschappelijk gevoelige onderwerpen. Zij publiceert daarom altijd uit naam van de organisatie, en niet op persoonlijke titel van haar medewerkers. Deze willen namelijk niet kunnen worden aangesproken op de inhoud van het artikel. In de online gepubliceerde onderzoeken staat de auteur vermeld in de metadata."

In dit voorbeeld is er geen gerechtvaardigd belang. De organisatie schiet er namelijk niets mee op om de naam van de auteur in de metadata te publiceren, terwijl de (privacy)gevolgen voor de auteur groot kunnen zijn.

Andere aspecten

Met alleen een grondslag bent u er nog niet. De AVG kent namelijk een aantal beginselen waar organisaties zich aan moeten houden. Bij het verwerken van metadata zijn de belangrijkste doelbinding, dataminimalisatie en dataretentie.

Doelbinding betekent dat als persoonsgegevens voor doel A worden verwerkt (bijvoorbeeld het bijhouden van aanpassingen van een document in het advocaten-voorbeeld) zij niet zonder hier vooraf over te informeren voor doel B (bijvoorbeeld online publicatie) mogen worden gebruikt. Dataminimalisatie stelt dat niet meer metadata mag worden verwerkt dan noodzakelijk is voor het doel waarvoor dit gebeurt. Wil men dus alleen zien wie welke wijzigingen op een document aanbrengt, dan is het niet nodig vast te leggen op welk moment dit is gebeurd. Als laatste dataretentie: metadata mogen niet langer worden opgeslagen dan nodig is voor het doel waarvoor het wordt verwerkt. Als het doel dus niet langer bestaat, moeten de metadata worden verwijderd. Denk bijvoorbeeld aan het archiveren van dossiers, waarbij het niet langer van belang is precies te weten wie op welk moment aan het dossier heeft gewerkt.

Rechten van betrokkenen

Los van de vraag of een organisatie überhaupt metadata mag verwerken, geeft de AVG betrokkenen ook bepaalde rechten. Een daarvan is het recht op inzage; een betrokkene kan vragen om een overzicht van de persoonsgegevens die van hem worden verwerkt (let op: ook het opslaan/opgeslagen houden van gegevens is een verwerking). Dit betekent dat de organisatie ook in beginsel de metabestanden in een interne zoektocht moet achterhalen en hierover moet rapporteren. Daarbij kan de betrokkene verzoeken zijn persoonsgegevens te laten verwijderen. Gehoor geven aan deze verzoeken is onhaalbaar wanneer geen helder beeld bestaat welke metadata intern aanwezig is.

Conclusie

Na het onderzoeken van meer dan 250 organisaties, sommige zeer groot, internationaal en in gevallen zelfs behorend tot de vitale infrastructuur, blijkt metadata aanwezig te zijn in bijna elk document. Buiten de informatie die u hiermee aan een hacker blootstelt, kan dit ook privacyrechtelijke consequenties hebben. Hoe zit dit binnen uw organisatie? Is het bij u wel goed geregeld? Heeft u al stappen ondernomen, of gaat u op basis van dit artikel stappen ondernemen? Wij zijn benieuwd!

Links

Het onderzoek van Auke is te vinden op http://rp.delaat.net/2016-2017/p96/report.pdf.
Exiftool (software voor het bekijken/bewerken van metadata): https://www.sno.phy.queensu.ca/~phil/exiftool/

Foto: van links naar rechts: Pieter van Dijken (jury voorzitter), Rob van Diermen, Armando Panman de Wit (tweeling broer van Sebastian) en Thijs van Ede.

UITREIKING JOOP BAUTZ INFORMATION SECURITY AWARD

Op woensdag 10 oktober werd het jaarlijkse Security Congres georganiseerd door NOREA, ISACA NL Chapter en natuurlijk ons aller PvIB. Debbie Reinders had het weer prima voor elkaar in de Johan Cruijff Arena in Amsterdam met wederom meer deelnemers dan de voorgaande jaren. Traditioneel wordt tijdens het Security Congres ook de jaarlijkse Joop Bautz Information Security Award (JBISA) uitgereikt voor de beste afstudeerscriptie op het gebied van informatiebeveiliging. Uit vele inzendingen heeft de jury een drietal kandidaten genomineerd:

1. **Rob van Diermen, met als onderwerp: 'The Internet of Things: a privacy label for IoT products in a consumer market';**
2. **Thijs van Ede, met als onderwerp:'Detecting Adaptive Data Exfiltration in HTTP Traffic';**
3. **Sebastian Panman de Wit, met als onderwerp: 'Dynamic detection of mobile malware using real-life data and machine learning'.**

Voorafgaand aan de bekendmaking van de winnaar kreeg elk van de genomineerden de gelegenheid om zijn onderwerp nader toe te lichten. Omdat Sebastian in Zuid-Amerika verbleef, deed zijn tweelingbroer Armando – op uitstekende wijze - de presentatie.

Na deze presentatie werd voor elke inzending een korte samenvatting van het juryrapport gegeven door juryvoorzitter Pieter van Dijken. Daarna kwam het moment waarop de drie genomineerden met spanning hadden gewacht: de bekendmaking van de winnaar. Met behulp van Jos Wetzels (JBISA winnaar in 2017) kregen de genomineerden een exemplaar van hun juryrapport en kreeg winnaar Sebastian Panman de Wit een cheque. Na afloop poseerden alle genomineerden met Pieter op het veld van de Johan Cruijff Arena.

De drie genomineerde verslagen kunt u vinden op de website van JBISA: https://www.jbisa.nl

Auteurs: Tom Bakker en Lex Dunn

SMART RISK MANAGEMENT

Omkaderd door de richtlijnen van ISO 31000 wordt in dit artikel het concept van 'SMART risk management' geïntroduceerd. Fundamenteel aan SMART risk management is het isochroon meten van de effecitiviteit van risicobeheersingsmaatregelen en de analyse van en rapportage over de corresponderende gegevensstromen.

Ik besloot onlangs om de ISO 31000:2018 richtlijnen voor risicomanagement door te nemen. Ik had mezelf geestelijk voorbereid op het lezen van een lang, saai en taai document. Niets bleek minder waar. Het document bleek relatief kort, goed gestructureerd en helder geschreven te zijn. Daarnaast is de focus van het document niet, zoals men misschien zou verwachten, primair gericht op het riskmanagement proces, maar is er ruim plaats gereserveerd voor:

- value creation and value protection;
- leadership and commitment.

Toch ben ik waarschijnlijk het meest te spreken over de definitie van het begrip 'risico' in deze versie van ISO 31000. De definitie van het begrip risico in dit document luidt: 'Risico is het effect van onzekerheid op doelstellingen'. De ISO 31001 koppelt via deze definitie dus risico aan doelstellingen. We merken ook op dat volgens de ISO 31000 richtlijnen het effect niet alleen negatief, maar ook positief mag zijn.

Met deze definitie kunnen we als vakgenoten wel wat, denk ik. En wat we ermee kunnen, wordt duidelijker als we de brug herkennen naar het SMART-principe voor het formuleren van doelstellingen. SMART-doelstellingen zijn volgens Wikipedia: 'Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden'.

De centrale stelling van dit artikel volgt uit de vraag: als doelstellingen SMART zijn, waarom zou het effect van onzekerheid op deze doelstellingen dat dan niet zijn? Of specifieker: als doelstellingen met een aanvaardbare nauwkeurigheid meetbaar zijn, waarom zou dat niet gelden voor het effect van onzekerheid op deze doelstellingen? Deze vraag leidt tot de volgende definitie van het begrip

Figuur 1 - Effectiviteit door risicobeheersingsmaatregelen

'SMART risk': 'SMART risk is het effect van onzekerheid op doelstellingen die SMART gedefinieerd zijn.'

In lijn met SMART risk definiëren we 'SMART risk management' als: 'Een samenstel van gecoördineerde SMART-activiteiten en SMART-maatregelen met als integraal doel het effect van onzekerheid op een samenstel van SMART-doelstellingen tot een aanvaardbaar niveau te beperken'. Het integrale doel van risk management is telkens het waarborgen dat de doelstellingen van een organisatie binnen daarvoor geldende toleranties worden gerealiseerd.

SMART control

Uitgaande van de eerder besproken definitie van het begrip risico definieert ISO 31000 tevens begrippen zoals 'risk source', 'risk controls' en 'events'. We staan stil bij het begrip control dat ISO 31000 vrij vertaalt definieert als: 'Een maatregel die invloed heeft op de kenmerken van risico's'. Gebruikelijke controls reduceren risico langs risicobeheersingsdimensies zoals kosten, doorlooptijd, RPO, RTO en SLA compliance. In dit artikel stellen we dat de handhaving van een risicobeheersingsmaatregel, een control, tevens inherent een doelstelling zal vormen. Wordt deze doelstelling SMART gedefinieerd, dan is het concept van een SMART control herkend.

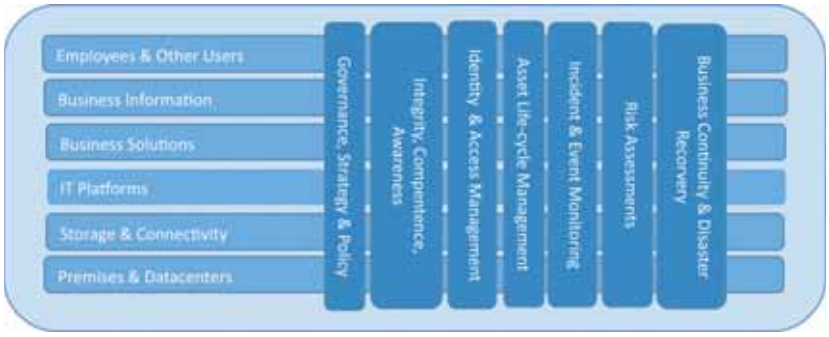
Meetbaar en tijdsgebonden

De beginselen van meetbaarheid en tijdsgebondenheid zijn verankerd in de definities van SMART- doelstellingen en SMART controls. Basisbeginsel van SMART risk management is het isochroon meten van de effectiviteit van controls die SMART gedefinieerd zijn. Met andere woorden: de effectiviteit van risicobeheersingsmaatregelen dient bijvoorbeeld maandelijks, wekelijk of dagelijks gemeten te worden. Figuur 1 toont als voorbeeld voor een fictieve organisatie, isochroon de effectiviteit van risicobeheersings-maatregelen op het gebied van bijvoorbeeld IT Platform Asset security en IAM. Het mag uit dit figuur evident zijn dat de effectieve analyse van trend, correlatie en uitzicht afhankelijk is van de isochroon gemeten effectiviteit van de betreffende risicobeheersingsmaatregelen.

Realistisch

Figuur 2 toont een voorbeeld van een instrument dat in het artikel Enterprise Control by Design gepubliceerd in iB-magazine nummer 1, 2018 een weergave van een risicobeheersingslandschap is genoemd. Bij de effectieve risicobeheersing over een landschap op deze wijze weergegeven zal telkens de wie, wat, waar, wanneer, waarmee van risicobeheersingsdoelstellingen voor ieder relevant kruispunt gespecificeerd zijn. Deze – en soortgelijke visualisaties van het risicobeheersingslandschap - zijn, in mijn

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



Figuur 2 - SMART IT Risk Management Landschap

ervaring, geschikt gebleken om met een holistische blik risicomanagement met betrokkenen te bespreken.

Effectiviteit

Het isochroon meten van de effectiviteit van risicobeheersingsmaatregelen op de verschillende kruispunten en voor diverse risicobeheersingsdimensies creëert een gestructureerde stroom van gegevens die risicomanagement processen kan sturen. Deze gegevensstroom is de basis van data-driven risk managent en biedt aanknopingspunten voor de inzet van 'machine learning' en kunstmatige intelligentie voor de risicobeheersing. Als voorbeeld van het isochroon meten van de effectiviteit van een risicobeheersingsmaatregel beschouwen we een typische IAM-maatregel voor Joiners, Workers en Leavers. Doorgaans is het bijvoorbeeld van belang dat de toegangsrechten van medewerkers tijdig verwijderd worden als medewerkers de organisatie verlaten of van functie veranderen. Het isochroon meten van de effectiviteit van deze maatregel zal doorgaans assurantie bieden aan externe auditors in het kader van de jaarrekeningcontrole. Door de effectiviteit van risicobeheersingsmaatregelen, langs risicobeheersings-dimensies zoals kosten en compliance, ook cumulatief op de kruispunten in het landschap te projecteren is overzicht, inzicht en uitzicht in de effectiviteit risicobeheersing voorhanden.

Agile Manifesto

Een analyse van de 12 beginselen die ten grondslag liggen aan the Agile Manifesto biedt verschillende aanknopingspunten met SMART risk management. In Agile/Scrum worden bijvoorbeeld in een vaste cadans, dus isochroon, user-stories afgeleverd via Sprints. Het al dan niet geautomatiseerd meten van de effectiviteit van risicobeheersingsmaatregelen voor het einde van een Sprint is een ideaal aanknopingspunt met SMART risk management. Denk hierbij aan statische code analyse en fuzz testing. Belangrijk is wel dat de op deze wijze gevonden issues geen impact mogen hebben op de cadans van de sprints.

Impact en waarschijnlijkheid

Risico wordt klassiek gedefinieerd als het product van impact en waarschijnlijkheid. In de laatste jaren is, in de context van risicoassessments, de evaluatie van de velociteit van risico tevens steeds meer gebruikelijk. De onderstaande tabel biedt SMART definities van deze begrippen in lijn met de bovenstaande definitie van SMART risk.

Term	Omschrijving
SMART impact	Een maat voor het effect als een specifieke doelstelling niet binnen afgesproken toleranties valt.
SMART probability	De kans dat het effect m.b.t een specifieke doelstelling niet binnen afgesproken toleranties valt
SMART velocity	Een maat voor de tijd tussen risk events en hun corresponderende impact op betreffende doelstellingen

Tabel 1 hierboven koppelt, in lijn met ISO 31000, deze begrippen aan specifieke doelstellingen. Door de koppeling van deze begrippen aan specifieke, tijdsgebonden en meetbare doelstellingen, komt het kwantitatief beheer van operationeel risico steeds meer binnen handbereik. Deze observatie wordt aannemelijker als we het effect van onzekerheid op doelstellingen, dus risico volgens ISO 31000, zien als random of stochastische variabele. In de praktijk is de statistische analyse van deze variabelen en hun afhankelijkheden haalbaar. Het mag ook duidelijk zijn dit artikel slechts summier deze en andere thema's aanstipt. Gegeven tijd en gelegenheid zal de auteur in de toekomst deze onderwerpen verder uitdiepen.

Handbereik

De lezer van dit artikel zal herkennen dat de auteur te spreken is over de ISO 31000 richtlijnen voor risicomanagement. De ISO 31000:2018 definitie van het begrip risico en het alom bekende SMART principe voor het definiëren van doelstellingen zijn in dit artikel samengevoegd bij de introductie van SMART risk management. Door de isochrone meting van de effectiviteit van risicobeheersingsmaatregelen langs verschillende risicobeheersings-dimensies is SMART risk management een data-driven benadering van risicobeheersing die overzicht, inzicht en uitzicht voor een risicobeheersingslandschap binnen handbereik brengt.

