iB
INFORMATIEBEVEILIGING
jaargang 15 - 2015
#6

Scheiding tussen werk en daad

Advanced Business Impact Analysis (deel 2)

Information Security Officer: spelen met invloed

Drie boekbesprekingen

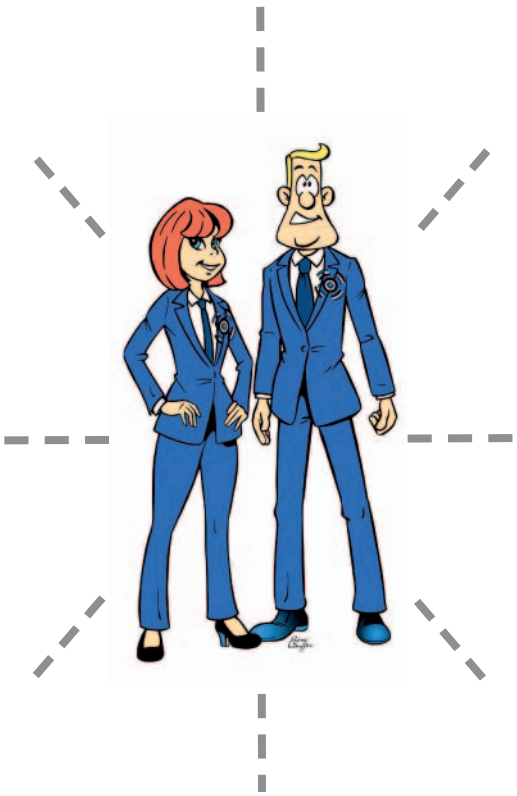
Modelling Threat Scenarios

Gezocht: Security Engineers!

SecureLink is opgericht in **2003** en heeft **200** enthousiaste SecureLinkers. We hebben **4** vestigingen verdeeld over Nederland en België.

"Realiseren van veilige innovatieve IT-infrastructuren."

Het hoofdkantoor van SecureLink bevindt zich in Sliedrecht (regio Rotterdam). Jouw werkgebied ligt vooral in de Randstad, maar ook de rest van Nederland.



Onze klanten

Detail • Klantgerichtheid • Respect • Commitment Bezieling • Creativiteit • Enthousiasme

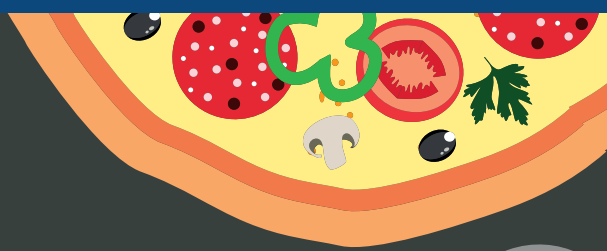
"Naar hartenlust experimenteren in een lab met state-of-the-art apparatuur."

Secure UNIVERSITY

Jouw groei en ontwikkeling staat voorop. Samen zorgen wij ervoor dat jouw certificeringen up-to-date blijven!

Interesse in deze vacature?
Neem contact op met Tim Boerakker via T +31 88 1234 200 of mail naar jobs@securelink.nl.
Kijk voor meer informatie op www.securelink.nl.

PIZZA sessie met CTO Peter Mesker!



Wij nodigen je graag uit op **1 oktober** op ons hoofdkantoor in Sliedrecht om een pizza te komen eten met onze CTO!

Tijdens deze avond komen de meest **actuele security trends** aan bod en heb je de mogelijkheid hierover zelf met de CTO in gesprek te gaan. Daarnaast willen wij je ook de kans geven kennis te maken met SecureLink en een aantal van onze collega's!

Ben jij erbij?
Meld je aan bij Tim Boerakker • tim.boerakker@securelink.nl.

Programma
17.00 uur Ontvangst in Sliedrecht met pizza
17.30 uur Intro
17.45 uur Trends en ontwikkelingen binnen security
18.45 uur Vragen
19.30 uur Borrel

GOVERNANCE, RISK, COMPLIANCE

Ik kom in mijn praktijk met regelmaat situaties tegen waarin door uitvoerenden over een security-onderwerp uitgeroepen wordt: 'Hadden we maar ... hiervoor'. De '...' staan dan voor beleid, een proces, maatregelen, een standaard, of iets dergelijks. Als uitvoerende zit je dan ook aan het eind van de verantwoordingsketen. Bij van alles wat je doet moet je er verantwoordelijkheid voor nemen en er verantwoording over afleggen. Het zou inderdaad fijn zijn als je dan een aantal zaken die je in moet richten, kunt inrichten met hulp van buiten. Dat je niet altijd in die situatie zit dat je alles maar moet beslissen en dan pas achteraf te horen krijgen dat je het niet goed gedaan hebt.

De uitvoerenden hebben direct te maken met alle risico's die met die uitvoering gepaard gaan. Het maakt het makkelijker als je (uitvoerbare) kaders krijgt waar je je binnen moet bewegen (vanuit governance) en ook weet op welke regels je beoordeeld gaat worden, zodat je al aan het aantonen daarvan kunt gaan werken.

Dan kun je ook keuzes maken om te outsourcen of de cloud in te gaan. Elke keer dat je een leverancier inschakelt creëer je een nieuw GRC-krachtenveld. Een deel van jouw risico geef je over aan de leverancier. Daarvoor in de plaats moet je dan een stuk governance inrichten en zorgen dat je jouw compliance nog steeds kunt aantonen. Bij elk product met securityaspecten (en welk product heeft dat niet) verwacht ik dan ook dat GRC-krachtenveld te zien.

Maar dit is moeilijk. Je ziet de worstelingen van bijvoorbeeld Amazon en Google om Europese overheden te willen kunnen bedienen met goede product-GRC met de Europese regels en compliance vraagstukken meegenomen. Je ziet outsourcingproviders die met minder kosten GRC-problemen van de klant moeten zien op te lossen, omdat de klant dat niet doet en er niet voor betaalt.

Als informatiebeveiligers kunnen we dit niet alleen oplossen. In deze uitgave wel een aantal artikelen die kunnen helpen bij het oplossen van dit krachtenspel. Functiescheiding, business impact-analyse, risicoanalyse. Veel leesplezier.

Lex Borger, hoofdredacteur

In dit nummer

SCHEIDING TUSSEN WERK EN DAAD

Een functioneel stappenplan voor het inrichten van de klassieke controle-technische functiescheiding

Met enige regelmaat staat het in de krant. Een medewerker van een organisatie heeft een grote som geld overgemaakt naar een bankrekeningnummer in een ver oord en is vervolgens met de noorderzon vertrokken. Medio vorig jaar overkwam het de Belastingdienst nog. Een medewerker had met één transactie 20 miljoen euro verduisterd. Om dit soort fraude, maar ook andere typen, te voorkomen, richten organisaties een hele set aan maatregelen in. Een belangrijk onderdeel hiervan is functiescheiding. Maar hoe pak je dat aan? En hoe zet je de theorie om naar iets dat ook echt werkt in de praktijk?

De theorie

(Controle-technische) functiescheiding is een term die iedereen die iets met bestuurlijke informatieverzorging [1] te maken heeft wel kent. De doelstelling van functiescheiding is om een transactie op te delen in een beperkt aantal schakels van het omloopproces en te verdelen over meerdere functionarissen, zodat het niet mogelijk is dat één functionaris de transactie kan uitvoeren zonder dat deze op één of andere manier wordt verantwoord [2].

Het creëren van tegengestelde belangen staat hierbij centraal. Je waarborgt hiermee dat niet één persoon in staat is de keten in zijn geheel te beïnvloeden [3]. Functiescheiding is een eis die in alle normenkaders voor interne beheersing terugkomt. De basis van functiescheiding bestaat uit het inrichten van de organisatie zodat de taken:

- **Beschikken [4];**
- **Uitvoeren;**
- **Bewaren;**
- **Registreren;**
- **Controleren;**

verdeeld worden over het proces dat de keten vormt.

De praktijk

Er bestaat een kloof tussen het theoretische concept van functiescheiding en de implementatie ervan in de praktijk. Organisaties vinden het lastig om de organisatorische inrichting te vertalen naar een systeeminrichting. De auteurs vinden een mogelijke verklaring hiervoor in het feit dat de organisatorische inrichting veelal een efficiency-benadering beoogd (we verdelen taken zodat we sneller en beter resultaat behalen), terwijl de systeeminrichting een integere uitvoering beoogd (met mogelijke negatieve effecten voor de efficiency in de uitvoering). De auteurs zijn van mening dat de één de ander niet uitsluit en hebben hiervoor een stappenplan ontwikkeld. Dit artikel beschrijft dit stappenplan. Het stappenplan is de afgelopen jaren ontwikkeld en geïmplementeerd bij onder meer een grote verzekeraar en enkele overheidsinstanties. In deze gevallen werd functiescheiding geïmplementeerd als onderdeel van een omvangrijker programma, dat gericht was op het verbeteren van Identity & Access Management (IAM). Het stappenplan biedt een methode om functiescheiding op een degelijke wijze te inventariseren en in te richten, waarbij efficiency en integriteit goed op elkaar aansluiten.

Om de doelstelling van het stappenplan te verduidelijken, gaan de

auteurs eerst kort in op de eisen aan functiescheiding en welke mogelijkheden er zijn om functiescheiding in te richten. Vervolgens behandelen we het stappenplan, gevolgd door een praktijkcasus.

Eisen aan functiescheiding

De eisen aan functiescheiding zijn in verschillende normenkaders [5] grotendeels gelijk. Er zijn slechts kleine onderlinge verschillen. Waar het ene normenkader meer nadruk legt op risicoafweging, weegt vastlegging bij de ander zwaarder. Als we de verschillende aspecten uit alle normenkaders combineren, komen we tot de volgende definitie:

"Functiescheiding is ingericht als van alle kritische processen (ketens) en de daarbij ondersteunende systemen, de autorisaties zodanig zijn ingericht dat de taken en verantwoordelijkheden zijn verdeeld over meerdere personen, zodat er geen ongecontroleerde of ongeautoriseerde wijzigingen kunnen worden gedaan bij de uitvoering van het kritische proces. De hiervoor benodigde autorisaties, functiescheidingsregels, kritische processen en classificatie, de totstandkoming en het beheer van de functiescheidingsregels zijn eenduidig vastgelegd."

Deze definitie brengt de aspecten risicoafweging, het verdelen van taken & verantwoordelijkheden en vastlegging bij elkaar. Daarnaast stellen we de eis dat functiescheiding door autorisaties wordt afgedwongen, iets wat we met de hedendaagse middelen niet meer dan normaal vinden.

Nu we weten welk uitgangspunt we voor onszelf hanteren, kijken we naar de manier waarop functiescheiding kan worden ingericht.

De manieren om functiescheiding in te richten

Zoals hierboven al aangegeven, gaan we ervan uit dat functiescheiding door autorisaties wordt afgedwongen. Hoe kunnen we dit in de praktijk inrichten? Dit kan op vier manieren, namelijk 1) het inrichten in functies, 2) functiescheiding in een systeem, 3) afdwingen met businessregels of 4) functiescheiding met behulp van query's.

1. Inrichten in functies (organisatorische inrichting)
Dit is de basis van functiescheiding. Vanuit een efficiency- of integriteitsvraagstuk worden taken bij verschillende medewerkers belegd. Omdat een medewerker die taken heeft, krijgt hij de bijbehorende autorisaties. Iemand met andere taken krijgt andere autorisaties. De autorisaties zijn daarmee niet bewust gescheiden, dan wel alleen bij de initiële inrichting. Naarmate de organisatie groeit, medewerkers andere taken erbij krijgen, van functie verwisselen of meer applicaties gaan gebruiken, is het overzicht op functiescheiding veelal verloren.

2. Functiescheiding in een enkel systeem
Leveranciers van systemen die kritische processen ondersteunen leveren deze systemen veelal op met een set rollen die de functionaliteit van de applicatie scheiden waar dat nodig is. Door de rollen aan verschillende medewerkers toe te delen ontstaat functiescheiding. Zolang een medewerker niet meerdere rollen krijgt, is functiescheiding in het systeem zelf geborgen.

3. Functiescheiding afdwingen met businessregels
Hedendaagse IAM-systemen bieden de functionaliteit om functiescheidingsregels als 'business-rules' te definiëren. Denk hierbij aan een regel als: "het moet nooit mogelijk zijn dat een gebruiker de rechten 'voorbereiden betaling' en 'goedkeuring betaling' tegelijkertijd toegekend krijgt." De functiescheidingsregel als business-rule kan dankzij het IAM-systeem over de hele organisatie worden toegepast en biedt meer objecten ter vergelijking dan alleen autorisaties, denk aan afdelingen, functies, team, etc. We gaan hier verder op in bij stap 4 van het stappenplan.

4. Functiescheiding met behulp van query's
Als een IAM-systeem geen businessregels ondersteunt, kan er vaak wel gebruik worden gemaakt van rapportagefunctionaliteit. Met query's kan bijvoorbeeld gezocht worden naar "alle gebruikers met de autorisatie 'voorbereiden betaling' en 'goedkeuring betaling', ook al wordt een overtreding niet automatisch door het systeem ondervangen. Het is zodoende nodig om naderhand nog een handmatige (schonings-)actie uit te voeren.

Nu we weten welke norm we hanteren en hoe functiescheiding in de praktijk kan worden ingericht, beschrijven we de realisatie, het stappenplan.

Het stappenplan voor het inrichten van functiescheiding

Aan de hand van de eerder beschreven norm en de verschillende manieren om functiescheiding in te richten, is het mogelijk om een stappenplan te formuleren.

Marcel Dusink (links) is I&AM adviseur en IT auditor bij Insite Security. Marcel is te bereiken via mdusink@insiteadvies.nl.
Wilfred Hanekamp is IT auditor bij Insite Security. Wilfred is te bereiken via whanekamp@insiteadvies.nl.

