Plan van Aanpak
Master Thesis

Evelien Roos
0456705

Document: Plan van Aanpak
Auteur: ing. E. Roos
Studentnummer: 0456705
Emailadres: me@evelienroos.nl
Afstudeerbegeleider: L. Consoli
Email: l.consoli@science.ru.nl
Onderwerp: Vulnerabilities as monsters
Versie: 1.3
Datum: 06-11-2006

Voorwoord

Als afsluiting van de master Informatiekunde van de Radboud Universiteit Nijmegen voer ik deze afstudeeropdracht uit.
Mijn afstudeeropdracht is een onderzoek wat onderdeel is van het onderzoek van W. Pieters en L. Consoli *"Vulnerabilities as monsters: the cultural foundations of computer security".*
Het doel van het onderzoek is inzicht te krijgen in de filosofische achtergrond van informatiebeveiling in de informatiekunde.
Er wordt hierbij geprobeerd helder te krijgen hoe de culturele factoren van informatiekunde een rol spelen bij informatiebeveiling. Deze kant van de informatiebeveiliging wordt volgens de onderzoekers vaak onderbelicht.

Dit Plan van Aanpak geeft een beeld weer van de activiteiten waaruit de afstudeeropdracht zal bestaan en de afspraken die gemaakt worden tussen afstudeerder en afstudeerbegeleider.

Inhoudsopgave

1.Inleiding

Het onderzoek wat ik uitvoer is een onderdeel van een lopend onderzoek 'Vulnerabilities as monsters' [1] van Wolter Pieters en Luca Consoli.
De inspiratie van het onderzoek komt vanuit het proefschrift van Martijntje Smits [2] waarin zij handreikingen geeft hoe men om zou kunnen gaan met de invoering van nieuwe technologieën.

Het doel van het onderzoek is om vanuit een cultureel oogpunt te kijken naar kwetsbaarheden in de informatiebeveiliging. Een model is opgesteld wat een strategie beschrijft hoe men om zou kunnen gaan met kwetsbaarheden in de informatiebeveiliging. Hiermee kunnen kwetsbaarheden wellicht eerder opgespoord kunnen worden.

Het resultaat van mijn onderzoek is, dat de geïnterviewden het model leren kennen en eventueel kunnen gebruiken bij het voorkomen van bedreigingen. Wanneer blijkt dat het model geschikt is en toepasbaar is binnen de praktijk zouden er meer mensen gebruik van kunnen maken.

1.1 Martijntje Smits

Ingenieur, filosofe en onderzoeker Martijntje Smits beschrijft in haar proefschrift 'Monsterbezwering, de culturele domesticatie van nieuwe technologie' hoe de huidige samenleving om zou kunnen gaan met nieuwe technologieën. Smits refereert in haar proefschrift regelmatig naar de werken van cultureel antropologe Mary Douglas waarin de visie van Douglas over reinheid, risico's en gevaar in de samenleving wordt beschreven[3,4].
Smits ontwikkelde op basis daarvan de 'monstertheorie', waarbij de risico's, uit de werken van Douglas, gezien worden als een monster, een dubbelzinnig fenomeen, iets dat buiten elke culturele categorie valt of juist eigenschappen van meerdere culturele categorieën heeft.

1.2 Culturele categorie

Wij kijken naar de wereld op een bepaalde manier, zo krijgt de wereld betekenis. Die duiden we aan in culturele categorieën. Een indeling van de wereld in culturele categorieën is dus een manier om de maatschappij in te delen. Culturele categorieën zijn flexibel en aanpasbaar en zijn niet per sé de categorieën zoals die daadwerkelijk bestaan, zoals de (biologische) categorie man en vrouw.
Wanneer er sprake is van botsende culturele categorieën, dan zou er volgens Smits sprake zijn van een monster.

Smits erkent in onze huidige samenleving ook deze monsters: de monsters van de technologische vernieuwing. In het monstermodel wordt ervan uitgegaan dat monsters door de maatschappij zelf gecreëerd worden.
Zo kunnen oude kleren bijvoorbeeld ingedeeld worden in de culturele categorie 'afval' maar ook in de culturele categorie 'grondstoffen voor nieuwe kleding', zoals bijvoorbeeld gebeurt met afgedankte kleding bij het Leger des Heils waarvan hippe kleding voor de jongerenlijn van de Bijenkorf gemaakt wordt.