Referenties

IB-magazine nummer 1, 2018 'Enterprise Control by Design'
https://nl.wikipedia.org/wiki/SMART-principe
https://www.agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/

OVER LIJKEN GAAN

De klap viel in Portugal. Een ziekenhuis had daar de dubieuze eer om als eerste beboet te worden onder de GDPR. In dat ziekenhuis hadden 1000 personen toegang tot medische gegevens, maar er waren slechts 296 artsen werkzaam. Met de overige informatiebeveiliging was het ook slecht gesteld volgens de Portugese toezichthouder (CNPD). Voor dat gapende gat in de beveiliging viel een boete van 4 ton.

Het is nogal wat met die medische gegevens. Vooral omdat het best vaak misgaat. Zo gaat Dela letterlijk over lijken om geld te verdienen. Radar kwam erachter dat de organisatie zonder toestemming van nabestaanden vingerafdrukken afnam om daar leuke hebbedingetjes van te maken en te verkopen in hun webshop. Ik lees dat en denk: wat dacht je in vredesnaam toen je bezig was met het bedenken van dit onzalige plan? Ook na je dood heb je nog steeds recht op privacy. Je nabestaanden kunnen weliswaar niet meer terecht bij de AVG, maar het grondrecht op privacy is nog steeds van toepassing en zo ook het medisch beroepsgeheim. Maar veel belangrijker nog, ethisch klopt dit natuurlijk van geen kanten. Er wordt handel gedreven met het lichaam na overlijden, duidelijk mensonwaardig gedrag.

En meest recent kreeg het UWV ook een bescheiden tikje van onze eigen privacywaakhond. AP had al vanaf 25 november 2015 erop gewezen dat voor het inloggen op het werkgeversportaal door alle gebruikers gebruik dient te worden gemaakt van meerfactorauthenticatie. Daar worden immers gezondheidsgegevens verwerkt van werknemers en daarmee moet uitermate zorgvuldig worden omgegaan. Toegang met een gebruikersnaam en wachtwoord volstaat dan niet. Het UWV had toegezegd in mei 2018 de boel op orde te hebben. Dat is tot op heden niet het geval. AP heeft het UWV nu een last onder dwangsom opgelegd. Op 31 oktober 2019 moeten ze echt alles in werking hebben. Zo niet, dan moet 1,5 ton per maand betaald worden met een maximum van 9 ton. Let wel, het UWV weet dan dus al 4 jaar (!) wat ze moet doen. Vergeeft u mij als ik zeg dat ik dit toch wel enigszins schandalig vind?

En ze zijn niet de enigen die de fout ingaan met medische gegevens. Lukraak wat voorbeelden: in januari bleek dat Rijkswaterstaat een rapport met vertrouwelijke, medische informatie over een medewerker verspreid had onder de collega's die zij beschuldigde van pestgedrag. In februari werden de medische gegevens van sporters bij een hack buitgemaakt. In maart bleek dat ongelooflijk veel medewerkers van het Hagaziekenhuis het medisch dossier hadden ingezien van soapster Barbie. In april kwam naar buiten dat Jumbo medische gegevens van medewerkers gebruikte voor een subsidieaanvraag. In september bleek dat een Nijmeegse zorginstelling bij de verhuizing naar een nieuw pand vergeten was medische dossiers mee te nemen.

Juist medische gegevens moeten nog beter beschermd worden, omdat wij daarvan met elkaar hebben afgesproken dat die zo privé zijn, dat eigenlijk (bijna) niemand daar wat mee te maken heeft. En toch gebeurt het nog met de regelmaat van de klok dat de privacy van personen wordt geschonden. Gezien de gevoeligheid van de gegevens en de ernst van de gevolgen bij een inbreuk daarop, mag er wat mij betreft veel strenger opgetreden worden, want blijkbaar is het afspreken met elkaar (en in de wet) onvoldoende incentive om zuinig met medische gegevens om te gaan.

Mr. Rachel Marbus
@rachelmarbus op Twitter

IEMAND HEEFT IETS FOUT GEDAAN...

Alleen ik was het niet. Als variant op het aloude `Er is iets fout gegaan, maar niet door mij'. We zien dit de laatste tijd weer steeds vaker: de mens krijgt de schuld. De mens is de zwakke, zwakste schakel. Dus moet de mens gestraft worden met bergen aan regels, waar de vele goeden dan maar onder de kwaden moeten lijden. Het kan blijkbaar niet goedschiks. Slechte mens, u allen. Terwijl:

- Flexibiliteit vereist is om als organisatie te overleven. De boel zó dichttimmeren dat een mens niets meer fout kan doen, zal dus niet werken. Ja, natuurlijk kunnen we dure managers en executives alle declaraties boven een tientje laten afvinken tegen uurtarieven die ver uitgaan boven een tientje – en dan multi miljoenenprojecten in de soep laten lopen. Want in zo'n gevangenisregime wil geen enkele projectmanager (of welke medewerker dan ook) die wat waard is, werken. Dat schiet lekker op hè, met voorkomen van onnodige kosten? Dat schiet lekker op hè, met het bereiken van de doelstellingen van de organisatie – lees: de crisis komt sneller dichterbij dan Max Verstappen (met een goede motor).
- Het slechts enkele uitzonderingen betreft die kwaad in de zin hadden. En die zullen niet worden tegengehouden door een steeds fijnmaziger net. Want zij zullen als eersten opmerken dat het net wel fijnmaziger is geworden, maar er dus kwadratisch meer mazen zijn. En het web is zwak; hooguit zullen de kleine vliegjes worden gevangen, maar de grote vliegen gaan er dwars doorheen.
- Het niet degenen zijn die per ongeluk wat misdeden die aangepakt moeten worden. Zij (de absolute meerderheid) poogden immers uit goede wil om de organisatie- en de aantoonbaar daaruit afgeleide (Huh? Dat zou voor het eerst zijn!) persoonlijke doelstellingen te halen. Damn the torpedoes, full speed ahead! Vooral omdat ik die uitdrukking nog eens in een column wilde stoppen.
- Het aanwijzen van de mens als zwakste schakel is nou niet echt je van het op motivationeel gebied, zeker niet als de ervaring leert dat zoiets de opmaat is voor nóg meer drempels en barricades tegen het behalen van die organisatie- en persoonlijke doelen. En hoeveel 'managers' overschatten niet hun eigen vaardigheden en motieven én onderschatten die van hun medewerkers? Dat is vaste prik bij alle onderzoeken ernaar, zonder dat dit ooit werd opgelost. Misschien wel onoplosbaar is, maar val dan niet de verkeerden lastig met fail-tagging.
- Als een medewerker faalt, is het de manager die faalt. Die had immers toezicht moeten houden. Wat deed hij dan; als Calimero aanschuiven bij Echt Belangrijke vergaderingen? Dus als er een categorie moet worden aangeduid als zwakste schakel, is dat het 'management'. Van laag tot hoog. Overigens is er vrijwel overal zelfselectie geweest dan wel omhoog vallen door gebrek aan gewicht. Alleen de echt grote leiders willen de besten om zich heen, de rest zoekt steun tegen het eigen imposter syndrome.
- Waar de mens faalt, is de mens nooit (dat kunnen we wel concluderen) de enige 'control' die er was of is. Altijd ging er nog veel meer fout, faalden vele andere controls. Vooral de organisatorische controls – die inherent zo veel zwakker zijn dan de in applicaties en diepere technologie - lagen embedded controls. Maar ja, die laatste zijn duur en onbegrijpelijk voor wie niet is ingevoerd in de betreffende materie, dus worden op z'n best wat krakkemikkig en onvolledig geïmplementeerd en nog meer zo onderhouden. De organisatorische controls

J. van der Vlugt CISA CRISC, Jurgen, is zelfstandig professional voor information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl

moeten dat opvangen, maar doen ze dat ook? Ze zijn a priori zwakker, minder (sic) goed geïmplementeerd en slecht onderhouden. Want we moeten de auditor nog tegenkomen (ondergetekende al of niet incluis) die daadwerkelijk de opzet van het stelsel van controls toetst en op basis daarvan concludeert dat de werking twijfelachtig moet zijn. Want in de opzet van het stelsel zelf ligt de mogelijkheid besloten dat het effectief de risico's gaat beheersen. Als de opzet gaten laat, zullen die zelfs bij perfecte implementatie nog gebreken in de werking laten. De werking is niet `herhaald vaststellen van bestaan'. Wie dat nog beweert, geeft ronduit een valse verklaring. Maar de werking, dat is het feitelijk resulterende beheersing van risico's door het stelsel van controls.

- Daarbij nog opgemerkt dat effectieve risicobeheersing tevens efficiënt is, hetgeen wil zeggen dat niet alles wordt gedaan (want dat is heel kostbaar) c.q. geïmplementeerd, dus moeten we er rekening mee houden dat de restrisico's bestaan en zullen toeslaan. Laag risico betekent een kans van 1 (zegge en schrijve één) dat dat risico zich zal manifesteren in een event. Alleen is de geprognosticeerde frequentie laag. Alleen als een risico nul (0) is, zal er geen event zijn (of niet worden opgemerkt bij gebrek aan impact) De frequentie is immers gelijk aan het aantal events gedeeld door de verlopen tijd. Geprognosticeerd op basis van historische cijfers. Waardeloos, morgen is anders dan het verleden, zelfs rekening houdend met doorlopende trends - op basis van gut feeling van één of een aantal betrokkenen. Dat kan werken, mits transparant en door echte deskundigen waarop dan dus behoorlijk wordt gesteund, maar zijn ze ook aanspreekbaar op de gevolgen?
- De mens was of is dus niet de zwakste schakel, want dat de mens momenten van zwakte had en heeft, was al wel bekend. Zo gedwongen door werkdruk, (korte- en langere-termijn-) vermoeidheid, momenten van onoplettendheid, gebrek aan (onderhouden!) opleiding etc.

Zodat dus, als de mens dan even een beetje tijd over had (nou ja, we weten heus wel dat geen werknemer acht uur van de acht uur productief is op een dag), deze uit plichtsbesef zelf om ontspanning zoekt van de gespannen boog en wat rondsurft op het web. Op zoek naar kennisvermeerdering, als het jaarbudget p.p. nog te weinig is voor een dagje (relevante) cursus, of op zoek is naar verbreding van het perspectief en fysieke (ont)spanning. Dat daarbij wat malware werd gedownload en vast per ongeluk werd aangeklikt (als dat al nodig was), betekent dat er al heel veel controls kennelijk niet hebben gewerkt… Als dan de laatste line of defence -vrijwel onvermijdelijk- eens niet perfect werkt, tsja. En ja, de mens is in dezen een line of defence want hij staat tussen bedreiging en kwetsbaarheid.

Intermezzo: Niet als een 'line of defence' quod non: die staat tussen mensen die hun targets proberen te halen en de externe auditors of regulators die van alles willen weten maar op afstand moeten worden gehouden met per line steeds wolliger taal. Al die laatste lines of defence staan niet tussen enige bedreiging en kwetsbaarheid dus zijn er geen. Einde intermezzo.

De mens is in heel veel van dit soort gevallen dus juist de sterkste schakel: als al het andere niet werkt, komt het aan op de mens – die alerter en opmerkzamer is dan welke andere control dan ook, en flexibeler in het opvangen van issues die buiten de bandbreedte van de voorgaande controls viel. De mens is niet de zwakste maar de laatste schakel. Detectief en correctief, omdat het op straffe was van sanctie en het verboden was om preventief af te wijken van het gemankeerde stelsel van controls.
De mens brandmerken als zwakste schakel betekent dat hij uit eigener beweging niet mag bijdragen aan eigen kennisonderhoud of überhaupt aan het behalen van de organisatiedoelstelling boven het voldoen aan de misplaatste pietlutregeltjes. De mens benoemen als zwakste schakel is als vol gas op een betonnen muur inrijden en dan de schuld geven aan de autofabrikant dat de kleur van de airbag niet past bij het interieur. Ja, dat is een onzin-vergelijking.
Niet meer doen dus, de mens de schuld geven. De schuld afschuiven op de mens is voor zwakkelingen. De mens is niet de zwakste schakel, maar de sterkste.
En daarom kunnen we met een positieve noot eindigen. Zorg eerst eens dat de boel van al die andere controls een keertje op orde komt! Waarom van een gebruiker verlangen dat die een complex én lang wachtwoord moet onthouden, als een 2FA-oplossing (met alle gebreken van dien) de beveiliging met veel grotere stappen verbetert. Of de rechten op (netwerk)schijven en systemen nou eindelijk wél eens goed worden ingeregeld, zodat malware geen write kan doen. En de firewallcomplexen (en patching in het algemeen ook) zo goed zijn onderhouden, dat van known exploits weinig te vrezen valt. Etc.etc.
En gebruik dan, daarna, ook de kracht van de mens! Stuur ze veel vaker op (relevante, please!) cursus, geef meer aandacht aan de successen van near misses waar de mens in last resort schade voorkwam, steun de mens in de `awareness-campagnes' in het alert zijn, en in het op flexibele manier beheerst bereiken van de organisatie¬doelstellingen. Dat is waar mensen voor zijn, dat is waar ze goed in zijn.

AUTONOMOUS

Gartner tells us in its Top 10 Strategic Technology Trends for 2019 (1) that autonomous things are number one in the list. Autonomous things use artificial intelligence (AI) to perform tasks traditionally done by humans. We are talking robotics on a new level of sophistication and with greater levels of autonomy than seen in previous generations of robot technology. The types of autonomous things include vehicles, drones, appliances, embedded software agents and specialised industrial robots such as agricultural harvesting machinery. The spaces in which these devices operate include the physical land, sea and air environments and the logical digital environment often referred to as cyberspace. The levels of capability, coordination and intelligence vary widely according to the application. Some require human assistance (or perhaps we should say some are designed to assist human activity – after all, who is in charge here?) whereas some, such as farming machinery, can work completely autonomously without a human operator.

What does all this mean for business risk and the need for security to manage risk?

Digital disruption is the term that has been coined to describe how the introduction of digital technology is completely changing some business models in some business sectors. Some examples from the past include digital photography, digital entertainment, digital music, electronic banking, and digital publishing of written materials (books, papers and the like). In each of those cases the entire industry has been remodelled. The changes span the whole value chain (and contributing processes) of those businesses affected, from product innovation and design, product marketing and sales, goods and services production, delivery to customers and after-sales service. Some traditional functional service providers have been disintermediated and found themselves with no business. Some traditional manufacturers and suppliers have met the same demise. Those that succeed as their business sector undergoes digital disruption are those that see the changes coming and adapt their business processes early. New entrants often have an advantage of no legacy. Agility is the key to success in such a volatile world. One thing is certain: autonomous things will bring on another round of digital disruptions that might threaten your business model. As with all risks, there is the huge opportunity but an equally large threat. Are you even looking to see what's coming over the horizon for you?