Deze vier werkwijzen hebben elk hun eigen voor- en nadelen:

	1. In functies	2. In systeem	3. Businessregels	4. Query's
Wordt functiescheiding vooraf gecontroleerd?	Ja (eenmalig)	Ja	Ja	Nee
Kun je autorisaties van verschillende systemen combineren?	Ja	Nee	Ja	Ja
Wordt een combinatie geblokkeerd als er een overtreding in de keten plaats vindt?	Nee	Alleen als de keten beperkt is tot het systeem	Ja	Ja

Tabel 1 - Overzicht aspecten inrichten functiescheiding

Het stappenplan bestaat uit de volgende stappen:

Stap 1: Beleid definiëren
In stap 1 definiëren we het beleid, ofwel de uitgangspunten. Welke informatie moet door middel van functiescheiding worden beschermd? Welke beheers doelstellingen heb je? Welke inrichting dekt voldoende het risico?

Stap 2: Kritische processen inventariseren
In stap 2 werk je toe naar een overzicht van de kritische processen. Dit is een exercitie die de organisatie vaak al op een of andere manier heeft uitgevoerd [6]. Vanuit de kritische processen worden de ondersteunende systemen benoemd.

Stap 3: Gewenste functiescheiding inventariseren
Een inventarisatie dient in eerste instantie zo volledig mogelijk te zijn (uiteraard naar redelijke inspanning). Door de inventarisatie vanuit verschillende perspectieven uit te voeren, is het aannemelijk dat de functiescheidingsregels de organisatie voldoende afdekken. Daarom kijken we in stap 3 achtereenvolgens naar de geld- en goederenstroom, het systeemperspectief en de BIV-betrouwbaarheidsaspecten.

Functiescheiding vanuit de geld- en goederenstroom
De geld- en goederenstroom is voor alle organisaties in kaart te brengen. De binnenkomende of uitgaande geld- en goederenstromen zijn het beste te identificeren als ze de grenzen van de organisatie overschrijden (in- en uitgaande geldstromen). Dit is het startpunt. Door een grote uitgaande geldstroom terug de organisatie in te volgen, worden de processtappen en de bijbehorende systemen duidelijk. We volgen het proces in omgekeerde volgorde. Neem bijvoorbeeld het uitbetalen van een declaratie aan een klant. Een declaratie is onderdeel van een grote betalingsrun bij een bank.

Het betalingssysteem van de bank heeft een betalingsbestand ontvangen van de organisatie. Het betalingsbestand wordt aangemaakt door een financieel systeem. Hiervoor zijn goedkeuringen nodig. Het financiële systeem wordt weer gevoed door een materiesysteem. Hierin is het besluit genomen dat de declaratie uitbetaald wordt. Het materiesysteem wordt op zijn beurt gevoed door een klantregistratiesysteem. Hier zijn initieel de gegevens van de klant in opgeslagen, onder meer het rekeningnummer van de klant. In al deze systemen is er een moment waarop een kritisch gegeven kan worden gewijzigd. Denk aan het wijzigen van het rekeningnummer, het goedkeuren van de declaratie of het creëren van een betaalbestand. Al deze activiteiten hebben tenminste twee autorisaties [7], één voor het voorbereiden van de wijziging, de ander voor het opslaan van de wijziging. Neem alle autorisaties (van het klantregistratie-, het materie- en het financiële systeem) op in de inventarisatie. Beschrijft ook de functie van de autorisaties in de gehele keten. Dit is van belang als een systeem meerdere functionaliteiten biedt. Figuur 1 biedt een overzicht.

Functiescheiding vanuit het systeemperspectief
Een organisatie heeft kritische en niet-kritische systemen. Zo goed als alle systemen hebben een functioneel beheerder, super-user of iemand met soortgelijke kennis. Deze super-user is bekend met alle functionaliteit en eventuele externe databronnen van het systeem. De super-user van een declaratiesysteem is bijvoorbeeld bekend met alle regels die het systeem hanteert om declaraties in specifieke workflows af te handelen. Door samen met de super-user alle processen van het systeem te doorlopen, is het mogelijk om vanuit dit systeemperspectief tot noodzakelijk te scheiden autorisaties te komen.

Functiescheiding op basis van de BIV-betrouwbaarheidsaspecten
De BIV-betrouwbaarheidsaspecten beschikbaarheid, integriteit en vertrouwelijkheid bieden ook een manier om tot de gewenste functiescheiding te komen. Waar de geld- en goederenstroom en het systeemperspectief zich richten op integriteit bieden de aspecten

Figuur 1 - Overzicht uitgaande geldstroom

vertrouwelijkheid en beschikbaarheid een ander perspectief.

Functiescheiding op basis van vertrouwelijkheid heeft veel te maken met de wijze waarop iemand toegang krijgt tot de informatie. Door eerst de vertrouwelijke informatie te benoemen en vervolgens het toegangsproces te doorlopen, is het mogelijk om tot noodzakelijke scheiding van autorisaties te komen.

Het beschikbaarheidsaspect van functiescheiding heeft te maken met de vraag wie in staat is om grote verstorende wijzigingen in de infrastructuur door te voeren. Dit is veelal geborgd binnen het IT-proces wijzigingsbeheer en kan worden opgevangen door de autorisaties voor deployement op te splitsen en te verdelen over de leden van het change-advisory-board.

Stap 4: Gewenste functiescheiding vertalen naar concrete functiescheidingsregels

De vertaling van gewenste functiescheiding naar daadwerkelijke functiescheidingsregels is niet altijd eenvoudig. Uit stap 2 en 3 kan bijvoorbeeld de eis naar voren komen dat het doorvoeren van een wijziging in productie opgedeeld dient te worden over twee personen. Maar misschien is er geen systeem dat deze handeling in zijn geheel ondersteunt. Het is aannemelijk dat er in dit geval software wordt geïnstalleerd en dat deze handeling alleen kan worden uitgevoerd met een admin-account. Het uitgeven van dit (tijdelijke) account kan dan wel met een extra goedkeuring worden ingericht. Het is belangrijk om alle aspecten voor ogen te hebben. Geavanceerde IAM-systemen kunnen alle attributen van een identiteit gebruiken om een vergelijking te maken. Denk hierbij aan de autorisaties die een medewerker heeft, maar ook aan zijn of haar functie, team, afdeling of functierol (zie ook figuur 2). Hierbij kunnen combinaties gemaakt worden in de trant van:

- Alleen medewerkers van de afdeling X mogen toegang hebben tot applicatie Y.
- Niemand mag tegelijkertijd een productieaccount en een testaccount hebben.
- Een medewerker die geen leidinggevende is, mag nooit declaraties goedkeuren.

Stap 5: Inrichting voor het afdwingen van functiescheiding kiezen en regels in het systeem inrichten

De besproken manieren voor het afdwingen van functiescheiding komen nu aan bod. Veelal bepaalt de techniek welke manier mogelijk is, maar als er meerdere keuzes beschikbaar zijn, is het nuttig om op basis van de eerste inventarisatie een keuze voor één of meerdere manieren van afdwingen te maken.

Stap 6: Goedkeuring vragen en eerste resultaten evalueren

Bij het inrichten veranderen functiescheidingsregels in beperkte mate, omdat de techniek haar beperkingen toont. De wijze waarop ze daadwerkelijk in het systeem staan, is de definitieve versie. Deze versie dient te worden geformaliseerd door goedkeuring van de eigenaar. Goedkeuring is eenvoudiger te verkrijgen door de regels samen met de eerste resultaten aan te bieden. Deze evaluatie biedt het startpunt voor verdere aanscherping van de regels.

Stap 7: Regels en totstandkoming beschrijven

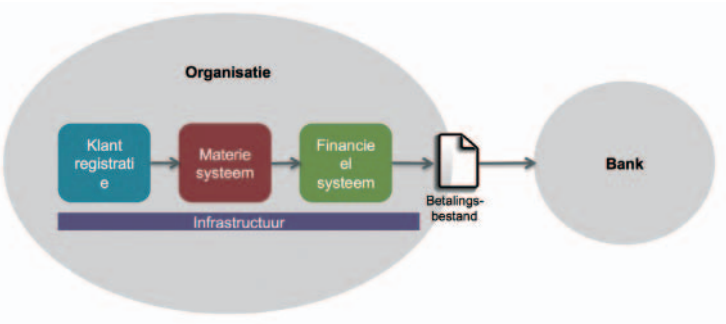
De functiescheidingsregels zoals die in het systeem zijn ingevoerd, moeten in een document worden vastgelegd. Per regel moet ook de achterliggende redenatie en totstandkoming van de regel worden beschreven. Dit is van belang voor het proces van het verbeteren van de regels en het toetsen van de functiescheidingsregels.

Stap 8: Proces voor onderhoud van de regels inrichten

Om de veranderingen in de organisatie bij te houden, is het van belang om een proces in te richten dat de functiescheidingsregels periodiek herziet, evalueert en bijwerkt.

De toegevoegde waarde van het stappenplan

Het stappenplan biedt een leidraad voor het inrichten van functiescheiding en biedt de lezer hopelijk een leidraad voor de



Figuur 2 - Verschillende objecten die leiden tot een kritische combinatie

overbrugging van theorie en praktijk. Het stappenplan omvat alle aspecten die moeten worden overwogen om te komen tot een degelijke inrichting en een onderhoudbaar proces. Het combineert kennis op individuele 'eilandjes' (van bijvoorbeeld functioneel beheerders of senior-users) en bundelt deze tot een werkbaar overzicht. Deze helikopter-view vergroot het realiseren van een zo volledig mogelijke inrichting van functiescheiding. Zo vormt het de basis voor een zo goed mogelijke beveiliging van de kritische ketens.

Praktijkcasus: functiescheiding bij een grote verzekeraar

De auteurs hebben het stappenplan bij een verzekeraar uitgevoerd. Tot op dat moment had de verzekeraar alleen functiescheiding in de applicaties zelf ingericht. De implementatie van een nieuw IAM-systeem bood de gelegenheid en technische functionaliteit om op meerdere manieren functiescheidingsregels af te dwingen. De verzekeraar had met haar toezichthouder afgesproken om de beveiligingsmaatregelen te toetsen conform Cobit 4.1.

Uit de inventarisatie (stap 2 en 3) kwam in totaal een zestigtal functiescheidingsregels naar voren die moesten worden ingericht. Veruit de meeste regels waren erop gericht om scheiding aan te brengen op basis van organisatie brede kenmerken. Denk hierbij aan de scheiding van rechten tussen de verzekerdenadministratie en de declaratieadministratie. Deze regel zorgt ervoor dat rechten van medewerkers die een tijdelijke of nieuwe functie uitoefenen bij een andere afdeling dan waar ze eerder hebben gewerkt, komen te vervallen, ongeacht hoe deze zijn toegekend (individueel of via hun profiel). Een tweede voorbeeld van een grote scheiding was het afschermen van productie voor ontwikkelaars en het afschermen van testomgevingen voor functioneel en technisch beheer.

Een tweede type regel was het beschermen van een individuele afdeling. Denk hierbij aan de afdelingen Financiën, Personeelszaken en Juridische zaken. Deze regels zijn geformuleerd in de vorm: alleen medewerkers die werken voor Juridische zaken hebben toegang tot juridische applicaties.

Een derde type regel was 'de gewenste overtreding'. Dit was een regel waarbij men wist dat deze overtreden zou gaan worden. Dit type regel werd gebruikt als extra controlemaatregel. Een voorbeeld hiervan is een autorisatie die alle leidinggevenden van een organisatie krijgen (bijvoorbeeld accorderen urenverantwoording). Een manager krijgt vanuit zijn profiel altijd urenverantwoording toegekend, maar door de functiescheiding wordt deze ook geblokkeerd. Personeelszaken krijgt hier vervolgens een melding van en keurt het accorderen alsnog goed. Personeelszaken gebruikt deze regel als extra controle bij het toekennen van manager-autorisaties. Een bijkomend voordeel is dat Personeelszaken automatisch op de hoogte wordt gesteld als autorisaties, tegen de regels in, worden gedelegeerd naar een niet-leidinggevende.

Nadat de regels waren vertaald naar voor het IAM-systeem leesbare code, werden de regels geactiveerd. Door deze activatie ging het systeem zoeken naar overtredingen op de regels. Dit leverde initieel zo'n 3.000 overtredingen op. Een overtreding kon meerdere keren plaatsvinden op eenzelfde regel bij eenzelfde medewerker, omdat de medewerker dezelfde autorisatie op verschillende wijze toegekend kan krijgen (via een losse autorisatie, maar ook via een rol). Bij deze initiële activatie zijn de functiescheidingsregels nog niet afgedwongen. Er is voor gekozen om eerst uit te zoeken of de regels de juiste uitwerking hadden. Na de 3.000 overtredingen te hebben geanalyseerd, zijn de regels aangescherpt. Bij een tweede activatie kwam er nog steeds een aanzienlijk aantal overtredingen naar voren, maar dat kwam met name door de 'gewenste' overtredingen, zoals het voorbeeld van de autorisatie voor het accorderen van urenverantwoording door leidinggevenden. Nadat ook deze waren beoordeeld, bleef een beperkte set overtredingen over (circa 350) die daadwerkelijk beoordeeld moesten worden, om vervolgens te schonen of toe te staan.

Tijdens een evaluatie van de werking van de functiescheidingsregels waren leidinggevenden positief. Ze waren van mening dat elke overtreding een nuttige melding was, ook al werd vervolgens besloten om de overtreding toe te staan. Daarbij gaf de inrichting van functiescheiding de mogelijkheid om niet-kritische autorisaties vrijer toe te delen, wetende dat een zestigtal regels de écht kritische combinaties beschermde.