1.3 Monsterbenadering

In het proefschrift van Smits beschrijft zij dat bij het invoeren van nieuwe technologieën vier manieren zijn om de monsters die hier ontstaan te behandelen. Het monster wordt heilig verklaard en met open armen ontvangen (monsteromhelzing) of deze wordt verguisd en verbannen (monsteruitdrijving).
Smits beschrijft nog een derde en vierde methode als aanvulling op de eerste twee methodes zoals die beschreven worden door Douglas.
De derde methode is assimilatie: dingen die niet in de categorieën passen, monsters, worden onderkend maar niet meteen afgewezen. Monsters worden geassimileerd, ze worden niet als bedreiging ervaren, maar als een uitdaging en “zowel het karakter van het oorspronkelijke monster als de opvattingen waar het een weerlegging van was, worden drastisch herzien” [1, blz. 156]
De vierde methode is het niet uitstoten maar aanpassen van de monsters aan de bestaande categorieën zodat hun dreiging weggenomen wordt, monsteraanpassing.

1.4 Informatiebeveiliging

Volgens Pieters en Consoli bestaat er een analogie tussen de monsters uit de monstertheorie van Smits en de kwetsbaarheden in de beveiliging van systemen. Zij zijn van mening dat er dreigingen of kwetsbaarheden zijn doordat deze niet in een bestaande culturele categorie van de informatiekunde te plaatsen zijn [2] of doordat deze niet herkend zijn als kwetsbaarheid.

Als een ding de status krijgt van een computervirus wordt het een bedreiging. Dat iets wordt pas een computervirus zodra het het label computervirus krijgt.
Een virus is eigenlijk een programmaatje (vaak gemaakt met negatieve bedoelingen) maar het wordt niet gezien als virus totdat het door de maatschappij bestempeld wordt als een virus.
Een link in een pdf-document wordt niet gezien als een risico totdat hackers er gebruik van weten te maken om automatisch een website te laden als het document geladen wordt.
De link in het pdf-document is een voorbeeld van een ding dat niet gezien wordt als een kwetsbaarheid, tot het iets doet wat lijkt op een kenmerk van een virus. Vanaf dat moment wordt het gezien als een kwetsbaarheid.

Vanuit het onderzoek van Pieters en Consoli is er behoefte ontstaan om te weten wat experts op het gebied van informatiebeveiliging van het nieuwe model vinden en of zij zich kunnen vinden in de analogie.
Naar aanleiding van de uitkomsten van de interviews zal gekeken worden of er aanpassingen op het model moeten plaatsvinden.

1.5 Onderzoeksvraag

Wat vinden de ondervraagde experts van de informatiebeveiliging van het model van Pieters en Consoli m.b.t. kwetsbaarheden in de informatiebeveiliging, welk gebaseerd is op de monstertheorie van Smits?

Deelvragen

1. Hoe wordt er omgegaan met bedreigingen en kwetsbaarheden in de informatiebeveiliging?
2. Hoe ziet de analogie tussen de 'monstertheorie' en de kwetsbaarheden in de informatiekunde

eruit?
3. Hoe kan het monstermodel uitgelegd worden aan de experts in de informatiebeveiliging?
4. Wat vinden de ondervraagde experts van de informatiebeveiliging van het model van Pieters en Consoli?
5. Moet het model van Pieters en Consoli aangepast worden aan de bevindingen uit de interviews?

2. Verantwoording

2.1 Relevantie

Het onderzoek wat ik uitvoer moet duidelijk maken of het model dat zij opgesteld hebben aansluit bij de informatiebeveiliging en toepasbaar is op de informatiekunde. De vraag is derhalve of het model toepasbaar en bruikbaar is zodat kwetsbaarheden niet alleen achteraf maar ook van te voren (met het model) opgespoord kunnen worden.

2.2 Functionaliteit

Het onderzoek wat ik uitvoer is een praktijkvalidatie om het opgestelde model aan de praktijk te toetsen en de experts de mogelijkheid te geven aan te geven of er aanpassingen of uitbreidingen van het model nodig zijn.