That's the strategic risk, but what about the operational risks? It is clear from all human attempts to automate and mechanise processes that there are some serious health and safety issues to be addressed. Whilst AI has certainly gained some ground in recent years, can it really replace human intelligence? The Attributer believes that right now (and maybe forever) it cannot. So, to what degree are we prepared to trust the operation of autonomous machines? We drew attention to this issue in the previous Attributer blog column with regard to verification of fake or flawed information. AI can only look out for the input signals for which it is programmed. Human intelligence has a huge capability to spot very subtle changes in the input that signal some potential threat – not just single changes but multiple simultaneous changes of minute significance individually, but of major significance collectively. The human can 'sense' a situation that doesn't 'feel' right without necessarily being able to analyse immediately all the reasons why. It seems doubtful that AI will ever achieve this level of intelligence. What AI can do is analyse huge numbers of possible actions very quickly and choose the optimum one for the given situation. It can also follow a programmed process without deviation, something at which humans are not so good. We must be clear – humans do some things better than AI and AI has its advantages too.

SABSA views risk as the effect of uncertainty on objectives. In any business system we can express the objectives as a Business Attributes Profile, with measurement and performance-monitoring built in. We can analyse our potential autonomous operation targets and get a clear differentiation between those that are viable and those that are not, within the performance criteria for efficiency, effectiveness and safety that we deem appropriate. As always, if it's a complex business system, SABSA has the intellectual tools to analyse the risks, both opportunities and threats.

The Attributer

References

(1) https://gtnr.it/2qRdwKm

DE FEESTDAGEN VOOR CYBERCRIME

In de maanden november en december zijn veel mensen druk met de voorbereidingen voor de feestdagen. In deze periode kennen we bij ons in Nederland niet alleen ons sinterklaasfeest, maar doen we tegenwoordig ook mee in de Amerikaanse drukte rond Thanksgiving, Black Friday, Cyber Monday en Kerst. Uit onderzoek van Motivaction (1) blijkt dat ongeveer twee derde van de Nederlanders inmiddels op de hoogte is van het bestaan van Black Friday. Daarnaast wint de uit China overgewaaide Singles Day ook bij ons aan populariteit. Singles Day op 11 november is één van de grootste online en offline winkeldagen in de wereld. Alibaba scoort op die ene dag een omzet van meer dan 20 miljard dollar (2). Consumenten kopen in november en december meer dan in andere maanden. Winkels die kleding, juwelen, consumentenelektronica, sportartikelen en boeken verkopen, kunnen een kwart van hun jaaromzet in deze periode halen (3).

De feestdagen zijn dus druk voor consumenten, banken en winkeliers. Waar geld omgaat, zijn meestal ook criminelen. Ik vroeg mij af of het ook een drukke tijd is voor de cybercriminelen. Halen zij ook een kwart van hun jaaromzet uit deze periode? Als ik de Amerikaanse media moet geloven, is deze tijd van het jaar hoogtijd voor fraude en identiteitsdiefstal. Consumenten worden deze periode overspoeld met advertenties en e-mails waarin mooie aanbiedingen staan. De hoeveelheid marketing die op ze afkomt, kan ze afleiden en verleiden. Veel kans dus dat men niet doorheeft dat een verbinding niet veilig is, een link in een e-mail leidt tot narigheid of dat men online bestelt bij een bedrijf dat niet bestaat. Of valt het allemaal wel mee? Ik wilde hier graag meer over weten, dus ik ging op zoek naar meer informatie.

Phishing en nep-apps

Twee vormen van cybercrime die bij dit onderwerp passen, zijn phishing en nep-apps. Kaspersky (4) schrijft in hun Beyond Black Friday Threat Report dat phishing het hele jaar door redelijk constant is, met een gemeten piek op de specifieke dag van Black Friday. Het rapport is echter verwarrend, omdat de illustratie die bij deze tekst wordt getoond juist een piek op Cyber Monday laat zien.

Phishers maken volgens Kaspersky veelvuldig misbruik van de naam Black Friday, omdat het de aandacht van de consumenten trekt. Ook Fox-IT waarschuwde in december 2017 (5) voor een stijgend aantal phishing e-mails met een feestdagen thema.

Met dit gegeven ben ik gaan zoeken op de website van de Fraudehelpdesk. Daar staan heel veel voorbeelden van valse e-mails gepubliceerd. Zoekopdrachten met relevante feestdag-tags zoals Sinterklaas, Kerst, Black Friday, Cyber Monday of met namen van bekende online retailers leverden geen voorbeelden op van relevante, verdachte e-mails die door fraudehelpdesk.nl zijn gepubliceerd. In juni 2016 was er wel een valse e-mail in omloop waarin gewaarschuwd werd voor fraudeurs tijdens de kerst- en nieuwjaarsperiode. Er zijn enkele voorbeelden te vinden waarbij namen als Amazon of eBay werden gebruikt om de aandacht te trekken, maar die e-mails waren niet in de feestdagenperiode gepubliceerd. De waarschuwingen voor phishing e-mails met een feestdagenthema worden dus niet onderbouwd door voorbeelden bij de fraudehelpdesk.

Naast phishing waarschuwen experts voor fraude met nep-apps voor de smartphone, smartwatch, tablet of een ander mobiel apparaat. RSA stelt dat mobile apps een grotere bron van fraude zijn dan mobile browsers. Zij stellen dat 80% van de mobiele fraude komt door apps (6). RiskIQ waarschuwt dat 1 op de 25 apps voor Black Friday nep is en uit is op het stelen van creditcardgegevens. Sommige apps zijn speciaal ontworpen om malware op de telefoon van de gebruiker te laden (7). Naast apps voor het kopen van aangeboden producten kunnen er ook problemen ontstaan met nagemaakte apps voor betalen. Volgens de consumentenbond hebben zich in Nederland ooit wel problemen met mobiel bankieren voorgedaan. Vooral rondom nep-bankapps of apps die een laag over de bankapps tonen (8). Net als bij phishing, wordt er in Nederland in de publieksvoorlichting geen duidelijke feestdagen-piek van nep-apps gerapporteerd.

De cybercrime economie

De meeste publieke rapportages over de winsten van cybercrime laten de data op jaarbasis zien. Dit is ook het geval voor rapportages over soorten bedreigingen en criminaliteit. Hierdoor is het onmogelijk om op basis van openbare bronnen iets te kunnen zeggen over seizoensinvloeden op omzet en winst.
Een studie uitgevoerd in opdracht van Bromium (9) schat dat de totale cybercrime economie per jaar 1,5 triljoen Amerikaanse dollar aan winst maakt. Daarbinnen wordt de jaarlijkse winst van handel in persoonsgegevens geschat op zo'n 160 biljoen dollar. Het gaat hierbij om handel in onder andere gestolen credit- en debitcard data,

Nicole van Deursen werkt als onderzoeker en consultant. Nicole is bereikbaar via nicolevdeursen@hotmail.com.

Experts en cybersecuritybedrijven geven tips om fraude tijdens de feestdagen te voorkomen

inloggegevens voor bankieren en loyaliteitsprogramma's. De opbrengst van ransomware is in het geheel een stuk kleiner: 'slechts' 1 biljoen dollar. Hoeveel van deze winst behaald wordt tijdens de feestdagen is niet gespecificeerd.

Waarschuwingen en adviezen

Diverse experts en cybersecuritybedrijven geven tips en adviezen aan consumenten, retailers en financiële instellingen om fraude tijdens de feestdagen te voorkomen. Dit zijn voornamelijk bronnen uit de VS, waar de meeste cyberaanvallen op organisaties ter wereld voorkomen (10). In Nederland is het behoorlijk stil rondom dit thema. Wat verder opvalt, is dat er weinig wordt gediscussieerd over de situatie in organisaties die geen e-commerce of financiële transacties verwerken. Een survey in het VK (11) liet zien dat 41% van de ondervraagden van plan was online te gaan winkelen op Black Friday of Cyber Monday vanaf de werkplek én tijdens werktijd. Wellicht moeten organisaties iets extra doen om hun assets te beschermen, als blijkt dat ook hun medewerkers massaal tijdens werktijd online gaan om aanbiedingen te scoren? In het cybersecurity bewustzijnsonderzoek van Alertonline (12) is namelijk te lezen dat medewerkers zich niet veel zorgen maken over online veiligheid op het werk. Dat vinden ze de verantwoordelijkheid van de werkgever. Het onderzoek vond ook dat veel Nederlanders geloven dat https of een groen slotje garant staat voor een veilige website. Bovendien neemt de bekendheid met online gevaren, zoals spoofing, juist af.

Conclusie

Het stijgend aantal aanleidingen om ook in Nederland in november en december een commerciële promotie-actie te starten, lijkt op het eerste gezicht niet te leiden tot een evenredig stijgende angst voor cybercriminaliteit. Op de diverse voorlichtingswebsites in Nederland staan geen relevante voorbeelden of specifieke fraude waarschuwingen. Dit in tegenstelling tot Engelstalige media waar een kakafonie van meldingen van gevaar, angst en drama te vinden is. In Nederland is het een stuk stiller. Wellicht komt dat omdat in Nederland in de sinterklaas- en kerstperiode verhoudingsgewijs minder wordt uitgegeven dan in andere landen. In de Nederlandse e-commercebranche wordt de omzet in de hele periode op 22 miljard euro geschat (13). (Noot voor de lezer: vergelijk dit bedrag nog even met de omzet van Alibaba in 24 uur op 11 november.) Nederland staat in de Ferratum Barometer (14) wat uitgaven betreft al 2 jaar onderaan de lijst van 20 landen die vergeleken worden. Toch staat in diezelfde lijst juist Nederland op de 3e plaats voor online aankopen en op de 3e plaats voor mobiel gebruik. En als ik dat combineer met het gegeven dat de bekendheid met online gevaren juist afneemt, stelt die stilte mij niet helemaal gerust. Misschien wordt het tijd dat we met elkaar wat meer details over de beschikbare data openbaar maken om daardoor bij te dragen aan de analysemogelijkheden. Dan kunnen we daarmee ook met elkaar gerichte voorlichting en maatregelen afstemmen.

NB: Dit artikel is geschreven begin november 2018, dus vóór de feestperiode. Dit blad zal de lezer bereiken in december. Ik hoop dat het een rustige tijd voor alle security collega's is geweest.

Bronnen

(1) https://www.motivaction.nl/kennisplatform/nieuws-en-persberichten/black-friday-in-nederland-vooral-bekend-bij-millennials
(2) https://www.youtube.com/watch?v=qmPn9iiZCY0
(3) https://nrf.com/media/press-releases/nrf-forecasts-holiday-sales-increase-between-36-and-4-percent
(4) Kaspersky lab. Beyond Black Friday Threat Report 2017.
(5) https://blog.fox-it.com/2017/12/12/criminals-in-a-festive-mood/
(6) RSA. Whitepaper The Current State of Cybercrime. 2018.
(7) https://www.riskiq.com/press-release/1-25-black-friday-apps-fake-finds-riskiq-threatening-10-8b-projected-black-friday-online-sales/
(8) https://www.consumentenbond.nl/betaalrekening/mobiel-bankieren
(9) Dr. M. McQuire. Into the Web of Profit. Understanding the growth of the cybercrime economy. Bromium. 2018
(10) Symantec. Internet Security Threat Report. Volume 23. 2018
(11) https://www.beaming.co.uk/press-releases/maintain-cyber-security-employees-shop-online/
(12) Nationaal Cybersecurity Bewustzijnsonderzoek, 2018.

HENK DE RUITER

Voor wie mij nog niet kent: mijn naam is Henk de Ruiter en ik werk als Trusted Advisor bij Sogeti. Op dit moment ben ik ingezet als Security Manager bij Vattenfall/Nuon en bij Sandd. In 2013 ben ik toegetreden tot het PvIB-bestuur als penningsmeester.

Ik ben lid van de PvIB, omdat ik graag mijn kennis en kunde wil delen. Mijn ervaring als leider/manager kan ik goed gebruiken om 'onze' professionals te laten groeien, zodat we met z'n allen kunnen bijdragen aan een veiliger Nederland. Misschien een tikkeltje ambitieus, maar daar is niets mis mee – vind ik althans.

Als ik naar ons vakgebied kijk, zie ik aan de ene kant een groeiend tekort aan cybersecurityspecialisten en aan de andere kant een verschuiving door AI, blockchain en een toekomst met quantum computing, waardoor alles anders zal worden ook voor ons. We moeten cybersecuritymaatregelen niet achteraf, maar gelijk al meenemen. Zorg daarom voor een inherent en veilig design, propageer veilig gedrag (cybersecurity by design en by default), zorg voor autonomie van detectie en zorg voor gelaagdheid van beveiligingsmaatregelen (waarbij informatie in de toekomst intrinsiek veilig is met homomorphic encryption).

Wat ik nog graag met u wil delen, is de presentatie van Koen Bertels (TU Delft) tijdens het Security Congress over de ontwikkeling van de toekomstige quantum computer (deze studie heeft recent ook een Europese subsidie ontvangen). Het was prachtig en inspirerend om te zien dat zo'n ingewikkeld vraagstuk met passie en duidelijkheid wordt gepresenteerd.
Vanuit cybersecurity moeten we dit goed in de gaten houden, want alle huidige encryptiemethoden zijn compleet niet meer toereikend. Daar tegenover staat dat quantum computing meeneemt dat informatie intrinsiek veilig is, omdat informatie bij 'aftappen' zichzelf vernietigt. Is het tegen die tijd niet zo dat de informatiebeveiliger niet meer nodig is?

Waar ik de PvIB over vijf jaar zie? Een periode van vijf jaar is in deze tijd erg lang, maar ik geloof dat informatiebeveiliging dan nog steeds een fundamentele zaak is, dus ook voor ons als beroepsgroep. Mét passie voor het vak, enthousiasme voor ons als vereniging, ruimte voor discussie en conflicten die leiden tot groei. Kortom, een leerfabriek. En als we kijken waar het heengaat met de informatiebeveiligings-wereld dan is het toch prachtig dat wij in dit vakgebied werkzaam mogen zijn?

Henk de Ruiter

AVG... WAT MOETEN WE ERMEE?

"Privacyrecht is niet te handhaven zonder structurele en preventieve technische maatregelen", stelde `privacyridder' John Borking, buitengewoon lid van het College Bescherming Persoonsgegevens. Borking is één van de auteurs van een door het ministerie van Binnenlandse Zaken uitgegeven publicatie genaamd: `Privacy Enhancing Technologies (PET), een witboek voor beslissers'. Doel was om met PET de juridische verplichtingen om te zetten in technische specificaties. Waarbij de gedachte was dat door het toepassen van PET tijdens de ontwikkeling van producten en diensten (zoals IT systemen) privacy verhogende maatregelen konden worden meegenomen. `Privacy by design' dus, populair gezegd. Allemaal bedacht en beschreven door onder andere John Borking in 2004.

