Het versterken van de zwakste schakel in de informatie beveiliging

Plan van aanpak Versie 3.1.1

Naam: ing. D. (Dick) Janssen
Afstudeerdocent: dr. L. (Luca) Consoli
Referent: dr. P. (Patrick) van Bommel
Plaats, datum: Nijmegen, 11 april 2005
Richting: Informatiekunde
Studentnummer: 0345032
E-mail: dickjanssen@student.ru.nl
Mobiel: 06-47082319
Versie: 3.1.1
Status: Bèta

Inhoudopgave

1. Inleiding

Na aanleiding van de film “Hackers” waarin de goeroe onder de hackers Kevin Mitnick de hoofdrol speelt is dit onderwerp me gaan fascineren. In de film komt naar voren hoe makkelijk gevoelige informatie te verkrijgen is door gebruik te maken van het fenomeen social hacking. Social hacking ook wel bekend als social engineering kan beschreven worden als “de kunst en wetenschap om mensen te laten doen wat jij wil” (Bernz) [1], of “door hackers gebruikte psychelogische trucs met als doel het verkrijgen van gevoelige informatie om toegang te krijgen tot beveiligde systemen (Palumbo) [1]. Omdat mijn interesse vooral ligt op het gebied van Security en Ethiek leek me dit een ideaal onderwerp voor een afstudeeronderzoek.
Tijdens het onderzoek gaat er bekeken worden hoe dit fenomeen bestreden kan worden en wie er een verhoogd risico loopt slachtoffer te worden van dit fenomeen.

Dit document zal dienen als basis voor het uitvoeren van dit onderzoek. In dit document worden alle aspecten van het onderzoek gedetailleerd beschreven met de bedoeling een bepaalde structuur te geven aan het uitvoeren van het onderzoek.

Hoofdstuk 2 zal beschrijven wat nou de precieze probleemstelling is van dit onderzoek zodat duidelijk wordt welk probleem er speelt en hoe waarom dit ook daadwerkelijk als een probleem ervaren wordt. Tevens wordt er duidelijk gemaakt in welke kennisgebied het onderzoek zich bevindt, wat de reden is van het onderzoek en in welke vorm het antwoord op de probleemstelling vastgelegd wordt.

Hoofdstuk 3 zal gaan over het theoretische kader waarbinnen het onderzoek zal worden uitgevoerd. Dit kader zal bestaan uit bepaalde theorieën en methoden die gebruikt zullen worden in het onderzoek. Tevens worden er in hoofdstuk deelvragen beschreven met de bij behoorde aanpak van de deelproblemen.

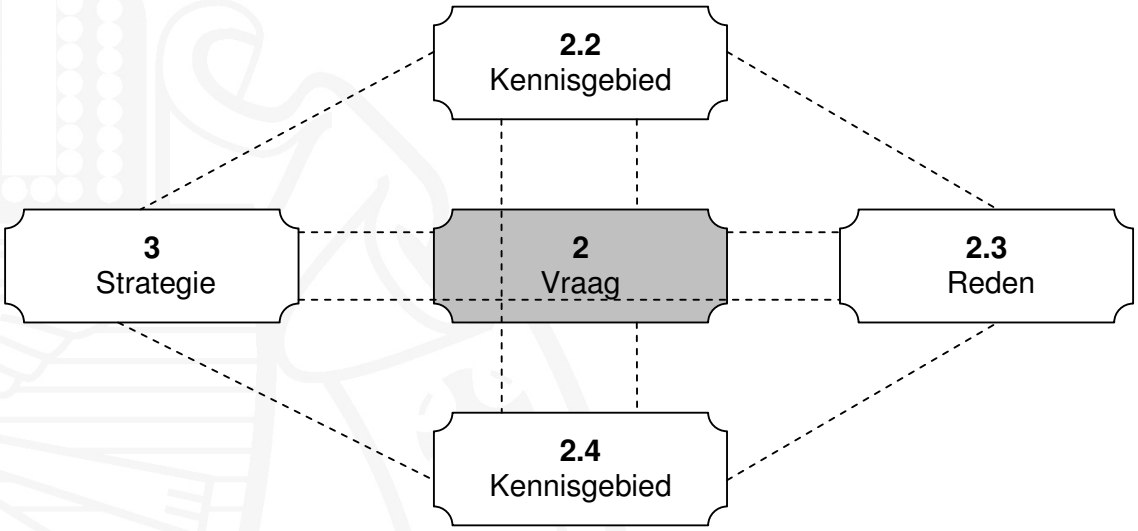
In Hoofdstuk 4 zullen alle afspraken die gemaakt zij met betrekking tot dit onderzoek worden vastgelegd.
.
Hoofdstuk 5 zal een overzicht weergeven van contact informatie van de betrokken bij dit onderzoek.

In hoofdstuk 6 zal een literatuurlijst bevatten van literatuur (Boeken, artikelen, grijs/overig) die tijdens de voorbereiding op het onderzoek gebruikt zijn.

In hoofdstuk7 wordt een planning van het project uiteengezet met daarin de verschillende fasen; voorbereiding, materiaal analyse, materiaal verwerking, rapportage.

2. Probleemstelling

Voor het opstellen van de probleemstelling is gebruik gemaakt van de methode: “Een onderzoek voorbereiden van Heinze Oost [2]. In deze methode staat het volgende model centraal:



Figuur 1: Structuur model van de probleemstelling

Zoals het model weergeeft staat “de vraag” centraal binnen de probleemstelling en staat in relatie met een aantal andere aspecten. Deze aspecten kunnen gezien worden als een soort puzzelstukjes die in elkaar moeten passen. Als de stukjes perfect in elkaar passen kan er aangenomen worden dat de kwaliteit van de probleemstelling gegarandeerd is. Bij elk puzzelstukje staat door middel van een hoofdstuk nummer aangeven waar dit aspect is terug te vinden binnen dit plan van aanpak.