Het uiteindelijke model zal voor eenieder die met informatiebeveiliging te maken heeft handreikingen aangeven hoe er vanuit een cultureel oogpunt omgegaan kan worden met informatiebeveiliging en hoe cultureel gedrag mede de kwetsbaarheden binnen de informatiebeveiliging bepaalt. Ook wordt hierin aangegeven hoe de culturele factor bepalend is bij het omgaan met kwetsbaarheden binnen de informatiekunde.

2.3 Motivatie

Het onderzoek wordt uitgevoerd omdat de meningen van de experts in dit onderzoek over dit model nog niet gepeild is en nog niet duidelijk is of het model ook in de praktijk bruikbaar zou kunnen zijn. Het onderzoek van Pieters en Consoli wil een ander licht op de informatiebeveiliging laten schijnen. Namelijk die vanuit een meer filosofisch en cultureel oogpunt.
Ze willen weten wat de betekenis is van culturele aspecten als het gaat om security.

3.Theoretisch kader

3.1 Kennisgebied

Het kennisgebied wat hoort bij dit onderzoek is informatiekunde, met name de informatiebeveiliging binnen de informatiekunde. De technische kant is in dit onderzoek minder relevant. Het onderzoek draait meer om de culturele aspecten met betrekking tot de informatiebeveiliging.

3.2 Termen

Om duidelijkheid te verschaffen in de termen die tijdens het onderzoek gebruikt worden, heb ik deze hieronder uitgelegd.

- Model: beschrijving van een manier hoe men met iets om kan gaan.
- Informatiebeveiliging: het geheel van maatregelen om onjuist gebruik van informatie, programma's etc. te voorkomen.
- Kwetsbaarheid: een zwakheid die misbruikt of gebruikt zou kunnen worden waarbij de gevolgen van dit gebruik/misbruik anders zijn dan het beoogde doel van eigenaar van die zwakheid of kwetsbaarheid.

3.3 Veronderstellingen

Aangenomen wordt dat de experts die geïnterviewd worden niet op de hoogte zijn van het model van Smits en dat van Pieters en Consoli. Deze dienen daarom tijdens het interview geïnformeerd te worden wat het model inhoudt. Zonder een goed begrip van dit model zijn de antwoorden op de vragen die gesteld worden niet relevant.

4. Methode

4.1 Gekozen domein

De interviews met de experts zijn de belangrijkste informatiebron. Daarom is het belangrijk goed na te denken over welke experts geïnterviewd zullen worden. Geprobeerd zal worden een evenwichtige verdeling tussen experts uit het bedrijfsleven en uit de academische wereld te maken.
Deze experts zullen benaderd worden door de onderzoeker zelf, welk de experts selecteert op basis van publicaties in verschillende media.
Omdat niet alle informatiebeveiligingexperts geïnterviewd kunnen worden i.v.m. de tijdsplanning zal geprobeerd worden minimaal 10 experts te interviewen. De experts zullen in week 45 een uitnodiging ontvangen.

4.2 De gekozen variabelen

Relaties

Het onderzoek moet uitwijzen of er het model aansluit bij de praktijk en kan worden gezien als een praktijkvalidatie. Bij een praktijkvalidatie wordt het opstelde model getoetst aan de praktijk. In dit onderzoek gebeurt dit door middel van interviews met experts.

4.3 Het beantwoorden van de deelvragen

Zoals al eerder vermeld bij de probleemstelling (zie 1.4) kan de onderzoeksvraag worden opgedeeld in enkele deelvragen. Middels de antwoorden op de deelvragen wordt getracht de onderzoeksvraag te beantwoorden. De deelvragen kunnen niet los van elkaar gezien worden en alleen als ze allen beantwoord worden zal dit onderzoek het gewenste resultaat hebben.

Voor de verschillende deelvragen worden verschillende manieren van informatieverzameling toegepast.

4.3.1 Deelvraag 1:

Hoe wordt er omgegaan met bedreigingen en kwetsbaarheden in de informatiebeveiliging?