Boost

De hype in 2018 rond de Algemene Verordening Gegevensbescherming (AVG) zorgde voor een enorme boost in het privacybewustzijn in organisaties en bij burgers. De vraag is of de principes van privacy enhancing technologies voor ontwerpers van IT-systemen en softwareontwikkelaars dagelijks in de praktijk worden toegepast. Sterker nog: het aantal trainingen, cursussen en workshops over privacy by design zijn op één hand te tellen en het lijkt wel of we het allemaal wel weten en kunnen.

Feit is dat ik als security consultant in de dagelijkse praktijk nog steeds moet uitleggen dat het niet handig is om persoonsgegevens en transactiegegevens in één database te stoppen. Of dat ik moet uitleggen dat databases technische voorzieningen moeten hebben om persoonsgegevens eenvoudig te kunnen verwijderen en dat een vinkje niet voldoende is. Dat ik moet uitleggen dat je op testsystemen geanonimiseerde persoonsgegevens dient te gebruiken. Ik kan zo nog wel even doorgaan.

In de AVG-hype van 2018 is de markt het implementeren van preventieve technische maatregelen volkomen vergeten. Een bijkomstigheid van de AVG-hype is het ontstaan van nieuwe functies zoals Privacy Officer, Functionaris Gegevensbescherming of Data Protection Officer. Niet dat deze nieuwe functies overbodig zijn, nee de mensen die dit uitvoeren doen prima werk. Echter, de geschiedenis leert ons ook dat bij nieuwe wetgeving die IT raakt, nieuwe functies ontstaan die na een paar jaar weer verdwijnen. Een mooi voorbeeld zijn de SOX en Basel II security specialisten. Zij vullen nu de kaartenbakken bij het UWV.

Met wetjes, regeltjes, processen en privacy officers komen we er niet. Feit is dat het AVG-geweld nu zal moeten doordenderen in de IT techniek. En dat de techneuten privacy enhancing technologies NU moeten oppakken.

Bron

https://www.pleio.nl/pages/view/84075/dossier-privacy-enhancing-technologies-pet

Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, elektronische & technische beveiliging, fraudedetectie & -bestrijding, en bewaking & beveiliging voor de toonaangevende vakbladen in Nederland en België. Ronald is bereikbaar via ronald@eygendaals.nl.

OKTOBERMAAND = CONFERENTIEMAAND

Infosecurity 2018 (31 oktober/1 november)

Ook dit jaar werd de beurs weer gehouden. De plaats was, zoals gebruikelijk, Jaarbeurshal 1 te Utrecht. Een kleine, overzichtelijke beurs met een professionele uitstraling. Opvallend was dat op bijna geen enkele stand het woord 'cyber' ontbrak. Daarmee is dat woord hét modewoord van dit jaar geworden. Veel aandacht was er, niet verrassend, voor GDPR/AVG compliance 'oplossingen'.

Beide dagen toonden een redelijk druk bezocht beurs, waar de bezoeker weliswaar geen innovaties in grote getale op zich af zag komen, maar wel een verdieping van de in eerdere jaren aangehaalde thema's. Het toont de groei naar volwassenheid van de veiligheidssector aan, waardoor innovaties wat meer op de achtergrond raken.

Naar wens kon men deelnemen aan menig interessante lezingen/presentaties. Verder was het veel gezellig netwerken met oude bekenden en nieuwe relaties. De catering was weer goed verzorgd. Kortom, de bezoeker kan met tevredenheid terugkijken op deze beurs. Zeker met de aanwezigheid van Norea en PvIB met een eigen, centraal gelegen stand. Hopelijk vonden onze (toekomstige) leden dat ook!

Tom Bakker & Chris de Vries

One Conference (NCSC) (2/3 oktober in Den Haag)

Met een geschiedenis van meer dan vijftien jaar is de One Conference (voorheen NCSC/Govcert Symposium) één van de oudste securityconferenties in Nederland. Gratis toegankelijk, áls je inschrijving tenminste door het NCSC toegelaten wordt. Met de naamswijziging in 2013 en de inbreng vanuit Economische Zaken lijkt de focus wel wat waziger te worden, wat vooral dit jaar goed te merken was. Natuurlijk waren er de nodige parallelle sessies met inbreng van NCSC, Nationale Politie en buitenlandse sprekers. De befaamde 'No publicity'-tracks gaven als vanouds een inkijkje in de keuken van opsporingsdiensten waar je anders weinig van hoort. Waar in het verleden de sessies nog in tracks met bepaalde thema's waren georganiseerd, kwam dat dit jaar minder uit de verf. Technische sessies (onder ander over Internet of Things-honeypots) werden afgewisseld met meer algemene verhalen over crisismanagement en updateprocessen.

De enige verbindende factor was het overvloedige gebruik van het voorzetsel 'cyber'. En de plenaire presentaties waren van een wisselend niveau. Michel van Eeten gaf een inkijk in de beveiliging (of niet) van connected consumentenapparaten en blijft je als spreker boeien. De duo-presentatie van McAfee leek echter meer op naamsbekendheid gericht dan dat er nieuwe inzichten uit bleken. Zo bleef al met al dit jaar de One Conference toch vooral een plek om te netwerken met collega's die je anders niet ziet.

Patrick Dersjant

IC18: Infographics Conference (12 oktober in Hilversum)

Infographics Conference is een netwerkbijeenkomst en congres voor infographics en datavisualisatie. Zowel de sprekers als het publiek bestaan uit een mengelmoes van journalisten, visueel ontwerpers, studenten en medewerkers van organisaties die complexe problemen moeten communiceren aan non-experts. En dat soort communicatie komen wij als security mensen dagelijks tegen. Er waren twee presentaties die er voor mij uitsprongen.

De eerste was een presentatie van de Onderzoeksraad voor de Veiligheid. Wanneer men daar begint aan een onderzoek na een ramp denkt men vanaf het begin al in beeld. Je kunt niet een onderzoeksrapport, als het af is, aan de communicatieafdeling geven en om een leuk plaatje vragen. De communicatiespecialisten moeten vanaf het begin van het onderzoek al betrokken worden, zodat ze goed begrijpen waar de boodschap over gaat en wat het doel is. Beeldcommunicatie vraagt om een strakke regie. In ons vakgebied kennen we deze manier van denken wel in verband met crisiscommunicatie. De andere presentie ging over Legal Design. De advocatuur produceert dikke dossiers vol tekst. Veel advocatenkantoren hebben dan ook een afdeling voor legal information design. Het helpt vaak bij een rechtszaak als het dossier wordt ondersteund met een tijdlijn van gebeurtenissen of een afbeelding van sociale netwerken rondom een persoon. Gelijk hebben is namelijk niet hetzelfde als gelijk krijgen en visuele communicatie helpt daarbij. Zou visuele communicatie ook voor security specialisten helpen om wat vaker gelijk te krijgen?

Nicole van Deursen

DE WET BEVEILIGING NETWERK- EN INFORMATIESYSTEMEN: EEN REDDER IN NOOD?

We kunnen er niet meer omheen: de digitale dreigingen nemen in hoog tempo toe. Niet alleen overheidsinstellingen zijn het doelwit, maar ook bedrijven en individuen zoals jij en ik. Om Nederland digitaal veiliger te maken, zal naar verwachting binnenkort de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) in werking treden. In de volksmond ook wel de Cybersecuritywet. Op het eerste gezicht een goed initiatief, maar wat nog moet blijken is of deze nieuwe wet is opgewassen tegen het duistere werk van cybercriminelen. Eerst zien, dan geloven.

De Wbni is de Nederlandse vertaling van de Europese Netwerk en Informatieveiligheid richtlijn (NIB-richtlijn). Deze wetgeving beoogt de digitale veiligheid én weerbaarheid in Europa te vergroten. Per lidstaat is er momenteel een wisselend niveau van paraatheid bij incidenten en een verschillend niveau van bescherming van bedrijven en consumenten. Dit kan er toe leiden dat uitwisseling van informatie over dreigingen en incidenten achterwege blijft. Een gemeenschappelijk Europees beleid en meer eenheid bij de beheersing van informatiebeveiligingsrisico's in netwerk- en informatiesystemen moet daar verandering in brengen. De NIB-richtlijn spoort Europese lidstaten aan om een gezamenlijk schild te vormen tegen digitale dreigingen, de gevolgen van cyberincidenten te verkleinen en daarbij beter samen te werken. De lidstaten worden aldus gestimuleerd de NIB-richtlijn om te zetten in nationale wetgeving. In Nederland heeft dat geresulteerd in de Wbni.

Een zorgplicht én dubbele meldplicht

De Wbni schrijft voor dat organisaties passende technische en organisatorische maatregelen moeten treffen op basis van een gedegen risicoafweging. Daarbij is een zorg- én meldplicht gecreëerd voor incidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening. Deze zorgplicht houdt in dat organisaties maatregelen treffen om ICT-risico's te beheersen, incidenten te voorkomen en de gevolgen van incidenten te beperken. In de praktijk gaat het erom dat wanneer een cyberincident zich voordoet, een bedrijf zijn techniek en organisatie op orde moet hebben om de digitale 'brand' direct te kunnen blussen en de schade te beperken. De NIB-richtlijn bepaalt dat elke lidstaat een toezichthouder aan moet wijzen. In ons land is het Agentschap Telecom, onderdeel van het Ministerie van Economische zaken en Klimaat, de handhavende toezichthouder voor de energiesector, de internetinfrastructuur en de digitale dienstverleners. Voor aanbieders van essentiële diensten binnen sectoren als de financiële markt, de zorg en transport zullen aparte toezichthouders aangewezen worden.
Daarnaast geldt er een dubbele meldplicht. Incidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening moeten worden gemeld bij zowel de aangewezen toezichthouder als het Nederlands Cyber Security Centrum (NCSC). Het NCSC fungeert voor Nederland als het CSIRT, een Cyber Security Incident Response Team. Een CSIRT is een team dat waarschuwt voor cyberrisico's en biedt hulp bij cyberincidenten. Het zorgt voor een dynamische risico- en incidentanalyse. Zo kan een bank door het CSIRT gewaarschuwd worden wanneer zich in de sector een dreiging van een DDoS-aanval bestaat. Ook kan die hulp krijgen wanneer een incident zich daadwerkelijk voordoet.

Aanbieders van essentiële diensten

De Wbni richt zich primair op aanbieders van diensten die onmisbaar zijn voor kritieke economische en maatschappelijke activiteiten. De NIB-richtlijn noemt hen 'aanbieders van essentiële diensten' (hierna: AED). Je kunt daarbij denken aan energiebedrijven, banken en de gezondheidszorg.
Essentiele diensten zijn vandaag de dag dermate afhankelijk van netwerk- en informatiesystemen, dat verstoring hiervan kan leiden tot maatschappelijke ontwrichting. Het is dus van belang dat deze systemen betrouwbaar en goed beveiligd zijn. Vandaar dat er vanuit de Wbni een zorgplicht op hen rust. In de NIB-richtlijn staat een opsomming van diensten die als essentieel worden beschouwd, maar het is aan de lidstaten zelf om daar verder invulling aan te geven. De Wbni zal voor de betreffende AED's dus pas gaan gelden wanneer zij hiervoor zijn aangewezen door de overheid.

Vitale aanbieders

Daarnaast bestaan er in ons land aanbieders van diensten die cruciaal zijn voor de instandhouding van de Nederlandse infrastructuur, maar die in de Europese NIB-richtlijn niet beschouwd worden als essentiële dienst. Dit zijn

Beaubine Adriaansen is Cyber Security & Privacy consultant bij Strict Academy en actief binnen het Governance, Risk & Compliance team. Beaubine is bereikbaar via b.adriaansen@strict.nl

Verstoring van essentiële diensten kunnen leiden tot maatschappelijke ontwrichting

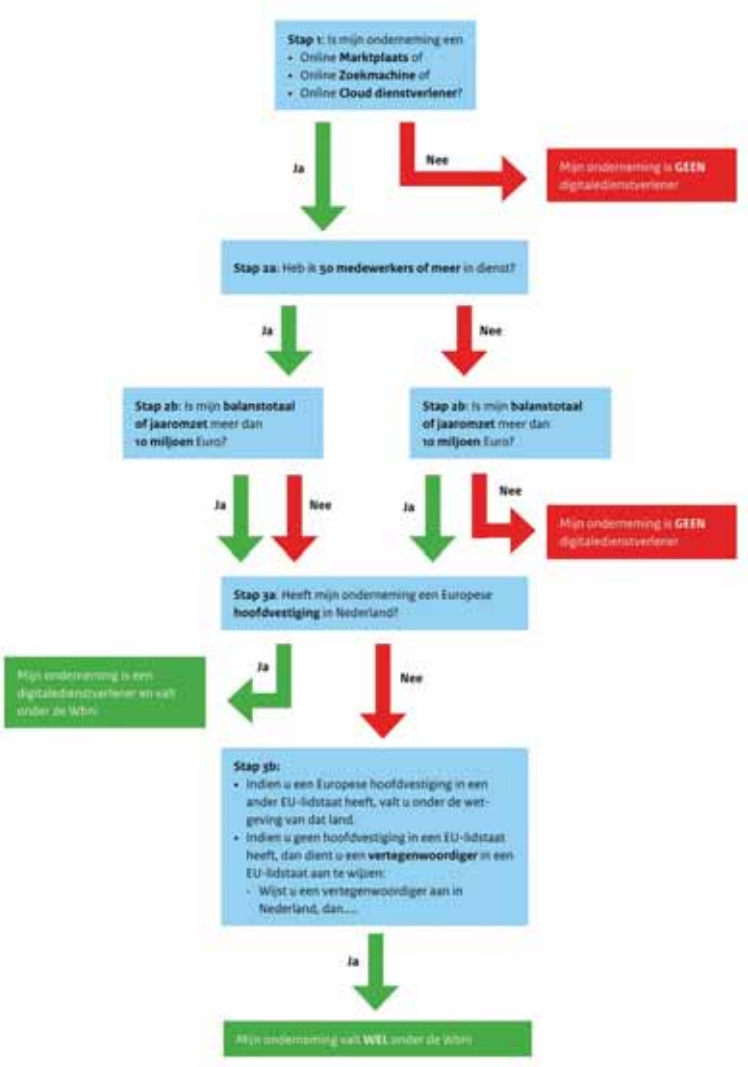
vitale aanbieders. Denk hierbij bv. aan de waterkeringen, die het laaggelegen Nederland beschermen tegen overstromingen. Deze vitale aanbieders zijn reeds opgenomen in de huidige Wet gegevensverwerking en meldplicht cybersecurity (Wgmc). De Wgmc zal worden opgenomen in de Wbni. Gevolg hiervan is dat de verplichtingen uit de Wgmc zullen blijven gelden voor vitale aanbieders die niet onder de NIB-richtlijn vallen. Het komt erop neer dat voor vitale aanbieders enkel een meldplicht bij het NCSC zal bestaan.

