Interview
Hans Alfons over CRAMM en beveiligen in Afghanistan

Auteur: Lex Borger >Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.
Hans Alfons is security officer bij Univé. Hij is te bereiken via e-mail: h.alfons@unive.nl.

Na jaren bij de Nederlandse Defensie te hebben gewerkt, werkt Hans Alfons sinds kort als Information Security Officer bij het Univé bedrijfsonderdeel Distributie. Voor zijn aanpak van informatiebeveiliging binnen de Koninklijke Landmacht kreeg Hans in 2005 met zijn team het Risk Management Bedrijf Award en haalde hij de tweede plaats bij de Joop Bautz Award. In 2009 ontving Hans de koninklijke onderscheiding 'Lid in de Orde van Oranje Nassau met de zwaarden', voor het inrichten en onderhouden van informatiebeveiliging in de breedste zin van het woord. Hierbij inbegrepen de militaire missies naar Irak en Afghanistan.


Lex Borger.


Hans Alfons.

Ik sprak met Hans over zijn visie op, en zijn ervaring met informatiebeveiliging. Wat mij opviel was de rust en eenvoud die Hans uitstraalt als hij over zijn passie spreekt. Ik heb in mijn optekening getracht die stijl vast te houden. Hans had zoveel te vertellen, dat we besloten hebben dit gesprek over twee nummers van Informatiebeveiliging te verdelen. In deze uitgave het tweede deel, waarin Hans spreekt over CRAMM en beveiligen in Afghanistan.
"De CRAMM methodiek is rond 1995 naar Nederland gehaald door Deloitte, In 2000 is het importeurschap overgegaan naar 3-Angle. Ik ben er meteen bij betrokken geweest en we hebben een eerste proef gedaan bij Defensie. We hebben ook gekeken wat de beheerwaarde ervan was. Een ander gemak wat CRAMM biedt, is dat je maatregelen kunt exporteren naar een ander systeem. Je kunt dus CRAMM door een externe partij laten uitvoeren, dat laat je eens in de zoveel tijd doen. Vervolgens moet je zorgen dat je zelf een managementsysteem hebt waarin je alles verwerkt. Zo komen we van CRAMM naar het Intergrale Beveiligings Informatie Systeem (IBIS). Bij Defensie hebben we een systeem ontwikkeld waarin iemand een aanvraag kan doen, bijvoorbeeld 'ik wil een geheim systeem gebruiken in die kamer van dat gebouw, mag dat?' Dat systeem bevat het beveiligingsplan, dat vanuit CRAMM is geïmporteerd. Het systeem is zó verfijnd, dat ik kan zien aan de ruimteaanduiding van het systeem hoe die ruimte beveiligd is. De mensen van fysieke beveiliging hebben heel gedetailleerd in een deel van die database een goedkeuring gegeven dat die ruimte op norm is. Dan krijg je het informatiesysteem waarbij je kunt zien in de aanvraag wie van het personeel ermee gaat werken. Daar kun je ook goedkeuring voor geven. Vervolgens kijk je naar de rubricering van het systeem en als alles goed is, dan mag je daar ermee werken. Als je nu verder kijkt hoe IBIS is opgebouwd, zit er een module in waar risicomanagement mee gedaan wordt. Het doel van die module is om de behoefte van Defensie te bevredigen. Zij moeten in staat zijn om van de eenheden die gereed moeten kunnen staan binnen een dag vast te stellen dat ze aan de beveiligingsnormen voldoen. Dat rolt daar gewoon uit. Als je weet wat de BIV-classificatie is, dan weet je ook wat de set met maatregelen is. Wij hadden in CRAMM de mogelijkheid om aan te geven welke componenten je meeneemt, en konden aangeven volgens welke rubricering je gaat werken en wat je beschikbaarheidseis is. Nadat dit is ingevoerd, rolt je set aan maatregelen eruit. En we hadden daarin ook geregeld dat de eisen omgezet werden naar normenkaders. Dan wist de commandant die te velde ging wat het normenkader is waar hij aan moest voldoen. Dan heb je het voordeel, omdat je bij Defensie werkt, dat er voorbereidend werk is gedaan. Dus je weet wat de beveiligingsniveaus zijn van bepaalde componenten die zijn aangekocht op dat niveau. Daarna is de controle heel simpel, als jij die componenten meeneemt, dan zit dat beveiligingsniveau er in. Dus eigenlijk moet je het zo zien: je weet wat je wilt, je gaat naar de kast toe, haalt de Legoblokken eruit, die prik je op elkaar en dan heb je de beveiliging op orde. De keuze van de componenten is hierin cruciaal. We moesten hiervoor de expertise in het bedrijf hebben. Wij hebben heel nauw samengewerkt met mensen van de luchtmacht en van de landmacht die wij in de beginfase bij het project hebben betrokken en die hebben de blokken die op uitzending zouden kunnen gaan gedefinieerd, met duidelijke omschrijving wat daarin zat. Die blokken die definieerden we dan in CRAMM. En als jij dan een homebase-link had, dat is een straalzenderverbinding naar waar ook ter wereld, dan moet die op een bepaalde manier beveiligd zijn. Die heb je mobiel en die heb je statisch, in het beveiligingsplan heb je dat al beschreven. Dus als ze zo'n homebase-link meenemen, dan weet je ook wat het bijbehorende pakket met maatregelen is. Dan ga je er al van uit dat er in zo'n inzetgebied sowieso tot en met geheim gewerkt gaat worden. Daar houd je dus al rekening mee. In het systeem wat we na CRAMM ontworpen, hebben we de blokken in gestopt en je