Voor bedrijven en de overheid is het belangrijk dat gevoelige en geheime informatie niet in verkeerde handen zal vallen. Met de huidige stand van de techniek wordt het steeds moeilijker om deze informatie te beschermen. Dit als gevolg van de hogere connectiviteit. Bedrijven en overheden zijn aangesloten op het World Wide Web en daarmee zijn ze verbonden met de hele wereld. Er zijn tal van gespecialiseerde bedrijven die zich bezig houden met het beveiligen van informatie. Deze bieden vaak technisch oplossingen die ongewenste toegang tot informatie kunnen voorkomen. Echter niet alle beveiligingsproblemen kunnen opgelost worden met geavanceerde technologieën omdat de mens ook nog altijd een rol zal spelen. Een systeem kan waterdicht beveiligd zijn maar er zullen altijd mensen toegang hebben tot dit systeem. De menselijke factor wordt namelijk vaak gezien als “de zwakste schakel in de informatiebeveiliging” omdat mensen goedgelovig, ongeïnformeerd, goed van vertrouwen en behulpzaam zijn. De social hacker zal zich dan ook richten op deze “zwakheden van de mens” om zo alsnog toegang te krijgen tot de beveiligde de informatie.
In dit onderzoek zal er gekeken worden naar bedrijven die vaak slachtoffer zijn van social hacking aanvallen. Om te bepalen welke bedrijven dit zijn zal gekeken worden vanuit de social hacker: wat zijn de drijfveren van de social hacker en hoe sluiten deze aan bij een bepaald bedrijfsprofiel.

Tijdens dit onderzoek zal ik me dus gaan richten op bedrijven die voldoen aan het profiel omdat deze bedrijven het meeste baat hebben bij de uitkomst van dit onderzoek.

De probleemstelling van het afstudeeronderzoek zal dan ook zijn:
"Wat zijn de drijfveren van de social hacker om bedrijven te kiezen als potentieel slachtoffer van een social hack poging, en wat is de relatie tussen deze drijfveren en een bedrijfsprofiel, en hoe kunnen bedrijven die voldoen aan dit bedrijfsprofiel zich wapenen tegen social hacking."

Het zwaartepunt zal vooral liggen op het eerste gedeelte van de probleemstelling. De koppeling tussen de drijfveren en een bedrijfsprofiel zal uitgebreid onderzocht worden zodat bedrijven die voldoen aan dit profiel de uitslag van het onderzoek kunnen beschouwen als een soort waarschuwing; ze zijn namelijk een potentieel slachtoffer van de social hacker.

Het laatste van de probleemstelling zal in mindere mate onderzocht worden. Er zijn namelijk al vele onderzoeken gedaan naar het voorkomen van social hack pogingen maar er wordt wel gekeken hoe deze oplossingen het beste toegepast kunnen worden bij de bedrijven die voldoen aan het opgestelde bedrijfsprofiel en waar al gebruikte oplossingen nog verbeterd kunnen worden.

2.1 Doelstelling

Ik zal het eindrapport schrijven met de gedachte dat het ook echt toepasbaar is voor een bedrijf. Het zal dus geschreven worden voor het bedrijfsleven in de vorm van een adviesrapport. Het zal de bedoeling zijn dat bedrijven die voldoen aan het bedrijfsprofiel zich er van zich bewust worden dat ze een potentieel slachtoffer van social hack pogingen zijn en daarom passende maatregelen nemen om dit te tegen te gaan. In dit onderzoek zullen dus methoden om problemen tegen te gaan vergeleken worden, dit maakt het een vergelijkend onderzoek. Maar omdat het doel is om de beste oplossing te bieden kan dit onderzoek beter bestempeld worden als een evaluatie onderzoek.

2.2 Kennisgebied

Het kennisgebied waarbinnen het onderzoek zich zal bevinden zal worden ingeperkt door bepaalde methoden die gebruikt gaan worden en bepaalde keuzes die gemaakt zullen moeten worden.
Het vakgebied waarbinnen dit probleem zich begeeft is het vakgebied van de beveiliging van informatie systemen en dan specifiek de menselijke kant hiervan. Dit vakgebied is bestaat al zolang er informatie systemen bestaan en is te bestempelen als zeer dynamisch. Er worden namelijk continue nieuwe methode en technieken ontwikkeld om informatiesystemen te kunnen beveiligen. Er zal dus gekeken vanuit het beveiligingsstandpunt.
Verder zal het onderzoek zich ook nog bevinden op het gebied van bedrijfskunde, door middel van bedrijfskundige methoden wordt er een bepaald bedrijfsprofiel opgezet. Verder zal er onderzoek gedaan worden in het gebied ICT en samenleving, er wordt namelijk onderzoek welke ethiek de social hacker hanteert en welke principes en drijfveren hieruit volgen. Er zal dus gekeken worden wat de plaats is van de social hacker binnen de samenleving en wat de relatie is met de ICT.
De methoden die tijdens het onderzoek gebruikt zullen worden komen aan bod in het volgende hoofdstuk

2.3 Reden

Het beantwoorden van de onderzoeksvraag is, als geheel, de moeite waard, omdat bedrijven vaak schade leiden door social hacking aanvallen. Doordat de beveiliging van de informatie systemen binnen bedrijven steeds geavanceerder wordt is het bijna onmogelijk voor een hacker om met behulp van technische hulpmiddelen en technieken binnen te komen in deze systemen. De hacker zal zich dan ook gaan richten op de zwakste schakel in de beveiliging van informatie systemen: de mens.