Digitale dienstverleners

De laatste categorie organisaties waarop de Wbni zich richt zijn digitale dienstverleners, de zogenaamde 'Digital Service Providers' (hierna: DSP). Volgens de NIB-richtlijn is een DSP 'een rechtspersoon die een digitale dienst aanbiedt'. Dit is verder verbijzonderd tot de categorieën onlinemarktplaats, onlinezoekmachine en cloudcomputerdienst. Wanneer een cyberincident zich voordoet, rust ook op hen de zorgplicht en de meldplicht bij zowel het Agentschap Telecom als het NCSC. In tegenstelling tot AED's zullen DSP's niet worden aangewezen door de overheid. DSP's moeten zelf de inschatting maken of zij gebonden zijn aan de verplichtingen van de Wbni aan de hand van criteria in de NIB-richtlijn. De organisatie:

- is een onlinemarktplaats óf levert een onlinezoekmachine of een cloudcomputerdienst;
- heeft een hoofdvestiging in Nederland of is hier vertegenwoordigd;
- heeft vijftig of meer medewerkers in dienst;
- heeft een balanstotaal of jaaromzet van meer dan tien miljoen euro.

Voldoet een organisatie aan deze criteria, dan valt deze onder de Wbni. Deze criteria zorgen in de praktijk echter voor nogal wat onduidelijkheid, hetgeen zich onder andere heeft geuit in Kamervragen. De NIB-richtlijn laat in de formulering expliciet ruimte voor interpretatie welke bedrijven als DSP gezien moeten worden. Wat valt er precies onder een onlinemarktplaats? En als een mogelijke



Figuur 1 - Wbni voor digitale dienstverleners

DSP een omzet van minder dan 10 miljoen euro per jaar heeft, waarom hoeft een cyberincident dan opeens niet gemeld te worden? Vragen als deze rijzen her en der op. Hier moet de wetgever nog duidelijkheid scheppen.

Zowel actief als reactief toezicht

Waar regels zijn, is handhaving nodig. Voor AED's vertaalt zich dit naar een actief toezichtbeleid. Dit houdt onder andere in dat het Agentschap Telecom bevoegd is om een beveiligingsaudit uit te (laten) voeren bij een AED of deze te verplichten zelf een audit uit te laten voeren door een externe auditor. Dit om inzicht te verkrijgen in het geïmplementeerde beveiligingsbeleid en de geïmplementeerde beveiligingsmaatregelen van de

organisatie. Er zal onder andere gekeken worden naar de opzet, het bestaan en de werking van het risicomanagementproces. Bij DSP's zal er sprake zijn van reactief toezicht. Dat houdt in dat er alleen inspecties plaats zullen vinden op basis van signalen en incidenten. Wanneer blijkt dat incidenten niet gemeld zijn of de organisatie niet voldoet aan de beveiligingseisen in de nakoming van de zorgplicht en de organisatie zich dus niet aan de Wbni houdt, heeft het Agentschap Telecom de bevoegdheid om handhavend op te treden met bindende maatregelen en boetes. Dit kan betekenen dat een organisatie bepaalde maatregelen moet treffen of juist een gedraging moet stoppen. Daarnaast kan er bijvoorbeeld een dwangsom worden opgelegd voor elke dag dat wordt nagelaten te voldoen aan de Wbni.
Voor nu blijft echter in het midden hoe dit toezicht zal worden vormgegeven. Net als de precieze invulling van de begrippen zorg- en meldplicht. Het is dus nog even afwachten hoe streng en op welke manier het Agentschap Telecom en andere toezichthouders zullen optreden.

Vertaling naar de praktijk

Dat de meldplicht bestaat is duidelijk, maar wanneer moet er precies gemeld worden? Het gaat erom dat een incident een aanzienlijk verstorend effect heeft op de dienst die geleverd wordt.
Ter illustratie kan wederom gedacht worden aan een DDoS-aanval op een bank. Wanneer een bank het slachtoffer wordt van zo'n aanval, kan dit als gevolg hebben dat er enige tijd geen gebruik kan worden gemaakt van internetbankieren. Daarbij is de vraag, wanneer kan men werkelijk spreken van een meldplichtig incident met een verstorend effect?
De NIB-richtlijn heeft daarvoor bepaalde relevante factoren omschreven. Het gaat vooral om het aantal getroffen gebruikers, de omvang van het geografische gebied en de duur van het incident. Voor DSP's heeft de richtlijn daar ook de omvang van de verstoring van de werking van de dienst en de omvang van de gevolgen van het incident voor de maatschappelijke en economische activiteiten aan toegevoegd. Het komt erop neer dat het bij de kwalificatie van een incident niet gaat om de aard van het incident, maar de nadruk ligt op de gevolgen daarvan. Kleine incidenten met amper gevolgen voor de dienstverlening hoeven dus niet worden gemeld.

Onnodig administratieve rompslomp?

AED's en DSP's zullen voortaan dus melding moeten maken van een cyberincident bij zowel de toezichthouder als het CSIRT. Waarom? Omdat deze instanties beide een ander doel dienen. Naar aanleiding van melding bij de toezichthouder zal deze in actie komen en controleren of de organisatie zich aan de Wbni heeft gehouden. Daarnaast biedt dit inzicht in de risico's binnen bepaalde sectoren, waardoor de toezichthouder aan de hand van het creëren van extra alertheid bij kan dragen aan het voorkomen van incidenten.

Het CSIRT kan naar aanleiding van een melding ondersteuning bieden gericht op herstel van de dienstverlening en andere ondernemingen waarschuwen voor mogelijke cyberaanvallen. Het is echter niet aan het CSIRT om te controleren of een organisatie zich aan de wet heeft gehouden. Dat is aan de toezichthouder.
De vraag is of het niet wenselijk is om in de nabije toekomst één gezamenlijk meldpunt te maken. Dit om administratief 'gedoe' te voorkomen en het de AED's en DSP's gemakkelijker te maken. In bepaalde gevallen is er zelfs sprake van een driedubbele meldplicht. Dit is aan de orde indien er bij een cyberincident sprake is van een datalek. Onder de Algemene Verordening Gegevensbescherming (AVG) bestaat namelijk de verplichting om een mogelijk datalek te melden bij de Autoriteit Persoonsgegevens. Ondanks dat elke melding een ander doel dient, zal samenwerking tussen de instanties en de mogelijkheid van één gezamenlijk meldpunt in de toekomst wellicht uitkomst bieden om onnodige administratie te voorkomen.

Hoog tijd voor voorbereiding

De komst van de Wbni, afkomstig uit de NIB-richtlijn, is de beantwoording van de behoefte aan een overkoepelende aanpak voor de digitale veiligheid in Europa. Het lijkt allemaal zo vanzelfsprekend: veilig het land door reizen met de trein, je smartphone opladen in een stopcontact en water uit de kraan. Maar deze systemen zijn kwetsbaar. Door digitale aanvallen kunnen zowel de vertrouwelijkheid, integriteit als de beschikbaarheid van de systemen negatief worden beïnvloed. Vandaar dat de Wbni verplichtingen oplegt voor onze digitale veiligheid. Samenvattend schept de Wbni voor AED's en DSP's:

- een zorgplicht om technische en organisatorische maatregelen te treffen;
- om ICT-risico's te beheersen;
- een plicht tot het melden van incidenten.

Of deze nieuwe verplichtingen ons daadwerkelijk digitaal weerbaarder maken, zal moeten blijken wanneer de wet in werking treedt. De Wbni is inmiddels aangenomen door de Eerste en Tweede Kamer. Wanneer deze precies in werking treedt is nog onduidelijk. Niettemin, hoog tijd voor AED's en DSP's om zich hierop voor te bereiden.

VOORSTELLEN NIEUWE REDACTIELEDEN

Als redactielid hoop ik mijn kennis en ervaring te kunnen delen met een groot publiek.

Fook Hwa Tan

Mijn naam is Fook Hwa. Mijn missie is het helpen van organisaties op hun digitale reis met betrekking tot informatiebeveiliging. Ik heb Informatica & Economie gestudeerd aan de Erasmus Universiteit Rotterdam. Door deze studie heb ik me altijd al beziggehouden met verschillende vakgebieden. Dat is ook de reden waarom ik informatiebeveiliging zo interessant vind: IT, HR, fysieke, juridische en andere aspecten die de revue passeren.

Na mijn studie heb ik bijna tien jaar gewerkt bij PwC Advisory als adviseur informatiebeveiliging. Ik hield me bezig met het adviseren van organisaties bij het inrichten van securitymanagement. De laatste vijf jaar heb ik voornamelijk organisaties in Nederland geholpen via Northwave. Hier heb ik eerst als Director Business Security een team van twee consultants tot ongeveer zeventien consultants opgebouwd om organisaties te ondersteunen bij vragen omtrent hun beleid, procedures en certificeringen op security gebied. Sinds juni dit jaar bekleed ik een nieuwe rol als Chief Quality Officer binnen Northwave. Ik ben verantwoordelijk voor security, privacy, continuity en quality binnen Northwave. Hierdoor ga ik me nog meer bezighouden met het vakgebied en daarbij intelligente oplossingen verzinnen voor MKB Nederland op de aspecten Business, Bytes en Behaviour. Ik probeer informatiebeveiliging betaalbaar en bereikbaar te maken voor een grotere groep organisaties.

Als redactielid hoop ik mijn kennis en ervaring te kunnen delen met een groot publiek, maar ook zelf te genieten van alle kennis en kunde van andere professionals op dit vakgebied. Als je vragen hebt op het gebied van securitymanagement, business continuity management of privacy management, dan kun je me altijd een berichtje sturen om hierover te sparren. Have a safe digital journey!

Lilian Knippenberg

Van voor tot achter lees ik iB Magazine altijd. Ik ben nu zo'n twee jaar lid van het PvIB en een hoogtepuntje van de maand is altijd als zowel de Quest als iB Magazine op de deurmat vallen. Ik houd ervan breed betrokken te zijn bij ons mooie vakgebied en in de breedte veel verschillende onderwerpen aan te raken. Inmiddels ben ik zo'n zes jaar bezig met informatiebeveiliging en privacy. Eerst in dienst van Het Oogziekenhuis Rotterdam, waar ik heel veel heb mogen leren over hoe je informatie beveiligt met de NEN 7510 in de hand. Gevoeliger gegevens dan gezondheidsgegevens vind je bijna niet: zowel op het gebied van privacy van patiënten, maar ook in termen van de waarde van informatie voor het primaire proces. Zonder beschikbare en integere data geen diagnose of behandeling. Na vier jaar daar ben ik nu in alweer een paar jaar in dienst bij Strict Cybersecurity. Hier vind ik de kennis en kunde om mezelf verder te ontwikkelen en help ik organisaties met uiteenlopende IT-vraagstukken op het gebied van risicomanagement, informatiebeveiliging en privacy. Op dit moment werk ik bij Schiphol als information security & risk officer en ben ik Functionaris Gegevensbescherming voor de gemeente West Maas en Waal. Mijn missie is om de wereld een stukje beter te maken door informatiebeveiliging praktisch en pragmatisch te maken, op basis van risico's onder het motto "niet lullen maar poetsen." U kunt zelf invullen waar ik tien jaar gewoond heb, voordat ik neergestreken ben in Delft. Ik word heel blij van sparren met vakgenoten en in discussie gaan over frameworks, maatregelen, kroonjuwelen en de "ethische" kant van privacy en iB. Ik krijg veel energie van het delen van kennis in presentaties en workshops en kom graag met iedereen in contact.

Ik word heel blij van sparren met vakgenoten en in discussie gaan over frameworks, maatregelen, kroonjuwelen en de "ethische" kant van privacy en iB.

Juist iB is een uitstekend instrument om bruggen te slaan tussen techneuten en beleidsmakers, tussen security-mensen en businessmanagers.

Patrick Dersjant

Ik ben Patrick Dersjant en sinds 2008 lid van het PvIB. In 1991 ben ik aan de – toen nog katholieke – Universiteit Nijmegen begonnen aan een studie beleidswetenschappen en Duitslandstudies. Niets met IT dus. Maar al hobbyend – en dat zullen veel iB-lezers herkennen – ben ik vrij vlug tóch de automatisering ingerold. En dan echt van onderaan: ik heb op diverse helpdesks gewerkt, vervolgens mezelf met uitbestedingen bezig gehouden en na een korte detacheringsperiode in 2002 bij de Rijksoverheid begonnen als Servicelevelmanager. Tien jaar geleden werd security mijn vakgebied en vijf jaar geleden kwam daar privacybescherming bij. En sinds ik in september begonnen ben als informatiemanager kijk ik weer met een bredere blik naar het vakgebied. De rode draad in al mijn functies was en is het op een goede manier inzetten van technologie ten behoeve van de gebruiker. Dat dat ook veilig moet gebeuren spreekt voor zich, maar wat dat in de praktijk betekent is al moeilijker. En weet je als techneut nog een beetje hoe het moet, wordt het voor digibeten al moeilijker. Hoe gebruik je PGP voor veilig berichtenverkeer? Is encryptie echt haarlemmerolie voor privacy-bescherming? Dat leg ik dus elke dag uit, om ervoor te zorgen dat security geen papieren exercitie voor een ISO-certificaat of in-control-statement blijft, maar bijdraagt aan het zo veilig mogelijk gebruiken van soft- en hardware. Toen Lex Dunn mij begin dit jaar benaderde voor een bijdrage aan de iB-redactie twijfelde ik dan ook geen moment. Juist iB is een uitstekend instrument om bruggen te slaan tussen techneuten en beleidsmakers, tussen security-mensen en businessmanagers. En hoewel de diepgang van de artikelen vaak uitstekend is, mag het voor mij voor de digibeet soms nog wat begrijpelijker. Daar zet ik me de komende tijd graag voor in!

PVIB: MEER SLAGKRACHT EN ZICHTBAARHEID IN 2019

Er speelt veel in ons vakgebied. Door de veranderende technologie ontstaan er steeds meer nieuwe vraagstukken. Een mooie uitdaging om daar als PvIB op in te spelen. Daarom is het belangrijk om onszelf als vakvereniging nog beter op de kaart te zetten én om onze slagkracht als ambassadeurs van ons vakgebied te vergroten.

Je bent als lid niet alleen hét visitekaartje van onze vereniging, maar ook een ambassadeur van het vakgebied.

Dankzij de tomeloze inzet van een aantal leden dat zich jaarlijks inzet zijn we vandaag de dag een succesvolle vereniging. Er blijkt alleen nog meer enthousiasme te zijn om bij te dragen aan onze vereniging. Om deze energie om te zetten in daadkracht, maken we het voor veel leden mogelijk om in een korte tijd toch iets bij te kunnen dragen. We geloven dat iedereen een steentje kan bijdragen en dat we met elkaar een hoop werk kunnen verrichten. Hoe gaan we dat doen?

Werkpakketten

We willen het komende jaar met verschillende werkvelden/projecten gaan werken. Daarbinnen worden de activiteiten opgedeeld in kleine 'werkpakketten', waar je als lid aan mee kunt doen. Door middel van deze werkpakketten kun je bijdragen aan de zichtbaarheid en de slagkracht van het PvIB in 2019.

Agile werken

We structureren dit op een 'Agile werkwijze'. Meerdere leden kunnen in verschillende trajecten (gebaseerd op hun eigen competenties) worden ingeschakeld. Niet iedereen zal evenveel tijd hebben om zich voor een lange periode in te zetten, maar dankzij deze werkpakketten kunnen leden kleine activiteiten uitvoeren. Geen vergaderingen, geen noodzaak tot langere betrokkenheid en geen nazorg. Gewoon kiezen, uitvoeren en klaar!
Aan wat voor werkpakketten kan je denken?