maakt daaruit de keuze: 'Wat neem je mee?' Je kon van bovenaf ook onmiddellijk vaststellen dat aan het beveiligingsniveau voldaan werd, want iemand moest aangeven dat hij dat blok mee heeft en dat hij de beveiliging van dat blok gecontroleerd heeft. Dus op hoog niveau was dat ook te zien en te controleren. Fysieke beveiliging neem je niet mee, die ga je ter plekke inrichten. Daar gaan mensen voor aan het werk. Die zeggen op een moment: 'ik heb aan de fysieke beveiliging voldaan, dus die IT-blokken kunnen nu ingevlogen worden.' Die IT-blokken vlieg je dan in, terwijl de fysieke beveiliging al geregeld is. De verantwoordelijke daarover geeft in het systeem aan dat hij dat geregeld heeft. Dus dit is weer te zien op hoog niveau. Die halen weer uit het systeem dat hun beveiliging op groen staat. Als je kijkt naar de awards die we gewonnen hebben, daarvoor hebben we twee zaken die we gedaan hebben ingezonden. Het risicomanagementproces en de toepassing daarvan door middel van een geautomatiseerd middel. Bij de risicomanagement-award lag de nadruk op het eerste gedeelte, bij de Joop Bautz-award lag de nadruk op het tweede gedeelte. Ze zijn wel als een geheel aangeboden. Bij de risicomanagement-award gaven ze aan dat ze het heel slim vonden dat je heel snel tot een beveiligingsplan kwam en vastgesteld hebt dat daar maatregelen zijn geïmplementeerd. Ook het anders denken was daar deel van. Hoe kan je simpel en eenvoudig tot hetzelfde resultaat komen? Bij de Joop Bautz-award ging het veel meer over de techniek, daar ging het voornamelijk om het programma. Dat hebben we niet gewonnen. We hebben wel gehoord dat er een tweede stemming nodig was. We hebben een certificaat gehad dat we tweede zijn geworden. We zien dat als bewijsvoering dat het systeem in orde was. Daar zijn we ook blij mee.

Afghanistan

In Afghanistan hebben we deze methodiek ook toegepast. Voor de inzet in Afghanistan vinden er voorbesprekingen plaats, daar bepaal je hoe de ICT zich gaat ontwikkelen. Wij zaten erbij om de beveiligingsaspecten in de gaten te houden. Daar wil ik een paar leuke voorbeelden van geven:

Bepantsering

Juist doordat je met risicomanagement bezig bent, heb je de maatregelset in je hoofd. Daardoor benader je dingen anders. Men bedacht dat gepantserde containers zouden worden gebruikt voor werkplekken. Ik snap dat, je kunt daar veilig werken in drieploegendienst. De werkploeg ligt dan gepantserd, de andere twee ploegen zijn op dat moment ongepantserd. De enige vraag die ik daarbij gesteld heb is 'Wat houd je over als de andere twee ploegen worden uitgeschakeld? Kun je dan verder werken?' Men heeft uiteindelijk iedereen onder pantser gebracht. En dan ging het er niet om dat ik dacht dat het handig was dat ze zouden overleven, het ging om de continuïteit van het bedrijfsproces.