Er zijn al veel onderzoeken gedaan naar de manier waarop deze aanvallen voorkomen kunnen worden maar nooit echt naar de vraag wie er nou eigenlijk het slachtoffer zijn van deze aanvallen en vooral waarom. Deze vraag ga ik in dit onderzoek dan ook beantwoorden.

Vaak hebben bedrijven niet in gaten dat ze een potentieel slachtoffer zijn van social hacking pogingen met als gevolg dat ze hier ook niet op voorbereidt zijn. Aan de hand van de uitkomst van dit onderzoek zullen bedrijven, die voldoen aan het opstelde bedrijfsprofiel, zich realiseren dat ze daadwerkelijk een potentieel slachtoffer zijn en dat ze dus passende maatregelen moeten treffen. Dit onderzoek zal dus duidelijk een praktische relevantie omvatten omdat er een oplossing wordt gezocht voor een praktisch probleem. De gewenste situatie zal bestaan uit de situatie waarin bedrijven, die geïdentificeerd zijn als potentiële kandidaat, zich bewust worden van het feit dat ze kwetsbaar zijn en dat ze daarom passende maatregelen moeten treffen om een social hack poging te voorkomen. Door middel van onderzoek wordt dus vastgesteld wie deze potentiële kandidaten zijn en welke maatregelen ze kunnen treffen.

2.4 Antwoord

Het domein waarbinnen het onderzoek zich zal begeven is het domein van de Informatiekundige. Er wordt gekeken naar de menselijke aspecten van de informatie beveiliging. In het volgende hoofdstuk zal per deelvraag aangegeven worden binnen welk subdomein de vraag zich begeeft en welke variabelen hierbij horen. Het antwoord op de probleemstelling zal in de vorm van een adviesrapport worden gegeven. In het antwoord komt naar voren welke bedrijfsprofielen kwetsbaar zijn en welke oplossingen er voor deze bedrijven geboden kunnen worden.

3. Theoretisch kader / methode

Binnen een onderzoek komt men ten minste één van de volgende drie onderzoeksstrategieën tegen: 'case study', 'survey' of 'experiment'. Het intensief bestuderen of observeren van enkele, soms zelfs één, onderzoekseenheden betreft een 'case study'. In een survey wordt juist een grote groep systematisch ondervraagd of geobserveerd op een groot aantal kenmerken. Bij een experiment wordt een oorzakelijk verband getoetst door systematische variatie van mogelijke oorzaken. In dit hoofdstuk wordt per deelvraag uiteengezet welke methode(s) en gebruikt worden.

Binnen dit onderwerp wordt er eerste gekeken welke manieren van social hacken er allemaal bestaan zodat hier later passende preventie maatregelen aan gekoppeld kunnen worden. Echter zal er eerst bekeken worden wie de potentiële kandidaten van zo'n hack poging zijn. Dit wordt vastgesteld door de drijfveren van de hacker te achterhalen en deze te koppelen aan een bepaald bedrijfsprofiel.

Om te komen tot een passende oplossing zal er gekeken moeten worden vanuit de stakeholders. De stakeholders van dit onderzoek zullen bestaat uit:

- Bedrijven (slachtoffers)
- Hackers/crackers (boosdoeners)
- Beveiligingsbedrijven/instanties (voorkomers)

Iedere stakeholder zal zijn rol spelen rondom dit fenomeen. Elke stakeholder zal dus in meer of mindere mate betrokken moeten worden bij dit onderzoek.

Social hacking wordt tijdens dit onderzoek bekeken vanuit de negatieve kant. Dus het brengt schade, in welke vorm dan ook, toe aan een bedrijf.
Er zijn namelijk ook situaties waarin social hacking ervaren kan worden als positief waarbij het een bedrijf geen schade zal toebrengen. Vaak zien hackers het als een uitdaging binnen te breken in een bedrijf om zo de kwetsbaarheid van zo'n bedrijf bloot te leggen. Dit is een voorbeeld van een positief effect van social hacking omdat het bedrijf hierop kan anticiperen om zo een toekomstige inbraak te voorkomen zonder dat er daadwerkelijk schade wordt toegebracht. Maar van de andere kant is dit ook gevaarlijk omdat nu bekend waar de zwakheden van het bedrijf liggen zodat er door kwaadwillende hier gebruik van gemaakt kan worden (in de periode dat er nog geen maatregelen zijn getroffen). Er zal dus duidelijk moeten worden vastgesteld waar de scheidingslijn tussen negatief en positief zal liggen.

Om het onderzoek op een gestructureerde manier uit te voeren zullen de volgende deelonderwerpen onderzocht worden:

a. Wat is social hacking
b. Drijfveren achter social hacking
c. Social hacking in relatie met bedrijfsprofiel
d. Voorkomen van social hacking

3.1 a. Wat is social hacking

Probleemstelling
Om te komen tot een antwoord op de algemene probleemstelling van het onderzoek zal eest bekeken worden wat social hacking nou precies inhoudt. Er zal bekeken worden welke manieren van social hacking worden toegepast en welke schade er hierdoor ontstaat.
In dit deelonderzoek zal er vooral gekeken worden naar bestaande casussen waarin social hacking al dan niet geslaagd is uitgevoerd. Er wordt in dit gedeelte gekeken vanuit de getroffen bedrijven. Er wordt dus vastgesteld welke manieren er gebruikt worden zodat in het laatste onderdeel van het onderzoek hiervoor passende maatregelen getroffen kunnen worden.

Onderzoeksdoel
Het doel van dit deelonderzoek is om duidelijk te maken dat social hacking wordt ervaren als een probleem en op welke manieren het wordt toegepast.

