Hogeschool van Arnhem en Nijmegen

Afstudeerverslag

Beveiligingsarchitectuur bij Univé

Ontvangers: **Hogeschool van Arnhem en Nijmegen (in drievoud)**

Afstudeerder : Matthijs Koot (106576, IC4A)
Opleiding : Informatica
Periode : feb.‘05 t/m jun.‘05

Bedrijf : Univé Verzekeringen, Zwolle
Opdrachtgever : Security Management

Versie ter inzage

Ondertekening

Alleen indien zowel de afstudeerder als de opdrachtgever dit document hebben ondertekend mag het als authentiek worden beschouwd en komt het in aanmerking voor acceptatie door de Hogeschool van Arnhem en Nijmegen. Indien één van beide niet heeft ondertekend wordt het verslag op voorhand afgewezen door de hogeschool.

Naam van afstudeerder :

Handtekening van afstudeerder :

Naam van opdrachtgever :

Handtekening van opdrachtgever :

Inhoudsopgave

Managementsamenvatting

Ter afsluiting van de opleiding HBO Informatica aan de Hogeschool van Arnhem en Nijmegen heeft Matthijs Koot tussen 31 januari en 3 juni 2005 een afstudeeropdracht uitgevoerd bij Univé Verzekeringen te Zwolle. Het doel van een afstudeeropdracht is dat een student aantoont dat hij/zij alle competenties heeft verworven die aan de betrokken opleiding zijn verbonden. De bewijsvoering daarvoor omvat een afstudeerverslag, de opgeleverde producten en een presentatie van beide tijdens de afstudeerzitting. Een afstudeercommissie beoordeelt het geleverde werk; bij een positief resultaat heeft de student de opleiding met succes afgerond en volgt een HBO diploma.

Univé is een coöperatieve organisatie, met 36 leden die in totaal 150 regiokantoren exploiteren. De cluster Security Management maakt deel uit van de centrale koepelorganisatie en treedt Univé-breed op tactisch niveau adviserend, coördinerend, controlerend en initiërend op inzake informatiebeveiliging. Eén van de aandachtspunten van Security Management is beveiliging van de ICT-infrastructuur van Univé, die met de verdere integratie van ICT en bedrijfsprocessen steeds belangrijker wordt bij de primaire bedrijfsvoering. Naast preventieve maatregelen bevinden zich binnen de beveiliging van de infrastructuur idealiter ook detectieve maatregelen. Laatstgenoemde is het onderwerp van de afstudeeropdracht: hoe kan Univé toezicht houden op de veiligheid van de infrastructuur?

Bij aanvang van het afstuderen is besloten om het antwoord op die vraag in twee fasen te zoeken. In de eerste fase, het vooronderzoek, is een inventarisatie gemaakt van technologische bedreigingen die anno 2005 spelen binnen ICT-infrastructuren. Er is een aanpak verzonnen om te bepalen in hoeverre die bedreigingen op de infrastructuur van Univé van toepassing zijn en welke beveiligingsmaatregelen aanwezig zijn (of niet). Die aanpak is ten uitvoer gebracht, met als resultaat een ruw inzicht in de status van de beveiliging van die landelijke infrastructuur. Conclusie: gegeven de verwachte opkomst van webtechnologie binnen Univé en decentralisatie van ICT-beheer is een groei van het aantal *potentiële* directe en indirecte bedreigingen van binnenuit op de infrastructuur aannemelijk. Niet alle bedreigingen zijn of kunnen worden tegengegaan met preventieve maatregelen, waardoor detectieve maatregelen een zinvolle keuze lijken, ook vanuit professioneel oogpunt van beveiliging.

In de tweede fase, het hoofdonderzoek, zijn twee technische verschijningsvormen van zulke detectieve maatregelen onderzocht: intrusion detection/prevention en consolidatie van loganalyse. De theorie van beide maatregelen is onderzocht en beschreven in een onderzoeksrapport. Alle onderzoeksvragen konden daarbij worden beantwoord – bronmateriaal bleek ruimschoots voorhanden binnen de academische wereld. In een drietal cases worden de maatregelen teruggekoppeld naar mogelijke toepassingsgebieden binnen de infrastructuur van Univé. Conclusie: intrusion detection/prevention kan misbruik of afwijkingen van gebruik van de infrastructuur detecteren, maar is doorgaans een complexe puntoplossing. Consolidatie van loganalyse wordt binnen beveiligingscontext *Security Information Management* genoemd en heeft een zeer brede focus. Het beoogt een holistisch overzicht van de beveiliging van een infrastructuur, waarbij meldingen van vele heterogene beveiligingscomponenten worden geconsolideerd en gecorreleerd. Beide maatregelen zijn ondersteunend voor de totale beveiliging en kunnen bijdragen aan compliancy met eventuele toekomstige Nederlandse of Europese afgeleiden van wet- en regelgeving als de Amerikaanse Sarbanes-Oxley en HIPAA. Er is een indicatie gegeven van technische en beheermatige randvoorwaarden waaraan producten zouden moeten voldoen om inpasbaar te zijn binnen Univé.

Als laatste activiteit binnen de afstudeerperiode is een Proof-of-Concept opstelling gerealiseerd waarbinnen is geëxperimenteerd met een combinatie van diverse detectieve controls. Er is een viertal hacking scenario's ten uitvoer gebracht om te ondervinden of en hoe de detectieve werking van die opstelling was. Conclusie: in de gebruikte opstelling werden tijdens de hacking scenario's diverse beveiligingsgerelateerde meldingen gegenereerd, maar konden de scenario's niet middels correlatie worden gereconstrueerd. Een andere opstelling, misschien met andere configuraties of andere componenten en betere correlatiefuncties, had wellicht wél kunnen voorzien in die behoefte. Een tweede Proof-of-Concept met gespecialiseerde(re) componenten wordt geadviseerd.

Met uitzondering van enige tussentijdse uitloop zijn alle activiteiten uitgevoerd volgende de planning. Na concretisering van de richting van het afstudeertraject is zonder problemen gewerkt aan de geplande deliverables. Gedurende de hele afstudeerperiode is regelmatig werkoverleg geweest om de voortgang en de verwachtingen te beheersen. De enige belangrijke tegenslag gedurende het afstuderen was de *no-go* voor de Proof-of-Concept met IBM Tivoli Risk Manager. Er is toen uitgeweken naar een alternatief product, NetIQ Security Manager, waardoor de theorie toch nog (deels) in praktijk kon worden getest. Alle geplande deliverables zijn tijdig opgeleverd en voldoen aan de gestelde eisen. Samenvattend kan worden gesteld dat de opdracht is afgerond conform de doelstellingen.

1. Inleiding

Ter afronding van de opleiding HBO Informatica aan de Hogeschool van Arnhem en Nijmegen heeft de auteur van dit verslag in vier maanden tijd een afstudeeropdracht uitgevoerd bij Univé Verzekeringen te Zwolle. Het afstuderen is de periode waarin de student moet aantonen dat hij/zij beschikt over de competenties (kennis, vaardigheden, houding) die van een afgestudeerde hbo'er – in dit geval een informaticus – worden verlangd.

Dit verslag is een eerste bewijsvoering waarmee de auteur de afstudeercommissie hoopt te overtuigen van zijn competenties. Tijdens de afstudeerzitting in juni 2005 zal de inhoud van het verslag in een presentatie worden toegelicht. Nadien worden zowel de opgeleverde resultaten als de kennis van de afstuderende student door de afstudeercommissie aan een kritische evaluatie onderworpen. Ten slotte volgt een definitieve waardering in de vorm van een cijfer.

Achtereenvolgens komen in dit verslag aan de orde:

- een beschrijving van de organisatie Univé;
- het afstudeerproject:
    - de probleem- en doelstelling;
    - de aanpak;
    - het verloop;
    - het resultaat;
    - conclusies en aanbevelingen;

Ter afsluiting zal een evaluatie worden gegeven van de verschillende aspecten van het afstuderen.

2. Bedrijfsbeschrijving Univé

De Nederlandse verzekeraar Univé is een coöperatieve organisatie –vergelijkbaar met de Rabobank– waarbinnen sinds een reorganisatie in juli 2003 een viertal bedrijfsonderdelen wordt onderscheiden: het Concern en de business units Univé Schade, Univé Zorg en Marketing & Verkoop (zie Appendix A – Organogram (top-level)). De kernactiviteiten van Univé zijn momenteel schade- en zorgverzekeringen, maar op diverse manieren wordt het dienstenpakket uitgebreid; zo is er een franchiseconstructie voor makelaars en worden via de onafhankelijke Stichting Univé Rechtshulp rechtsbijstandverzekeringen aangeboden.