Stroomvoorziening

Men had de simpele gedachte uit beheersmatig oogpunt dat het slim was om alle aggregaten bij elkaar te zetten. Daarbij hadden ze wel aan continuïteit gedacht, want ze hadden een serie van drie aggregaten. Een draait, de andere staat stand-by en de derde is reserve. Dat was dus goed geregeld. Het enige nadeel was dat alles op een grote hoop bij elkaar stond. Dus als je daar een explosie hebt, ben je alles kwijt. Gewoon door vragen te stellen over hoe ze dat dan zouden oplossen, zie je dat ze dan zelf ook met ideeën komen: 'Laten we de aggregaten dan spreiden.' En dat hebben ze ook toegepast. Dus de kwetsbaarheid van een beschadiging bij een

aanval is hierbij ondervangen, de andere aggregaten blijven beschikbaar om het over te nemen.

Een ander aspect van Afghanistan is dat beveiliging niet het doel is. Eerst dacht ik 'Ja jongens, beveiligen is toch ook belangrijk', maar uiteindelijk merk je dat er twee dingen zijn. En daar onderscheid Defensie zich niet van Univé. Je hebt de business, bij Defensie is dat de operatie, en je hebt beveiliging. Uiteindelijk zul je altijd zien dat de directeur, degene die verantwoordelijk is voor de business c.q. operatie, dat ook als primair doel neemt. Beveiliging is altijd ondergeschikt. Dus is het de taak van een beveiliger om dat op een juiste manier onder de aandacht te brengen.

En zo kijk ik ook naar CRAMM, je hebt de maatregelen, je kijkt ernaar en je kijkt naar de omgeving waar je zit en je kiest wat het beste bij de omgeving past. En dat kan gemakkelijk zijn dat geen van de maatregelen direct bruikbaar is. Dan ga je nadenken. Er staat in CRAMM 'er moet een omheining rond het complex staan.' Wat is nou een omheining? Als je de foto's van Afghanistan ziet, zie je allemaal grote zakken zand staan. Dat is nou een omheining. En daar ligt dan prikkeldraad op of voor. Zo los je dat op. Wat CRAMM ook voorschrijft is 'de inrichting moet zoveel mogelijk volgens rechte lijnen lopen.'

Dan denk je bij jezelf 'Ja, dat klinkt allemaal logisch,' maar je ziet ook vaak dat mensen gaan bouwen volgens de contouren van het veld. Dan krijg je dode hoeken. Dan zie je dus dat je als informatiebeveiliger ook de fysieke beveiliging mee moet nemen in je kennis en expertise om te kunnen zeggen 'hoe doe je dat nou precies?' Aan het grootste gedeelte van de fysieke beveiliging hebben wij allemaal bijgedragen. Ook het omgekeerde kwam voor. Dat komt omdat de vakgebieden eigenlijk niet losstaan van elkaar, maar in elkaar overlopen.

Hetzelfde geldt voor de brandweer. Er was ook een brandweercommandant mee. Hij had bepaalde ideeën over hoe het kamp er uit mag zien. We kwamen tot de conclusie dat het in Afghanistan anders was dan in Nederland. Je wilt de wetgeving wel volgen, maar dat botst met andere dingen. Toen wij daar vanuit de drie expertises aanwezig waren, zag je de expertises ook in elkaar schuiven. Als ik vanuit informatiebeveiligingsoogpunt zei 'dat wil ik eigenlijk zo beveiligen', dan zei de brandweer 'houd er rekening mee, dat zit zo' en de fysieke organisatie had ook zijn eigen idee. Uiteindelijk kies je dan de beste oplossing om het daar te doen. En dat wil

niet zeggen dat dan 100% de informatiebeveiligingsoplossing gekozen wordt. Nee, je probeert de meest werkbare oplossing te kiezen. Bijvoorbeeld, als wij praten over een militaire operatiekamer, dan snapt iedereen wel dat dat zwaar beveiligd moet worden als we in Nederland zouden zijn. In Irak was het gewoon een tent. Dat komt voort uit een belangrijk aspect van hoe we objecten beveiligen, door met ringen van beveiliging te werken. Als je een locatie hebt waar alleen maar eigen personeel zit, met de juiste machtiging, dan maakt het niet uit of de operatie in een tent zit of dat het zwaar beveiligd is. Als je de serverruimte als voorbeeld neemt, dat kan een gewone kamer zijn. Mits je maar weet wie naar binnen gaat, dat je weet wie er langs komt zodat ze niet moedwillig beschadiging kunnen aanbrengen. En vervolgens moet je een ring van beveiliging om de buitenzijde van het gebouw leggen, dus goede toegangsbeveiliging tot het gebouw. Dat zie je bijvoorbeeld hier bij Univé. Je komt hier niet gemakkelijk binnen en mensen laten hun laptop staan als ze weglopen. Dan ga je het risico bekijken en dan constateer je dat de ring van beveiliging hier op de rand ligt. Het enige wat hier nog een nadeel lijkt is dat mensen niet overal geclusterd zijn per afdeling. Hierdoor weet je niet eenvoudig of er een vreemd iemand tussen zit. Je hebt hier op kantoor ook geen documenten, dus die kunnen niet gestolen worden. Laptops zijn beveiligd met encryptie. Dus wat wil je hier eigenlijk stelen? Ringen van beveiliging leggen is een betere aanpak dan overal maximaal beveiligen. Want dat zie je ook toegepast worden. Maximaal beveiligen is domweg alle maatregelen uitvoeren die moeten, zonder er verder over na te denken. Die ringen van beveiliging kun je op verschillende plaatsen leggen. Het hangt ervan af wat je hebt hoe je dat doet. Er zijn twee aspecten:

1. *Het financiële aspect*
   Als je een groot bedrijf bent en je gaat je belangen beveiligen, dan kan dat in een kleinere ruimte. Je zegt dan 'daar stop ik mijn hoogste belangen, dan kan de rest een stukje minder.' Je ziet dat nu een heleboel mensen afhankelijk zijn van hun laptops, en daar veel informatie doorheen laten gaan waarvan het toch niet handig is als iemand anders daar vanaf weet. In die situatie mag je de serverruimte wat minder beveiligen, maar dan moet je de buitenkant beter beveiligen. Dat zijn allemaal financiële afwegingen van wat de risico's zijn die je loopt en waar je dan die ring van beveiliging legt.

2. *Logische toegangsbeveiliging*
   Bij computersystemen heb je altijd nog de logische toegangsbeveiliging, dus je bent niet zomaar bij de data. Dat is al een maatregel wat maakt dat wij het niet erg zouden moeten vinden dat er een vreemde in je serverruimte loopt, ervan uitgaande dat jij je servers goed

beveiligd hebt. Dan doet een persoon al zoveel moeite om bij de data op een server te komen - we gaan er niet vanuit dat hij steelt, dat is een ander verhaal - voor de fysieke beveiliging. Het gaat even om de denkwijze. Je zag dat de fysieke beveiligers bij de landmacht op een bepaald moment ook begonnen in te zien dat een computer geen wapen is. Je wilt dat het niet gestolen wordt, maar je neemt bij de computer extra beveiligingsmaatregelen om te voorkomen dat men over de data kan beschikken. Dat is van cruciaal belang. Dus als je de computer stuk maakt is de data niet beschadigd, omdat die data altijd nog ergens anders staat.

De fysieke beveiliging richt zich op het voorkomen van fysieke schade. Bij ICT mag dat best voorkomen, want als alles goed beveiligd is, hebben we altijd nog een back-up. Belangrijke systemen draaien altijd nog ergens anders, dus dan zorg je voor je continuïteit.

Bij de landmacht zie je dat fysieke beveiliging en ICT-beveiliging in elkaar geschoven zijn. Bij Univé-VGZ-IZA-Trias zie je dat wat minder. De beveiliging wordt daar op verschillende plaatsen gerealiseerd en dat zou ook moeten worden samengebracht. Ik hoop dit samen met mijn collega's in de komende tijd te realiseren. En zo komen we op het volgende onderwerp.

Univé-VGZ-IZA-Trias

Ik zocht iets zodat ik met mijn passie, informatiebeveiliging, door kon gaan. Eigenlijk