Referenties:

[1]Bestuurlijke informatieverzorging omvat alle activiteiten met betrekking tot het systematisch verzamelen, vastleggen en verwerken van gegevens, gericht op het verstrekken van informatie ten behoeve van het besturen-in-engere-zin, het doen functioneren en het beheersen van een huishouding, en ten behoeve van de verantwoording die daarover moet worden afgelegd [1].
[2][1] Starreveld, Van Leeuwen, van Nimwegen, et. Al. (2002): Bestuurlijke informatieverzorging, deel 1: Algemene Grondslagen, 5e druk.
[3] Jans, E.O.J (2001) Grondslagen administratieve organisatie Deel A: Algemene beginselen, negentiende druk, Groningen/Houten, Wolters-Noordhoff.
[4]Het geven van opdrachten, machtigingen en het aangaan van verplichtingen als het geven van kwijtingen [1].
[5] ISO27001: A.10.1.3, CoBIT4.1: PO4.11, BIR 11.2.1
[6]als uitkomst van een business impact assessment, risicoanalyse, etc.
[7]als maar één autorisatie het wijzigen van een rekeningnummer 'beschermt', dan is het raadzaam dit te aan te passen en op te splitsen naar twee autorisaties.

4 & 5 NOV 2015 JAARBEURS UTRECHT

VAKBEURZEN, SEMINARS EN ONLINE MATCHMAKING VOOR IT-MANAGERS EN IT-PROFESSIONALS

REGISTREER NU VOOR GRATIS TOEGANG:

WWW.INFOSECURITY.NL | WWW.STORAGE-EXPO.NL | WWW.THETOOLINGEVENT.NL

KEYNOTES | SEMINARS | CASE STUDIES | RUIM 150 EXPOSANTEN

Mede mogelijk gemaakt door:

Reed Exhibitions marqit

Hoofdmediapartner:

COMPUTABLE

Jaarbeurs

ADVANCED BUSINESS IMPACT ANALYSIS (DEEL 2)

Verbeterd risico-management door gerichte impactbepaling

Alle bedrijven lopen risico's, waardoor er een kans bestaat dat bedrijven hun verplichtingen naar hun stakeholders - zoals klanten of aandeelhouders - niet meer kunnen nakomen en daardoor zelf schade leiden. Het is dus van vitaal belang dat bedrijven de relevante risico's identificeren en vervolgens managen. De stap in het risicomanagementproces waarin de impact van een bepaalde dreiging op het behalen van business doelstellingen wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Dat is de conclusie van een aantal interviews en een expertsessie met verscheidene information-security-consultants met meerjarige ervaring in het ondersteunen van organisaties met het uitvoeren van BIA's. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds het risico wordt gelopen om te investeren in onnodige veiligheidsmaatregelen.

In deel 2 van dit artikel de geconstateerde onvolkomenheden besproken.. Deze maand zullen we een aantal mogelijke verbeterpunten bespreken voor zowel de korte, als de wat langere termijn.

Geconstateerde tekortkomingen

In het artikel van vorige maand zijn enkele tekortkomingen geïdentificeerd van het BIA-proces zoals dat nu in het bedrijfsleven wordt uitgevoerd. De tekortkoningen zijn divers. Zo is er bij degenen die de BIA uitvoeren vaak te weinig zicht op de belangen van hogere of aanpalende organisatieniveaus, met het gevolg dat belangrijke risicoscenario's over het hoofd worden gezien. Daarnaast worden dimensies als reikwijdte en tijdsduur van een incident vaak achterwege gelaten en leidt het vaststellen van een worst-case-scenario tot ambiguïteit. Tot slot is het bepalen van de impact van incidenten niet eenvoudig. Niet alleen door het ontbreken van data, maar ook door het feit dat er vaak een discrepantie bestaat tussen de scope van de verantwoordelijke persoon en de impactsoort, denk aan een IT-specialist die moet beoordelen wat de impact is van een data-breach op de aandeelhouderswaarde van een onderneming.

Door deze tekortkomingen, resulterend in onjuist ingeschatte impacts van cyberdreigingen, loopt men het risico dat enerzijds werkelijk relevante risico's niet in beschouwing worden genomen. Anderzijds loopt men het risico om te investeren in onnodige maatregelen. De praktijk is vaak dat de BIA als proces wordt doorlopen omdat dat onderdeel is van een ISO-standaard. Met de resultaten wordt echter niet gedaan wat ermee gedaan zou moeten worden. Het is duidelijk dat een andere aanpak nodig is. Bepaalde verbeteringen kunnen daarbij al op korte termijn worden doorgevoerd. Andere hebben meer tijd nodig.

Korte-termijn-verbeteringen

De BIA dient uitgevoerd te worden op verschillende organisatie-niveaus. De BIA-vragen dienen dan ook specifiek voor elk organisatieniveau (scope) gedefinieerd te zijn. In eerste instantie zou een dergelijke gelaagdheid bereikt kunnen worden door een voorselectie van bestaande vragen te maken, waarbij rekening gehouden wordt met relevantie van de vragen voor het specifieke organisatieniveau. Sluiten de vragen goed aan bij de doelstellingen van de verantwoordelijke manager? Bij alle vragen zou aangegeven moeten worden door wie, en op welk organisatieniveau ze dienen te worden beantwoord. Vragen over verlies van vertrouwen door de financiële wereld of over impact op de beurskoers zijn typisch de vragen waarover een directie zich zou moeten uitspreken. Ziehier het gedachtengoed van de Networked Risk Management methodiek, waarover later meer. Ook zou impact beter ingeschat kunnen worden als de karakteristieken van incidenten duidelijker zouden zijn omschreven. Tijdsduur en reikwijdte zijn daarbij belangrijke elementen. Bijvoorbeeld de omvang en tijdsduur van hacking van systemen om de impact hiervan op de vertrouwelijkheid van informatie gerichter te kunnen inschatten. Ook de karakteristieken van de dienst - waar in de life-cycle, kritieke dienst of niet – moeten en kunnen beter omschreven worden. Door dit te doen kan al op korte termijn een betere BIA worden uitgevoerd, met meer zeggingskracht. De tekortkomingen op het gebied van het beantwoorden van vragen, kunnen ook deels op korte termijn worden weggenomen. Door een voorselectie te maken van generieke vragen op basis van bedrijfskenmerken, wordt bereikt dat de BIA beter aansluit op de behoeftes van een specifiek bedrijf. Niet alle impact categorieën zijn immers even relevant voor verschillende bedrijven. Zo is bijvoorbeeld aandeelhouders-waarde alleen relevant voor aan de beurs genoteerde bedrijven. Ook kunnen verschillende impact types in mindere of meerdere mate relevant zijn voor een specifiek bedrijf. Het kwantificeren van impact gaat gemakkelijker indien degenen die bij het uitvoeren van de BIA betrokken zijn, gewapend worden met manieren om de impact van verschillende scenario's op hun bedrijfsvoering te bepalen. Als men bijvoorbeeld over relevante data zou beschikken kan de impact realistischer worden bepaald. Dit kan bewerkstelligd worden door voor bepaalde type impacts - bijvoorbeeld verlies van klanten, reputatieschade - te inventariseren welke data er bestaat en welke databronnen er nog nodig zijn om enige kwantificatie van impacts te faciliteren, al is het op het niveau van ordegrootte. Dan pas kunnen overwogen business cases rondom te treffen maatregelen opgesteld worden, en kan een doordacht besluit genomen worden over risico-acceptatie.

Lange-termijn-verbeteringen

Voor het verbeteren van sommige geconstateerde tekortkomingen van de BIA - zoals bijvoorbeeld tekortkomingen gerelateerd aan scope-bepaling, of tekortkomingen door gebrekkige aansluiting van vragen op de doelstellingen de scope-verantwoordelijke - is een tijdspanne van enkele jaren

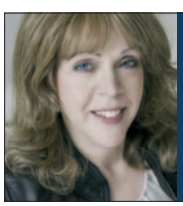
Milena Janic promoveerde aan de Technische Universiteit Delft, op het gebied van performance van informatie- en communicatienetwerken en diensten. Zij werkt als consultant en onderzoekster bij de expertisegroep Information Security van TNO. Haar focus ligt op onderzoek en consultancy op het gebied van risicomanagement, identity- en access-management en privacygerelateerde vraagstukken.

nodig. Op lange termijn is een omslag vereist in de manier waarop risicomanagement wordt gedaan: een paradigm shift. Onlangs heeft TNO een Networked Risk Management (NRM)-methodiek ontwikkeld en aangedragen, die de onvolkomenheden van ISO 31000 en 27005 adresseert en daarmee een aantal geconstateerde onvolkomenheden van het traditionele risicomanagement aanpakt. Één van de belangrijke aanvullingen die NRM introduceert is definitie en gebruik van het begrip "scope". Daar waar ISO-standaarden ervan uitgaan dat de scope duidelijk is, blijkt dat in de praktijk geenszins het geval te zijn. Om een voorbeeld te geven: vaak bestaat onduidelijkheid over wie waarvoor verantwoordelijk is, met als gevolg dat de besluitvorming rond de daaraan gerelateerde risico's ontbreekt. Daarom wordt de scope in NRM helder gedefinieerd als zijnde de ruimte waarbinnen een manager verantwoordelijk is om een aantal verplichtingen na te komen. Zo zijn voor de scope van een Raad van Bestuur hun verplichtingen aan aandeelhouders of overheid relevant. Ook een werkproces kan als scope gedefinieerd worden, als de verplichtingen (requirements) van dat proces duidelijk geïdentificeerd zijn, en een manager voor het nakomen van deze verplichtingen verantwoordelijk is. Ook kan een manager verplichtingen aan zichzelf definiëren die nodig zijn om zijn eigen business-doelen te halen. Gezonde bedrijfsvoering houdt dan in dat de verplichtingen aan derden en aan zichzelf worden nagekomen.

Verder worden in NRM risico's uitgesplitst in verplichtings- en verwachtingsrisico's. Een verplichtingsrisico is een risico van het niet kunnen nakomen van een verplichting. Naast verplichtingsrisico's worden ook verwachtingsrisico's geïdentificeerd. Een manager is voor het waarmaken van zijn verplichtingen doorgaans ook afhankelijk van anderen. Deze afhankelijkheden uiten zich in verwachtingen die een manager heeft van andere scopes om zijn doelstellingen te halen. Het belang van een gegeven verwachting wordt bepaald door de mate waarin het vervullen ervan bijdraagt aan het nakomen van verplichtingen. Als een manager een verwachting heeft van een andere scope, dan bestaat verwachtingsrisico uit de mate waarin die verwachting niet ingevuld wordt of gaat worden. De BIA is in NRM de inventarisatie van verplichtingen en de bijbehorende impacts voor een scope. De schade wordt bepaald die een manager verwacht te lijden bij het niet nakomen van een verplichting, en dat is niets anders dan de impact van het niet nakomen van de verplichting. De uiteindelijke BIA-lijst zal alle verplichtingen bevatten waarvan de impact voor de scope en verantwoordelijke manager onacceptabel hoog is. Van elk van deze verplichtingen is vastgelegd tegenover welke partij deze geldt. Tevens is de impact ingeschat van het niet nakomen van de verplichting. Om deze verplichtingen af te dekken, wordt vastgesteld hoe deze verplichtingen worden waargemaakt en worden de bijbehorende verwachtingen gedefinieerd, die een manager heeft aan zichzelf of aan anderen. De geïdentificeerde verwachtingen die een manager aan derden heeft, worden verplichtingen in de scopes waar deze derde partijen voor verantwoordelijk zijn. Kortom: vanuit de NRM-gedachte heeft het uitvoeren van de BIA betrekking op het inventariseren van verplichtingen en het bepalen van de schade die resulteert als de verplichting niet wordt nagekomen. NRM vult de huidige risicomanagement-methodes op een aantal vlakken aan, zoals onder andere de definitie en het gebruik van "scope". Hiermee is een groot aantal tekortkomingen uit de vorige sectie, geadresseerd. Echter, ook hier geldt dat het nodig zal zijn dat de scope-verantwoordelijke de impact van het niet kunnen nakomen van verplichtingen, kan inschatten.

Conclusies

Het bepalen van de impact die een bepaalde dreiging kan hebben op de business is een belangrijk onderdeel van risicomanagement. De stap in het risicomanagementproces waarin deze impact wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. In dit artikel hebben we een aantal mogelijke verbeterpunten voorgesteld, zowel op korte als wat langere termijn. Zo vinden we dat er op korte termijn al veel kan gewonnen worden door bijvoorbeeld de BIA beter te laten aansluiten bij de organisatieniveaus waarvoor deze wordt uitgevoerd. Voor andere geconstateerde tekortkomingen is een omslag nodig in de manier waarop risicomanagement wordt gedaan: een paradigm shift. Het denken in verplichtingen en verwachtingen is het gedachtengoed van Networked Risk Management (NRM), een door TNO ontwikkelde methodiek, die in dit artikel nader is toegelicht. Vanuit de NRM-gedachte heeft het uitvoeren van de BIA betrekking op het inventariseren van relevante verplichtingen en het bepalen van de schade die resulteert als een bepaalde verplichting niet wordt nagekomen. Wij geloven dat door in ieder geval de tekortkomingen aan te pakken die op korte termijn kunnen worden opgelost, een organisatie zich beter kan wapenen tegen huidige en toekomstige security-dreigingen.



Eldine Verweij is als kwantitatief bedrijfseconoom afgestudeerd aan de Erasmus Universiteit Rotterdam en werkt als consultant en onderzoekster bij de expertisegroep Strategic Business Analysis van TNO. Haar focus ligt op onderzoek en consultancy met betrekking tot de economics van cybersecurity en kosteneffectiviteitsafwegingen binnen de informatiebeveiliging.

Wordt u een CISO in 5 dagen?

CISO staat voor Chief Information Security Officer. Veelal is deze functie gepositioneerd op board level in organisaties. Van CISO's wordt nogal wat verwacht. Niet alleen dat ze op strategisch niveau kennis hebben van o.a. riskmanagement, security beleid, wet- & regelgeving maar dat ze ook een grote rugzak met management-, advies-, sales- en leiderschapvaardigheden meebrengen.