Binnen het Concern bevindt zich de afdeling Beheer & Exploitatie, die het rekencentrum beheert voor de BU Schade, Marketing & Verkoop en voor de Onderlingen. De afdeling is ingedeeld in vier teams: Helpdesk, Operations, Test & Support en Infrastructuur, Ontwikkeling en Beheer (IOB). De cluster Security Management valt binnen team IOB (zie Appendix B – Organogram Concern **à** Beheer & Exploitatie) en is onder andere belast met het opstellen van beleid en normenkaders voor informatiebeveiliging en het selecteren van technische en organisatorische beveiligingsmaatregelen om de informatieveiligheid te waarborgen. Security Management heeft een tactische rol en treedt Univé-breed adviserend, coördinerend, controlerend en initiërend op.

3. Het afstudeerproject

3.1. Achtergronden

De ICT-infrastructuur is van essentieel belang voor de goede uitvoering van de bedrijfsprocessen van Univé. Het verzekeringsproces is in verregaande mate geautomatiseerd. Op tientallen locaties bedient Univé haar klanten via kantoorbalie, telefoon, buitendienstmedewerkers en de Univé website. Op backoffice systemen worden de vele verzekeringstransacties verwerkt die dagelijks plaatsvinden.

Het is daarom van groot belang dat de ICT-infrastructuur beschikbaar is en dat de verwerking van gegevens integer en vertrouwelijk is. Univé is daarom continu bezig met het inrichten van beveiligingsmaatregelen van de ICT-infrastructuur. Een bijzondere groep van risico's is gerelateerd aan het Internet en aanverwante technologie. Zowel van buitenaf als van binnenuit is het mogelijk om aanvallen uit te voeren op Univé servers, werkplekken, en het netwerk zelf.

De rekencentra van Univé (gevestigd in Alkmaar, Assen en Zwolle) hebben te maken met een toenemende decentralisatie van de operationele beheertaken, enerzijds veroorzaakt door organisatorische verschuivingen – de onderdelen van Univé worden zelfstandiger als het gaat om ICT – en anderzijds door technologische veranderingen – veel nieuwe systemen en componenten kunnen op afstand worden beheerd via bijvoorbeeld software agents, webinterfaces en management protocollen en de beheerders bij Univé maken graag van die mogelijkheden gebruik. Daarnaast spelen e-commerce en webtechnologie een steeds grotere rol bij de bedrijfsvoering; verzekeringen worden steeds vaker afgesloten via de website van Univé en de backoffice systemen zullen migreren naar een op webservices gebaseerde omgeving.

3.2. Probleemstelling

Security Management heeft momenteel nauwelijks of geen inzicht in wat er op of met de Univé infrastructuur gebeurt, waardoor onverhoopte aanvallen op de infrastructuur pas kunnen worden ontdekt als er schade is aangericht. Gezien de groeiende kans op (in)directe bedreigingen vanaf zowel binnen als buiten op de infrastructuur als gevolg van verzelfstandiging van de bedrijfsonderdelen wordt het bij het proces van informatiebeveiliging steeds belangrijker om dat inzicht te hebben.

3.3. Doelstelling

Er diende een inventarisatie te worden gemaakt van de (soorten) bedreigingen die spelen op een ICT-infrastructuur, waarna zou worden ingeschat in hoeverre de huidige Univé infrastructuur is beschermd tegen die bedreigingen. De uitwerking van die opdracht zou het vooronderzoek vormen. In het vervolgonderzoek zou een advies worden gegeven over een oplossing waarmee Univé zicht kan krijgen op wat er op de infrastructuur gebeurt. Daarbij zouden IDS/IPS en geconsolideerde loganalyse (of eigenlijk, zoals later zou blijken, *security information management*) nader worden beschouwd.

3.4. De aanpak

Om tot de gewenste doelen te komen is in eerste week na overleg met Security Management (bestaande uit André Koot, Egbert Dijkgraaf en René van Dijk) in het Project Initiatie Document (PID) *Cyberdefense* vastgesteld dat het afstudeerproject uit twee fasen zou bestaan: een vooronderzoek en een hoofdonderzoek. In het vooronderzoek zou een inventarisatie worden gemaakt van technologische bedreigingen op ICT-infrastructuren, waarna de infrastructuur van Univé in het licht van die bedreigingen zou worden beschouwd. Het resultaat zou een inschatting zijn van de bedreigingen waar die infrastructuur eventueel nog niet tegen zou zijn beveiligd. In het hoofdonderzoek zouden de achtergronden van intrusion detection en consolidatie van loganalyse worden uitgewerkt, om vervolgens te leiden tot een advies voor implementatie bij Univé.

3.4.1. Vooronderzoek

De beschikbare tijd voor dit vooronderzoek was opgesplitst in twee delen: bureauonderzoek (drie weken) en veldonderzoek (twee weken). Uit het bureauonderzoek diende te blijken met welke bedreigingen ICT-infrastructuren anno 2005 in het algemeen te maken hebben en hoe die bedreigingen vanuit tactisch niveau kunnen worden geadresseerd. Bij het veldonderzoek diende vervolgens op basis van informatie uit interviews een inschatting te worden gemaakt van de mate waarin de Univé infrastructuur tegen die bedreigingen is beschermd, om zodoende eventuele ontbrekende maatregelen te identificeren.

De lijn van vraaginstelling in het vooronderzoek was als volgt:
- Wat zijn de doelstellingen van informatiebeveiliging?
- Hoe worden die doelstellingen bedreigd?
- Hoe kan tegen die bedreigingen worden beschermd?
- Welke bedreigingen zijn bij Univé van toepassing en in hoeverre is tegen die bedreigingen beschermd?

De precieze activiteiten van het vooronderzoek staan in de onderstaande tabellen (in chronologische volgorde).

Bureauonderzoek			
Stap	**Activiteit**	**Hoe**	**Beoogd resultaat**
1	Formuleer de onderzoeksvragen	Op basis van PID en in overleg met SecMgmt.	Geformuleerde onderzoeksvragen.
2	Onderzoek de fundamenten van informatiebeveiliging.	Bureauonderzoek (literatuur, internet).	Inzicht in de achtergronden van het onderwerp.
3	Verzin een model waarbinnen zowel bedreigingen als maatregelen op een begrijpelijke en consistente manier kunnen worden gerelateerd aan de infrastructuur.	Bureauonderzoek (literatuur, internet, eigen kennis) en overleg met SecMgmt.	Generiek model dat als kader kan worden gebruikt voor de bedreiginganalyse.
4	Inventariseer de technologische bedreigingen.	Bureauonderzoek (literatuur, internet, eigen kennis).	Opsomming van meerdere concrete bedreigingen.
5	Categoriseer de bedreigingen op zo'n manier dat ze per categorie hanteerbaar zijn bij controle op geïmplementeerde maatregelen (groepering).	Bureauonderzoek (literatuur, internet, eigen kennis) en overleg met SecMgmt.	Hanteerbare groepen van bedreigingen als input voor de bedreiginganalyse.
6	Verzin een classificatiemethode en classificeer de bedreigingen.	Bureauonderzoek (literatuur, internet, eigen kennis) en overleg met SecMgmt.	Inzicht in het wereldwijd voorkomen van bepaalde bedreigingen 'in het algemeen'.

Veldonderzoek			
Stap	**Activiteit**	**Hoe**	**Beoogd resultaat**
7	Inventariseer de componenten van elke laag uit het model bij Univé.	Veldonderzoek – interviews en bestuderen	Input voor de bedreiginganalyse.

		van topologieschema's.	
8	Inventariseer de bedreigingen die op die componenten spelen en de getroffen beveiligingsmaatregelen.	Veldonderzoek – interviews.	Input voor de bedreiginganalyse.
9	Beoordeel de mate waarin de getroffen maatregelen beschermen tegen de bekende bedreigingen (de bedreiginganalyse).	Bureauonderzoek in overleg met SecMgmt.	Inzicht in de mate waarin tegen de bekende bedreigingen is beschermd.
10	Trek een conclusie.	Bureauonderzoek in overleg met SecMgmt.	Afronding van vooronderzoek.