Lespakketten en ondersteuning onderwijs

Eén van de manieren waarop we een bijdrage kunnen leveren, is door het geven van een presentatie over informatiebeveiliging. Bijvoorbeeld op de basisschool van je kinderen of in je woonwijk. Het PvIB zal een praktisch lespakket samenstellen voor leden die dit gaan doen. Tevens hebben we toegezegd dat PvIB ondersteuning en support gaat leveren aan het MBO. Dit doen we in samenwerking met de onderwijstafel van de HSD.

Hybride leraren

Enkele hogescholen en universiteiten hebben PvIB onlangs benaderd met de vraag of er leden zijn die, naast hun eigen baan, ook een aantal dagen/dagdelen gastcolleges willen geven. Ook wel 'hybride leraren' genoemd. In 2019 willen we met een of twee hogescholen een pilot gaan draaien.

Soft skills

In 2019 willen we ook, samen met onze leden, meer aandacht besteden aan specifieke skills. Deze skills worden niet altijd primair genoemd binnen ons vakgebied, maar zijn wél van belang om effectief te werken. Te denken valt aan schrijfvaardigheid, presentatie en communicatie- en adviesvaardigheden.

Ambassadeurs

In Cybersecuritybeeld Nederland 2018 (CSBN 2018) van de NCTV staat: 'Er is sprake van een continue digitale dreiging voor de nationale veiligheid. De Nederlandse maatschappij en economie zijn volledig afhankelijk geworden van digitale middelen. De gevolgen van aanvallen en uitval kunnen groot en zelfs maatschappij ontwrichtend zijn'.

Je bent als lid niet alleen hét visitekaartje van onze vereniging, maar ook een ambassadeur van het vakgebied. En als ambassadeur willen wij graag activiteiten in 2019 ondernemen die het maatschappelijk belang ondersteunen. Dit gaan we organiseren middels verschillende projecten met elkaar en in samenwerking met het onderwijs, private en publieke sector.

Artikel schrijven

Andere projecten waar je aan kunt denken, zijn: het schrijven van een recensie van een boek of congres, een uur lesgeven op een MBO, een Roundtable organiseren en het begeleiden of het schrijven van een artikel, column of expertbrief.

Inschrijven

De trekker van de Agile-werkwijze is Evert van Zanten, voormalig voorzitter van de commissie Kennis & Innovatie. In het eerste kwartaal van 2019 verschijnt er op de site van het PvIB een aparte pagina waar iedereen zich kan inschrijven voor een project. Houd deze dus goed in de gaten!
Heb jij nog aanvullende ideeën, opmerkingen of over de projecten? Schroom dan niet om contact met ons op te nemen via jessicaconquet@pvib.nl.

VIER MANIEREN OM SECURITY-RESULTAAT TE VERKNALLEN!

In de aanloop naar het Oud en Nieuw vuurwerk 2018 noem ik vier manieren om security-resultaat te verknallen:

1. **Onderschat de aanvalskracht van je tegenstander.**
2. **Overschat de kracht van je eigen verdediging.**
3. **Denk te makkelijk over security als vak.**
4. **Doe te moeilijk richting je security-personeel.**

Bij elke manier doe ik een suggestie voor een "goed voornemen" voor het komende jaar 2019 (en verder natuurlijk).

1. Onderschat de aanvalskracht van de tegenstander

De cybercriminelen hebben als aanvallers hun duistere zaakjes beter georganiseerd dan de verdedigers aan de security-kant. De boeven werken onderling meer samen, ook wereldwijd, en hebben meer en betere kennis die ze vaker met elkaar delen. Gratis of in ruil weggeven via dark web fora, of zelfs verkopen aan elkaar via CAAS (Crime As A Service). Er wordt ook verkocht aan of geruild met zeer ruimdenkende veiligheidsdiensten van nation states (black hat hacking as a service). Als je vandaag als security-specialist denkt: "Deze encryptie is weliswaar te kraken, maar alleen door veiligheidsdiensten en daarvan hebben we niets te vrezen", dan sus je jezelf in slaap. Want die kraaktechniek is morgen – of hooguit overmorgen – ook beschikbaar voor criminelen. Geheime diensten passen overigens ook steeds vaker technieken toe die eerder alleen door criminelen werden gebruikt.
En hackingtechnieken uit andere landen of continenten zijn veel gemakkelijker te exporteren en elders te implementeren dan security-maatregelen. De criminelen voelen zich immers in hun werkwijze, organisatie en informatie-uitwisseling niet gehinderd door zoiets als privacy-wetgeving. En doordat criminele bendes het begrip 'deadline' soms letterlijk toepassen, motiveert dit hun betaalde (of gedwongen) leveranciers in hevige mate om de toegezegde deliverables op tijd en binnen alle verwachte kwaliteitseisen op te leveren. Verder zijn aan de misdaadkant de beschikbare budgetten in het algemeen hoog, want voor de aanvallers is een zwakke security bij hun tegenstander een bron van opbrengsten. Hun investering in een aanval levert vrijwel zeker meer geld op. De cybercriminelen hadden het in eerste instantie gemunt op bijvoorbeeld banken om daar geld te stelen, als in een digitale bankroof. Maar via inzet van ransomware worden door middel van chantage of afpersing ook andere bedrijven, organisaties of zelfs particulieren slachtoffer. Via phishing-mails of misbruik van websites voor dating en vacatures worden met behulp van social engineering mensen overgehaald om 'vrijwillig' geld over te boeken aan de criminelen. Oplichting dus. En ook afdelingen die gewend zijn aan uitbetalen, zoals salarisadministraties en crediteurenafdelingen, zijn in elke organisatie een (theoretisch) interessant doelwit omdat ze nu eenmaal een uitgaande geldstroom hebben. Door de grote en groeiende groep aanvallers, die onderling samenwerken, groeit het risico voor een organisatie, zeker als die slechts beducht is voor één aanvallersoort.

Advies: *probeer voortdurend de TTP (tools, techniques, procedures) van de groep tegenstanders zo goed mogelijk in kaart te brengen en wapen je daartegen.*

2. Overschat je eigen verdedigingskracht

"Ken de vijand en ken uzelf, en u kunt 100 slagen vechten zonder nederlaag", zei Sun Tzu en hij kon het weten, want hij was een succesvolle Chinese militaire strateeg. Het gaat er dus niet alleen om threat intelligence (inlichtingen) over de vijand te hebben, maar ook informatie over jezelf en je eigen verdediging is noodzakelijk om de oorlog niet te verliezen. En die informatie moet volledig en juist zijn. Helaas schort het daar in security-land een enkele keer aan. Je weet dan niet alle zaken die je eigenlijk wel zou moeten weten, en wat je wel 'weet', is niet altijd juist. Thuis heb ik onder andere twee Windows 10 computers en eentje met Windows 7 die vrijwel de hele maand ongebruikt en uitgeschakeld in de kast staan. Elke maand ben ik op Patch Tuesday een groot deel van de dag (weliswaar naast andere activiteiten) bezig met het downloaden en installeren van patches en tussendoor

Robert Metsemakers is als ervaren IT auditor en informatiebeveiliging expert beschikbaar voor security advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

opnieuw starten van die computers. Aan het eind van zo'n dinsdag kan ik dan wel naar waarheid zeggen: "mijn machinepark is 100% gepatcht en up-to-date". Maar als je in je organisatie 400, 4.000 of nog meer machines hebt, krijg je dat natuurlijk niet in één dag af. En dan is het, op een moment dat malware zoals Petya (klinkt als 'patched', want voor de daar misbruikte kwetsbaarheid was al lang een patch beschikbaar) uitbreekt, jammer genoeg niet meteen duidelijk hoeveel nog-niet-gepatchte machines in je organisatie in potentie gevaar lopen. Bovendien, als je heel veel machines in gebruik hebt, zijn er altijd wel bijzondere projecten zoals pilots, waarin de betreffende gebruikers reeds Windows 10 hebben, terwijl de rest van de organisatie nog op Windows 8 zit. Of dat op een klein aantal servers Windows XP 'moet' blijven draaien vanwege bepaalde onmisbare legacy-software die alleen op dat oudere operating system werkt. Of de organisatie staat toe dat gebruikers hun eigen telefoon of tablet mogen gebruiken om bedrijfsinformatie te benaderen, maar het is lastig af te dwingen dat ze die eigen machines voortdurend bijwerken met (security) patches. Wanneer ze het niet bijhouden, kun je dat weliswaar bij het verbinden zien en hen daarom de toegang tot die data ontzeggen. Maar dan kunnen ze hun werk niet doen en geef je als werkgever nutteloos hun salaris weg. Je hebt daarom bij een groter machinepark misschien wel vier of vijf verschillende patch-percentages tegelijk nodig, namelijk voor elke omgeving of netwerkdeel apart. Ze zullen trouwens waarschijnlijk ook nog onderling verschillen en elk in een ander tempo veranderen.

Je weet met andere woorden als aangevallen of – als collatoral damage – kwetsbare partij in de meeste gevallen niet volledig over je eigen situatie wat je eigenlijk wel zou moeten weten voor een totaalbeeld. En dat totaalbeeld is nodig om de juiste tegenacties te bepalen en in die verzameling vervolgens hun onderlinge prioriteit en volgorde als verdedigingsmaatregelen te bepalen. Bijvoorbeeld: wat is het patch-niveau van software op onze werkplekken, op de servers, op de laptops en op de BYOD-apparaten die in eigen beheer van de medewerkers zijn? Deels is dit een probleem van alle tijden, want je kunt nu eenmaal niet alles weten. Of: het is te duur om alle denkbare informatie te registreren en verzamelen, dus wordt er een keuze gemaakt.

'Meten is weten', maar aan de andere kant: je krijgt (alleen) wat je meet! Zeker wanneer je het meten beperkt tot enkele KPI's (Key Performance Indicator). De mens is nu eenmaal een economisch wezen en streeft dus naar maximalisatie van de opbrengst bij een bepaalde inspanning, of naar minimalisatie van de inspanning om het vooraf bepaalde doel te bereiken. Dit economische uitgangspunt gebruiken veel mensen die geld willen verdienen bij het bedenken wat ze nou vandaag weer eens zullen gaan doen op het werk. Als je de beloning voor je medewerkers bijvoorbeeld afhankelijk maakt van het aantal in een periode opgeloste IT audit issues, is er een tendens om veel kleine issues op de actielijst te plaatsen. Waarvan dan een hoog percentage in korte tijd wordt opgelost. Wordt men aan de andere kant afgerekend op een laag aantal openstaande IT audit issues aan het eind van een periode, is de neiging juist om een beperkt aantal grote issues te formuleren. Die dan vaak bestaan uit meerdere onderling afhankelijke issues, welke uit de aard der zaak slechts zeer langzaam (of zelfs nooit) volledig worden opgelost.

Sinds mijn eerste college Administratieve Organisatie, waar het ook ging over de zojuist genoemde (menselijke) tendensen, ben ik daarom een enthousiast voorstander van functiescheiding. Dat wil zeggen dat degene die registreert wat de status van bijvoorbeeld het patchen is, een andere persoon is dan degene die verantwoordelijk is voor het uitvoeren van de activiteit (het patchen zelf). Functiescheiding verbetert de betrouwbaarheid van de gerapporteerde gegevens. Organisaties die – om wat voor reden dan ook – meerdere taken bij één functionaris beleggen, lopen een risico dat die persoon de bereikte status of uitgevoerde activiteiten te rooskleurig (of op een andere manier foutief) presenteert. Ik heb het hier natuurlijk niet over uw organisatie beste lezer, maar bedoel alle andere bedrijven en organisaties in de wereld.

Een te sterke focus op slechts een beperkt aantal KPI's kan er naar mijn mening toe leiden dat de andere zaken onvoldoende aandacht krijgen van de medewerkers. Daardoor kan de informatie over de verdedigingskracht onvolledig zijn. Op het marineschip is dan het dek blinkend gepoetst en de ankerketting is voortreffelijk opgerold, zodat niemand erover kan struikelen. Het vaartuig is op tijd feestelijk gepavoiseerd (= met seinvlaggen versierd), maar onderdeks is er van alles loos omdat de bemanning daar niet óók nog tijd en aandacht aan heeft besteed.

Wanneer een organisatie zoals dat in georganiseerde bendes gebeurt (zie paragraaf 1) heel letterlijk 'afrekent' met onvoldoende presteerders door ze met veel spektakel uit de organisatie te verwijderen, versterkt dit de tendens van 'zaken te rooskleurig weergeven'. Naar mijn idee is dit ingebakken in het menselijke DNA en wordt dit ongewenste gedrag onder druk alleen maar erger. Daar waar je dus in de meeste gevallen onvolledig bent in alle informatie die je over je eigen situatie zou moeten hebben voor een goede verdediging, is dan wat je wel meet helaas ook nog eens onjuist voorgesteld. Vaak te positief, al helpt het principe van functiescheiding tussen beschikken, uitvoeren, bewaren, registreren en controleren overigens óók bij het vermijden van een te negatieve weergave, zoals dat optreedt bij zwart geld betalingen of een 'zaak-in-de-zaak'. Als voorbeeld: een barkeeper

Security als vak is moeilijker dan je denkt en dat geldt op strategisch, tactisch en operationeel niveau

brengt een zelfgekochte fles whisky mee naar zijn werk, die hij per glas voor normale prijzen verkoopt aan uw klanten – terwijl ze genieten van de barkrukken, toog, muziek, verlichting en verwarming die u als café-eigenaar heeft betaald – en steekt daarbij de opbrengst in eigen zak. Die omzet had u liever zelf in de boeken gehad!