zocht ik iets waarbij ik datgene wat ik uitgedacht had bij Defensie in de praktijk kon brengen. Ik vond een vacature die daar honderd procent aan voldeed. Op vijf minuten voor het sluiten van de markt heb ik een e-mailtje verstuurd, ik ben op gesprek geweest en mijn conclusie was dat de bij Defensie gebruikte methode ook hier toepasbaar is.
Als ik ga kijken naar mogelijkheden voor geautomatiseerde systemen om de informatiebeveiliging bij Univé-VGZ-IZA-Trias (UVIT) te ondersteunen dan moet ik op de markt kijken wat er is. UVIT beschikt over een aantal CRAMM-licenties. Het enige wat ik dus moest doen is zoeken naar een soort IBIS.
Bij UVIT heb ik met de diverse functionarissen informatiebeveiliging de methodiek van de Koninklijke Landmacht besproken en aangegeven dat dit de controleerbaarheid van het informatiebeveiligingsproces voor onder andere de interne accountantsdienst en de Nederlandsche Bank zal vergroten.
Aan de hand van de risico's uit FIRM (van de Nederlandsche Bank) is een UVIT risicomodel gemaakt en met gebruik van de ondersteunende tool CRAMM kan je aantonen welke informatiebeveiligingsrisico's gekoppeld zijn aan de het UVIT-risicomodel en met welke maatregelen de informatiebeveiligingsrisico's worden gemitigeerd.
Als vervanger van het tool IBIS zijn we nu met een pakket bezig, STREAM van Acuity Risk Management. Wat ik daarvan belangrijk vind is dat wat we ook in IBIS hadden … Ik zal een voorbeeld geven: functioneel beheerders dienen iedere drie maanden voor hun systemen aan te geven dat de beveiligingsmaatregelen waar zij verantwoordelijk voor zijn nog aanwezig zijn en werken.
Dit wordt nu schriftelijk gedaan. De beveiligingsfunctionaris consolideert de gegevens en rapporteert dit aan zijn directeur en de afdeling Risk & Compliance. Als iedere functionaris die verantwoordelijk is voor beveiligingsmaatregelen dat doet op zijn gebied zoals fysieke beveiliging, personele beveiliging, netwerkbeveiliging enzovoort, dan weten diverse functionarissen op verschillende managementlagen elke drie maanden door middel van allerlei rapportages, managementsamenvattingen, enz. hoe de beveiliging van de hele of een gedeelte van de organisatie er voor staat.
Door de input van Stream, iedere drie maanden of bij wijzigingen te laten uitvoeren/controleren door de functionarissen die verantwoordelijk zijn voor informatiebeveiligingsmaatregelen genereer je door middel van dwarsdoorsneden, managementsamenvattingen, dashboardsinformatie voor het management.
Wat de output betreft kan je het zo gek maken als je zelf wilt. Op elke laag kun je de directe chef, bijvoorbeeld de IT-directeur, tonen dat al zijn systemen en processen op orde zijn. De controlerende instanties kunnen hun relevante gegevens, in een op hun gewenste format eruit halen. De functionaris informatiebeveiliging overziet zijn speelveld tot op het laagste niveau. En ook de Raad van Bestuur overziet real time op een dashboard de beveiliging van UVIT.
En als je nu ziet hoeveel werk er mee gemoeid is om gegevens te verzamelen en om te zetten naar diverse managementinformatie en dat dit op reguliere basis gebeurt, dan is er grote tijdwinst te behalen met een geautomatiseerd systeem.
Dit is mijn beeld, we zullen zien of het werkelijkheid wordt. Je moet toch een toekomstvisie hebben…"

Podium

Afgelopen november tijdens de ALV zijn Tom Bakker en Kees van der Maarel toegetreden tot het bestuur van het PvIB. Tom volgt André Koot op in het bestuur. Tom heeft zich in nummer 2 van 2009 al eerder voorgesteld toen hij toetrad tot de redactie van dit blad. Hieronder stelt Kees van de Maarel zich aan u voor.

"Mijn naam is Kees van der Maarel. Tijdens de ALV van vorig jaar ben ik als bestuurslid van het PvIB gekozen. In het bestuur neem ik de taak over van Piet Goeyenbier namelijk, het helpen ontwikkelen van de Young Professionals.
Net als Piet werk ik bij de Rijksauditdienst als IT en Operational auditor. In 1992 ben ik in het vakgebied van de informatiebeveiliging gestapt. In eerste instantie voor de theoretische onderbouwing van mijn werk heb ik de IT-auditopleiding gevolgd (kan ik aanbevelen!). Na diverse functies als informatiebeveiliger heb ik in 2001 de overstap gemaakt naar het auditing vakgebied. Daarbij blijft informatiebeveiliging / IT-security een belangrijk aandachtsgebied. Naast het beoordelen van de betrouwbaarheid van informatiesystemen en

het onderzoek naar bedrijfsvoeringsprocessen ben ik betrokken bij de ontwikkelingen op informatiebeveiligingsgebied binnen de Rijksoverheid. Daarnaast heb ik als hobby er lol in bewustwordingssessies op het gebied van informatiebeveiliging te geven en (natuurlijk in opdracht) aan social engineering te doen.
Kortom, ik ben en voel mij volop betrokken bij de ontwikkelingen rond informatiebeveiliging. Omdat ik daarnaast veel plezier heb in het in beweging brengen van mensen ben ik blij met het aandachtgebied Young Professionals dat ik bij PvIB heb gekregen.
Informatiebeveiliging is een lastig onderwerp. Mijn ervaring is dat als je voor jezelf de lat niet hoog legt, en met kleine beetjes tegelijk aan de slag gaat het een bijzonder leuk en uitdagend vakgebied is!"