3.4.2. Hoofdonderzoek

Het onderzoek was opgedeeld in drie delen: bureauonderzoek (drie weken), veldonderzoek (een week) en experimenteel onderzoek (vier weken). Bij het bureauonderzoek dienden de theoretische concepten achter intrusion detection/prevention en geconsolideerde loganalyse en de rol die beide maatregelen binnen een beveiligingsarchitectuur hebben te worden onderzocht. Bij het veldonderzoek diende een interview te worden afgenomen waaruit duidelijk zou worden welke beveiligingsdomeinen bij Univé kunnen worden onderscheiden en op welke plaatsen in de infrastructuur monitoring maatregelen wenselijk zijn (of juist niet). Samen met opgedane ervaring in het eerste deel van de experimentele fase zouden de volgende vragen kunnen worden beantwoord:

- welke netwerkkoppelingen, systemen of applicaties zijn relevant?
- welke eisen dienen aan de loganalyse en IDP-architectuur te worden gesteld?

Ten slotte zou een advies worden geformuleerd over de inpassing van intrusion detection/prevention en geconsolideerde loganalyse bij Univé.

De lijn van het hoofdonderzoek was als volgt:
- Wat is intrusion detection/prevention?
- Wat is consolidatie van loganalyse?
- Hoe kunnen beide maatregelen worden ingezet bij Univé?

De precieze activiteiten van het hoofdonderzoek staan in de onderstaande tabellen (wederom in chronologische volgorde).

Bureauonderzoek			
Stap	**Activiteit**	**Hoe**	**Beoogd resultaat**
1	Formuleer de onderzoeksvragen	Op basis van PID en in overleg met SecMgmt.	Geformuleerde onderzoeksvragen.
2	Onderzoek de fundamenten van intrusion detection/prevention (IDS/IPS).	Bureauonderzoek (literatuur, internet).	Theoretische kennis van IDS/IPS.
3	Onderzoek de fundamenten van consolidatie van loganalyse.	Bureauonderzoek (literatuur, internet).	Theoretische kennis van consolidatie van loganalyse.

Veldonderzoek			
Stap	**Activiteit**	**Hoe**	**Beoogd resultaat**
4	Inventariseer de beveiligingsdomeinen bij Univé.	Veldonderzoek – interview van SecMgmt.	Inventarisatie van de verschillende beveiligingsdomeinen.

Experimenteel onderzoek			
Stap	**Activiteit**	**Hoe**	**Beoogd resultaat**
5	Maak een plan voor een Proof-of-Concept opstelling waarin de werking van IDS/IPS en loganalyse wordt gedemonstreerd.	Bureauonderzoek en overleg met SecMgmt.	Project Initiatie Document voor een experiment (incl. doelstelling, planning, middelen, …).
6	Voer de Proof-of-Concept uit.	Experimenteel onderzoek.	PoC-opstelling en kennis omtrent de werking van de gekozen componenten.
7	Trek een conclusie.	Bureauonderzoek en overleg met SecMgmt.	Afronding van hoofdonderzoek.

3.5. Het verloop

Zowel het vooronderzoek als het hoofdonderzoek zijn vrij behoorlijk verlopen volgens de oorspronkelijke planning (zie het PID *Cyberdefense*). Het initiële PID is ruim een week later opgeleverd dan de datum die is genoemd in de voorschriften van het afstudeerboekje; de oorzaak daarvoor lag enerzijds bij de tijd die vanuit Univé nodig bleek om de afstudeeropdracht een concrete richting te geven, anderzijds bij het verlate contact vanuit de hogeschool. Deze vertraging had geen negatieve impact op de rest van het afstudeertraject; er is in diezelfde periode alvast kennis vergaard over de fundamenten van informatiebeveiliging.

Het vooronderzoek is één week uitgelopen, vooral vanwege de tijd die is gebruikt om een zinvolle aanpak te bedenken voor het snel verkrijgen van een basaal inzicht in de beveiliging van de infrastructuur van Univé. Er is gekeken naar Threat Modeling en OCTAVE, maar beide bleken achteraf niet bruikbaar om binnen zeer korte tijd inzicht te krijgen in een grote infrastructuur. Uiteindelijk is een vrij simpel model gebruikt, maar er was relatief veel tijd nodig om tot die beslissing te komen. Verder was de voortgang van de interviews afhankelijk van de beschikbaarheid van de geïnterviewden. De meeste geïnterviewden waren redelijk enthousiast en gaven uit zichzelf relevante informatie waar ik niet expliciet naar had gevraagd (omdat ik nog niet wist dat onderwerp X, Y of Z bij Univé speelden). Enkele personen zijn pas geïnterviewd na afloop van de geplande tijd voor het vooronderzoek. De resultaten van het vooronderzoek zijn tussentijds teruggekoppeld met de opdrachtgever en na enkele kleine aanpassingen geaccordeerd. De uitloop heeft geen negatieve impact gehad op de rest van het afstudeertraject; eveneens als bij de PID-fase zijn in die uitlooptijd alvast enkele activiteiten verricht voor de hoofdfase.

Bij het hoofdonderzoek is met veel passie gezocht naar wetenschappelijk bronmateriaal, dat achteraf ten overvloede vindbaar bleek. Het lezen van dat materiaal kostte veel tijd, maar de geïnvesteerde tijd heeft zich terugbetaald in de snelheid waarmee de theoretische delen van het hoofdonderzoek konden worden uitgewerkt. Eén van de lastigste onderdelen van het hoofdonderzoek - waarover overigens nog steeds geen volledige duidelijkheid is – was het onderzoek naar de relatie tussen SIM en IDS. De conclusie was dat beide maatregelen bijdragen aan toezicht op de infrastructuur, maar dat op verschillende abstractieniveaus doen (‘SIM is een meta-IDS’). Met die conclusie is de vraag over de plaatsing van intrusion intelligentie echter nog niet beantwoord: welke intelligentie is nodig op het niveau van een individuele sensor en welke intelligentie op het niveau van SIM om succesvol te correleren maar tegelijk schaalbaar te zijn? Die vraag behoeft eigenlijk een aanvullend onderzoek.

Om de theorie terug te koppelen naar de situatie bij Univé was een Proof-of-Concept (PoC) gepland. De precieze invulling van de PoC is tot stand gekomen op basis van informatie uit het vooronderzoek en gesprekken met diverse leveranciers. IBM Tivoli Risk Manager leek dé keuze voor Univé (zie de argumenten in het hoofdonderzoek), dus is een PID opgesteld met een beschrijving van doel, middelen, planning, et cetera, gericht op Risk Manager. Vanwege de complexe aard (lees: steile learning curve) van Risk Manager is in overleg met Univé besloten dat externe expertise noodzakelijk was om binnen de beschikbare tijd een PoC-opstelling te realiseren. Uiteindelijk bleek het niet mogelijk om de externe expertise binnen de beschikbare tijd in te zetten, waarna (wederom) in overleg met Univé is uitgeweken naar het vrijelijk te evalueren NetIQ Security Manager, dat als zelfstandig product een stukje eenvoudiger is op te zetten dan Risk Manager. Om de werking van de PoC te testen zijn enkele hacking scenario’s bedacht en tot uitvoer gebracht; de resultaten daarvan zijn twee weken na de geplande einddatum van de hoofdfase opgeleverd. In de oorspronkelijke planning was een bufferzone opgenomen van twee weken; die buffer heeft de totale uitloop uiteindelijk voldoende opgevangen.