Advies: *laat de kwaliteit van de eigen verdediging breed, frequent en door onafhankelijke personen meten om zo volledig en juist mogelijk te zijn.*

3. Denk te gemakkelijk over het vakgebied security

Security als vak is moeilijker dan je denkt en dat geldt op strategisch, tactisch en operationeel niveau.
Op strategisch niveau noemt de Amerikaanse security specialist Dan Geer in zijn lezingen security het moeilijkste vak ter wereld, terwijl men meestal rocket science en hersenchirurgie als bijzonder moeilijk en ingewikkeld ziet. Maar daar zijn de te behandelen onderwerpen al miljoenen of honderdduizenden jaren hetzelfde! De zon heeft er verder geen financieel belang bij om de onderzoeker voor de gek te houden. De natuurwetten gaan zich niet anders gedragen doordat een wetenschapper er naar kijkt. Een patiënt kan niet snel zijn bloedgroep veranderen terwijl er bij hem/haar een bloedproef wordt genomen. Een cybercrimineel kan dat allemaal wel en heeft er ook een groot belang bij, omdat hij/zij wil doorgaan met de illegale activiteiten. Een patiënt wil snel genezen. De ontwikkelingen in de IT gaan bovendien vele malen sneller dan de ontwikkelingen in het heelal (een nieuwe planeet of ster is er niet zomaar 1-2-3) of in het menselijk lichaam. Security moet als vakgebied dus veel sneller mee ontwikkelen met die IT dan dat chirurgen moeten meebewegen met ontwikkelingen in de menselijke hersenen.
Tactisch niveau zie ik als het vertalen van het security-beleid naar concrete maatregelen en projecten. Daarbij is het lastig dat veel security-beleid, vanwege de eraan verbonden risico's, bepaalde handelingen of gedrag compleet verbiedt of ze alleen toestaat onder strenge, beperkende voorwaarden. Geen onversleutelde USB-stick of webmail gebruiken om vertrouwelijke bedrijfsinformatie het pand uit te krijgen. Parkeren van meegebrachte auto's alleen in de op de grond geschilderde parkeervakken. Roken mag, maar alleen buiten en het telt niet als arbeidstijd. Op zich zijn dat begrijpelijke, duidelijke en te verdedigen voorschriften, maar het is toch goed om periodiek te controleren of de medewerkers zich er inderdaad aan houden. Of tenminste, welk percentage van de medewerkers dat wel doet! Dat blijkt in de praktijk nog best veel (extra) werk, zo precies bijhouden hoeveel medewerkers zich aan de redelijke afspraken houden…
Een ander voorbeeld: toegang verlenen tot een mobiele app met een wachtwoord (dus zonder tweede factor zoals een token) mag, maar alleen als dat wachtwoord, door de lengte en ingewikkeldheid ervan, voldoende moeilijk via een brute force aanval te raden is. Dit terwijl de business juist vraagt om een gemakkelijke oplossing. Ja, ze weten nu wel dat cloudgebruik security-risico's in zich draagt, maar ze willen die 'computer van iemand anders' toch gebruiken, soms zelfs als 'shadow IT'dus geheel buiten het medeweten of de bemoeienis van de IT-afdeling om. Ze zijn wel bereid om klanten een wachtwoord te laten gebruiken, maar dan wel een simpele. Eentje van vier cijfers en de klant hoeft deze slechts één keer per jaar te veranderen en mag deze ook op 9999 zetten en een minuut later weer de oude code instellen. Toegegeven: niet alle gebruikers zoeken zo de rand en de mazen van het security-beleidsnet op, maar sommige helaas wel en daar ben je dan de hele dag mooi druk mee als security officer annex business-enabler.
Op operationeel niveau is security moeilijk omdat de verdediger nu eenmaal altijd in het nadeel is. Per definitie kan hij/zij alleen reageren op het initiatief (de aanval) van de aanvaller. De verdediger moet in de spreekwoordelijke voetbalwedstrijd voortdurend waakzaam zijn en de aanvaller hoeft slechts kort te pieken. Want in één qua aandacht gemiste minuut kan de verdediger (zoals een keeper) de voetbalwedstrijd verliezen, en een aanvaller (zoals de spits van de tegenpartij) kan in slechts één geslaagde minuut de voetbalwedstrijd winnen. Verder is de operationele laag veel breder en er zijn dus meer mensen betrokken dan in de strategische en tactische laag. Dus moeten er ook meer mensen gemotiveerd en gestimuleerd worden om tot gedragsverandering te komen. In veel organisaties is het zo, heb ik gehoord en gelezen, dat een beperkt deel van de medewerkers security héél belangrijk en interessant vinden: de leden van die groep werken allemaal op de afdeling Security. Dan is er een groep medewerkers die security ook tamelijk belangrijk en

Men kan ze 'nerds' noemen en dat vinden ze niet eens een scheldnaam

interessant vinden: dit zijn de personen die erover praten bij de koffie-automaat en die met mails en posts op intranet reageren op de security awareness posters gericht op infomatiebeveiligingsbewustzijnsverhoging (te lang voor Scrabble). En dan is er nog een grote groep medewerkers die security juist onbelangrijk vindt, die er mogelijk zelfs een hekel aan heeft en nog belangrijker, er nauwelijks iets aan doet. Dit maakt het inherent moeilijk om de door de kleine groep 1 bedachte maatregelen door de grote groep 3 uitgevoerd te krijgen. Hoe goed groep 2 als 'leading coalition' daarbij ook meehelpt door het geven van positief commentaar of hoe welwillend zij de security-acties 'gedoogt' door juist geen negatief commentaar te geven.
Naarmate security stap voor stap, van beleid via maatregelen naar concrete acties, de operationele laag bereikt, wordt het dus veel meer werk en dat maakt het ook moeilijker uit te voeren. Denk aan wat je na een (bijvoorbeeld CISSP) examen zegt: "Het was niet moeilijk, maar vooral véél". Ook dijt het werkveld nog steeds uit. De oude security-risico's gaan niet weg en behoeven nog steeds tijd en aandacht. Zoals 'social engineering', gericht op het hacken van de mens als zwakste schakel in de totale security-keten. Of 'dumpster diving', gericht op het door de aanvaller verzamelen van onnadenkend door medewerkers weggegooide maar nog steeds leesbare informatie. Maar er komen wel steeds nieuwe risico's en nieuwe soorten en nieuwe voorbeelden van bestaande soorten malware bij, die allemaal óók aangepakt zullen moeten worden. Het speelveld wordt dus steeds breder. En de security-professional die de mogelijke risico's van nieuwe activiteiten in kaart moet brengen, heeft daarmee een steeds langere lijst van zaken die in het verleden al zijn gebeurd, in de eigen organisatie of elders, om uit te kiezen en dus aan te vinken op de security-checklist. Zodat het speelveld ook langer wordt. Met – in veel organisaties – een gelijkblijvend of zelfs dalend aantal spelers in het team dat het spel moet spelen.

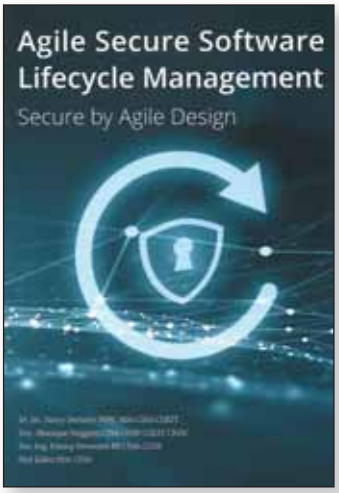
Advies: *bedenk bij het vaststellen van plannen, ambities en doelen in security dat Keulen en Aken ook niet in één dag zijn gebouwd.*

4. Doe te moeilijk richting je security-personeel

Managen van personeel vraagt altijd tijd en aandacht. Echter, het managen van security-personeel is misschien wel moeilijker dan van 'gewoon'(u snapt wat ik bedoel) personeel. Goed security-personeel binnenhalen en tevreden houden is lastig.

In de groep IT-personeel zie ik meer introverten of autisten dan op andere afdelingen. Ook meer hoogbegaafden (Bill Gates, Steve Jobs), met bijzondere hobby's (bergbeklimmen en dat als Nederlander!), afwijkende favoriete muzieksoorten (schlagers, hardrock), excentrieke kledingstijlen (zwarte T-shirts, vaak met prikkelende teksten) en opvallende haardrachten (schouderlang, dreadlocks of ingeschoren Mickey Mouse figuren). Bij security-afdelingen is dat percentage soms zelfs nog hoger dan op andere IT-afdelingen. Men kan ze 'nerds' noemen en dat vinden ze niet eens een scheldnaam. Ze werken met passie in een voor de buitenwereld onduidelijk en vaak ook oninteressant werkgebied. Onder voortdurende tijdsdruk, altijd reagerend op onverwachte aanvallen, datalekken, responsible disclosure meldingen, bedieningsfouten van andere medewerkers en achteraf ontdekte fouten in software die met grote spoed, maar wel foutloos moeten worden gepatcht (zie paragraaf 2).
Voor zover security-specialisten (of generalisten) niet al vanaf de wieg 'anders' zijn, beïnvloeden deze omstandigheden op den duur hun manier van werken. Met andere woorden: deze 'nerds' moeten op een andere manier gemanaged worden, dat vergt maatwerk en is dus tijdrovend voor leidinggevers. 'Micromanagement', zoals het zeer strikt laten naleven van 'regeltjes' waarvan het nut door de nerds in twijfel wordt getrokken, werkt hier vaak averechts. In het algemeen zijn het gemotiveerde professionals, met een passie (of zelfs roeping) voor het vak, die vanuit zichzelf hun werk zo goed mogelijk willen doen, aldus Mathieu Weggeman, die zijn interessante managementboek samenvat in de titel.

Advies: l*ees daarom, als leidinggevende of leidingontvanger, Mathieu Weggeman - "Leidinggeven aan professionals? Niet doen!".*



BOEKREVIEW

Titel: Agile secure software lifecycle management
Ondertitel: Secure by agile design
Schrijvers: dr. Iec. Barry Derksen MMC Msc CISA CGEIT
drs. Monique Neggers CISA CISM CGEIT CRISC
drs. Ing. Danny Onwezen RE CISA CISM
Stef Zelen Msc CISA
Taal: Engels
Aantal pagina's: 80
ISBN-nummer: 978-90-817866-2-1
NUR-code: 100

Soms verrast een boek je. En dit is er zo een. Je verwacht een droog, dor boekje over veilige software ontwikkeling en je krijgt een vlot leesbare tekst waarbij de schrijvers de moeite hebben gedaan om een heldere inleiding te schrijven. Elke gebruiker van software gaat er eigenlijk min of meer van uit dat deze veilig te gebruiken is. Of omdat het gekocht is bij een grote partij als Microsoft ("… dan zal het toch wel goed zijn? Iedereen gebruikt het.") of omdat … tja, waarom eigenlijk? In dit boek komt dit 'waarom' uitgebreid aan de orde. De nadruk ligt hierbij op het managen van de levenscyclus van veilige software op lenige, flexibele wijze. Het is een alternatieve methode voor programmamanagement ontstaan in de jaren 90. Het is een afzetten tegenover het traditionele projectmanagement volgens de 'Waterfall' methodiek. Het essentiële verschil zit hem in de korte tijdlijnen, het betrekken van de klant bij de ontwikkeling, kleine teams en meerdere 'sprints' (elke sprint 2 tot 3 weken lang) bij toepassing van de 'agile secure software lifecycle management'. Belangrijke, filosofische uitgangspunten: Scrum (oftewel leren door doen) en DevOps (samentrekking van 'Development' en 'Operations' met als doel de samenvoeging van software development en -operaties). Het mooie is dat in dit boek niet alleen de theorie wordt besproken, maar, door de in het boek toegepaste 'Sprints', ook de toepassing in de praktijk aan bod komt, vermoedelijk zelfs bij de realisatie van dit boek. Dit zowel door de beperkte omvang in pagina's alsook door de heldere uiteenzetting in de verschillende 'sprints' (lees hoofdstukken). De lezer(es) wordt slim en aanschouwelijk meegenomen in het belang en de wijze van deze ICT-veiligheidsaanpak.
Hij/zij krijgt in deze 80 pagina's een snelcursus met behoorlijke diepgang in methodiek en belang van software veiligheid. Niet alleen als een gedachte achteraf, maar juist vanaf de start bij de ontwikkeling van de software. De methodiek wordt gekaderd in het 'Secure Software Framework' (is de controle over veiligheidskennis en het nastreven / noodzaak van bestaan van een goed gefocust ontwikkelproces) bestaande uit de vier hoofdaspecten t.w.: vereisten ('requirements'), bedreigingen ('threats'), invoering ('implementation') en verificatie ('verification'). Het boek sluit af met verwoording van de overheidsvisie over de weg welke partijen (bedrijven (groot & klein), software ontwikkelaars, overheden (nationaal & internationaal) enz. met elkaar moeten bewandelen om te komen tot digitale hard- & software veiligheid. Als de pilaren daartoe worden geformuleerd:

- standaard veiligheidsvereisten;
- contact momenten en
- interne 'Secure Software Development (SSD)' processen bestaande uit: risico's in beeld houden, veiligheidsvereisten handhaven en organisaties te brengen tot hogere volwassenheidsniveaus.

Al met al een aanrader voor al diegenen die een goed overzicht willen verkrijgen met betrekking tot dit thema.
Eindoordeel: vette 8

CISO-24

Voor de liefhebbers verwijs ik graag nog naar de recente CISO-24 bijeenkomst waar het thema aan de orde kwam: 'Agile in control' met als presentatoren Brian Teunissen & Michel Zandbergen. Hun presentatie sloot toevallig erg mooi aan bij dit boek, waarbij bij als verrijkingen aan de orde kwamen:

- het structurele verschil tussen de Angelsaksische denkwijze en het Rijnlands denken, waarbij een lans voor het laatste gebroken werd;
- de grotere vrijheid welke met 'agile' wordt ervaren (grotere autonomie en volwassenheid);
- de samenhang van 'Agile & Scrum' in de praktijk.

Tijdens deze CISO-bijeenkomst is met name ook ingegaan op de invloeden die uitgeoefend worden op de kwaliteit & de volwassenheid van Scrum teams. Uitgangspunt is het denken in effectiviteit boven denken in efficiëntie. Interessant vermeld nevenbegrip: technische schuld (= niet gebouwd volgens architectuur code, maar wat toekomstig tot (veiligheids)problemen zou kunnen leiden). Voor diegenen die ook met praktijkmensen van gedachten willen wisselen; een aanrader om deze presentatoren eens te benaderen.

Auteur: Chris de Vries

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.

ACHTERDEUR PROBLEMATIEK

Uit een onderzoek van Bloomberg kwam afgelopen kwartaal naar voren dat Chinese spionnen de hardware van fabrikant Super Micro van achterdeurtjes zouden voorzien door kleine chips aan het ontwerp toe te voegen. Onderzoek van een aantal grote Tech bedrijven leidde niet tot bewijzen die de claim van Bloomberg onderschreven. Maar dat kon de onrust die bij velen is ontstaan niet wegnemen.

Zijn hardware backdoor risico's waar we vandaag de dag als organisaties rekening mee moeten houden? En wat kun je als organisatie doen om te voorkomen dat je het slachtoffer wordt van dit soort kwetsbaarheden of om de kans op misbruik via hardware kwetsbaarheden te verkleinen?