Het bestuderen van relevante literatuur kan een beeld geven hoe er nu omgegaan wordt met kwetsbaarheden in de informatiebeveiliging. Gekeken wordt naar de culturele invloeden op de informatiebeveiliging.

Ook in de interviews worden er vragen gesteld hoe er door de experts in de informatiebeveiliging omgegaan wordt met kwetsbaarheden.
Door literatuurstudie zal tevens worden onderzocht wat de huidige situatie is binnen de informatiebeveiliging. Wat doen mensen om aanvallen, virussen etc. te voorkomen?

4.3.2 Deelvraag 2:

Hoe ziet de analogie tussen de 'monstertheorie' en de kwetsbaarheden in de informatiekunde eruit?

Door middel van het bestuderen van literatuur wordt een beeld gevormd van het model van Smits en geprobeerd de analogie te begrijpen. Ook de gesprekken met de afstudeerbegeleider moeten duidelijk maken hoe de analogie eruit ziet.

4.3.3 Deelvraag 3:

Hoe kan het monstermodel uitgelegd worden aan de experts in de informatiebeveiliging?

Er moet bedacht worden hoe het model voorgelegd kan worden aan de experts in de informatiebeveiliging op een heldere en duidelijke manier zodat deze hier een goede reactie op kunnen geven. Dit moet gebeuren op een korte en krachtige manier. De experts moeten snappen wat het model inhoudt en wat er uitgelegd wordt. Daarbij is een korte introductie met heldere voorbeelden een vereiste.

4.3.4 Deelvraag 4:

Wat vinden de ondervraagde experts van de informatiebeveiliging van het model van Pieters en Consoli?

Door middel van open gestructureerde interviews met informatie-experts en specialisten op het gebied van informatiebeveiliging wordt geprobeerd een antwoord te verkrijgen op deze onderzoeksvraag.
Daarbij wordt eerst het model van Smits voorgelegd en daarna het model van Pieters en Consoli. Hierbij worden voorbeelden aangedragen om de persoon in kwestie kennis te laten maken met het model en daarna wordt gekeken of de monstertheorie toepasbaar zou kunnen zijn voor de beveiligingsproblematiek binnen de informatiekunde.

4.3.5 Deelvraag 5:

Moet het model van Pieters en Consoli aangepast worden aan de bevindingen uit de interviews?

Wanneer uit de open interviews met informatie-experts blijkt dat aanpassingen aan het model van Pieters en Consoli wenselijk zijn, wordt gekeken of deze aanpassingen ook uitgevoerd kunnen worden Wanneer uit de interviews blijkt dat er uitbreidingen van het model gewenst zijn zullen deze uitbreidingen opgenomen worden als advies in de scriptie.

5.Tijd en faseringschema

5.1 Voorbereiding

Om het onderzoek voorspoedig te laten verlopen is een goede voorbereiding noodzakelijk.
Door middel van het Plan van Aanpak wordt duidelijk hoe een antwoord verkregen zal worden op de onderzoeksvraag.

De activiteiten in deze fase zijn:

- Oriëntatie onderzoeksdomein
- Opstellen Plan van Aanpak

5.2 Uitvoering

De vragen die tijdens het interview gesteld worden moeten ingeleid worden door een toelichting op het model en voorbeelden van herkenbare situaties. Mocht het doel van het model niet duidelijk zijn of niet begrepen worden dan kunnen de antwoorden uit de interviews geen bijdrage leveren aan het onderzoeksresultaat.

De bijbehorende activiteiten in deze fase zijn:

- Opstellen interviews
- Afnemen interviews

5.3 Verwerken

De resultaten uit de interviews zullen verwerkt worden tot een verslag waarbij de gedane uitspraken behandeld zullen worden. Wanneer blijkt uit de interviews dat het model aangepast zou moeten worden, wordt dit in het onderzoeksrapport beschreven.