Nu vraagt u zich, gezien de titel van deze pagina af *"Kan ik dit in 5 dagen leren?"*.
Het antwoord op deze vraag is NEE. Dat kan niet!

Maar wat moet u dan doen als u de CISO functie ambieert? De Security Academy heeft een CISO traject ontwikkeld waarmee u zowel de methoden en technieken als ook de persoonlijke vaardigheden die voor deze functie noodzakelijk zijn leert.

ISMP®

De ISMP titel staat voor de Post-HBO opleiding Information Security Management Professional. In deze opleiding van 15 weken verkrijgt u de benodigde inzichten en vaardigheden voor het adequaat ontwikkelen, implementeren, beheren en bewaken van het Information Security Management proces. De opleiding is officieel geaccrediteerd als Post-HBO opleiding bij het CPION.

CISO Masterclass

Na afronding van de Post-HBO opleiding kunt u de CISO Masterclass volgen. De CISO Masterclass is een compacte, intensieve, hands-on training van drie dagen, waarin deelnemers gaan ontdekken hoe zij invloed uit kunnen oefenen op de bestuurslaag.
Onderwerpen als managementstijlen, leiderschap, overtuigen, verkopen van de boodschap en herkennen van hoe de organisatie is opgebouwd en functioneert (politiek) spelen de hoofdrol in deze training.

Na afronding van beide trajecten (ISMP en CISO Masterclass) kunt u zich nogmaals de vraag stellen: *"Kan ik in 5 dagen CISO worden?"* U zult tot de conclusie komen dat deze vraag nog steeds met NEE beantwoord zal worden.

De vraag *"Heb ik na afronding van het Security Academy CISO traject wel genoeg bagage om de CISO functie te vervullen?"* kunt u positief beantwoorden. JA dat heeft u zeker!

Voor meer informatie over de Post-HBO Information Security Management Professional (ISMP) opleiding en de CISO Masterclass verwijzen wij u graag naar onze website. Of neem even contact met ons op voor meer informatie.

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL

BURGERLIJKE ONGEHOORZAAMHEID EN PRIVACYPROTEST

Waar ik me tien jaar geleden nog vaak een roepende in de woestijn voelde, zie ik tegenwoordig steeds vaker dat privacyprotest niet langer slechts van de 'informed few' afkomt, maar meer en meer uit de maatschappij zelf. Kritiek is iets wat niet altijd goed valt bij degene die het ontvangt, maar het is een noodzakelijk goed alleen al omdat het helpt discussie aan te wakkeren. Waarom zijn bepaalde keuzes gemaakt? En, belangrijker nog, kan het eigenlijk niet anders (lees privacyvriendelijker)?

Zo zamelt dokter Chantal van het Zandt geld in om een kort geding te kunnen starten tegen de plannen van minister Schippers. De materiële controles van zorgverzekeraars op mogelijk frauduleuze zorgdeclaraties vormen volgens haar een ongeoorloofde inbreuk op de privacy van patiënten en doorbreken het medisch beroepsgeheim. Tijdens controles kunnen de zorgverzekeraars volledige inzage in de dossiers eisen. Patiënten hoeven daar geen toestemming voor te geven en hebben daar doorgaans geen wetenschap van, zo stelt zij.

Duitse burgers schijnen massaal hun identiteitspapieren in de magnetron te stoppen om zo de op afstand uitleesbare RFID-chip te vernietigen. Zij vrezen dat de chip door kwaadwillenden uitgelezen kan worden (hoewel studies aantonen dat dit onwaarschijnlijk is). Dat wordt hen overigens niet altijd in dank afgenomen, een 29-jarige Duitse man werd onlangs op het vliegveld van Frankfurt gearresteerd omdat hij door dit trucje "illegaal officiële documenten had veranderd".

Ook social media wordt steeds meer en steeds vaker ingezet om gehoor te geven aan privacyprotesten. Vooral Twitter is daarvoor een veelgebruikt medium. Indien een overheid of een bedrijf in het nieuws komt met een potentieel privacyaantastend plan, zie je in het kielzog van dat nieuws vele commentaren verschijnen (recentelijk bijvoorbeeld over de beveiliging van Wifi in de trein, Spotify en haar privacypolicy en de voorgenomen wetgeving over de bevoegdheden van AIVD en MIVD). Bedrijven en overheden zelf beginnen daar mondjesmaat ook meer "podium" voor te geven. Getuige onder meer de toenemende hoeveelheid instanties met een responsible disclosure beleid. Ook zijn verschillende van hen zelf steeds actiever in het communiceren met klanten.

Overigens kan elke burger cq klant ook melding maken van privacyinbreuken bij het CBP. Jaarlijks ontvangt de toezichthouder zo'n 7000 tips. Het CBP gebruikt deze om keuzes te maken waarnaar zij onderzoek gaat doen. In 2013 en 2014 gingen de meeste tips over identificatie en/of het gebruik van het Burger Service Nummer, de doorgifte van persoonsgegevens aan derden en heimelijke waarneming.

Niet elk protest zal de privacywereld kunnen veranderen en plannen gaan wellicht toch door ondanks de protesten. Maar als je niets zegt, zal er zeker niets veranderen. Ik ben er in ieder geval als Privacy Officer blij mee, het biedt mij hulp om in mijn werk issues op de agenda te plaatsen. Want hoezeer je ook compliant met de wet wilt handelen en de processen zo privacyvriendelijk als mogelijk inricht, privacy blijft ook vaak iets wat te maken heeft met gevoel. Een privacyinbreuk wordt ervaren door mensen en dat gevoel willen zij steeds vaker delen. Het is aan overheden en bedrijven om te luisteren en te handelen.

Mr. Rachel Marbus
@rachelmarbus op Twitter

UITDAGING VOOR GEMEENTEN ZIT NIET IN "GEBLUNDER"

Reactie op column van Rachel De Blunderende Gemeente / IB5-2015

Rachel Marbus snijdt in haar column in Informatiebeveiliging #5 een belangrijk onderwerp aan: gemeenten zorgen niet goed voor de privacy van hun burgers.

Haar analyse van het probleem schiet m.i. echter tekort. Er is meer aan de hand dan geblunder. Naar mijn mening is het juist de Rijksoverheid die cruciale fouten maakt bij de architectuur van informatiestromen.

Marbus stelt voor om bij elke gemeente (393 stuks!) een onafhankelijke 'privacy-officer' te plaatsen. Nou is dat een prachtidee voor een grote gemeente. Voor Rotterdam of Utrecht kan ik me er best wat bij indenken.

Maar ik wil u even voorstellen aan een gemeente bij mij naast de deur. De organisatie van de gemeente Zoeterwoude (6000 inwoners) heeft 24 fte in dienst. Vierentwintig. Als deze gemeente de mogelijkheid kreeg een 25e ambtenaar in dienst te nemen dan kan ik mij, zelfs als beveiligingsfanaat, heel goed indenken dat dat geen privacy-officer wordt.

En daar zit het probleem. De Rijksoverheid heeft, door informatie eindeloos te 'ontsluiten', de gemeente Zoeterwoude en honderden andere relatief kleine, toch al overbelaste organisaties verantwoordelijk gemaakt voor de bescherming van het hele doopceel van alle 17 miljoen inwoners van Nederland. Waar de gemeente Vlieland zich tot voor kort slechts zorgen hoefde te maken over de privacy van de 1000 eilandbewoners wordt tegenwoordig van ze verwacht te waken over, zo ongeveer, alle data over iedereen.

Het probleem beperkt zich overigens niet tot gemeenten. Mijn huisarts (5 parttime medewerkers) kan met een druk op de knop zo het medisch dossier openen van iedereen met een burgerservicenummer. Moet daar ook een onafhankelijk privacy-officer worden aangesteld? Eigenlijk wel, maar u ziet hoe onhaalbaar dat is. Straks is half Nederland privacy-officer.

Helaas, was het maar zo dat het probleem alleen maar bestaat uit 'blunders'. Daar kan je een verbeterplan op zetten, mee aan de slag. Maar het probleem is veel structureler. De Rijksoverheid heeft informatie vergaand ontsloten en daarbij de verantwoordelijkheid voor de beveiliging doodleuk bij de talloze eindpunten (gemeenten, huisartsen, apothekers, ...) neergelegd. Maar je kunt niet van een kleine organisatie verwachten dat ze een passende beveiliging optuigen voor een extreem privacygevoelig bestand over miljoenen mensen. De 'blunders' die we zien zijn symptomen, niet de oorzaak van de kwaal.

Er is een probleem gecreeërd waar we nog wel een tijdje mee te maken zullen hebben. Totdat er een omslag in het denken bij de Rijksoverheid plaatsvindt (neem beveiligingsrisico's serieus als je een architectuur bedenkt, in plaats van iets waar je achteraf een loodgieter voor belt) zullen we met regelmaat incidenten zien bij gemeente X en gemeente Y.

Mark Koek is zelfstandig ethical hacker en beveiligingsadviseur bij QCSec. Sinds 1999 werkte hij o.a. bij GOVCERT.NL, Deloitte en Fox-IT. Daarnaast was hij in zijn vrije tijd tot 2014 gemeenteraadslid en fractievoorzitter van D66 in de gemeenteraad van Leiden.

INFORMATION SECURITY OFFICER: SPELEN MET INVLOED

Informatiebeveiliging is een kwaliteitsaspect dat verbonden is aan bijna alles wat zich in een organisatie afspeelt. Als Information Security Officer vervul je een centrale rol en word je geconfronteerd met de meest uiteenlopende vraagstukken en risico's. Je invloed is echter niet vanzelfsprekend, en je ontleent deze vaak niet aan je hiërarchische positie. Je zult je gezags- of autoriteitspositie moeten verdienen én behouden. Maar let op, verdienen is iets anders dan afdwingen. Het vergroten van je invloed zonder in de afdwing-valkuil te stappen kan een behoorlijke uitdaging zijn.

Je kunt iedereen het spreekwoordelijke mes op de keel zetten om dingen voor elkaar te krijgen, maar na een paar maanden wil niemand meer met je samenwerken en lunch je alleen. Vanuit de inhoud gezien heb je waarschijnlijk gelijk en horen die risico's zo snel mogelijk te worden behandeld. Wil je echter op de lange termijn succesvol blijven, dan zul je anders te werk moeten gaan. Dit begint met het besef dat een goede relatie met je collega's cruciaal is voor een goede informatiebeveiliging. Wanneer je als bikkelharde handhaver door de organisatie trekt, dan zullen deze collega's je doorgaans (bewust of onbewust) buitenspel proberen te zetten. Uitzonderingen daargelaten is dat niet de wijze waarop je je invloed wilt vergroten. Het geeft wellicht resultaten op de korte termijn, maar je verspeelt op deze manier wel je eigen houdbaarheid.

Goede beveiliging niet vanzelfsprekend

Veel organisaties kenmerken zich tegenwoordig door de aanwezigheid van tegenstelde belangen, een sterke focus op functionele vernieuwing, werken onder hoge tijdsdruk, en een klantvraag die centraal staat. Hartstikke prima, maar niet wanneer beheer- en onderhoudswerkzaamheden van het bestaande ICT-landschap hieronder lijden. Deze vormen namelijk de basis voor een betrouwbare informatievoorziening, en wanneer de noodzakelijke aandacht hiervoor ontbreekt hopen de risico's zich in hoog tempo op.

Als Information Security Officer voel je dat het tijd is om in actie te komen, maar de ervaring leert dat dit niet gemakkelijk is. Een gedragen informatiebeveiligingsproces ontbreekt, de budgetten en beschikbare handjes voor het komende jaar zijn al grotendeels vergeven, en er is structureel geen prioriteit voor het implementeren van risico-mitigerende maatregelen. Inhoudelijk heb je een sterk verhaal met goede argumenten, maar op de werkvloer word je vaak ervaren als degene die kritische vragen stelt op een moment dat niemand erop zit te wachten. En omdat er doorgaans geen sprake is van een hiërarchische verhouding met je collega´s, zul je je omgeving op een andere wijze moeten beïnvloeden.

Begrijp het spel

Inhoudelijke kennis is absoluut noodzakelijk, maar niet de enige succesfactor. Op de juiste manier participeren in ´het spel´ wat zich dagelijks binnen de organisatie afspeelt, is minstens zo belangrijk. Investeer daarom ook in het begrijpen van de formele én informele context waarbinnen je opereert. Hoe loopt de besluitvorming? Wie zijn de spelers in het politiek bestuurlijke krachtenveld? Voor welke argumenten zijn ze gevoelig? Hoe reageren ze op elkaar? Wie trekt er achter de schermen aan de touwtjes? Hoe krijg je iemand het beste in beweging? Welk wisselgeld kun je hiervoor inzetten?

De antwoorden op dergelijke vragen geven inzicht in het politieke en culturele karakter van de organisatie, en helpen je om de paden naar jouw succes (acceptabele risico's) te kunnen bepalen. Maar het moeilijkste moet dan nog komen, en dat is het spelen van het spel. Pas wanneer dit lukt, ben je in staat jouw inhoudelijke kennis optimaal te benutten.

Verleiden zonder cadeautjes

Participeren in het spel is bepaald geen sinecure. Dit is met regelmaat de plek waar de tegengestelde belangen boven komen drijven en er wordt gevochten voor elke centimeter. Voor je het weet ben je getuige van het betere ellebogenwerk en doordachte politieke manoeuvres.

Omdat de reikwijdte van je invloed binnen het spel zich zelden beperkt tot de collega's met een formele rol in het besluitvormingsproces, is het belangrijk om met iedereen een goede relatie te onderhouden en continu te werken aan het vergroten van je autoriteitspositie. Deze zaken zijn namelijk bepalend voor de mate waarin collega's bereid zijn hun medewerking te verlenen, of zich openlijk achter je standpunt willen/durven scharen.