4. Het resultaat

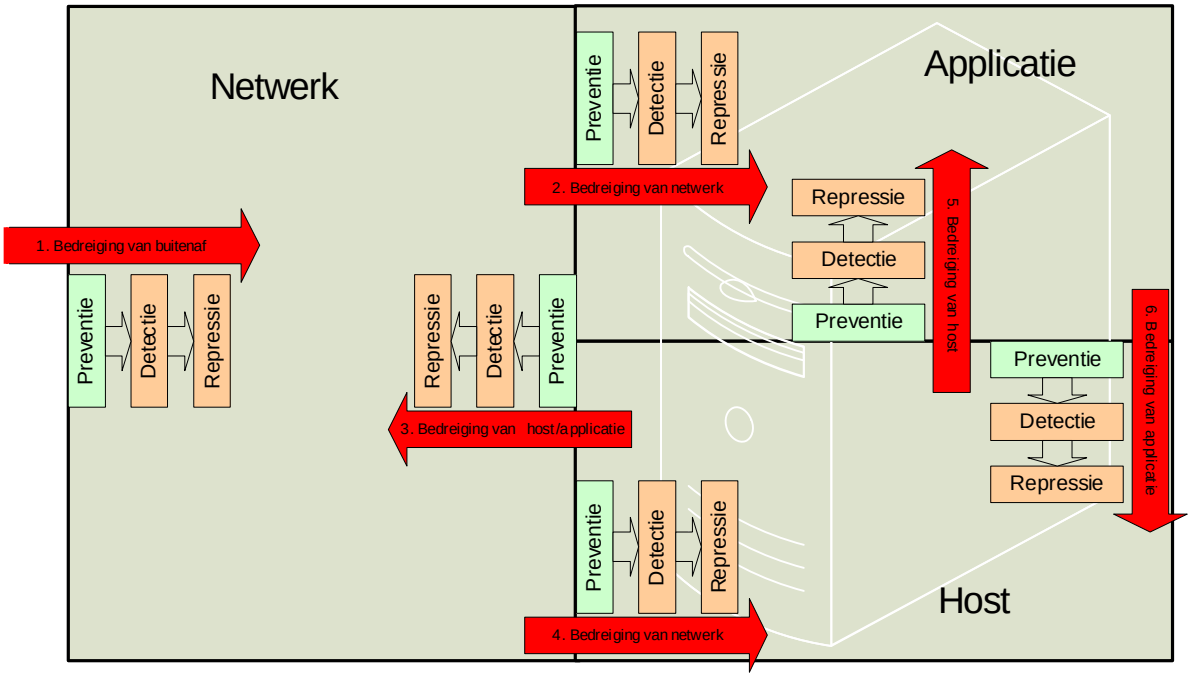
In het PID *Cyberdefense*, zoals goedgekeurd door Univé en ICA, zijn twee resultaten gedefinieerd. In dit hoofdstuk worden de verwachte resultaten met de werkelijke resultaten vergeleken en wordt geprobeerd duidelijk te maken welke waarde de resultaten hebben voor Univé.

4.1. Resultaat 1: inleidende studie

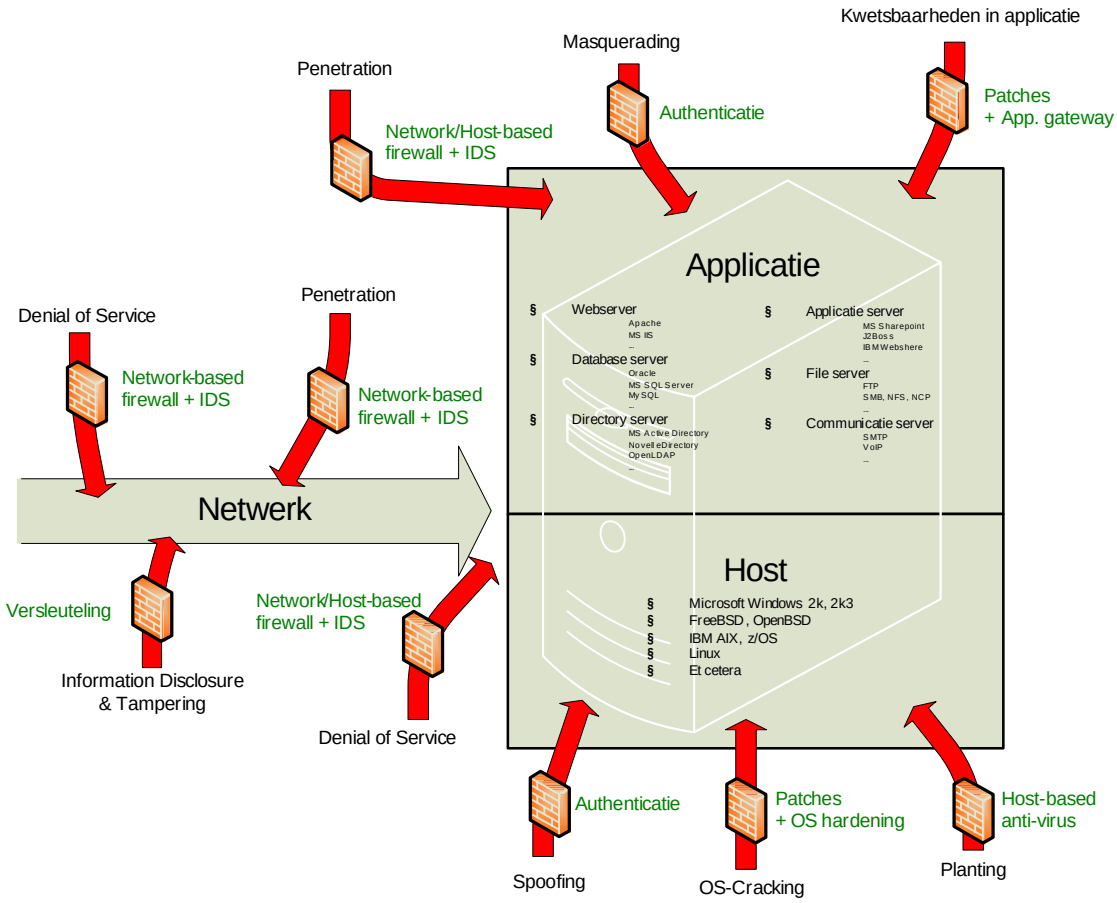
Het eerste resultaat werd in het PID als volgt gedefinieerd:

1. *Een inleidende studie bestaande uit:*
   a) *Een review van de belangrijkste bedreigingen in het Internetdomein. Denk hierbij aan spam, DDoS, poort-80 aanvallen. De review bestaat uit een korte bureaustudie van beschikbare literatuur op het web en in leerboeken;*
   b) *Een beschrijving van de gewenste beveiligingsarchitectuur, gewenst in de zin van overeenkomstig professionele inzichten van de internationale ICT-security beroepsgroep (SOLL-situatie);*
   c) *Een vergelijking van de gewenste beveiligingsarchitectuur met de huidige Univé beveiligingsarchitectuur (SOLL confronteren met IST).*

Het uiteindelijke resultaat is bij dit verslag als bijlage opgenomen: Appendix E – Vooronderzoek. Resultaat 1-a kan worden teruggevonden in bijlage 17 van het vooronderzoek en beslaat in totaal 57 bedreigingen, 40 maatregelen en 207 combinaties van hoe de maatregelen die bedreigingen kunnen tegengaan. Resultaat 1-b is gerealiseerd in de vorm van een abstract model:



Kern van dit model is dat op zowel applicatie-, host- als netwerkniveau zowel preventieve als detectieve en correctieve maatregelen worden genomen. Op de volgende pagina is een afgeleid schema zichtbaar waaraan ter illustratie een aantal bedreigingen en maatregelen is toegevoegd.



Het applicatie-host-netwerk model is als basis gebruikt voor een methode waarmee een inschatting is gemaakt van de mate waarin de infrastructuur van Univé is beschermd tegen verschillende soorten bedreigingen (resultaat 1-c). De bedachte methode is bruikbaar voor toekomstige bedreiginganalyses en staat, hoewel in eerste instantie voor hen ontwikkeld, in principe los van Univé. De aanpak is gebaseerd op het feit dat veel concrete technologische bedreigingen gelijksoortige gevolgen hebben en met gelijksoortige maatregelen zijn tegen te gaan. Essentieel is dat deze aanpak is ontworpen als een bruikbare methode om in redelijk korte tijd een inschatting te kunnen maken van de beveiligingsituatie van een grotere infrastructuur; het is geen fundamenteel-wetenschappelijke methode waarbij de beveiliging wordt getoetst aan een vastgestelde norm – er wordt geïnventariseerd op basis van interviews en beschikbare topologieschema's. De in het vooronderzoek gebruikte methode is complementair aan bestaande methoden als *threat modeling* van Microsoft en *attack trees* van Bruce Schneier (waarbij overigens ook niet wordt getoetst aan een norm).

Ter illustratie: een network-based intrusion prevention systeem (NIPS) kan op netwerkniveau tegen meerdere vormen van Denial-of-Service (DoS) beschermen. Als het bekend is dat er geen NIPS aanwezig is op een bepaalde plek in de infrastructuur en er geen andere preventieve maatregelen aanwezig zijn, dan mag worden aangenomen dat het netwerk op die plek kwetsbaar is voor verschillende vormen van DoS. Welke vormen dat precies zijn - SYN flooding, smurf attacks, ARP poisoning, … -, is hierbij (relatief) onbelangrijk; feit blijft dat er niets is gedaan om DoS-bedreigingen op dat punt tegen te gaan. Omgekeerd geldt dat ook: als er wél een NIPS aanwezig is op die plek, mag worden aangenomen dat er tegen verschillende vormen van DoS wordt beveiligd. De precieze werking van de NIPS is daarbij (relatief) onbelangrijk; feit blijft dat er in dat geval wél iets is gedaan om DoS-bedreigingen op dat punt tegen te gaan. *Het is dus geen keiharde toetsing* – een keiharde toetsing vereist een duidelijk normenkader en uitgebreide penetratietests en is daarom ten eerste niet binnen de afstudeertijd te realiseren, ten tweede ligt een

keiharde toetsing niet op het kritieke pad van de afstudeerplanning. Andere factoren die een rol spelen bij de beoordeling OK/NOK (zoals gebruikt in het hoofdstuk "Korte bedreiginganalyse Univé" van het vooronderzoek) zijn de beveiligingseisen die aan een bepaald deel van de infrastructuur worden gesteld en de grootte van de kans dat een dergelijke bedreiging werkelijk plaatsvindt.