Deelproduct
Dit deelonderzoek zal resulteren in een document waarin alle methoden van social hacking beschreven worden en tevens zal er beschreven waarom social hacking ervaren wordt als een probleem voor getroffen bedrijven. De methoden van social hacking zullen worden ondergebracht in een model zodat er een bepaalde structuur in de aanvalsmethoden blootgelegd kan worden.

Gebruikte methoden
Voor het opstellen van een lijst met methoden van social hacking zal er een literatuur study uitgevoerd worden. De methode die gebruikt gaat worden is de case study methode. Er wordt gezocht naar bestaande casussen en deze worden dan ondergebracht in een model. Verder zal er een literatuur study gebruikt worden om te achterhalen waarom bedrijven social hacking ervaren als een probleem. Het model zal opgesteld worden volgende de Petrinet methode van Carl Adam Petri [3] Een **petrinet** is een bepaald type schema dat in de informatica wordt gebruikt om processen weer te geven.

Motivatie strategiekeuze
Er is gekozen voor een case study omdat dit praktijk cases zijn die ook daadwerkelijk hebben plaatsgevonden. De betrouwbaarheid is hiermee dus gegarandeerd. Er zal in dit geval dus niet vanuit de theorie maar echt vanuit de praktijk gekeken worden.

Verankering

Kennisgebied:	Security en informatiekunde
Keuzes:	Ik heb er voor gekozen om vanuit de praktijk de kijken welke methoden er worden toegepast om zo een zo realistisch mogelijk beeld hiervan te krijgen.
Veronderstellingen:	Ik ga ervan uit dat het fenomeen regelmatig optreed en dat er daarom ook genoeg casussen te vinden zijn.

Precisie:

Bereikt domein :	+/- 20 casussen van social hacking
Bedoeld domein:	Alle methoden van social hacking die gebruikt zijn in de praktijk

Variabele	Antwoordcategorie
Manieren van social hacken	Beschrijving van de manier, resultaat, uitgevoerde stappen
Problemen die ontstaan	Beschrijving soort probleem, schade als gevolg van probleem

Nu de problemen en de manieren van social hacking vastliggen, gaan we kijken wat de drijfveren van social hacker zijn. Aan de hand van de bestudeerde casussen kunnen de drijfveren van de hacker worden gedestilleerd.

3.2 b. Drijfveren achter social hacking

Eerst wordt er gekeken welke rol de stakeholders spelen binnen de social hacking problematiek. In dit deelonderzoek wordt er dus vooral gekeken vanuit de hackers zelf. Wat zijn de achterliggende ethische principes, speelt te cultuur van het te hacken bedrijf ook een rol. Tevens wordt er gekeken hoe social hacking door de hacker verantwoord wordt.

Probleemstelling
Om er achter te komen wat er allemaal speelt binnen de social hackers gemeenschap zal er enerzijds een literatuur/case studie verricht worden maar de focus zal liggen op het praktijkgedeelte. Om antwoord te krijgen op de vraag: “Wat zijn de drijfveren van de social hacker” zal er contact moeten worden gelegd met de hackers gemeenschap.

Onderzoeksdoel
Het doel van dit deelonderzoek is om helder te krijgen wat de drijfveren van de social hackers zijn.

Deelproduct
Dit deelonderzoek zal een document opleveren waarin beschreven wordt wat de drijfveren van de social hacker zijn en in welke categorie deze valt. Categorieën kunnen bestaan uit financiële overwegingen, ethische principes, cultuur etc.

Gebruikte methoden
Er zal een literatuuronderzoek gedaan worden naar de drijfveren van de hacker. Vervolgens zullen de resultaten hiervan terug gekoppeld worden naar (ex)hackers om zo te verifiëren of deze juist zijn. Dit zal gebeuren in de vorm van interviews.

Een optie om informatie in te winnen is bij de bekende hacker Kevin Mitnick. Deze is tegenwoordig werkzaam bij een groot beveiligingsbedrijf en heeft net een boek geschreven over dit onderwerp.

Motivatie strategiekeuze
Er is gekozen voor te kijken vanuit de social hacker om er zo achter te komen wat zijn drijfveren zijn. Verder wordt er gebruik gemaakt van feedback omdat er eerst in literatuur bekeken wordt wat de drijfveren zijn en deze vervolgens getoetst worden door middel van interview(s) met de (ex)social hackers.

Verankering
Kennisgebied: Informatiekunde
Keuzes: Ik heb gekozen voor het internationale niveau omdat ik verwacht dat er maar beperkte bronnen beschikbaar zijn.

Veronderstellingen: Ik ga er vanuit dat het handelen van de social hacker gebaseerd is op onderliggende drijfveren.

Precisie:
Bereikt domein: Lijst met drijfveren van +/- 20 social hackers
Bedoeld domein: Lijst met alle drijfveren van de social hacker

Variabele	Score
Drijfveer van de social hacker	Beschrijving van de drijfveer, categorie van de drijfveer

3.3 c. Social hacking in relatie met bedrijfsprofiel

Probleemstelling
De eerder onderzocht drijfveren van de social hacker zullen gekoppeld worden aan een bepaald bedrijfsprofiel. Er wordt dus onderzocht wat de relatie is tussen de drijfveren van de social hacker en een bepaald bedrijfsprofiel. De achterliggende gedachte is dat de bedrijven die voldoen aan dit profiel en potentiële kandidaten zijn van social hack pogingen. In het volgende gedeelte van het onderzoek zal ik me dan ook richten op deze bedrijven omdat dit onderzoek voor hen het meest relevant is.

Onderzoeksdoel
De relatie leggen tussen de drijfveren van de hacker en een bedrijfsprofiel.