Kortom, als je eruit wil halen wat erin zit, heb je je collega's hard nodig. Maar hoe vergroot je nou je autoriteitspositie zonder de relatie met je collega's onder druk te zetten? De vele variabelen die van invloed zijn, maken het beantwoorden van deze vraag

Dennis Baaten is Security Consultant bij Baaten ICT Security. Dennis is bereikbaar via dennis@baaten.com

complex. Toch kun je als Information Security Officer een aantal dingen doen die bijdragen aan het vergroten van je autoriteitspositie, zonder dat daarmee je eigen houdbaarheid in het geding komt.

- **Beleid op orde** – zorg dat het informatiebeveiligingsbeleid op orde is, en zo hoog mogelijk in de hiërarchische boom is goedgekeurd. Dit voorkomt onnodige discussies, en helpt je bij het pareren van vragen zoals "waar staat dan dat dit moet?."

- **Aansluiten bij kernwaarden van de organisatie** – probeer tijdens het formuleren en/of onderbouwen van informatiebeveiligingsdoelen aansluiting te zoeken bij de kernwaarden van je organisatie. In de regel ontstaat hierover namelijk minder discussie omdat (bijna) iedereen deze erkent en niet zo snel zal tegenspreken.

- **Zichtbaarheid** – maak jezelf zo zichtbaar mogelijk. Bijvoorbeeld door aan te haken bij teamoverleggen, bilaterale overleggen met het management, of door het organiseren van awareness- en demosessies. Ga eens een dagje 'zwerven' op de werkvloer en toon interesse in het werk wat collega's doen. Leg contact, stel open vragen, en luister.

- **Geef complimenten** – je wordt verwacht kritisch te zijn, maar spreek het ook uit wanneer iets goed gaat. Een schouderklopje voor de beheerder die de nieuwe Java-patches snel heeft uitgerold, of een compliment voor de applicatiebeheerder die zijn autorisatiematrix goed op orde heeft. Voorkom dat de dingen uit jouw mond uitsluitend negatief zijn.

- **Practice what you preach** – het zijn vaak kleine simpele dingen, maar houd je aan je eigen regels. Vergrendel je pc bij het verlaten van je werkplek, zorg voor een schoon en opgeruimd bureau als er geen slot op de deur zit, gebruik geen cloud-diensten als je dat ook van je collega's verwacht. Je wilt niet uitstralen dat je het zelf allemaal niet zo nauw neemt met het volgen van de regels. Als jij je niet aan de regels houdt, komt er een moment dat dit tegen je wordt gebruikt.

- **Betrokken maar niet verantwoordelijk** – beleg de verantwoordelijkheid waar deze thuis hoort; zo dicht mogelijk bij de operatie. Blijf nauw betrokken, maar zorg dat de verantwoordelijkheid voor bijvoorbeeld het implementeren van maatregelen niet bij jou terecht komt. De Information Security Officer is nooit de probleem- of risico-eigenaar. Benadruk de verantwoordelijkheid van je collega's, maar biedt altijd aan om ze te helpen deze verantwoordelijk te nemen. Geef die credits maar één keer weg; help iemand een goede beurt te maken bij zijn/haar leidinggevende. Denk vanuit het belang van de organisatie.

- **Betrek de risico-eigenaar** – houd je niet alleen bezig met de ICT-afdeling (de aanbodzijde), maar betrek ook actief de business (de vraagzijde). Maak de business risicobewust, zodat deze de rol van risico-eigenaar op zich kan nemen. Een klant die vraagt om een goede beveiliging helpt enorm om de ICT-afdeling in beweging te krijgen. Zeker in omgevingen waar de klantvraag expliciet centraal wordt gesteld.

- **De eigenaar bepaalt risicobereidheid** – borg dat besluiten omtrent risico's op de juiste plek in de organisatie worden genomen; bij de risico-eigenaar. Deze bevindt zich zelden in de ICT-afdeling, maar bijna altijd bij de business. Wanneer de ICT-afdeling autonoom risico's wenst te behandelen, zonder de risico-eigenaar te betrekken, kunnen risico's uitsluitend worden verlaagd door het implementeren van (aanvullende) maatregelen. Alleen de eigenaar kan risico's accepteren. Vraag hierbij altijd om een risicoanalyse op basis waarvan het akkoord is gegeven. Enerzijds is dit de vastlegging van een geaccepteerd risico, en anderzijds geeft dit aan of de eigenaar goed heeft begrepen wat het risico inhoudt.

- **Risico-eigenaar betaalt de rekening** – een eigen budget kan voordelen hebben, maar is vaak ook een risico. Wanneer er met budgetten wordt gewerkt, zorg dan dat jij niet de budgethouder voor informatiebeveiliging bent. Hiermee voorkom je dat de implementatie van risico-mitigerende maatregelen afhankelijk wordt van jouw potje met geld. Een dergelijke directe betrokkenheid bij de uitvoering van het informatiebeveiligingsbeleid is niet gewenst.

- **Blijf die (tegen)druk geven** – jij stelt kritische vragen op momenten dat het anderen niet uitkomt. Dat hoort erbij, is gezond voor een organisatie, en zal nooit verdwijnen. Je behartigt nu eenmaal een belang binnen de organisatie wat vaak wordt ervaren als strijdig met andere belangen. Bij aanhoudende druk en uitblijvende resultaten, komt er een moment dat je collega's (vaak het management) zullen proberen om jouw druk te verminderen. Bekijk of het verstandig is je collega's tegemoet te komen, maar laat de druk niet (helemaal) wegvallen. Zonder druk stagneert vaak ook de voortgang, en dan kun je opnieuw beginnen.

- **Geef en neem op het juiste moment** – weet wanneer je op je strepen moet gaan staan, en zoek naar de juiste balans tussen geven en nemen. Ga je te vaak op je strepen staan (de bikkelharde handhaver) zonder dat dit het juiste effect sorteert, dan verliest dit voor je omgeving zijn waarde. Geef je teveel ruimte, dan word je ook niet serieus genomen. Bepaal

voor jezelf welk wisselgeld je hebt, en houd voet bij stuk wanneer het urgente risico's betreft die ook zo worden ervaren.

- **Onafhankelijke hiërarchische positie** – probeer met je hiërarchische positie je onafhankelijkheid te vergroten. Bij voorkeur dus niet binnen de ICT-afdeling, en wanneer dat wel zo is, dan liever in de staf in plaats van de lijn. In de basis geldt: creëer zoveel mogelijk afstand tussen jezelf en het organisatieonderdeel waarover je je het vaakst kritisch uitspreekt (en dat verantwoordelijk is voor de uitvoering). Dit voorkomt (de schijn van) belangenverstrengelingen.

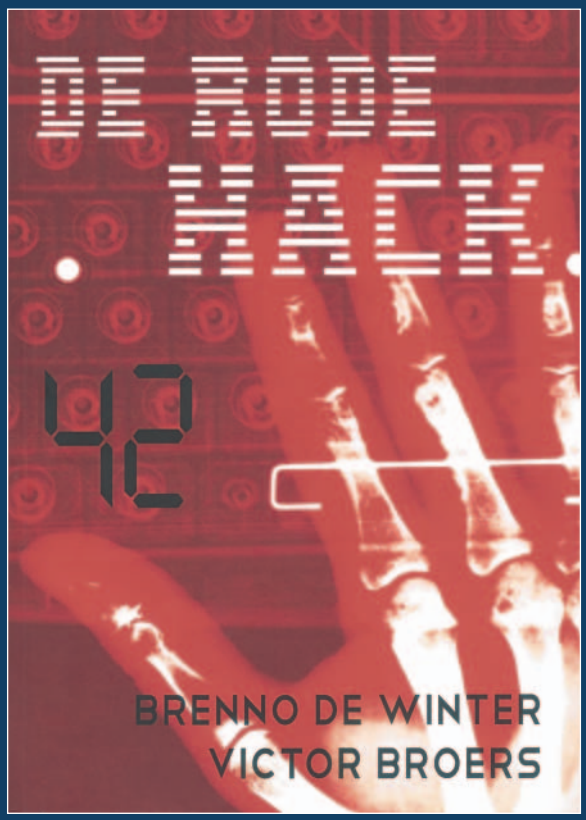
Blijf jezelf

Bovenstaande tips kunnen je helpen je effectiviteit als Information Security Officer te doen toenemen. Je wordt langzaam een informele autoriteit, met als gevolg dat je het spel gemakkelijker mee kunt spelen. Maar neem niets voor lief, en vergeet niet dat je voor het realiseren van een acceptabel risiconiveau grotendeels bent aangewezen op je eigen vaardigheden en inzichten. Bedenk hierbij dat organisaties zelden statisch zijn. Het vinden van de juiste modus waarin jouw toegevoegde waarde optimaal is, is een continu proces dat gepaard gaat met vallen en opstaan. Behaalde resultaten in het verleden bieden ook hier geen garantie voor de toekomst; morgen kan het zomaar anders zijn.

Het allerbelangrijkste is dat je jezelf blijft. Iedereen heeft een uniek karakter met voor- en nadelen die van invloed zijn op je gedrag. Uiteraard kun je leren je gedrag in jouw voordeel aan te passen, maar pas op dat je hiermee niet te ver van jezelf af komt te staan. Een goede manager/coach begrijpt dit en helpt je, binnen de kaders van je persoonlijkheid, met het optimaal leren benutten van je krachten. Wees creatief en voorkom dat je continu gedrag moet vertonen wat niet bij je past. Dat houd je niet vol en is bovendien geen prettig vooruitzicht wanneer de wekker 's ochtends weer afgaat.

DUBBELE BOEKBESPREKING: HELPENDE HACKERS EN DE RODE HACK

Titel: Helpende Hackers
Subtitel: Verantwoorde onthullingen in het digitale polderlandschap
Auteur: Chris van 't Hof
Taal: Nederlands
Pagina's: 255
Uitgever: Tek Tok Uitgeverij
Datum: Maart 2015
ISBN: 978-90-823462-0-6



Titel: De rode hack
Auteurs: Brenno de Winter, Victor Broers
Taal: Nederlands
Pagina's: 384
Uitgever: B for BooksdistriBution
Datum: Maart 2015
ISBN: 978-90-823231-0-8

Auteur: Lex Dunn (lex.dunn@capgemini.com)

Een dubbele boekbespreking, voor zover ik weet een primeur in het blad Informatiebeveiliging. Waarom? Omdat het toevallig zo uit komt! Tijdens de drukbezochte PvIB sessie over recente hacks op 26 Mei in Driebergen ben ik erin geslaagd om één van de weinige exemplaren van "Helpende Hackers" van Chris van 't Hof te bemachtigen. In de dagen daarna heb ik het direct gelezen, en viel me op dat Brenno de Winter een prominente rol had in het boek. Enige weken geleden had ik "De Rode Hack" gelezen, dus het leek me wel aardig beide boeken in één recensie te combineren.

Helpende Hackers van Chris van 't Hof

Chris is een welbekende spreker in het informatiebeveiligings-domein. Hij gaf ook een presentatie op de PvIB-sessie in Driebergen. Wij kennen hem natuurlijk ook van de column "Verantwoorde onthullingen" in ons aller lijfblad. Wie al die onthullingen trouw heeft gelezen zal veel herkennen in het boek. Veel van de gepresenteerde cases zijn al gepasseerd. Is daardoor het boek minder de moeite waard? Zeker niet! Allereerst heeft Chris veel achtergrondmateriaal toegevoegd, waarvoor in de columns geen plaats was. En verder, en wat mij betreft de grootste verdienste van het boek, zet hij het in het kader van de zich ontwikkelende "responsible disclosure". Een verschijnsel dat zo'n 10 jaar geleden nog volledig onbekend was, maar nu een redelijk geaccepteerde praktijk is. Vooral in Nederland, maar ook het buitenland begint zich er aan te wagen na eerst bij ons de kat uit de boom te hebben gekeken. In het boek geeft Chris een goed inzicht in de motivatie en achtergrond van de diverse partijen in cyber-security: de hackers, de security-officers, de opsporende en rechterlijke macht. Het blijkt dat veel hackers er niet a priori op uit zijn om iets te vernielen, of iets te stelen, maar vooral geïnteresseerd zijn in de werking van software en hardware en het blootleggen van kwetsbaarheden. Zij willen hun bevindingen delen met diegenen, die er wat aan kunnen doen om die gaten te dichten, waarbij zij wel de credits krijgen (en soms een of ander "lousy" T-shirt).
Maar er zijn ook hackers, die overdag een gerespecteerde baan hebben (bijvoorbeeld bij een ministerie) en in hun vrije tijd proberen zoveel mogelijk kwetsbaarheden te identificeren en opgelost te krijgen (0xDUDE lijkt de absolute leider in de ranglijst met 3993 gevonden kwetsbaarheden, ongetwijfeld ondertussen alweer wat meer). Alhoewel het OM zich het recht voorbehoudt om, ondanks de toezegging van een bedrijf een hacker niet te vervolgen als zij of hij een kwetsbaarheid meldt, toch tot vervolging over te gaan, lijkt ook daar meer begrip voor deze generatie te ontstaan. Het is niet altijd meer nodig ze met een stuk of tien zwaar bewapende leden van een arrestatieteam van hun zolderkamertje te lichten. Een uitnodiging voor een goed gesprek werkt vaak al zeer verhelderend voor beide partijen. Veel hackers die in het begin vaak ongeoorloofde of zelfs strafbare dingen deden, blijken nu "helpende hackers" om de weerbaarheid van onze BV Nederland te verhogen. En was dat nou net niet de bedoeling van die Nationale Cyber Security Strategie?