Maarten Hartsuijker

Standaard installateurswachtwoorden, voorspelbare of afleidbare WPA-keys, niet gedocumenteerde API's, gewhiteliste IP-adressen, "magische" request strings in software… we kennen de voorbeelden allemaal. Achterdeurtjes zijn van alle tijden. Vaak zijn ze aangebracht om toegang voor servicepersoneel te vergemakkelijken. En wordt de kans dat kwaadwillenden die toegang ontdekken en misbruiken gemarginaliseerd en het risico op misbruik weggeredeneerd. We weten inmiddels allemaal beter: achterdeurtjes worden continu gevonden en misbruikt. Maar een verhaal als dit is natuurlijk van een hele andere orde. Los van het waarheidsgehalte van het bericht is het interessant om te zien dat niemand eigenlijk meer verbaasd is als het waar blijkt te zijn. Nationale communicatie-infrastructuren zijn voor inlichtingdiensten al een vanzelfsprekend middel geworden om hun werk te doen. Dus waarom zou dat voor de supply chain ook niet het geval zijn? Het is normaal aan het worden om de communicatie van iedereen te tappen. Inlichtingendiensten zijn als de visserij: gericht vissen is inefficiënt, dus bijvangst is de regel in plaats van de uitzondering. En als je verantwoordelijk bent voor het onderscheppen van informatie en je merkt dat er steeds meer versleuteling plaatsvindt, dan is het niet gek dat je op zoek gaat naar de plekken waar de informatie nog wel eenvoudig zichtbaar is: zoals de endpoints en de cloud. Daarnaast weet je dat je niet de enige bent die op dit idee komt. Dus als je je nationale infrastructuur wilt beschermen, heb je vanzelfsprekend, bij voorkeur in de vitale infrastructuur, hardware in gebruik van leveranciers waar je zelf grip op hebt. En als je een grote IT-economie bent, heb je er wellicht baat bij dat het vertrouwen in de producten van andere economieën afneemt.

Maar wat doe je hier als doorsnee bedrijf aan? Sturen we vanaf morgen onze beste ingenieurs naar de productie- en


Maarten Hartsuijker


Lex Dunn


Tom Bakker


Fook Hwa Tan

assemblagelijnen bij spionagegrootmachten als China en de VS om in de gaten te houden of de afgenomen hardware betrouwbaar is? Dat is natuurlijk onhaalbaar. Verbindingen monitoren op onbekend verkeer lijkt hier de meest passende maatregel. Maar waarvandaan importeren we die oplossingen eigenlijk?

Lex Dunn

Even afgezien van de gang van zaken rondom het onderzoek van Bloomberg, is het risico van hardware backdoors wel degelijk aanwezig in vele apparaten. Vroeger hadden we de console poorten en RS-232C (seriële) poorten op veel apparatuur (deze tref je nog steeds vaak aan op OT/SCADA-systemen), waarmee je over het algemeen bijzonder snel in staat was om desastreuze handelingen op het betreffende apparaat te verrichten. En dat is vandaag de dag nog niet anders. Wat denk je van de grote hoeveelheid USB poorten op computers, tablets en mobiele telefoons? Meestal kun je vanaf die poort met speciale commando's een heleboel doen, want die poort wordt tijdens het fabricage proces ook gebruikt voor het testen van het apparaat. Maar ook als je een apparaat openschroeft, kom je goed bruikbare ingangen tegen. Op veel motherboards zit een debug poort, primair ook weer bedoeld voor testen tijdens fabricage, of tijdens reparatie, maar vaak ook goed bruikbaar voor malafide acties. Er is echter wel een groot verschil met de door Bloomberg beschreven extra chips in apparatuur (even afgezien van of het nou wel of niet waar is): deze chips zijn weliswaar hardware, maar ook via software op afstand te benaderen. En dat is een groot verschil met de bovengenoemde poorten, want om die te misbruiken heb je nog steeds fysieke toegang tot de apparatuur nodig. Het lijkt er dus op dat het risico van hardware backdoors alleen maar groter is geworden, ondanks de ontkenningen van Apple en anderen.

Tom Bakker

Er zijn vele softwarematige hacks geweest die zwakheden hebben gebruikt in zowel applicaties als besturingssystemen. Zo langzamerhand worden, als het goed is, wel preventieve en detectieve maatregelen getroffen. Dan is het logisch dat na de software zwakheden nu naar mogelijkheden wordt gekeken om hardware te misbruiken. Zo had je al de Intel-processoren problemen die recentelijk aan het licht kwamen.
Er van uitgaande dat het klopt wat Bloomberg heeft gemeld, hebben we nu te maken met staat actoren als China die geprobeerd zouden hebben met verborgen chips een achterdeur te laten inbouwen. Dat is niet echt verrassend. Het zou mij overigens niet verbazen als de Amerikanen dat ook (zouden willen) doen. Het interessante van deze kwestie is wel hoe men het voor elkaar heeft gekregen die zaken erin te krijgen. Dat kan toch niet zomaar ongemerkt bij de fabricage gebeuren? Dus die lui moeten ervan af geweten hebben. De uiteindelijke leveranciers/opdrachtgevers doen blijkbaar geen controles op het geleverde van onderaannemers. Wat kun je ertegen doen? Da's lastig. Om te beginnen monitoren op ongebruikelijk netwerkverkeer. De afgetapte data zal toch ergens heen moeten. Maar monitoren doe je toch al, niet? Dat zou in ieder geval een indicatie kunnen zijn dat er iets mis is. Controle van motherboards dan maar? Een extra chip detecteren die daar niet thuishoort? Lijkt mij lastig worden als er een chip zit die op die plaats hoort te zitten en er vertrouwd uitziet, maar blijkbaar iets anders doet dan de bedoeling is. Ik zou de oplossing nu niet weten. Wat ik wel weet is dat we dit wel vaker zullen gaan meemaken.

Fook Hwa Tan

Na het horen van het onderzoek van Bloomberg was er een hoop rumoer in de wereld. Mensen begonnen angstig te worden dat iedereen mee kon kijken met wat zij aan het doen waren. Ondanks dat veel mensen zeggen dat ze niets te verbergen hebben, is het natuurlijk ook zo dat elk individu het recht heeft op zijn of haar privacy. Waarom zou je dan nog backdoors willen hebben? Veel backdoors worden door ontwikkelaars tijdens het ontwikkelproces in software gebouwd om gemakkelijker onderdelen van software te kunnen testen zonder telkens te moeten inloggen. Kunst hierbij is wel, dat deze shortcut bij in productiename wordt verwijderd. Het is mogelijk zelfs nodig om additioneel aandacht te geven hieraan. Ook zijn backdoors handig voor rechtshandhavers, die er bij het onderzoeken van een misdrijf baat bij hebben om toegang te hebben tot gegevens op gegevensdragers. In veel opzichten wil iedereen dit ondersteunen om criminaliteit tegen te gaan. Het wordt echter wel weer lastig, wanneer het gaat om je eigen gegevensdragers die zonder je medewerking gelezen kunnen worden. Verder zien we ook vaak dat backdoors nuttig zijn wanneer gebruikers hun authenticatiegegevens kwijt zijn geraakt en toch bij hun informatie willen komen. Hier krijg je eigenlijk weer hetzelfde als het voorgaand punt, dat gebruikers het niet erg vinden als het uitkomt. Maar wel wanneer dit wordt misbruikt of zonder medeweten wordt gedaan. Als conclusie kun je zeggen, dat mensen backdoors niet willen, maar dit mogelijk wel nodig achten in bepaalde situaties. Backdoors zijn dus zeker een risico! De enige oplossing die helpt om er achter te komen of het nieuws van Bloomberg waar of niet waar is, is om verkeer van en naar hardware continu te monitoren!

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
Tom Bakker
Bianca Brooijmans
Patrick Dersjant
Nicole van Deursen
Rik van Dijk
Lex Dunn
Maarten Hartsuijker
Lilian Knippenberg
Hugo Leisink
Rachel Marbus
Fook Hwa Tan
Chris de Vries

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

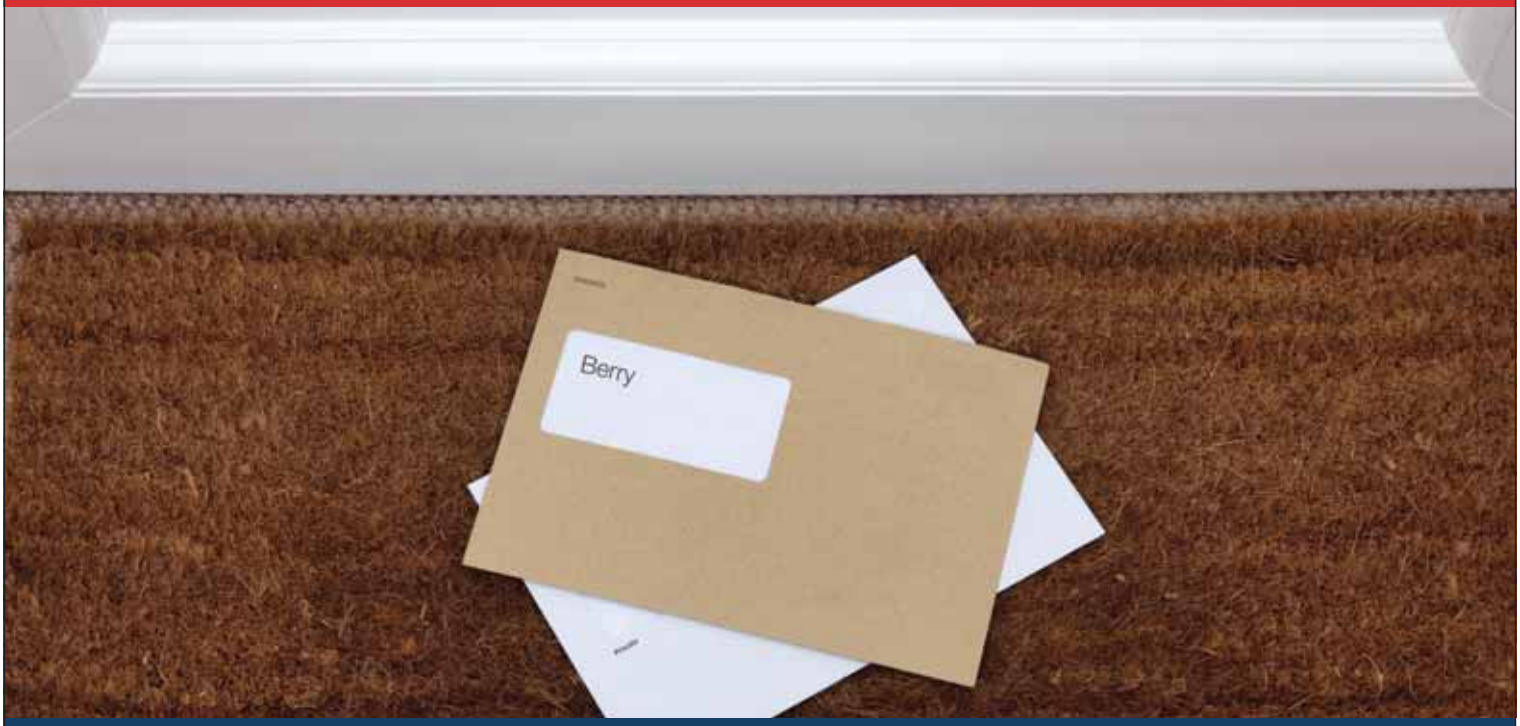
DRUK
VDR druk & print

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

ABONNEMENTEN
De abonnementsprijs in 2018 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063



NIET TE BELLEN, BEN BUITENSHUIS

Ik zat laatst even met mijn zoon te kletsen die mij vroeg waarom ik nog een huistelefoon had. Ik keek hem aan en moest even nadenken over zijn vraag. Ik besluit uit te leggen waarom ik een vaste telefoon heb. 30 jaar geleden werd het ineens populair om een draagbare telefoon aan te schaffen. De term draagbaar is een rekbaar begrip, want je moest destijds wel een redelijke stationwagon hebben om hem mee te nemen. "Maar jullie hadden buitenhuis geen telefoon?" was de volgende vraag. Dit had de neiging een lange zit te worden, dus schonk ik nog maar een rondje in. Geen telefoon betekent niet alleen dat je niet bereikbaar bent buiten de deur, maar ook geen navigatie, geen fototoestel, geen internet, geen agenda, geen mail, helemaal niks. Hij probeerde zich in te denken wat dat betekende en je zag hem in zijn denktocht verder en verder verdwalen. Ik gaf aan dat er nog steeds mensen zijn die een leven zonder smartphone willen hebben. Ik vervolgde door aan te geven dat er nu mensen in Nederland wonen die geen smartphone, tablet, pc of laptop hebben, omdat ze dat niet nodig vinden. Die hebben geen idee wat het betekent dat je userid is gehackt. Ze houden hun ogen op de weg in de auto en op de fiets. Als ze op visite komen, hebben ze niet een half oog op hun telefoon gericht, hoeven ze hun e-mail niet te checken, krijgen geen appjes, kijken niet hoeveel accu de telefoon nog heeft. Ze lopen wel een keer per dag naar de voordeur om te kijken of de postbode al langs is geweest. Het klinkt wel heel relaxt, maar kunnen we nog op een normale manier functioneren zonder al die hulpmiddelen? Kan ik het verkopen aan mijn baas dat hij mij `s avonds alleen kan bereiken als ik thuis ben en als mijn vrouw niet belt? Is het uit te leggen dat ik alleen via brievenpost te bereiken ben? Zou mijn bank nog opdrachten uitvoeren? Zou het UWV mijn uitkering wel uitbetalen? Veel mensen die bewust een leven kiezen zonder pc of andere middelen doen dat onder andere omdat iedere website of instantie een eigen userid en password vereist, overal andere eisen aan wachtwoorden stellen en als gebruiker heb je werkelijk geen idee of de omgeving wel een beetje beveiligd is. De overheid stelt alleen DigiD beschikbaar, maar dan ook alleen voor overheidsdiensten en DigiD is natuurlijk verschrikkelijk achterhaald. Mijn password is al 10 jaar niet ververst bij DigiD en maar niet te spreken over de overgevoeligheid op DDoS-aanvallen van de DigiD dienst en het daardoor verlammen van veel (overheids)diensten. Overheid, pak je verantwoordelijkheid en ontwikkel nu eindelijk die autorisatieschil die ook buiten de overheid gebruikt kan worden en wel veilig en robuust is.

Berry

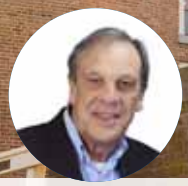
Business Resilience Masterclass

Woerden | 21 maart, 28 maart, 4 april, 11 april, 18 april

Inclusief Master Slot Event in het Grand Kasteel Woerden

JOHAN BAKKER
CISSP - ISSAP - CPT

GERT KOGENHOP
(HON.) MBCI - FINANCE - AT



MICHIEL KUETHE
CRISISMANANAGEMENT - AT

BRENNO DE WINTER
HACKER - BEVEILIGINGS- & PRIVACYEXPERT

Betrek het topmanagement bij de resilience van uw organisatie

De maatschappelijke ontwikkelingen vragen van de overheid en het bedrijfsleven een toenemende kennis op het gebied van Business Resilience.

Schrijf u nu in voor deze unieke Masterclass, waarin u in vier interactieve sessies ontdekt wat de combinatie van Information Security (IS), Business Continuity Management (BCM) en Crisis Management (CM) kan betekenen voor de resilience in uw organisatie.

Ter afsluiting vindt een Master Slot Event in het Grand Kasteel Woerden plaats, waarvoor u één of meerdere introducees mag uitnodigen.

Interesse in deze Masterclass? Neem een kijkje op onze website voor meer informatie of vraag de brochure aan.

Security Academy | www.securityacademy.nl
0348 40 80 61 | info@securityacademy.nl

SECURITY ACADEMY | SECO INSTITUTE