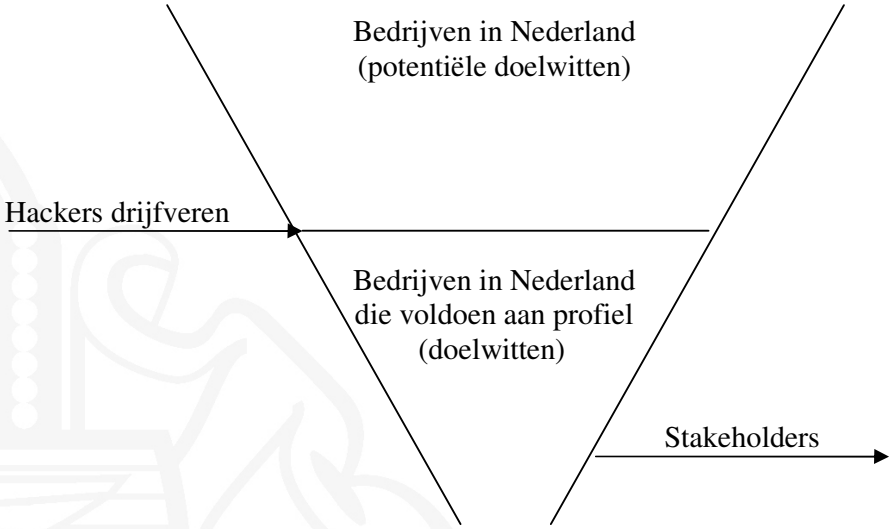
Deelproduct
Er wordt vastgelegd wat typische bedrijfskenmerken zijn.
De koppeling tussen de drijfveren van de social hacker en de relatie met een bedrijfsprofiel (bedrijf met bepaalde bedrijfskenmerken) wordt beschreven en toegelicht.

Gebruikte methoden
Tijdens dit deelonderzoek probeer ik ook te achterhalen welke bedrijven er vaak doelwit zijn van social hacking pogingen. Ik zal een relatie proberen te leggen tussen de hackers drijfveren en een bepaald bedrijfsprofiel. Een bedrijfsprofiel zal bestaat uit een aantal specifieke kenmerken van een bedrijf zoals: welke branche, welke cultuur, welke strategie, welke principes, welk product. Er zal alleen gekeken worden naar bedrijven op nationaal niveau. Dit is van belang voor het volgende deel van het onderzoek omdat daarin bedrijven benaderd zullen worden die aan dit profiel zullen voldoen.

De methode die gebruikt gaat worden zal bestaan uit een nog nader te bepalen methode (er worden een aantal methodes bekeken en de beste hieruit gekozen) die een bedrijf beschrijft aan de hand van zijn kenmerken. Die kenmerken samen vormen dan een bedrijfsprofiel.

Vervolgens zal de vergaarde data gecombineerd worden om zo te komen tot bedrijven met een bepaald bedrijfsprofiel die kwetsbaar zijn voor aanvallen van de social hacker.

Het volgende figuur illustreert de gekozen aanpak



Figuur 2: Het vaststellen van de stakeholders

Uitleg figuur:
Er wordt eerst uitgegaan van alle bedrijven in Nederland. Vervolgens wordt er gekeken naar de drijfveren van de hackers. Door een relatie te leggen tussen drijfveren en kenmerken van een bedrijf zal er een bedrijfsprofiel ontstaan. Dit bedrijfsprofiel zal in het volgende deelonderzoek een rol spelen omdat vanuit het bedrijfsprofiel stakeholders gezocht worden.

Motivatie strategiekeuze
Deze strategie is gekozen om te komen tot een doelgerichte groep van stakeholders die baat hebben bij de uitkomst van het onderzoek.

Verankering

Kennisgebied:	Informatiekunde en bedrijfskunde.
Keuze:	Ik heb er voor gekozen om de methode om een bedrijfsprofiel samen te stellen pas later te kiezen omdat ik verschillende methoden tijdens mijn studie geleerd heb en nog moet bekijken welke het meest geschikt is. De keuze voor Nederlandse bedrijven is voorgekomen uit het feit dat deze makkelijker te benaderen zijn (ook voor eventuele interviews) en we hebben dat niet te maken met landelijke cultuurverschillen.
Veronderstellingen:	Ik ga ervan uit dat er een relatie gelegd kan worden tussen de drijfveren van de social hacker en bepaalde bedrijfskenmerken.

Precisie:

Bereikt domein:	Methode om bedrijfsprofiel samen te stellen Bedrijfsprofiel van potentiële doelwitten Drijfveren gekoppeld aan bedrijfsprofiel
Bedoeld domein:	Methode om bedrijfsprofiel samen te stellen Bedrijfsprofiel van potentiële doelwitten Drijfveren gekoppeld aan bedrijfsprofiel

Variabele	Score
Bedrijfskenmerk	Beschrijving een bedrijfskenmerk, soort kenmerk
Bedrijfsprofiel	Beschrijving van een bedrijfsprofiel dat gekoppeld is aan drijfveren van de social hacker

3.4 d. Voorkomen van social hacking

Probleemstelling
Er wordt gekeken naar een aantal bedrijven die voldoen aan het opgestelde bedrijfsprofiel. Er wordt gekeken welke maatregelen er binnen bedrijven reeds worden getroffen om social hacking tegen te gaan. Zo kan er gedacht worden aan ethische codes en het effect hiervan of aan bepaalde trainingsprogramma's binnen bedrijven. Maar ook aan technische hulpmiddelen die een rol kunnen spelen tijdens het voorkomen van social hacking.