De Rode Hack van Brenno de Winter en Victor Broers

Brenno komt prominent naar voren in het boek van Chris, vooral natuurlijk met zijn Lektober-publicaties. Maar Brenno heeft, naast zijn journalistieke artikelen, ook samen met Victor Broers een interessant boek geschreven. Geen feitelijk verslag, maar een min of meer in roman vorm gegoten verslag van wat een werkelijke hack had kunnen zijn.
Het geheel speelt zich af in de financiële wereld van de Zuid-As in Amsterdam. In het boek komt een fictieve hoofdrolspeler na een persoonlijke crisis in aanraking met een aantal prominenten in de wereld van ICT en cyber-security. Hij besluit zijn verdere carrière daar aan te wijden, en komt dan in zijn rol als security-officer bij een nieuwe bank tot zijn verbazing transacties tegen die geen geld van de bank ontvreemden, maar saldo bijschrijven op willekeurige rekeningen. Dat dit tot grote paniek bij de banken en de overheid leidt mag duidelijk zijn. Zelf het hele Europese politieke circus komt aan bod met een kijkje achter de schermen.
Terzijde gestaan door een schone dame, die later een zeer merkwaardige rol blijkt te spelen, slaat onze held zich door de muren van ongeloof en ontkenning heen, die rondom zijn ontdekkingen worden opgeworpen. In de loop van het verhaal blijken nog meer bekenden uit de cyber-security-wereld in Nederland acte de presence te geven (overigens allemaal met hun volledige instemming). Tegen het einde van het boek komt Snowdon ook nog even om de hoek kijken, met een verklaring hoe die er (mogelijk) in geslaagd is uit Hong Kong te ontsnappen richting Rusland, terwijl alle grote inlichtingendiensten toch zeker wisten dat 'ie ergens anders naar toe ging.

Dat einde van het boek gaat ook ineens een stuk sneller, waardoor je het idee krijgt dat je iets gemist hebt in de opbouw van de verhaallijn. Wat mij betreft een goed boek om enerzijds inzicht te krijgen in wat een heel bedreigend scenario zou kunnen zijn, en anderzijds hoe daarop vanuit financiële wereld, overheid en opsporingsdiensten op gereageerd wordt. Het verhaal is duidelijk vanuit een grote persoonlijke ervaring van beide auteurs met de materie geschreven, en is dan ook zeker aan te raden. Zeker voor diegenen, die weten wat "42" betekent.

MODELLING THREAT SCENARIOS DEEL 1

Dit artikel gaat over het modelleren van threat scenarios; business aligned threat scenario-modelling om precies te zijn. Eerst zal het concept van een dreiging gedefinieerd worden in termen van Equity, Prospect en Material Events. Daarna zullen een aantal Key Risk Indicators gedefinieerd worden. Deze indicatoren doen dienst bij het analyseren van impact van material events op de business. Het Business Model Canvas zal ingezet om op een gestructureerde wijze tot een Threat Scenario Model te komen. Dit artikel focust op de introductie van de concepten. Een vervolgartikel zal aan de hand van een voorbeeld in detail ingaan op deze materie.

De concepten Equity en Prospect zijn aangewezen als belangrijke bouwstenen voor de doelstellingen van dit artikel. Equity wordt gedefinieerd als:

$$Equity = Assets - Liabilities$$

Deze vergelijking is de basis van de (kolommen)balans van ieder bedrijf. Het stelt dat vermogen het verschil is tussen bezittingen en schulden. In het artikel Treating Risk Prospectively [1] is concept prospect gedefinieerd als:

$$Prospect = Opportunity * Probability_{opportunity} - Risk * Probability_{risk}$$

Voor een bepaalde doelstelling is de prospect gedefinieerd als de verwachte opbrengsten verminderd met de risico's en andere kosten. Het is interessant om de relatie tussen Equity en Prospect nader te beschouwen.

De relatie tussen Equity en Prospect

Er is een vrij evidente relatie tussen Equity en Prospect. Als we ervan uitgaan dat alle probabilities gelijk zijn aan 1, oftewel als de onzekerheden zekerheden zijn, gelden de volgende vergelijkingen:

$$Equity = Assets - Liabilities$$

en

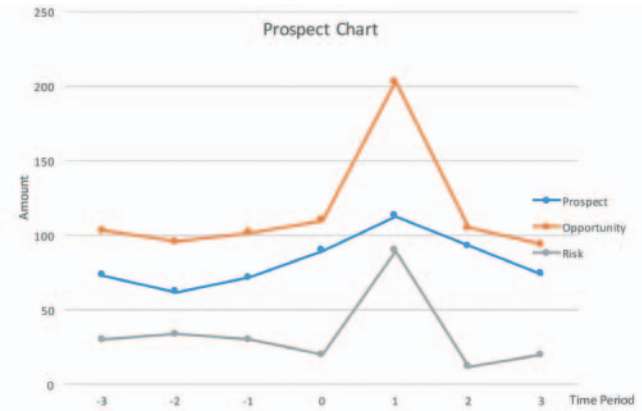
$$Prospect = Opportunity - Risk$$

Als geldende probabilities gelijk zijn aan 1 dan zijn Equity, Assets en Liabilities respectievelijk synoniem met Prospect, Opportunity en Risk. Deze stelling wordt verder toegelicht aan de hand van een zogenaamde prospect chart.

Michèlle Gittens studeert Economie en Bedrijfskunde aan de Universiteit van Amsterdam met de keuzerichting Financiering en Organisatie. Zij is te bereiken via michellegittens93@gmail.com.

Een prospect-chart

Een prospect-chart is een grafische weergave aan Equity en Prospect langs een tijdslijn. Figuur 1 geeft een voorbeeld.



Figuur 1 - Prospect-chart

Ten opzichte van een tijdstip tb in het verleden geldt voor alle tijdstippen $t \leq tb$ dat Equity = Prospect. Voor $t > 0$ geldt deze vergelijking niet. We stellen dat bij $t > 0$ de prospect gelijk is aan de verwachte Equity in tijdsperiode t. Een relevante vraag is: waarom verandert de prospect? Het antwoord op deze vraag geeft ons aanleiding om het concept van een Material Event te introduceren.

Material Events

Een Material Event is een gebeurtenis in de tijd die in materiële zin impact heeft op de prospect. De prospect op een tijdstip tk definiëren we als:

$$Prospect(t_k) = Prospect(t_0) + \sum_{t=1}^{k} ME_t$$

Hierbij is een Material Event (MEt) een gebeurtenis in tijdsperiode t met een materiële impact op de Prospect. In essentie is de stelling dat prospect in de toekomst sterk bepaald wordt door de Material Events uit het verleden.
Uit de definitie van een Material Event volgt al snel de definitie van een threat of een dreiging zoals wij dat in dit artikel willen hanteren.

Een dreiging definiëren we als 'een Material Event die de prospect doet afnemen'.

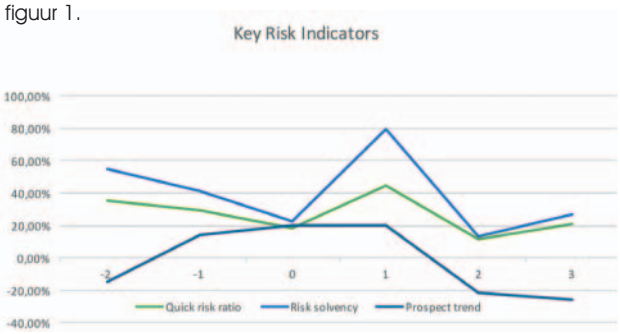
Key Risk Indicators

We nemen een zijstap en staan stil bij een aantal indicatoren die ingezet kunnen worden op een Enterprise Risk Dashboard. De indicatoren worden omschreven in tabel 1.

Indicator	Omschrijving
Prospect Trend	Geeft het verschil van de prospect op opeenvolgende tijdsperiodes
Quick Risk Ratio	De verhouding tussen de risk en de opportunity
Risk Solvency Ratio	De verhouding tussen de risk en de prospect

Tabel 1 - Key Risk Indicators

Figuur 2 geeft een voorbeeld van de bovenstaande risk-indicatoren correspondeert met de voorbeeld gegevens uit figuur 1.



Figuur 2 - Key Risk Indicators

De volgende stap die we willen nemen om tot een Business Aligned Threat Scenario Model te komen is de introductie van het Business Model Canvas.

Het modelleren van de business

We stellen dat de kwaliteit van een Business Aligned Threat Scenario Model sterk afhankelijk is van de kwaliteit van het Business Model en de architectuurmodellen die bij het opstellen van het Threat Scenario Model gebruikt worden. Voor het

Maurice Gittens CGEIT, CISA, CISM werkt als consultant met informatiemodelleren, informatieverwerking, informatiearchitecturen en informatiebeveiliging. Hij is momenteel risk strategy consultant bij een Nederlandse Bank. Hij is te bereiken via maurice@gittens.nl.

Prospect in de toekomst wordt sterk bepaald door de Material Events uit het verleden

Building blocks	Beschrijving
Customer segments	Brengt de doelgroep in kaart. Laat zien welke klanten het meest belangrijk zijn.
Value propositions	Laat zien welke onderscheidende en/ of waarde toevoegende proposities je de klant biedt en aan welke klantbehoefte voldaan wordt.
Key activities	Geeft de activiteiten weer die nodig zijn om de value propositions te kunnen bieden.
Key partners	Geeft aan welke partners het belangrijkst zijn en welke resources ze leveren.
Cost structure	Laat de kostenstructuur in relatie tot de key resources en de key activities zien.
Revenue streams	Toont waar de geldstromen vandaan komen en hoe deze ontstaan.
Customer relationships	Brengt de klantrelaties in kaart.
Key resources	De bedrijfsmiddelen (inclusief mensen) die essentieel zijn om de value propositions te bewerkstelligen.
Channels	De online en offline kanalen waarmee contact met de klant gehouden wordt.

Tabel 2 - Building Blocks van het Business Model

maken van Business Aligned Threat Scenario-modellen is het Business Model Canvas (BMC) [2] nuttig gebleken.
Het BMC is een instrument dat ingezet wordt bij het ontwerpen en analyseren van business-modellen.
Het BMC bestaat uit negen, zogenaamde, building blocks, die ieder een belangrijk aspect van een business-model dekt. Tabel 2 geeft een korte omschrijving van de building blocks, maar de lezer wordt uitgenodigd om meer over de materie te achterhalen.

Het BMC is een duidelijk hulpmiddel om de verschillende bedrijfsaspecten in kaart te brengen.
Anders gezegd, het BMC zet bedrijfsbelangen op een rijtje. Gebeurtenissen die afbreuk doen aan relevante bedrijfsbelangen horen onderdeel te zijn van het Threat Scenario Model.

Samenvatting

In dit artikel zijn de concepten geïntroduceerd die in een tweede deel gebruikt zullen worden om in meer concrete zin in te gaan op Business Aligned Threat Scenario Modelling. Eerst is de relatie tussen Equity en Prospect uitgewerkt en als basis gebruikt voor de definitie van Material Events. Verder zijn een aantal Risk Indicators geïntroduceerd die nuttig kunnen zijn bij het analyseren van de risicopositie van een onderneming. Als laatste is het Business Model Canvas geïntroduceerd. Dit instrument zal worden ingezet om bedrijfsbelangen ter analyse op een rijtje te zetten.

Deel 2 van dit artikel zal de bovenstaande concepten inzetten om in detail in te gaan op Business Aligned Threat Scenario Modelling.

Links

[1] Artikel in Informatiebeveiliging: "Management Risk Prospectively" in IB1 2015.
[2] Business Model Generation, A. Osterwalder, Yves Pigneur, Alan Smith, and 470 practitioners from 45 countries, (2010)

PRIVATE

The principles of information and data privacy are well established and have appeared for many years to be straightforward and simple. However the growth of online social media is making this issue more and more difficult to regulate according to these principles. One of the main areas for concern is the publication of digital photographs. We shall therefore re-examine a long-established SABSA attribute – private.

The principles in the European region focus on the concept of the data subject – the person to whom the information refers. Typical examples are medical records – kept by hospitals and doctors for legitimate purposes but not to be disclosed to third parties without the explicit permission of the data subject. However, the rules apply to any organization that keeps names and addresses and other personal data. The range of applicability is very wide indeed, to the extent that all organisations have data subjects and must comply with the national laws that implement the EU directive.

Individual data subjects may themselves divulge any or all of this information if they so choose, and with the surge in social networking on the web it has become popular and fashionable to share personal information that previous generations would have considered very private. Young people don't just wear their heart on their sleeve, as the saying goes, but they wear their life on their Facebook page and their Twitter account.

So, a family goes on holiday to some tourist destination and they all carry a full arsenal of photographic devices – smart phones, tablets and digital cameras. Digital photos cost nothing so they take hundreds and hundreds of them. As they pose for selfies or group photos they capture a certain amount of the environment around them, including other people unknown to them. Some of these people might possibly be famous celebrities, politicians or similar – people with a desire to segregate their public and private lives.

When the family returns home, or even while they are still travelling, they post selected pictures on Facebook or Tweet them from their Twitter account. They publish these photos for the entire world to see. So if a celebrity or similar person is shown in the picture, it is possibly embarrassing for that person if they would prefer not to be seen at that place on that day and time, or even worse, in the company of another person that suggests a private relationship not to be made public. The consequences might be serious for their private or public lives, depending on the context.

This begs several questions: Who is the data subject? Who is the data owner? Who has primacy over the data? Are there any data stewards involved and what are their responsibilities? Generally speaking it is an accepted principle that where the data concerns a living person that person is the data owner and has primacy over the protection or publication of that data. But in this use case it is not clear whether or not accidental strangers can be considered as data subjects in the photographs. If the photograph was shot in the public place this might be a case for declaring the data to be already in the public domain, but has that been tested in any court of law? If the 'accidental subject' complains to Facebook or Twitter, what policy should the management of those web sites adopt, since they could be considered to be 'data stewards' with responsibility for protecting the data according privacy principles?

It's a new emerging area of the digital age and of social networking. It is something about which we information risk and security experts need to get our thinking straight to be able to advise our masters and clients as to what policies they should adopt. As with all SABSA Attributes, it's about asking the right questions to prompt the right discussions amongst the stakeholders as to which risks are acceptable and which are not.