De volgende elementen uit het vooronderzoek hebben toegevoegde waarde voor Univé (SecMgmt in het bijzonder):

1. Een methode waarmee Univé momentopnames kan maken van infrastructurele beveiliging (d.w.z. een structurele inventarisatie maken van bedreigingen en maatregelen), bestaande uit een algemeen model (applicatie-host-netwerk) en een aanpak voor categorisatie en classificatie;
2. Een momentopname van de huidige stand van infrastructurele beveiliging 'in de wereld' (c.q. algemene bedreiginganalyse), bestaande uit verschillende tabellen met voorbeelden en classificaties, één tabel voor elke stroom van bedreigingen;
3. Een momentopname van de huidige stand van infrastructurele beveiliging 'bij Univé' (c.q. situationele bedreiginganalyse), bestaande uit verschillende tabellen met genomen maatregelen en classificaties, één tabel voor elke stroom van bedreigingen per deel van de infrastructuur;
4. De vaststelling dat er weinig wordt beschermd tegen bedreigingen van binnenuit terwijl er steeds meer mogelijkheden komen voor indirecte aanvallen (via een onbeveiligd draadloos netwerk bij een regiokantoor, via een slecht beveiligde RAS-server, et cetera).

4.2. Resultaat 2: een detaillering van IDS/IPS en loganalyse

Het tweede resultaat werd in het PID als volgt gedefinieerd:

> *2. Een detaillering van*
>
> *a) aanvalsdetectie en preventie met IDS/IPS;*
>
> *b) geconsolideerde loganalyse,*
>
> *bestaande uit:*
>
> *I. een beschrijving van de werking van genoemde maatregelen*
>
> *II. een onderzoek naar de beschikbare producten*
>
> *III. een literatuuronderzoek naar de kwaliteit van de producten*
>
> *IV. een inventarisatie van de inpasbaarheid en de scoping van de maatregelen binnen het verantwoordelijkheidsgebied van de afdeling BenE (dat zich overigens uitstrekt van het Rekencentrum in Zwolle tot en met de volledige KA-omgeving van Univé, en het landelijke netwerk)*
>
> *V. als de tijd het toelaat een proof-of-concept van één of meer geselecteerde producten*

Het uiteindelijke resultaat is bij dit verslag als bijlage opgenomen: Appendix F – Hoofdonderzoek. Resultaat 2-I kan worden teruggevonden in hoofdstuk 2 en 3 van het hoofdonderzoek en vormt het primaire onderdeel van dat rapport. Resultaat 2-II en 2-III zijn niet als zodanig gerealiseerd, vanwege twee redenen:

1. De IDP en SIM[1] producten zijn niet binnen de afstudeerperiode te evalueren omdat ze appliances betreffen of er geen evaluatieversies van te downloaden zijn. Zonder evaluatie kan er niet worden onderzocht en aangezien het materiaal op de website van de vendors zelf objectief noch bruikbaar is (zie bijvoorbeeld H2.2.6 van het hoofdonderzoek; NIDS wordt soms in de markt gezet als NIPS) is in overleg met SecMgmt besloten om te focus te leggen op de Proof-of-Concept met IBM Tivoli Risk Manager (zie verderop);

[1] In de loop van het onderzoek bleek dat het onterecht was om te spreken van 'consolidatie van loganalyse', omdat die formulering ook loganalyse ten behoeve van regulier systeembeheer adresseert (performance monitoring, et cetera). Uit verder onderzoek bleek dat de term 'security information management' (SIM) wordt gebruikt om specifiek te verwijzen naar 'consolidatie van beveiligingsgerelateerde loganalyse'. SIM is uiteindelijk een sleutelrol gaan spelen in het hoofdonderzoek – het resultaat van voortschrijdend inzicht in de materie.

2. Het is niet zinvol om bestaande reviews 'over te typen' – in plaats daarvan is er inzake IDP in H2.5 van het hoofdonderzoek een aantal verwijzingen opgenomen naar bestaande reviews/tests. Van SIM producten (ArcSight, NetForensics, Risk Manager) lijken nog geen reviews/tests beschikbaar te zijn.

Resultaat 2-IV is gerealiseerd in de vorm van een drietal Univé-specifieke cases waarin de maatregelen worden toegepast. Voor resultaat 2-V is een apart PID opgesteld, getiteld *Experiment IBM Tivoli Risk Manager* (zie Appendix G – PID 'Experiment IBM Tivoli Risk Manager'). In dat experiment zou een voor Univé representatieve testomgeving worden opgezet waarin IBM Tivoli Risk Manager binnen de bestaande Tivoli-omgeving van Univé functioneert als SIM-product, waarbij door onder andere een Cisco Secure IDS en een Windows 2003 Server meldingen zouden worden aangeleverd via Risk Manager agents. Vanwege de complexiteit van Tivoli en de eisen die Univé stelt aan experimenten in haar eigen testomgeving is daarvoor een externe IBM consultant aangetrokken. De werking van de Proof-of-Concept zou middels verschillende hacking scenario's worden getoetst. Uiteindelijk is om redenen die in het hoofdonderzoek zijn genoemd gekozen om binnen de Proof-of-Concept in plaats van IBM Tivoli Risk Manager gebruik te maken van NetIQ Security Manager. De verslaglegging van de uitvoer van de hacking scenario's binnen de Proof-of-Concept opstelling is beschikbaar in Appendix H – Verslaglegging van de Proof-of-Concept.

De volgende elementen uit het hoofdonderzoek hebben toegevoegde waarde voor Univé (en wederom voor SecMgmt in het bijzonder):

a. Kennis over het nut en de werking van IDS/IPS (incl. Proof-of-Concept);
b. Kennis over het nut en de werking van Security Information Management (incl. Proof-of-Concept);
c. Een drietal situationele cases bij Univé, waarmee SecMgmt het toepassingsgebied van IDS/IPS en SIM kan verklaren aan andere medewerkers;
d. Een indicatie en advies voor mogelijke toepassingsgebieden van beide maatregelen bij Univé;
e. Een voorbeeldaanpak voor het testen van een Proof-of-Concept met IDP en SIM producten (zie de hacking scenario's).

5. Conclusies en aanbevelingen

In het vooronderzoek is een inventarisatie gemaakt van de verschillende technologische bedreigingen die anno 2005 kunnen spelen en is binnen korte tijd een basaal inzicht gekregen in de beveiliging van de infrastructuur van Univé. Daarbij lag de nadruk op het ontdekken van aanwezige en ontbrekende maatregelen. Bij eventuele hiaten is aangegeven dat aanvullende maatregelen nodig zouden kunnen zijn, afhankelijk van het werkelijke risico dat zo'n hiaat wel of niet vertegenwoordigt. In het vooronderzoek is geconcludeerd dat het zinvol is de huidige beveiligingsarchitectuur aan te vullen met detectieve maatregelen om manifestatie van (directe en indirecte) bedreigingen van binnenuit tijdig te kunnen onderkennen. Toename van de integratie van webtechnologie bij primaire bedrijfsprocessen van Univé en decentralisatie van ICT-beheer zijn bij die conclusie de belangrijkste drijfveren.