De activiteiten tijdens deze fase zijn:

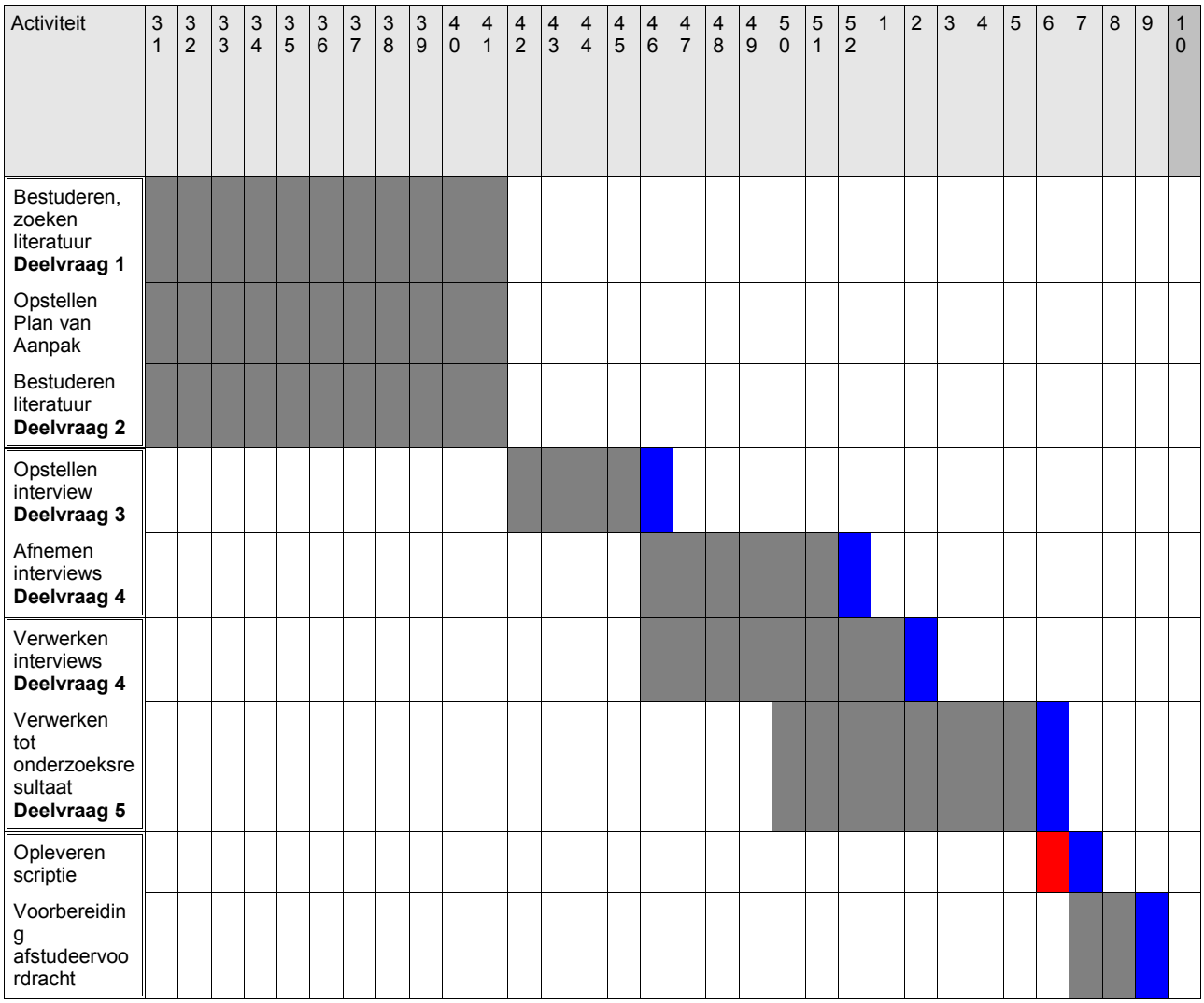
- Verwerken interviews
- Verwerken tot onderzoeksresultaat
- Conclusies en beantwoording onderzoeksvraag

5.4 Afronding

In deze fase, de afronding van het onderzoek en de afstudeeropdracht, worden alle resultaten verwerkt in een scriptie.

- Schrijven scriptie
- Voorbereiding afstudeervoordracht

5.5 Globale planning



Bufferweken

6. Afspraken

De afstudeerbegeleider is dhr Consoli. Getracht wordt eens in de twee tot drie weken een voortgangsgesprek te houden om de voortgang van het project te bespreken.
Indien nodig zal er ook communicatie kunnen plaatsvinden via email.

De afstudeerbegeleider geeft de afstudeerder inhoudelijke feedback op geleverde documenten, op de voortgang van het project en op de planning van het project.

De activiteiten van de afstudeerder worden thuis uitgevoerd daar haar thuissituatie het niet toelaat om full-time op de universiteit aanwezig te zijn.

7. Overzicht te gebruiken literatuur

1. Smits, M., *Monsterbezwering*, De culturele domesticatie van nieuwe technologie, Boom, 2002
2. Pieters, W., Consoli, L., *Vulnerabilities as monsters*: the cultural foundations of computer security (extended abstract), gepresenteerd op de conferentie ECAP '06, Trondheim (Norway), 22-24 June 2006
3. Douglas, M., *Purity and Danger: An analysis of the concepts of pollution and taboo*, Routledge, 1966
4. Douglas, M. *Risk and blame: Essays in Cultural Theory*, Routledge, 1992

Aan te raden literatuur:

1. Verbooy, H., *Computerethicus: Waakhond van de samenleving?,* IK, vierde jaargang, nummer 3, 2005, pag 9-13
2. 2Frissen, V., *De domesticatie van de digitale wereld,* Oratie Erasmus Universiteit 2004
3. 3. de Vries, G., *Leven in de risicosamenleving*, Amsterdam University Press, 2005
4. 4.Mitcham, C. *Thinking Through Technology: The Path Between Engineering and Philosophy*, University of Chicago Press, 1994
5. Latour, B., Science in Action, Harvard University Press, 1987.
6. Himanen, P, Spaendonk, M. van, *De hacker-ethiek en de geest van het informatietijdperk*, Random House, 2001
7. Overbeek, P., Roos Lindgreen, E., Spruit, M., *Informatiebeveiliging onder controle*, Pearson Prentice Hall, 2004

Thomas N. Burg , Monstermedia-Monströsität angesichts von Weblogs, 2006 http://randgaenge.net/texts/monstermedia, online 16.09.2006

T. Zijlstra, *Monstrous KM*, 2003 http://www.zylstra.org/blog/archives/001075.html, online 16.09.2006

Luiif, H., Klaver, M., *Bitbreak*, 2000 http://www.tno.nl/defensie_en_veiligheid/producten_en_diensten/beleidsstudies/veiligheid/information_operations/luiijfbitbreuk.pdf, online 16.09.2006

Overbeek, P., Roos Lindgreen, E., Spruit, M., *Informatiebeveiliging als beheerst proces*, 2000 http://primavera.fee.uva.nl/PDFdocs/2000-30.pdf online 16.09.2006

Hofman, A., Elsinga, B., *Security Principles*, pattern paper ingediend voor EuroPlop, 2003, http://www.platforminformatiebeveiliging.nl online 16.09.2006

Neys, C., *It'ers, regels en security awareness*, 2003 https://www.platforminformatiebeveiliging.nl/tikiwiki/tiki-download_file.php?fileId=53 online 16.09.2006

- Jochem, A. e.a., *Security Principes*, 2005 http://www.platforminformatiebeveiliging.nl/werkgroepen/hf_wg_expertbrieven.html, online 16.09.2006
- Boutellier, P., Ippel, P., *'Veiligheid gegarandeerd' en 'privacy gered'*, 2005 http://www.verwey-jonker.nl/images/dynamisch/D0543440.pdf, online 16.09.2006
- Kanters, F., *Communicatie als succesfactor voor informatiebeveiliging*, http://www.le-platane.nl/Publicaties/JBIB%202004-2005.pdf, online 16.09.2006
- Cultuurfilosofie van de techniek, Dijkshoor, J., online 16.09.2006 http://home.student.utwente.nl/j.w.dijkshoorn/cft/college5.html
- Oud, E., *De organisatorische aspecten van informatiebeveiliging*, **I**nformatiebeveiliging jaarboek 2004/2005 pag. 164-172, online 18.09.2006 www.euronet.nl/users/ernstoud/pdf/IB-JB2004.pdf
- http://www.digibewust.nl/