The Attributer

IT-SECURITY HEEFT OLYMPISCHE AMBITIES

Achmea verandert in een digitale verzekeraar. Steeds meer zaken worden online afgehandeld. Dat brengt ook een beveiligingsrisico met zich mee. Internetcriminelen azen namelijk op persoonsgegevens. Manager it-security bij Achmea, Henry Meutstege, vertelt hoe de verzekeraar zich wapent tegen cybercriminelen en inspeelt op de continu veranderende aanvalsmethoden en bedreigingen. ‘We willen de meest vertrouwde verzekeraar van Nederland zijn.’

'Cybercriminelen hebben hun 'werkterrein' verlegt van banken en de diefstal van creditcardgegevens naar organisaties die persoonsgegevens verwerken. Met gestolen gegevens van bijvoorbeeld verzekeraars proberen ze identiteitsfraude te plegen. Ze gebruiken die data bijvoorbeeld om onterechte claims in te dienen of verkopen de gegevens aan malafide organisaties die misbruik maken van subsidies', vertelt Meutstege.

De druk op de beveiliging van de systemen van de verzekeraar is groot. 'We houden dagelijks honderden tot soms wel duizenden aanvalspogingen tegen. Criminelen proberen via een beveiligingslek in een app of website binnen te dringen. Ook via gekopieerde sites en nepmails proberen ze gegevens binnen te hengelen (phishing red.). Ook komen DDoS-pogingen, waarbij criminelen hele websites proberen plat te leggen nog steeds voor.'

Het it-securityteam van de verzekeraar groeide de afgelopen jaren van twintig naar dertig man en is onderverdeeld in drie groepen. Medewerkers van het security operations center (soc) monitoren 24x7 de beveiliging van de systemen en anticiperen op incidenten. Testers controleren of nieuwe systemen,apps en webportals veilig zijn. De derde groep bestaat uit security consultants. Zij adviseren projectteams over de beveiliging van systemen en bedrijfsvoering (processen) van verzekeringsproducten. 'Naast de ambitie om onze bedrijfsvoering grotendeels te digitaliseren, willen we ook de meest vertrouwde verzekeraar van Nederland zijn. De lijnen tussen het security-team, de IT-directie en de raad van bestuur zijn kort', aldus Meutstege.

Persoonlijke ontwikkeling

Meutstege: 'Beveiliging draait om de stappen preventie, detectie en response en je ziet eigenlijk dat het een cirkel van continu verbeteren is. We zijn weerbaar tegen gevaren van buitenaf en leren continue van de aanpassingen die we doen. In vaktermen heet dat dan een resillient enterprise.' Hij vertelt dat de ambitie op de security afdeling hoog ligt. Meutstege: 'Ik wil mijn team zo sterk maken dat we in 2016 deel kunnen nemen aan de Cyberlympics. Dat is een prestigieus evenement waarin de beste red en blue teams van de wereld het tegen elkaar opnemen.'

'We willen constant blijven verbeteren en professionaliseren. Binnen security moet je continu aan je kennis werken.' Hij vertelt dat er voor de medewerkers dan ook veel aan persoonlijke ontwikkeling wordt gedaan. Meutstege: 'Van traditionele securityspecialisten en ethical hackers bestaat het beeld van een nerdy persoon die communicatief niet erg sterk is.

'Wij hebben mensen nodig die naast vakkennis ook aan de business kunnen uitleggen waar techniek over gaat. Ze moeten de risico's kunnen vertalen naar bedrijfs-processen en business-managers. Daarnaast moeten ze bereid zijn kennis en kunde telkens aan te blijven scherpen.'

Hij noemt een voorbeeld: 'Onze securitytesters hoeven bij business-managers niet aan te komen met: 'We zijn slachtoffer van SQL injection.' We willen juist dat ze zonder jargon kunnen uitleggen wat er aan de hand is. In dit geval gaat het erom dat je kan uitleggen dat er een programma actief is dat ongezien de database zou kunnen 'leeglezen', wat het risico is als zich zo'n incident voordoet en wat we er tegen kunnen doen.'

Meutstege vertelt dat de security afdeling verschillende tests en projecten uitvoert. 'Er zijn bijvoorbeeld red-team projecten waarin de ene groep testers scenario's bedenkt om systemen aan te vallen en de andere groep de systemen moet verdedigen. Ook worden er regelmatig security- en penetratietests gepland. 'Binnenonssecurity-team moet je continue aan je kennis blijven werken.'

1600 ICT'ers

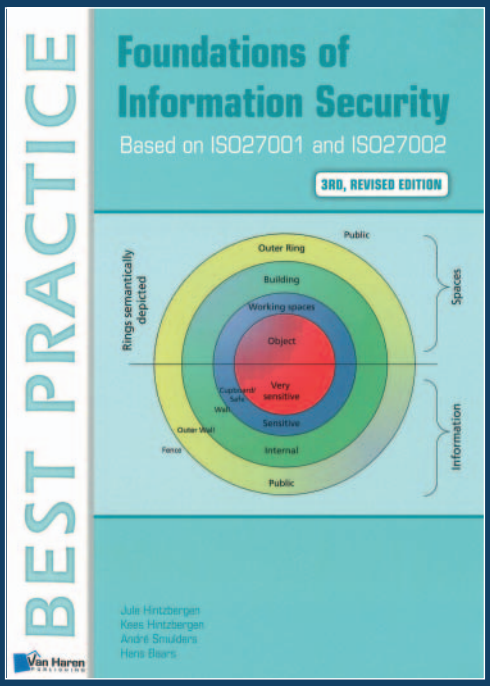
Achmea telt 17.000 medewerkers. Onder het bedrijf vallen vijf grote labels: Centraal Beheer, Zilveren Kruis, FBTO, Interpolis en Avero. Bij de organisatie werken 1600 ict'ers.

Aan de slag bij Achmea?

Kijk hier voor vacatures binnen het security-team.

Henry Meutstege is Senior IT Manager bij Achmea en binnen Achmea verantwoordelijk voor IT Security. Je kunt Henry bereiken op het e-mail adres henry.meutstege@achmea.nl

BOEK-BESPREKING



Boekreview: Foundations of Information Security, based on ISO27001 and ISO27002. Derde herziene uitgave.
Auteurs: Jule Hintzbergen, Kees Hintzbergen, André Smulders en Hans Baars
Aantal Blz: 188
ISBN: 978-94-018-0012-9
Uitgever: Van Haren publishing

In de serie Best Practice is dit jaar de derde herziene uitgave van Foundations of Information Security, based on ISO27001 and ISO27002 uitgegeven. De update van deze uitgave met de informatie uit nieuwe informatiebeveiligingsstandaarden maakt dat het boek, eerste uitgave 2005, weer helemaal bij de tijd is. Na een korte introductie van het boek, wordt het casusbedrijf geïntroduceerd bij de lezer, een boekwinkel. Bij enkele hoofdstukken wordt het bedrijf gebruikt om praktijksituaties te schetsen en hierover vragen te stellen zodat inzicht wordt verkregen hoe de behandelde onderwerpen kunnen worden toegepast in de praktijk.
De security-definities en -concepten worden behandeld, uiteraard de kwaliteitskenmerken CIA en risicomanagement: hierbij wordt ook de standaard ISO27005 benoemd en de relevante onderwerpen uit de standaard kort behandeld. Verwijzingen in de voetteksten naar informatie op het internet geven de lezer de mogelijkheid om zich verder te verdiepen. Deze bevatten weblinks naar opensource methoden en organisaties zoals bijvoorbeeld TOGAF en Sans.
Het opzetten van een informatiebeveiligingssysteem, dat past bij de organisatie en haar doelstellingen is een belangrijke voorwaarde om informatiebeveiliging in de organisatie succesvol te implementeren en in de dagelijkse praktijk uit te voeren. Kennis van de organisatie, de betrokken partijen bij de organisatie (interested parties) en methoden voor het continue verbeteren van het systeem worden behandeld en begrippen in deze context worden uitgelegd.
TOGAF wordt als opensource-methodiek aangehaald voor het beschrijven van de informatie-architectuur en de inrichting hiervan in een bedrijf. Vanaf hoofdstuk 5 is het boek ingedeeld conform de hoofdstukindeling van de ISO27002:2013 standaard. Prima stap van de auteurs, zodat het boek ook kan worden gebruikt als naslagwerk bij de implementatie van de ISO27002, om projectleden etc. meer informatie te geven als achtergrond bij de best practices in deze standaard. In de hoofdstukken 5 t/m 17 wordt op een heldere manier ingegaan op de onderwerpen in de overeenkomstige hoofdstukken van de ISO27002:2013 waarbij diepgaandere uitleg wordt gegeven over het onderwerp en de mogelijke maatregelensfeer.

Een greep uit de behandelde onderwerpen:
Het opstellen van informatiebeveilingsbeleid en de review hiervan zodat het informatiebeleid passend blijft op de organisatie, de informatiebeveiligingsorganisatie; rollen en verantwoordelijkheid en het organiseren van informatiebeveiliging, o.a. bij gebruik van mobiele communicatie en telewerken.

Informatiebeveiliging vanuit het HR-perspectief, welke maatregelen zijn te nemen voordat nieuwe medewerkers in dienst treden, tijdens het dienstverband en bij uitdiensttreden of wijzigingen in het dienstverband. Waarin zitten de waarden van het bedrijf? Assets. Assetmanagement gaat in op de verantwoordelijkheden voor deze assets, informatie in de vorm van documenten, gegevens in databases, computer-

Foundations of Information Security is een helder geschreven boek waarin de basisbegrippen en technieken over informatiebeveiliging begrijpelijk worden uitgelegd aan de lezer.

programma's (software) & hardware, media zoals CD-ROM's USB-sticks maar ook niet tastbare waarden zoals reputatie en imago. Uitleg wordt gegeven over het beheer van assets, hoe je hiermee omgaat en gebruikt. Het classificeren van assets die bepalend zijn voor de van toepassing zijnde beheermaatregelen. De term BOYD is geïntroduceerd en wat dit betekent voor het beheersen van de bedrijfsinformatie op of benaderbaar via dit persoonlijke IT-hulpmiddel.
Aandacht wordt besteed aan de logische toegangsbeveiliging op systeem- en applicatielaag en welke vormen van logische toegangsbeveiliging bestaan en de voor of nadelen hiervan voor een organisatie en/of informatie eigenaar.
Cryptografie wordt ingeleid met de introductie van Beleid en sleutelmanagement. Hierna worden de verschillende soorten cryptografiesystemen uitgelegd en aan de hand van voorbeelden wordt de werking toegelicht.

De Fysieke beveiliging en beschermen tegen invloeden van buitenaf van systemen en infrastructuur die opgesteld staan in Datacenters en andere locaties beschrijft o.a. het regelen van de toegang tot de systemen in de locatie ter bescherming van de systemen met data, het beheersen van omgeving in de vorm van temperatuur, luchtvochtigheid etc. En daarnaast het treffen van voorzieningen bij spanningsuitval en het uitbreken van brand om de onderbreking van de diensten aan de bedrijfsvoering te minimaliseren. 2 praktijkvoorbeelden illustreren het belang van fysieke beveiliging.
Beveiliging als onderdeel van het dagelijkse beheer beschrijft de rol van processen zoals change- en capacity-management. Aandacht wordt besteed aan het voorkomen van malware, phishing en spam geïllustreerd met voorbeelden gerelateerd aan de case. Definities worden verder uitgebreid gericht op bedreiging zoals virussen, malware en botnets.
Het nut en de noodzaak van het maken van back-ups en logging en monitoring komen aan bod om de continuïteit te kunnen borgen en vast te kunnen stellen wat de oorzaak van een mogelijke verstoring is geweest aan de hand van o.a. de logging. Tot slot passeert in dit hoofdstuk ook de beheersing van zwakheden in de techniek de revue.
De borging van Compliance is kort samengevat en in een aantal paragrafen is ingegaan op wet en regelgeving, intellectueel eigendom, privacy etc. Een overzicht van de diverse organisaties die standaarden, richtlijnen en best practices publiceren ronden dit hoofdstuk af.
Tot slot, in de bijlagen treffen we een verklarende woordenlijst aan, een overzicht van ISO27000-standaarden en een proefexamen ter voorbereiding op het EXIN Information Security Foundation-examen.
Foundations of Information Security is een helder geschreven boek waarin de basisbegrippen en technieken over informatiebeveiliging begrijpelijk worden uitgelegd aan de lezer. Het boek is voor iedereen geschikt die meer wil weten over informatiebeveiliging en de basiskennis op te doen over informatiebeveiliging nodig om het foundations-examen te kunnen doen.
Daarnaast kan het ook als naslag dienen voor personen die bij implementatie van een ISMS betrokken zijn om inhoudelijk meer informatie te krijgen over de onderwerpen uit de ISO27002:2013-standaard. Voor dit laatste is het handig dat de inhoudsindeling hierbij de norm volgt.

Gerhard Mars, CISM CISA is werkzaam als auditmanager bij Capgemini Nederland B.V. Hij is verantwoordelijk voor de uitvoering van de interne en externe kwaliteit-, IT-audits en assurance-verklaring o.b.v. ISAE3402.

NCSC GEBRUIKT SIVA-RAAMWERK IN NIEUWE RICHTLIJN

Nieuwe versie Beveiligingsrichtlijnen voor Webapplicaties

Het Nationaal Cyber Security Centrum (NCSC) heeft een vernieuwde versie van de Beveiligingsrichtlijnen voor Webapplicaties opgesteld [1]. Deze versie heeft het NCSC in samenwerking met deskundigen van UWV en Inspearit tot stand gebracht. Daarnaast zijn vertegenwoordigers vanuit diverse doelgroepen betrokken geweest bij de beoordeling van deze herziening.