In het hoofdonderzoek zijn twee technische verschijningsvormen van dergelijke detectieve maatregelen onderzocht. Consolidatie van beveiligingsgerelateerde meldingen staat bekend als *security information management* (SIM) en beoogt een holistisch beeld van de beveiligingsstatus van een infrastructuur. IDP is een puntoplossing die met goed geïmplementeerde detectiealgoritmen een waardevolle bijdrage kan leveren aan de SIM-informatievoorziening. Een groeiende trend in de IDP-markt zijn de preventiefuncties; daarmee wordt de beveiligingsarchitectuur naast detectie ook uitgebreid met een extra laag van preventie. De complexiteit en diverse knelpunten van IDP maken het selecteren, implementeren en onderhouden van (kennis van) IDP oplossingen een klus voor specialisten, waarvoor Univé externe expertise nodig zal hebben. Er zijn ter illustratie drie cases behandeld waarbij IDP toegevoegde waarde levert aan de beveiliging van de infrastructuur van Univé. Het selecteren, implementeren en onderhouden van een SIM oplossing is minder complex maar kan een belangrijk fundament vormen voor de vervulling van de behoefte die ten grondslag lag aan het hele afstudeertraject: de behoefte aan inzicht in wat er met en op de infrastructuur gebeurt. In een Proof-of-Concept is geëxperimenteerd met een opstelling waarbinnen de IDP producten Cisco Secure IDS 4235 en Snort zijn getest in samenhang met het SIM product NetIQ Security Manager. De focus van de experimenten – die als hacking scenario's zijn uitgevoerd volgende de standaard 'anatomie van een hack' – lag op de correlatiefuncties. De resultaten wezen uit dat de gebruikte producten in de gebruikte configuratie niet de gewenste correlatieresultaten leverden, dat wil zeggen niet in staat waren om verbanden te ontdekken tussen meldingen van heterogene componenten tussen de verschillende fases van een hacking aanval. Er zijn in het hoofdonderzoek aanbevelingen gedaan over het belang van een goede correlatiefunctie en (meer gespecialiseerdere) producten waarmee de gewenste correlatieresultaten wél zouden kunnen worden bereikt. Daarnaast is een indicatie gegeven van technische en beheermatige randvoorwaarden die gelden voor de implementatie van beide maatregelen bij Univé.

Het afstudeertraject is afgesloten binnen de geplande doorlooptijd, doch met kleine uitloop bij de deelfases. Alle deliverables zijn opgeleverd conform het PID *Cyberdefense*. Vanuit professioneel oogpunt worden SIM en IDP gezien als maatregelen die zich voordoen in een beveiligingsarchitectuur waarbinnen verder wordt gekeken dan beveiliging van de buitengrenzen. Het is aan het management van Univé om te beslissen of de gesuggereerde risico's de aanschaf van SIM en/of IDP rechtvaardigen, daarbij natuurlijk in overweging nemend of die risico's niet beter kunnen worden afgedekt of beperkt met *andere* maatregelen. Het strekt tot aanbeveling om voorafgaand aan zo'n beslissing eerst een tweede Proof-of-Concept uit te (laten) voeren, waarbij de werking van de maatregelen wordt gedemonstreerd in een representatieve opstelling en met geschikte SIM en IDP producten.

Rest slechts nog aan te geven dat het grootste deel van het uitgevoerde onderzoek niet beperkt is tot de organisatie van Univé. De aanpak die in het vooronderzoek is gekozen voor de bedreiginganalyse kan worden toegepast bij andere organisaties. De theorie en bevindingen rondom IDP en SIM hebben eveneens een ruimer bereik dan Univé: de enige onderdelen van het hoofdonderzoek die echt beperkt zijn tot Univé zijn de problematiek rondom CODA en de keuze voor IBM Tivoli Risk Manager. Vooral de opgedane kennis rondom SIM, correlatiefuncties en logging beleid lijken aanleiding tot een aanvullende publicatie om zodoende een kleine bijdrage te leveren aan het vakgebied informatiebeveiliging 'in het algemeen'.

6. Evaluatie

6.1. Univé als afstudeerbedrijf

Univé is een betrekkelijk grote organisatie met navenante mogelijkheden en perikelen. De mogelijkheden bij Univé uitten zich tijdens mijn afstuderen in het idee dat mijn onderzoek (indien de resultaten daartoe geschikt zouden zijn) een bijdrage levert aan fundamenten die Univé-breed worden gelegd. De resultaten van het onderzoek blijven dus niet noodzakelijk beperkt tot mijn directe omgeving, maar dragen in potentie een steentje bij aan iets dat zich zou kunnen uitspreiden naar tientallen locaties.

De perikelen die ik bij Univé heb ervaren zijn misschien een beetje inherent aan de bedrijfsvoering bij grotere organisaties. Zo heb ik bij aanvang van het afstuderen een verzoek ingediend om mijn werkstation te laten voorzien van Microsoft Project en Microsoft Visio, maar bleek dat pas vier weken later te kunnen worden gerealiseerd (ware het niet dat een behulpzame collega wat druk uitoefende) – van andere studenten hoor ik dat zulke problemen zich ook bij andere grote bedrijven voor doen (change management). Verder bleek er bij de Proof-of-Concept enige discrepantie te zijn tussen wat (budgettair) mogelijk leek en wat – met name gegeven de tijdbeperking – mogelijk bleek te zijn om externe expertise te kunnen financieren. Daardoor kon de PoC niet in de geplande vorm doorgaan en moest worden uitgeweken naar een alternatieve oplossing.

Rest alleen nog dat de kantine en koffieautomaten, evenals de werkplekken, prima in orde zijn (dat mocht gezegd worden). Bij de cluster Security Management, waar ik mijn opdracht heb uitgevoerd, heerst m.i. een formele sfeer en een niettemin prettige werkomgeving. Tijdens mijn afstudeerperiode heb ik te maken gehad met tien tot vijftien andere medewerkers van andere clusters, van wie het merendeel welwillend heeft geholpen met mijn afstudeeronderzoek.

6.2. De afstudeeropdracht

De oorspronkelijke afstudeeropdracht was vrij ruim geformuleerd, waardoor pas na de eerste weken van het afstuderen duidelijk is geworden wat de precieze richting van het afstudeertraject zou zijn. In overleg met Univé is gekozen voor een bedreiginganalyse en onderzoek naar IDS/IPS en consolidatie van loganalyse. Gedurende het afstuderen kreeg ik voldoende vrijheid om zelf bij te sturen; ik was in de gelegenheid om zelf producten te kiezen voor onderzoek, leveranciers uit te nodigen, contacten te leggen met andere kantoren van Univé, de richting van het theoretische onderzoek te bepalen, et cetera. Ik had zelfs de vrijheid om – indien beargumenteerd – af te wijken van de twee onderzochte maatregelen en in plaats daarvan andere maatregelen te onderzoeken. De afstudeeropdracht had dan een hele andere richting kunnen krijgen. Het belangrijkste keuzemoment betrof de beslissing om voor het experiment gebruik te gaan maken van IBM Tivoli Risk Manager, nadat enkele eerdere tests uitwezen dat het eerder bedachte OS-SIM (www.ossim.net) nog niet volwassen genoeg bleek om mee te experimenteren (OS-SIM bleek nog geen enkele vorm van correlatie te hebben geïmplementeerd en zou derhalve niet bruikbaar zijn voor Univé). Die keuze is verder beargumenteerd in H5.6 van het hoofdonderzoek (“SIM Proof-of-Concept”). De uiteindelijke resultaten van alle activiteiten zijn echter bevredigend en conform de verwachtingen.

6.3. Afstudeerdoelstellingen

In het afstudeerboekje staan de volgende (externe) doelstellingen geformuleerd voor het afstudeertraject:

“Het afstudeerproject maakt een wezenlijk onderdeel uit van het examen.
De student moet aantonen dat hij voldoet aan de competenties van de bachelor of ICT resp. Communications. Dit betekent dat de afstudeerder moet bewijzen dat hij de volgende competenties bezit

- *Kan in teamverband een opdracht tot een goed einde brengen, daarbij gebruikmakend van een projectmatige aanpak*
- *Is flexibel qua samenwerkingsverband en ICT-domein.*
- *Kan zelfstandig werken en in een (multidisciplinair) team resultaatgericht samenwerken.*
- *Betrekt de belangen van de verschillende partijen (van de informatievoorziening) bij het adviseren over en het inrichten van een projectorganisatie.*
- *Kan functioneren in een multidisciplinaire en internationale omgeving.*
- *Kan reflecteren op het eigen gedrag om feedback te geven en te ontvangen.*
- *Kan op diverse manieren effectief communiceren met verschillende geledingen.*

- *Heeft de juiste beroepshouding, is betrokken bij zijn taakstelling, intrinsiek gemotiveerd, kwaliteitsgericht, prestatiegericht en gericht op dienstverlening.*
- *Kan omgaan met de ethische aspecten die samenhangen met de beroepsuitoefening.*
- *Kan kennis up to date houden en uitbreiden, kan kennis uitdragen en heeft een lerende houding.*

Kortom, een afstudeerder dient te bewijzen dat hij op HBO-niveau zelfstandig kan opereren, dat hij bereid is initiatieven te ontplooien, dat hij discipline toont en dat hij creatief met problemen kan omgaan."

Bij de eerste ontmoeting met Univé bleek dat er bij de cluster Security Management genoeg werk te doen was voor twee of meer studenten. In het kader 'multidisciplinair samenwerken' had ik een afstudeerkoppel gevormd met een student Bedrijfskundige Informatica, eveneens van de ICA. Op het laatste moment bleek laatstgenoemde door persoonlijke omstandigheden nog niet te kunnen beginnen met afstuderen, waardoor ik uiteindelijk individueel bij Univé ben gaan afstuderen. Bij de cluster waar ik mijn afstudeeropdracht heb uitgevoerd zitten vooral medewerkers op tactisch niveau – het in teamverband kunnen samenwerken met andere ICTers heb ik daarom niet als zodanig kunnen bewijzen. Wel heb ik tijdens het vooronderzoek verschillende mensen gesproken van diverse 'pluimage' om de bedreiginganalyse te kunnen uitvoeren, waarbij ik heb geprobeerd om een vraagstelling te hanteren die voor de geïnterviewden werkbaar en begrijpelijk was. Ik heb tijdens dat onderzoek ook een bezoek gebracht aan de hoofdvestiging van de BU Zorg (Alkmaar).

Binnen het afstudeertraject heb ik twee projectplannen geschreven: één voor het afstuderen zelf en één voor de Proof-of-Concept, een onderdeel binnen het afstuderen. Beide projectplannen bleken ook achteraf te hebben voorzien in alle benodigde informatie; betrokken mensen, benodigde middelen, verwachte resultaten, planning. Alle activiteiten zijn vrij behoorlijk binnen de planning uitgevoerd en hebben geleid tot de beoogde resultaten.

Voorafgaand aan het voor- en hoofdonderzoek heb ik geprobeerd te achterhalen welke belanghebbenden er waren op verschillende niveaus binnen de organisatie; interne auditors, operationeel management (ICTers), tactisch management (Security Management), strategisch management (Concern Informatie Management). Daarbij heb ik continu gereflecteerd op mijn eigen positie – met enige nederigheid als nieuwkomer en stagiair, maar tegelijkertijd met voldoende assertiviteit en initiatief om mijn verantwoordelijkheid tot het uitvoeren van een zinvol onderzoek te kunnen dragen. Hoewel ik heb moeten constateren dat ik op hogere managementniveaus nog niet zo'n inhoudelijke gesprekspartner ben, heb ik de belangen op die niveaus kunnen achterhalen en ze meegenomen bij het uitvoeren van het onderzoek.

Voorts ben ik van mening dat mijn betrokkenheid, intrinsieke motivatie en 'live long learning' houding blijken uit mijn lidmaatschap van NGI en GvIB, mijn bezoek van 30 maart aan een seminar over SIM van Netlink, mijn bezoek van 20 april aan de TINE beurs in Amsterdam, mijn bezoek van 17 mei aan de IB-opleidingenmarkt in Rijswijk, het op eigen initiatief bijwonen van diverse gesprekken met consultants van Avensus, Fox-IT, IBM en Ubizen, het feit dat ik voor mijn afstuderen op eigen kosten enkele technische boeken heb aangeschaft, mijn (doch prille) hulp aan de inrichting van een nieuwe post-HBO security opleiding bij de ICA (MRSM) en ten slotte mijn intenties om na het afstuderen bij Universiteit van Amsterdam nog dieper in de beveiligingsmaterie te duiken en een artikel te publiceren over het afstudeeronderwerp.

6.4. Zelfreflectie

In eerdere projecten binnen mijn opleiding was bijna altijd sprake van projectgroepen die bestonden uit ongeveer acht studenten. De 'werkstage' aan het begin van het derde jaar en de afstudeerstage zijn de enige schoolprojecten die ik volledig individueel heb uitgevoerd. Ik keek met plezier uit naar het samenwerken met de eerdergenoemde BI-student (mede omdat ik had gehoopt van hem te kunnen leren over risicomanagement en bedrijfskunde) en betreurde dat ik als enige student moest beginnen bij Univé. Terugblikkend op de afstudeerperiode ben ik van mening dat ik mijn afstudeeropdracht met voldoende inzet heb uitgevoerd, maar dat er uiteindelijk een betere koppeling met de bedrijfsvoering van Univé had kunnen zijn als ik had samengewerkt met iemand die verstand heeft van de bedrijfskundige aspecten (risicoanalyse, doorberekening van de kosten van IDP/SIM, relatie met bestaande beheerprocessen, et cetera).

In de beginfase van het afstuderen ervoer ik het gebrek aan een duidelijke richting als een belemmering voor de voortgang van mijn afstudeertraject, maar na regelmatig vragen te stellen aan de opdrachtgever heeft er uiteindelijk toch op tijd een concretisering plaatsgevonden. Ik had het gevoel dat ik zelf misschien meer had kunnen doen om de opdracht sneller te concretiseren, hoewel ik achteraf eigenlijk niet kan verzinnen wát dat dan had moeten zijn.

Tijdens het vooronderzoek heb ik twee bestaande methoden onderzocht voor het uitvoeren van een bedreiging c.q. risicoanalyse. Gezien de context van mijn opdracht (Univé-brede infrastructuur) zocht ik een methode om snel een inzicht te kunnen krijgen in zoveel mogelijk bedreigingen die binnen die context speelden - de bestaande methoden leenden zich daar niet voor. Achteraf gezien ben ik misschien iets te ambitieus geweest en had ik wellicht beter een zeer beperkt deel van de infrastructuur uitgebreider moeten analyseren met zo'n bestaande, bewezen methode. Daar staat tegenover dat het doel van het vooronderzoek niet een volledige en formeel correcte analyse was, maar vooral een 'inleiding op de infrastructuur', waarbij een goede inventarisatie moest worden gemaakt van de relevante bedreigingen en de genomen maatregelen. Bovendien is de gebruikte aanpak in overleg met een RE gekozen en goedgekeurd, zodat ik de bedreiginganalyse niet heb gebaseerd op een ongefundeerde aanpak die 'zomaar eventjes' is verzonnen.

Het hoofdonderzoek heb ik zonder hindernissen kunnen uitvoeren; het grootste deel bestond uit het samenvattend van wetenschappelijke artikelen en het zoeken van achtergrondinformatie. Uiteraard heb ik de teksten met enige regelmaat teruggekoppeld met de opdrachtgever om duidelijkheid te krijgen over hun verwachtingen van het hoofdonderzoek.

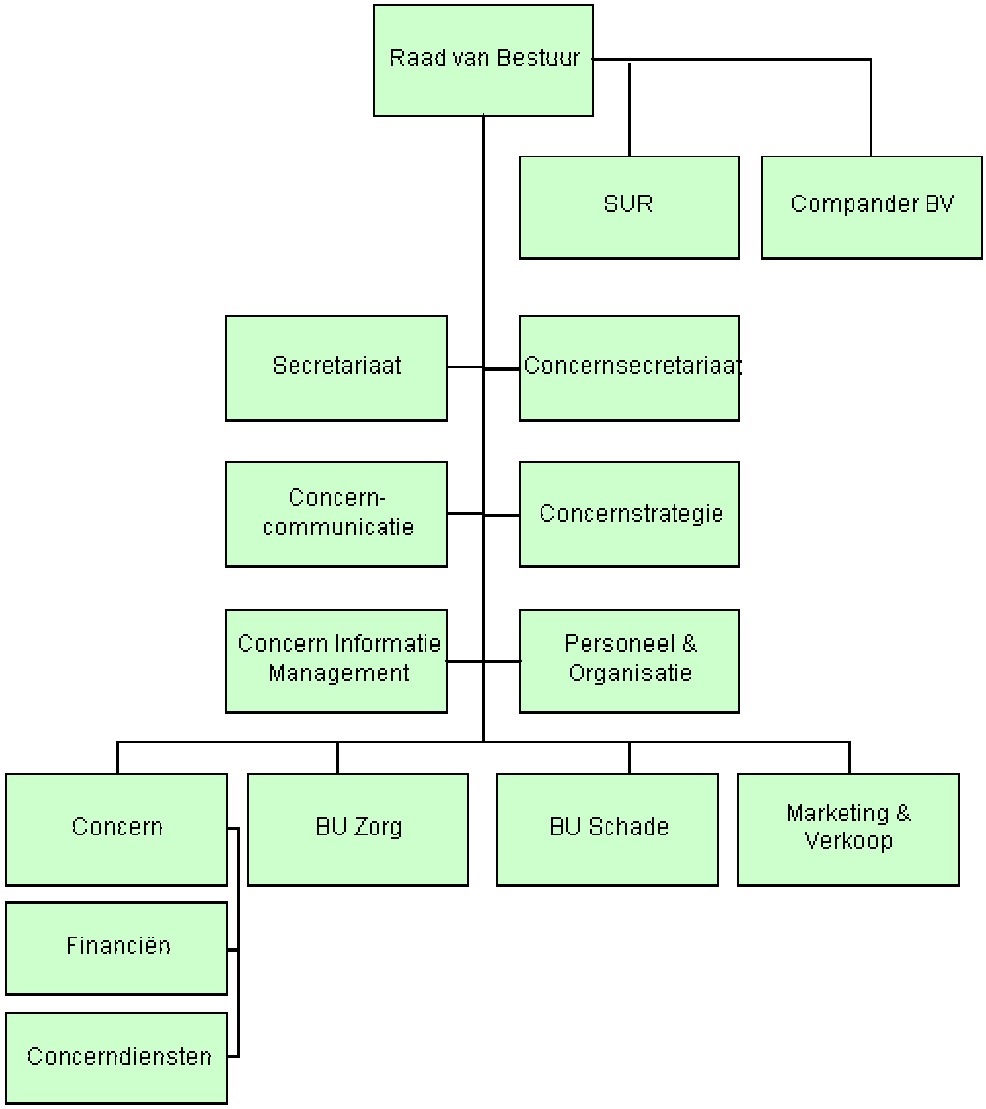
Voor de Proof-of-Concept heb ik vrijwel al mijn energie gestoken in Risk Manager, met dien verstande dat veel van mijn tijd verloren zou zijn als dat product niet in een PoC zou zijn te testen. Daarbij gaat het vooral om de tijd die ik heb gestoken in gesprekken met IBM en het lezen van de enorme hoeveelheid documentatie over Tivoli en Risk Manager (ter voorbereiding op de PoC). Toen inderdaad bleek dat een PoC van Risk Manager niet kon worden gerealiseerd ervoer ik dat als een tegenslag. Slechts één dag eerder had ik toevallig gesproken met Arno Coster van ISSB en gehoord dat NetIQ kosteloos en volledig is te evalueren. Daardoor was er voor mijn PoC dus ineens een alternatief voor Risk Manager. Als ik Arno niet had gesproken of als NetIQ niet had bestaan had ik echter geen PoC meer op kunnen zetten en zou er te weinig tijd over zijn gebleven om andere gespecialiseerde producten te verkrijgen (ArcSight, netForensics, …). Achteraf denk ik echter nog steeds dat ik de juiste keuze heb gemaakt door zoveel tijd te stoppen in Risk Manager. Risk Manager past prima binnen de bestaande infrastructuur van Univé en bevat (volgende de documentatie) geavanceerde correlatiefuncties, die bovendien naadloos aansluiten bij het theoretische deel van het hoofdonderzoek. Het is nog steeds een reële optie voor Univé. Het risico dat ik niet genoeg tijd over zou hebben voor een alternatieve PoC-opstelling heb ik dus bewust genomen. Gelukkig bleek NetIQ Security Manager vrij eenvoudig te temmen en is binnen de beschikbare tijd toch nog een interessant *praktisch* experiment uitgevoerd.

Samenvattend denk ik dat ik mezelf heb neergezet als een voldoende competente hbo'er.

Appendix A – Organogram (top-level)

Bron van organogram (intranet van Univé): http://uninet/smartsite.dws?id=43916

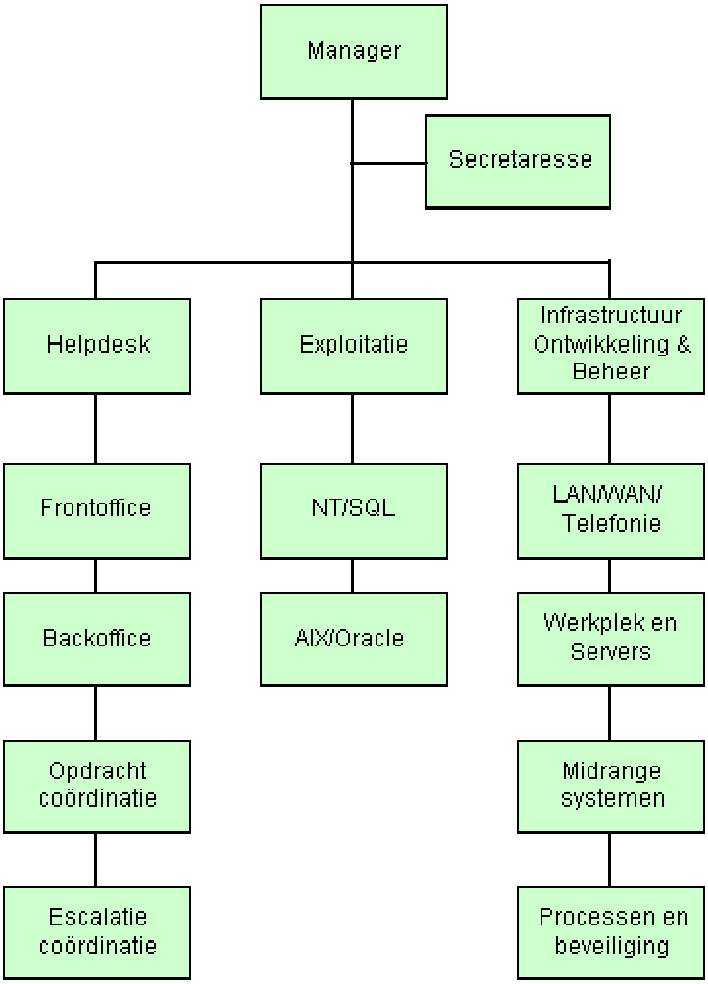
Hieronder staat een schematische weergave van de organisatiestructuur bij Univé, zoals geldt na de reorganisatie van 1 juli 2003. Er worden vier bedrijfsonderdelen onderscheiden: Concern, BU Zorg, BU Schade en Marketing & Verkoop.



Appendix B – Organogram Concern à Beheer & Exploitatie

Bron van organogram (intranet van Univé): http://uninet/smartsite.dws?id=13017

Beheer en Exploitatie



Appendix D – Team IOB

Bron (intranet van Univé): http://uninet/smartsite.dws?id=13017#3

De missie van het team is:
Het marktconform, zowel zelf als door derden, pro-actief en participatief ontwikkelen, in exploitatie brengen en tactisch beheren van generieke technische infrastructuren ten behoeve van Univé, en het leveren van ondersteuning aan de exploiterende partijen daar waar de inbreng van de technische kennis omtrent de producten benodigd is.
Dit omvat 3e-lijns support en het oplossen van problemen (conform ITIL).

De doelgroep van IOB omvat heel Univé. De focus ligt hierbij op generieke infrastructuren die Univé-breed uniform zijn en/of in exploitatie zijn bij de afdeling Beheer & Exploitatie te Zwolle. Specifieke systemen bij Business Units en/of Onderlingen die buiten bovenstaande scope vallen worden op aanvraag opgepakt mits deze werkzaamheden niet conflicteren met werkzaamheden voor de primaire doelgroep. Alleen door de (beperkte) bemensing gericht in te zetten op werkzaamheden is het mogelijk de gewenste prestaties te leveren. Binnen het aandachtsgebied 'Processen en Beveiliging' wordt verantwoordelijkheid gedragen voor:

- Het voorbereiden van een Univé-breed beveiligingsbeleid, inclusief een implementatieplan per jaar
- Het uitwerken van normen en procedures voor beveiligingsmaatregelen
- Het adviseren van de ICT-afdelingen en de BU's over nut en noodzaak van beveiliging
- Het adviseren over de procesinrichting van ICT-beheerprocessen
- Het begeleiden van audits en controles
- Het adviseren over wet- en regelgeving (zoals de Wet Bescherming Persoonsgegevens)
- Het stimuleren van een positieve houding bij de Univé medewerkers ten aanzien van beveiliging

Deze pagina is opzettelijk blanco.

Appendix E – Vooronderzoek

Deze pagina is opzettelijk blanco.

Appendix F – Hoofdonderzoek

Deze pagina is opzettelijk blanco.

Appendix G – PID 'Experiment IBM Tivoli Risk Manager'

Deze pagina is opzettelijk blanco.

Appendix H – Verslaglegging van de Proof-of-Concept

Deze pagina is opzettelijk blanco.