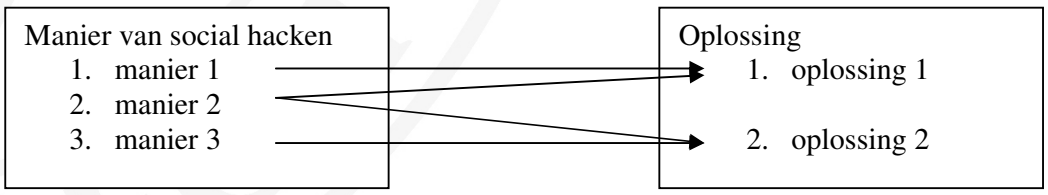
Onderzoeksdoel
Vaststellen wat bedrijven reeds doen om social hacking te voorkomen en tevens de verschillende manieren van social hacking te voorzien van een passende oplossing.

Deelproduct
Een document met waarin beschreven wordt welke maatregelen bedrijven reeds nemen om social hacking te voorkomen. Tevens zal er in het document een model worden opgenomen dat de relatie weergeeft tussen manieren van social hacking en de oplossingen hiervoor.

Gebruikte methoden
Er worden bedrijven benaderd en door middel van een interview wordt er onderzoek wat voor een methodes de bedrijven gebruiken om social hacking te voorkomen.

Om te komen tot bepaalde oplossingen voor de verschillende manieren van social hacking zal er gebruik worden gemaakt van een gedeelte van de systeemtheorie van Ashby. [4]

Het is van belang dat de verschillende manieren van social hacking die onderzocht zijn in het eerste deel van het onderzoek gerelateerd worden aan de bedachte oplossingen. In het ergste geval zal er voor elke manier een specifieke oplossing bedacht moeten worden. Zo'n oplossing zal dus kunnen bestaan uit een technische oplossing of uit bijvoorbeeld een bewustwordingsoefening of een combinatie hiervan. Het volgende figuur zal dit illustreren:



Figuur 3: De relatie tussen manieren van social hacken en oplossingen

Alle aspecten die in de andere deelonderzoeken zijn gedaan worden meegenomen om te komen tot een adviesrapport waarin beschreven wordt wat voor een maatregelen er door bedrijven getroffen kunnen worden. Een andere stakeholder die een rol speelt in dit deelonderzoek zijn de beveiligingsbedrijven. Er gaat gekeken worden wat voor een maatregelen en preventie methodes deze bedrijven adviseren. Er zal dus contact opgenomen worden met deze bedrijven met als doel het achterhalen van concrete informatie.

De globale aanpak van het onderzoek zal dus bestaan uit een theorie gedeelte in de vorm van veel cases en al reeds uitgevoerde onderzoeken en een praktijk gedeelte waarbij, hackers, verantwoordelijke mensen binnen bedrijven, en gespecialiseerde beveiligingsinstellingen geïnterviewd worden.

Motivatie strategiekeuze
Er is gekozen voor de aanpak omdat door middel van interviews met bedrijven het duidelijkste naar voren zal komen wat er precies gedaan wordt om social hacking te voorkomen. Verder zal een gedeelte van de theorie van Ashby [4] gebruikt worden om op een systematische manier te komen tot oplossing voor de verschillende manieren van social hacking.

Verankering

Kennisgebied:	Systeemtheorie en Informatiekunde
Keuzes:	Ik heb er voor gekozen om vanuit de praktijk te kijken welke maatregelen tegen social hacken genomen worden om zo een betrouwbaar beeld hiervan te krijgen. Dus de keuze voor de beveilings bedrijven is ook bewust omdat deze op dit vakgebied gespecialiseerd zijn. Ik heb gekozen voor gebruikt te maken van de systeemtheorie omdat deze op een gestructureerde manier een relaties kan leggen.
Veronderstellingen:	Ik ga ervan uit dat er binnen bedrijven en beveiligingsbedrijven reeds maatregelen getroffen worden om social hacking te voorkomen.

Precisie:

Bereikt domein :	Maatregelen van 5 bedrijven Oplossingen van 5 beveiligingsbedrijven
Bedoeld domein:	Lijst met oplossingen voor social hacking manieren

Variabele	Score
Maatregelen tegen social hacking	Beschrijving maatregel, maatregel voor welke methode

4. Afspraken

De afstudeerder levert een scriptie in de vorm van een adviesrapport en een plan van aanpak op welke voldoet aan de criteria gesteld door de opleiding informatiekunde. Het plan van aanpak zal opgesteld conform de richtlijnen besproken tijdens de cursus Onderzoekvaardigheden.

Het academische niveau blijkt uit heldere consistente formuleringen, die de toets der kritiek kunnen doorstaan. Jargon zal zoveel mogelijk worden vermeden. Als ingeburgerd jargon wordt gebruikt, dan dient bij het eerste voorkomen een verklarende voetnoot te worden geplaatst. Alle vaktermen worden opgenomen in een terminologielijst. Als er in de scriptie of in deeldocumenten bronnen worden gebruikt zal hiernaar verwezen worden.

De scriptie zal aan de volgende punten moeten voldoen:

- een goede formulering van de probleemstelling
- een samenvatting in de vorm van een abstract
- een heldere en goede inhoudelijke beschrijving van het verrichte werk
- een duidelijke conclusie
- een overzichtelijke literatuurlijst
- een goede schrijfstijl en correct taalgebruik
- een goede mondelinge presentatie

Het afstudeerproces zal aan de volgende punten moeten voldoen:

- een complex probleem analyseren en te modelleren
- literatuur bestuderen en toe passen
- een innovatieve oplossing formuleren en onderbouwen
- eventueel deze oplossing realiseren, en
- het verworven inzicht in een scriptie beschrijven en dit mondeling presenteren

5. Organisatie en informatie

In dit hoofdstuk zal algemene informatie over het project gegeven worden

5.1 Algemene informatie

Afstudeerbegeleider:	dr. L. (Luca) Consoli
Referent:	dr. P. (Patrick) van Bommel
Afstudeerder:	ing. D (Dick) Janssen

5.2 Contact gegevens

Naam:	dr. L. (Luca) Consoli
Telefoonnummer:	53065
Lokatie:	A2038a
Emailadres:	L.Consoli@science.ru.nl

Naam:	dr. P. (Patrick) van Bommel
Telefoonnummer:	52696
Lokatie:	A4030
Emailadres:	P.vanBommel@cs.ru.nl

Naam:	ing. D (Dick) Janssen
Telefoonnummer:	52165
Lokatie:	A3076
Emailadres:	dickjanssen@student.ru.nl

5.3 Organisatie

Dit onderzoek wordt uitgevoerd aan de Radboud Universiteit Nijmegen in opdracht van de afdeling Information Retrieval and Information Systems (IRIS).

Telefoon:	(024) 365 34 56
Lokatie:	Kamer A4021 (Verdieping #4) Toernooiveld 1 6525 ED Nijmegen
E-mailadres:	nicolem@cs.ru.nl
Postadres:	Postbus 9010 6500 GL Nijmegen

6. Bronnen

6.1 Boeken

Pekka Himanen, *The Hacker Ethic and the spirit of the Information Age,* New York: Random House, 2001

Bruce Schneider*, Secrets & Lies – Digital Security in a Networked World,* Indianapolis: Wiley Publishing, 2004

[2] Heinze Oost en Angela Markenhof, *Een onderzoek voorbereiden,* Baarn: HB uitgevers, 2003

[3] Wil van de Aalst en Kees Hee, *Workflow management modellen, methoden en systemen,* Schoonhoven: Academic Service, 1999

6.2 Artikelen

Sarah Gordon, *Technologically Enabled Crime: Shifting Paradigms for the year,* Elsevier Press' Computers and Security, 1995
http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html

Lita van Wel and Lamber Royakkers, *Ethical issues in web data mining,* Kluwer Academic Publishers, Ethics and Information Technology, June 2004, vol. 6, no. 2, pp. 129-140(12)
http://www.ingentaconnect.com/content/klu/etin/2004/00000006/00000002/05254849

J.Wayne King and Dale King, *Does it appear we are training the cyberspace criminal of the future?,* the international information & library review; vol. 32 (2000), afl. 3/4, pag. 463-472 (10) / 2000

[4] W.R. Ashby, Chapman & Hall, *An Introduction to Cybernetics*, London, 1957
http://pcp.vub.ac.be/books/IntroCyb.pdf

6.3 Grijs/overig

Barendsen, E. (2004). *Onderzoeksvaardigheden voorjaar 2004*
http://www.niii.ru.nl/home/Erik.Barendsen/onderwijs/onderzoeksvaardigheden/

Luca Consoli, *ICT en Samenleving 2 voorjaar 2004*
http://www.ru.nl/fil-beta/lucac/ICTS2_2005/icts2_index.html

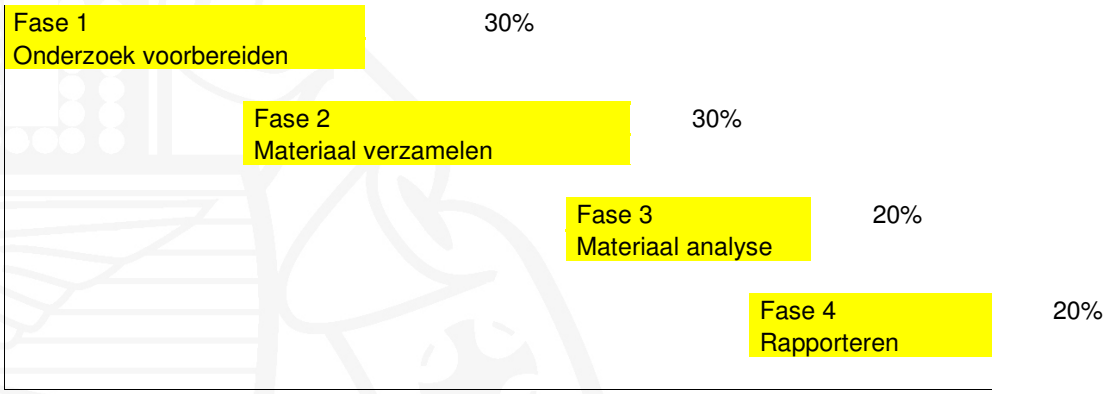
Bart Jacobs, *Security Protocols voorjaar 2004*
http://www.sos.cs.ru.nl/teaching/secprot2004/index.html

Joe Chappelle*, Movie: Takedown,* 2000

[1] Sarah Granger, *Social Engineering Fundamentals Hacker Tactics,* 2001
http://www.securityfocus.com/infocus/1527

7. Tijdsplanning

Hier wordt de globale tijdsplanning van het afstudeerproject weergegeven.
Het project bestaat uit 18 ects dat staat voor 504 uren dat staat +/- 13 weken.
Het project zal opgedeeld worden in 4 verschillende fase die elkaar deels zullen overlappen.
De volgende fasen zullen onderscheiden worden (met het percentage van de tijd die er voor staat):



Figuur 4: De verdeling van het onderzoek naar fasen uitgezet tegen het percentage tijd van het totaal

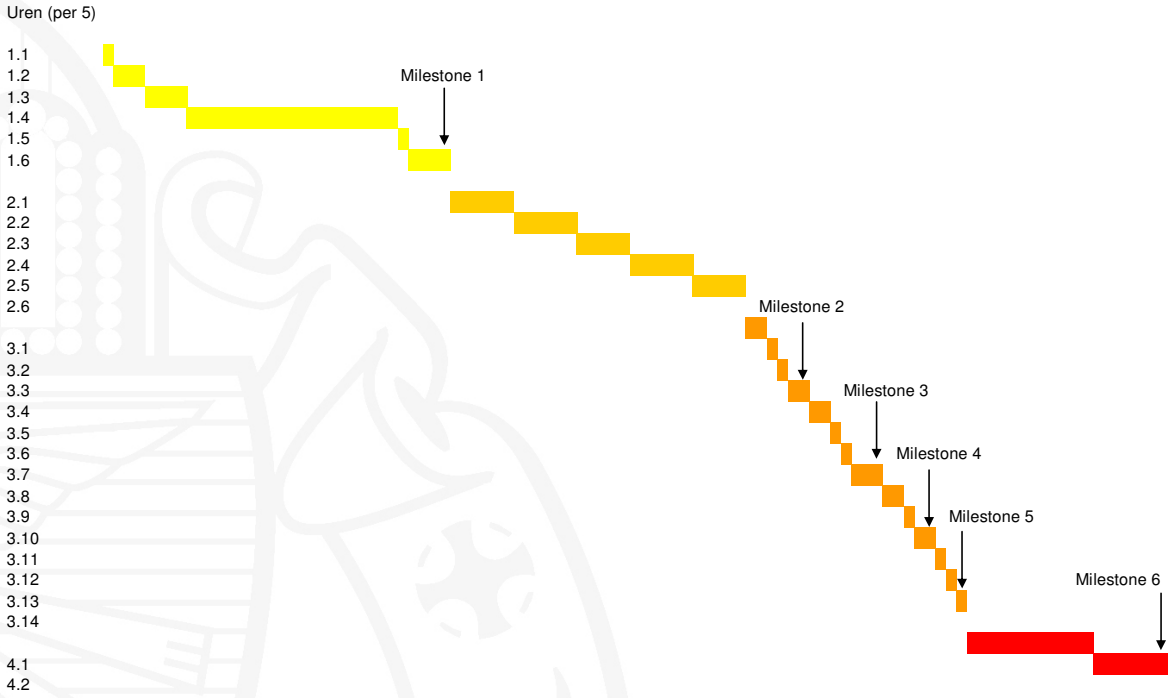
7.1 Deelactivteiten

Per fase is vastgelegd wat de deel activiteiten zijn en per deel activiteit is vastgesteld wat de werk tijd bedraagt:

Fase	Nr	Activiteit	Werktijd (in uren)	Percentage van het totaal
1	1.1	Intake gesprekken begeleiders	5	1,0%
	1.2	Zoeken literatuur	16	3,2%
	1.3	Bestuderen literatuur	20	4,0%
	1.4	Opstellen plan van aanpak	100	19,8%
	1.5	Bespreken plan van aanpak	5	1,0%
	1.6	Aanpassen plan van aanpak	20	4,0%
			166	32,9%
2	2.1	Zoeken literatuur voor deelvraag a	30	6,0%
	2.2	Zoeken literatuur voor deelvraag b	30	6,0%
	2.3	Zoeken naar bronnen voor deelvraag b	23	4,6%
	2.4	Zoeken literatuur voor deelvraag c	30	6,0%
	2.5	Zoeken literatuur voor deelvraag d	30	6,0%
	2.6	Zoeken naar bronnen voor deelvraag d	23	4,6%
			166	32,9%
3	3.1	Analyseer literatuur voor deelvraag a	10	2,0%
	3.2	Opstellen document voor deelvraag a	5	1,0%
	3.3	Verwerken feedback op document a	5	1,0%
	3.4	Analyseer literatuur voor deelvraag b	10	2,0%
	3.5	Interview bronnen voor deelvraag b	8	1,6%
	3.6	Opstellen document voor deelvraag b	5	1,0%
	3.7	Verwerken feedback op document b	5	1,0%
	3.8	Analyseer literatuur voor deelvraag c	15	3,0%
	3.9	Opstellen document voor deelvraag c	10	2,0%
	3.10	Verwerken feedback op document c	5	1,0%
	3.11	Analyseer literatuur voor deelvraag d	10	2,0%
	3.12	Interview bronnen voor deelvraag d	5	1,0%
	3.13	Opstellen document voor deelvraag d	5	1,0%
	3.14	Verwerken feedback op document d	5	1,0%
			103	20,4%
4	4.1	Schrijven scriptie	60	11,9%
	4.2	Verwerken feedback op scriptie	41	8,1%
			101	20,0%

Figuur 5: De verschillende activiteiten binnen de fasen met de bijbehorende werktijd in uren

Per fase wordt vastgelegd wat de werktijd is en wanneer er milestones bereikt worden.



Figuur 6: De verschillende activiteiten binnen de fasen met de bijbehorende werktijd in uren voorzien van milestones

7.2 Milestones

Milestone 1:
Dit plan van aanpak

Milestone 2:
Een document waarin alle methoden van social hacking beschreven worden en tevens zal er beschreven waarom social hacking ervaren wordt als een probleem voor getroffen bedrijven. De methoden van social hacking zullen worden ondergebracht in een model zodat er een bepaalde structuur in de aanvalsmethoden blootgelegd kan worden.

Milestone 3:
Een document waarin beschreven wordt wat de drijfveren van de social hacker zijn en in welke categorie deze valt. Categorieën kunnen bestaan uit financiële overwegingen, ethische principes, cultuur etc.

Milestone 4:
Er wordt vastgelegd wat typische bedrijfskenmerken zijn.
De koppeling tussen de drijfveren van de social hacker en de relatie met een bedrijfsprofiel (bedrijf met bepaalde bedrijfskenmerken) wordt beschreven en toegelicht.

Milestone 5:
Een document met waarin beschreven wordt welke maatregelen bedrijven reeds nemen om social hacking te voorkomen. Tevens zal er in het document een model worden opgenomen dat de relatie weergeeft tussen manieren van social hacking en de oplossingen hiervoor.

Milestone 6:
Scriptie