In februari 2012 publiceerde het NCSC de ICT-Beveiligingsrichtlijnen voor Webapplicaties. Deze ICT-Beveiligingsrichtlijnen voor Webapplicaties vormen een leidraad voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. De Beveiligingsrichtlijnen zijn breed toepasbaar voor ICT-oplossingen die gebruik maken van webapplicaties. Sinds de publicatie worden deze Beveiligingsrichtlijnen door veel sectoren toegepast.

SIVA-raamwerk

De voornaamste verandering ten opzichte van de versie uit 2012 is dat de structuur van de Beveiligingsrichtlijnen is verbeterd conform het SIVA-raamwerk voor auditreferentiekaders. Hierdoor zijn de verschillende richtlijnen logischer gegroepeerd en is het eenvoudiger om voor afzonderlijke doelgroepen een selectie te maken met voor die doelgroep relevante richtlijnen. Er is een beperkt aantal nieuwe richtlijnen toegevoegd en per richtlijn zijn de voorgestelde maatregelen herzien op basis van de huidige inzichten.

Het SIVA-raamwerk zal voor velen onbekend zijn. Twee van de auteurs van deze richtlijn, Wiekram Tewarie en Eric Nieuwland, schreven met Eline ter Meer in 2014 het boek 'SIVA - Methodiek voor de ontwikkeling van auditreferentiekaders' (ISBN 978-90-8659-670-6). Dit is in eigen kringen goed ontvangen, getuige de review in de IT Auditor [2]. Het wordt vooral 'praktisch' genoemd. Reden genoeg kennelijk voor het NCSC om het uit het auditdomein te trekken en in een richtlijn te gebruiken. De richtlijn is in twee versies gepubliceerd: De 'richtlijnen' (41 pagina's) en de 'verdieping' (108 pagina's). De eerste reacties bij de redactie geven aan dat de richtlijn wordt ervaren als een overzichtelijk document, maar het is ook abstract en omvangrijk. Je kunt natuurlijk wel verwachten dat jouw auditor zich wel moet kunnen vinden in jouw toepassing van deze richtlijn, het moet eenvoudig zijn dit aantoonbaar aan te pakken.

Is het gebruik van SIVA voor richtlijnen een handige zet? De redactie hoort graag ervaringen uit de praktijk.

Links:

[1] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[2] http://www.deitauditor.nl/beroepsontwikkeling-reglementering/siva-methodiek-voor-de-ontwikkeling-van-auditreferentiekaders/

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

BLACK HAT EN DEF CON 2015

De 2015-edities van Black Hat en DEF CON hebben weer plaatsgevonden in Las Vegas. Traditioneel wordt hier een hele serie nieuwe hacks in geuren en kleuren getoond aan de wereld, waarbij presentatoren met sterallures elkaar de loef proberen af te steken.

Wat zijn de hacks waar we nu echt bevreesd voor moeten zijn? En welke hacks zijn maar showverhalen? De redactie blikt terug.

Maarten Hartsuijker

Blackhat/Defcon 2015 stonden voor mij in het teken van twee presentaties: de inbraak in een Jeep en de Stagefright-bug in Android.

Toen Charly Miller en Chris Valasek in 2013 een Toyota Prius onder handen namen, werd hun aanval door verschillende fabrikanten gebagatelliseerd. Het feit dat ze bekabeld de voertuigcontrole over konden nemen maakte het voor velen een theoretische aanval. Dit jaar hebben ze vergelijkbaar onderzoek gecombineerd met een lek in de "connected"-software van Jeep. Hierdoor konden ze de besturing van de auto over nemen terwijl deze kilometers verderop op de snelweg reed. Hoewel ik uit eigen onderzoek weet hoeveel fouten er nog in connected-car-omgevingen te vinden zijn vond ik het resultaat van dit onderzoek confronterend. Het vragen van losgeld voor het vrijgeven van bestanden (ransomware) was nog nooit zo 2014. Binnenkort krijgen we op de snelweg slechts minuten de tijd om te kiezen tussen het overmaken van ons spaargeld of een frontale botsing.

De aankondiging van de Stagefright-bug zette Android-land op zijn kop. Deze enkele bug in combinatie met het slechte updatebeleid van OEMs als Samsung, HTC en LG zal er bij velen (in mijn omgeving in elk geval wel) toe hebben geleid dat Android per direct onderaan de zakelijke voorkeurslijst kwam te staan. De verkoopafdelingen van deze fabrikanten moesten overuren maken om hun klanten beterschap te beloven, zonder echter concrete toezeggingen te kunnen doen over wanneer Android-toestellen van nog geen jaar oud gepatcht zouden worden. Android leek jaren een goedkoop alternatief. Maar ga je de jaarlijkse afschrijving op basis van de "security levensduur" berekenen, dan blijkt goedkoop in eens duurkoop te zijn.


Lex Borger


Carlo Seddaiu


Maarten Hartsuijker

Carlo Seddaiu (gastbijdrage)

De Black Hat- en DEF CON-conferenties laten elk jaar weer duizenden hackers, script-kiddies en security-experts samen komen in Sin City Las Vegas. Zoals gebruikelijk vinden er elk jaar weer gekke dingen plaats tijdens de conferenties. Maar dat hoort erbij als je duizenden technofreaks bij elkaar brengt op een paar vierkante kilometer. De toon die wordt gezet dit jaar is duidelijk. Meer dan ooit is niets is meer veilig!

Het is goed om te bedenken dat de hacks die worden gedemonstreerd op de Black Hat- en DEF CON-sessies het topje van de ijsberg vormen. De presentaties van dergelijke hacks helpen om te laten zien dat we in een digitale samenleving bijzonder kwetsbaar zijn. De hack van de Jeep toont aan dat producenten op het gebied van veiligheid in het digitale domein nog veel te leren hebben. Het Internet of Things hangt onze auto, televisie, koelkast, boiler en nog veel meer zaken aan Wifi of Internet. De gevolgen van het blokkeren van de wielen terwijl een auto honderddertig rijdt, zijn duidelijk. Gaat de toekomst ons leren dat een oververhitte boiler brandgevaar kan opleveren? Of dat een vriezer die overdag expres hoger wordt gezet onverwachte voedselvergiftiging kan opleveren? Maak maar geen ruzie meer met die script-kiddie van de buren... Dat kon je nog weleens duur komen te staan bij volgende diepvriespizza! Hebben we straks een SIEM-oplossing nodig om ons huis te bewaken?

Voor wat betreft de hack die rootkits in verouderde CPU's mogelijk maakt kunnen we kort zijn. Leuk, maar alleen in speciale gevallen waar ze gebruikt worden een risico nog. Wat wel serieus misbruikt kan worden en dus een serieus risico vormt is de Android hack op afstand. Die trouwens kort daarna ook nog werd opgevolgd door een tweede... Dat zijn echt grote klappers omdat het patchen van dergelijke kwetsbaarheden veel te traag gaat door de meerlaagsinrichting van Android-patchmanagement: Google, fabrikanten en ISPs. Terwijl we een breed gebruik zien van de mobiele telefoon als "vertrouwd" apparaat voor vertrouwelijke communicatie, als authenticatiemiddel en om te bankieren. De mogelijke impact van misbruik op vele miljoenen gebruikers is groot. Is de implementatie van beveiliging in software en hardware van een gemiddelde mobiele telefoon eigenlijk wel van voldoende niveau? Als we kijken naar de LTE/3G-modemhack die volhardende malware in hardware mogelijk maakt ga ik twijfelen.

Het is goed om je te realiseren dat veel hacks vandaag de dag niet meer publiek gemaakt worden. Die worden voor veel geld verkocht in bepaalde circuits, waar bedragen van vijfentwintigduizend tot wel tweehonderdvijftigduizend euro normaal zijn. Laten we de hackers die deze informatie delen dankbaar zijn want het helpt om fabrikanten onder druk te zetten veiligheid als onderdeel van hun product te gaan zien. Dat levert ons als klant uiteindelijk een beter product op... Die SIEM-gekoppelde diepvries kunnen we dan hopelijk nog even uitstellen.

Lex Borger

Deze conferenties zijn ieder jaar weer goed voor een aantal verrassingen. Mijn persoonlijke top drie:

3. De NTLM-wachtwoordhashaanval via SMB-relay. Vijftien jaar na de introductie van Kerberos in Windows is NTLM nog steeds in gebruik en is het mogelijk NTLM-wachtwoordhashes buit te maken. Via het internet. Wordt het niet tijd om NTLM met pensioen te sturen?
2. We weten al dat statische radiocodes versturen om deuren op afstand te openen heel eenvoudig te hacken is (als je dat al een 'hack' mag noemen). Dus gebruiken we een voortrollende code: een code die elke keer anders is. Hoe krijg je als hacker een toekomstige code te pakken? Door vanaf een radio-in-the-middle een verzonden code op te slaan, maar verstoren richting de deur. De deur gaat niet open, de gebruiker stuurt een nieuwe code, wederom verstoord. De radio heeft nu een toekomstige code en opent de deur met de eerdere code die het onderschepte. Geniaal, eigenlijk.
1. Android ligt onder de loep. Daar waar Windows focuspunt één is voor hackers, krijgt Android nu ook zijn aandacht en de kwetsbaarheden worden gevonden. 'Stagefright' is een gemene: je hoeft maar een besmette MMS te ontvangen of op een andere wijze een besmet multi-mediabestand te gaan afspelen en je apparaat is overgenomen. Google krijgt een koekje van eigen deeg, want het heeft moeite om dit gepatcht te krijgen binnen de negentig dagen die ze anderen geven om kwetsbaarheden te herstellen. Van dit soort kwetsbaarheden gaan we er nog veel meer zien...

Links

[1] http://www.computerworld.com/article/2969805/cybercrime-hacking/10-scary-hacks-from-black-hat-and-def-con.html

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

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

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

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

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

ABONNEMENTEN 2015
De abonnementsprijs in 2015 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

DRIVE-BY-HACKING

Zoals jullie allemaal bekend is, leest Berry alles wat met techniek te maken heeft en zodoende kom je natuurlijk weleens berichten tegen die je verbazen. De OV-chipkaart is te hacken en dat is zo bedrieglijk eenvoudig dat zelfs mij dat gaat lukken. Helaas voor mij is openbaar vervoer niet echt mijn ding dus ik heb er niet heel veel aan. Geïnteresseerden kunnen even googelen op "OV-chipkaart hacken" en de vangst is dan groot. Tooltjes om je vele wachtwoorden wat eenvoudiger te bewaren zijn helaas ook niet helemaal veilig, ook dit is tijdens mijn vakantie gehackt. Lekker gevoel om ineens al je wachtwoorden kwijt te zijn in plaats van één. Ik schrijf ze toch maar weer op denk ik.

Het meest opmerkelijke nieuws op het hack-gebied was voor mij wel het hacken van auto's. Niet de oldtimers maar de huidige moderne auto's die zijn voorzien van allerlei computers om het verbruik beter te reguleren en startonderbrekers die het wegrijden zonder goede sleutels onmogelijk zou moeten maken. In eerste instantie kwam de Jeep Cherokee in het nieuws. Die kon gehackt worden, maar niemand pakte het bericht op. Als je een foto van de auto ziet weet je waarom: zo'n auto wordt niet gehackt. Toen kwam de Tesla in het nieuws, deze zeer geavanceerde en prachtige auto is alleen te hacken als je fysiek toegang hebt gehad tot deze auto. De eigenaar kan wel hacken maar de fabrikant geeft dan geen garantie meer.

Al jaren doen geruchten de ronde dat auto's met startonderbrekers te hacken zouden zijn. Alle fabrikanten ontkennen dit. Zo nu en dan plopt een berichtje op dat het mogelijk is. Natuurlijk is het mogelijk; een garage kan het immers ook als een sleutel is verloren of kapotgegaan. De garage heeft een inleesapparaat en kan daarmee een nieuwe sleutel maken. Natuurlijk moet daar wel een speciaal kastje voor aangeschaft zijn om dat te kunnen. In een autosleutel zit een chip die gecodeerd is. Op zich kan er een hele lange codeersleutel ingezet worden maar dat hebben de autofabrikanten niet gedaan met als gevolg dat de chips te hacken zijn.

Een paar jaar geleden kwamen Nederlandse onderzoekers erachter dat de chipbeveiliging in auto's te omzeilen was, maar zij mochten dit niet publiceren van de fabrikant omdat dit wel erg veel onrust in de markt kon geven. Het grappige (of moet ik 'treurige' zeggen) is dat de autofabrikanten met deze wetenschap bleven doorgaan met het fabriceren van autosleutels met daarin deze vijftien jaar oude chip verwerkt. Wanneer je nu een hagelnieuwe Volkswagen Passat haalt dan is deze redelijk eenvoudig te hacken. De verklaring van Volkswagen is dat het onmogelijk is om in een serie auto's aanpassingen te doen.

Ik ga u verklappen dat er zeer waarschijnlijk geen terugroepacties komen op de meer dan tweehonderd modellen waarvoor dit probleem opgaat.

Berry

Je weet pas écht of je veilig bent, als onze 'hackers' op bezoek zijn geweest

Cybersecurity. Dat willen we allemaal. Maar hoe zorg je ervoor dat je organisatie écht veilig is? Dat weet je pas als een professionele hacker op bezoek is geweest. Iemand die op verantwoorde wijze de zwakke plekken blootlegt én aanpakt. Voordat kwaadwillenden echte schade toebrengen. Nodig daarom eens een cyberexpert van Capgemini uit. Iemand die over het vakmanschap van een hacker beschikt en daarmee de digitale weerbaarheid van bedrijven en organisaties naar een hoger niveau kan tillen. Dan weet je pas écht of je veilig bent.

Geïnteresseerd?
Neem dan contact op met:

Matthijs Ros
06 45 70 66 60
matthijs.ros@capgemini.com
www.capgemini.nl/cybersecurity

People matter, results count

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING