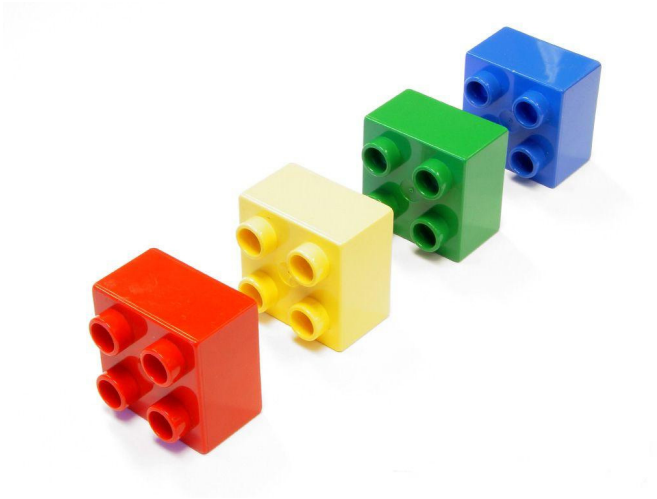
De bouwstenen van Social Engineering:
Een gestructureerd overzicht getoetst bij de overheid



Afstudeerscriptie
Master Informatiekunde

Versie:	Final
Afstudeernummer:	32IK
Auteurs:	Arjan Kieskamp 0441147 Robert Smit 0444855
Universiteit:	Radboud Universiteit Nijmegen
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Instituut:	Nijmeegs Instituut voor Informatica en Informatiekunde
Begeleiders:	dr. Martijn Oostdijk ir. drs. Wolter Pieters
Datum:	16 Augustus 2006

Voorwoord

Deze scriptie is het eindresultaat van het afstudeeronderzoek met als titel "*De bouwstenen van Social Engineering: Een gestructureerd overzicht getoetst bij de overheid*", als afsluitend onderdeel van de opleiding Master Informatiekunde. Het afstudeeronderzoek is uitgevoerd op de Radboud Universiteit te Nijmegen, binnen het Nijmeegs Instituut voor Informatica en Informatiekunde (NIII). Dr. Martijn Oostdijk en ir. drs. Wolter Pieters, beide verbonden aan de Security of Systems group, hebben ons in de periode van februari tot en met augustus 2006, begeleid.

Via deze weg willen we de verschillende mensen die geholpen hebben met het behalen van dit resultaat bedanken. In het bijzonder Martijn Oostdijk en Wolter Pieters voor hun vakkundige begeleiding en hun inhoudelijk commentaar. Daarnaast willen we de contactpersonen binnen de ministeries bedanken die er voor gezorgd hebben dat wij een deel van ons afstudeeronderzoek bij de overheid hebben kunnen uitvoeren. Tenslotte willen we de verschillende geïnterviewde personen binnen de ministeries bedanken voor hun tijd en informatie over Social Engineering bij de overheid.

Veel leesplezier toegewenst,

Nijmegen, 16 augustus 2006

Arjan Kieskamp & Robert Smit

Samenvatting (abstract)

Social Engineering is een bedreiging die gebruik maakt van de mens als zwakste schakel in informatiebeveiliging. De overheid vormt vanwege haar informatie, omvang en rol in de samenleving een interessant doelwit voor Social Engineering. Het is daarom noodzakelijk dat de overheid zich wapent tegen deze vaak onderschatte bedreiging. Vele artikelen zijn er al over Social Engineering geschreven, zij lichten echter maar een tipje van de sluier op. Een onderzoek naar wat Social Engineering precies omvat en de toetsing van deze resultaten bij de overheid om te bepalen of de overheid beschermd is, wordt weergegeven in deze scriptie.

Literatuurstudie heeft grotendeels bepaald wat Social Engineering omvat resulterend in een definitie, doelen en aanvallen van Social Engineering en de beschrijving van de Social Engineer en zijn of haar gereedschappen. Op grond van deze bevindingen is een conceptueel framework gevormd waarin Social Engineering visueel inzichtelijk is gemaakt. De belangrijkste constatering hierin is dat de plaats van de Social Engineer ten opzichte van de organisatie en het organisatiegebied van de organisatie bepalend zijn voor welke aanvallen er uitgevoerd kunnen worden en welke doelen er kunnen worden verwezenlijkt. De toetsing van de resultaten bij de overheid levert geen eenduidig antwoord op. De overheid werkt aan de bescherming tegen Social Engineering, echter 100% bescherming is in de praktijk onmogelijk.

De gevonden resultaten impliceren dat er een bredere, volledigere beschrijving van het begrip Social Engineering mogelijk is. Daarnaast is er een framework gevormd dat overzicht en structuur aanbrengt in Social Engineering. Resultaten van de toetsing bij de overheid duiden op de toegevoegde waarde van de literatuurstudie en het framework voor een organisatie, om zich beter te beschermen tegen Social Engineering

Inhoudsopgave

1 Inleiding

"*Mensen zijn de zwakste schakel in de informatiebeveiliging*" [37][48] [51][59].

Social Engineering speelt in op de mens als zwakste schakel in de informatiebeveiliging en wordt ook wel de kunst van het misleiden genoemd [59]. Om een idee te krijgen wat Social Engineering inhoudt zal hieronder een ingekort voorbeeld, uit het boek "The art of deception" van de Social Engineer Kevin Mitnick [59], worden weergegeven. Hierbij moet worden opgemerkt dat dit slechts één van de vele manieren is waarop Social Engineering kan plaatsvinden.

> Brian Atterby wil proberen in te breken op het netwerk van bedrijf X. Hiervoor heeft hij een inbelaccount met gebruikersnaam en wachtwoord nodig van een medewerker.
>
> Atterby belt naar het hoofdkantoor van bedrijf X en krijgt een telefoniste aan de lijn. Hij vraagt om door te worden verbonden met dhr. Jones. (Jones is een veelvoorkomende naam dus de kans is groot dat er wel een Jones werkzaam is in het bedrijf). Atterby wordt doorverbonden en heeft bij de telefoniste ook nog de voornaam en de afdeling van medewerker Jones weten te achterhalen. Atterby krijgt medewerker Jones aan de telefoon en verzint een verhaal dat het verzoek van dhr. Jones om het salaris over te maken op zijn spaarrekening is verwerkt. Jones reageert furieus en zegt dat hij dat verzoek nooit heeft gedaan. Atterby reageert vervolgens hierop door te zeggen dat hij alles kan terugdraaien maar dat hij daarvoor wel het medewerkernummer van Jones nodig heeft. Jones geeft het medewerkernummer aan Atterby die nu beschikt over de voornaam, achternaam, afdeling en medewerkernummer van Jones. Atterby neemt contact op met het systeembeheer van bedrijf X waarbij hij zich voordoet als Jones en vraagt om een inbelaccount. De systeembeheerder vraagt naar enkele gegevens die Atterby nu zonder problemen kan verstrekken waardoor er geen argwaan ontstaat bij de systeembeheerder. De systeembeheerder geeft vervolgens de gebruikersnaam: jdjones en vermeldt erbij dat deze hetzelfde is als de bestaande gebruikersnaam binnen het bedrijf. Tenslotte geeft de systeembeheerder ook het wachtwoord: "changeme" aan Atterby waardoor het nu kinderspel geworden is voor Atterby om in te loggen op het bedrijfsnetwerk [59].

Met dit voorbeeld wordt het duidelijk dat het niet nodig is om allerlei technische barrières te doorbreken om toegang te krijgen tot een netwerk maar dat het ook mogelijk is door de mens op de juiste manier te bespelen.

1.1 Aanleiding onderzoek

Drie aanleidingen liggen ten grondslag aan de uitvoering van dit onderzoek. Deze zullen hier kort worden toegelicht.

Persoonlijke aanleiding
De cursussen Security en Security in Organizations[1] hebben onze interesse gewekt om onderzoek te doen op het gebied van informatiebeveiliging, waar Social Engineering onderdeel van uitmaakt.

Maatschappelijke relevantie
Informatiebeveiliging wordt steeds belangrijker in informatie-intensieve organisaties. Dit maakt informatiebeveiliging een "hot topic" waarin op dit moment veel ontwikkelingen plaatsvinden wat onderzoek in deze richting interessant maakt.

Geschiktheid als afstudeeronderwerp
Social Engineering heeft een groot raakvlak met de opleiding informatiekunde omdat Social Engineering te maken heeft met de menselijke component van informatiebeveiliging waarbij de mens de zwakste schakel is in het beveiligen van informatie. De opleiding informatiekunde richt zich voor een groot deel op het aandachtsgebied tussen mens en ICT waar Social Engineering goed tussen past.

1.2 Probleemgebied

Over het onderwerp Social Engineering zijn al veel artikelen geschreven. Elke auteur behandelt vaak slechts een klein deel van het onderwerp of probeert met behulp van voorbeelden duidelijk te maken wat Social Engineering is. Geen enkel artikel is er in geslaagd een volledig beeld te scheppen wat het begrip Social Engineering nou precies omvat.

Omdat informatie steeds belangrijker wordt besteden steeds meer organisaties aandacht aan hun informatiebeveiliging. Social Engineering wordt vaak niet als serieuze dreiging meegenomen in de informatiebeveiliging waardoor organisaties een makkelijk doelwit zijn voor Social Engineering. Organisaties dienen daarom hun informatiebeveiliging op peil te brengen door Social Engineering als dreiging op te nemen. De overheid is de grootste informatie-intensieve organisatie van Nederland en werkt met allerlei gevoelige informatie over overheids- en burgerzaken. Van de overheid mag verwacht worden dat zij vanwege haar verantwoordelijkheid tegenover de burgers zorgvuldig met deze gevoelige informatie omgaat.

Omdat de mens de zwakste schakel is in informatiebeveiliging dient de overheid haar medewerkers te beschermen tegen Social Engineering. Vanuit de gedachte om in dit

[1] Beide cursussen zijn gegeven tijdens de opleiding Informatiekunde aan de Radboud Universiteit

onderzoek Social Engineering zo volledig mogelijk in kaart te brengen zal een poging gedaan worden om de overheid in de praktijk te toetsen om vast te stellen of de overheid voldoende beschermd is tegen Social Engineering.

1.3 Doelstelling

De doelstelling van dit onderzoek is het verduidelijken van het begrip Social Engineering. Dit zal gedaan worden door het opstellen van een begripsbepaling en een overzichtelijk conceptueel framework gebaseerd op bestaande literatuur. De begripsbepaling draagt bij aan de onderbouwing van begrippen genoemd in het framework. Het framework zelf moet bijdragen aan een verbeterd inzicht door te visualiseren wat Social Engineering precies inhoudt en te laten zien waar de bedreigingen zich in de organisatie kunnen bevinden. Deze inzichten kunnen organisatie gebruiken om zich beter te kunnen beschermen tegen Social Engineering.

Tevens heeft dit onderzoek als doel te bepalen of de overheid beschermd is tegen Social Engineering. Dit zal gedaan worden door interviews bij de verschillende ministeries af te nemen, waarna er een algemeen advies wordt opgesteld.

1.4 Probleemstelling

1.4.1 Onderzoeksvragen

1. **Wat omvat het begrip Social Engineering?**
2. **Is de overheid beschermd tegen Social Engineering?**

1.4.2 Deelvragen

Bij onderzoekvraag 1:

1. Wat is een bruikbare definitie van het begrip Social Engineering voor dit onderzoek?
2. Wat zijn de belangrijkste doelen van Social Engineering?
3. Welke mogelijke Social Engineering aanvallen zijn er en wat zijn de kenmerken hiervan?
4. Zijn er overige factoren die invloed hebben op Social Engineering?
5. Is Social Engineering te structureren in een framework zodat het inzichtelijker wordt?

Bij onderzoeksvraag 2:

1. Wat doet de overheid tegen Social Engineering?
2. Is de overheid bestand tegen de verschillende soorten aanvallen uit ons framework?
3. Is het framework van toegevoegde waarde voor een verbeterde bescherming tegen Social Engineering?

1.5 Strategie

In deze paragraaf zal een beknopt overzicht gegeven worden van de gehanteerde strategie bij de uitvoering van dit onderzoek. Voor een uitgebreide beschrijving met onderbouwing wordt verwezen naar het Plan van Aanpak.

De strategie bestaat uit de volgende opeenvolgende stappen:

1. **Uitvoeren literatuuronderzoek**
   Literatuuronderzoek dient uitgevoerd te worden om te bepalen wat er geschreven is over het onderwerp Social Engineering en welke artikelen er relevant zijn voor het onderzoek. De artikelen, afkomstig uit verschillende zoekmachines[2] voor wetenschappelijke artikelen, moeten bijdragen aan de beantwoording van onderzoeksvraag 1.

2. **Opstellen begripsbepaling**
   Aan de hand van de geselecteerde literatuur zal in de begripsbepaling antwoord gegeven worden op de verschillende deelvragen van onderzoeksvraag 1. De informatie uit de begripsbepaling zal voor een deel gebruikt worden voor het vormen van het conceptueel framework.

3. **Opstellen conceptueel framework**
   Door middel van informatie uit de begripsbepaling, brainstormsessies en visualisatie door prototyping zal een eerste poging gedaan worden een conceptueel framework op te stellen.

4. **Afnemen interviews bij ministeries**
   Informatieverzameling bij de ministeries vindt plaats via interviews met mensen die te maken hebben met de concrete invulling van het op hoog niveau opgestelde informatiebeveiliging beleid. Deze informatie wordt gebruikt bij het beantwoorden van onderzoeksvraag 2.

5. **Analyse interviews ministeries**
   De interviews worden met elkaar vergeleken om te bepalen welke overeenkomsten en verschillen er tussen de ministeries zijn. Deze resultaten worden gebruikt om onderzoeksvraag 2.1 te beantwoorden.

6. **Opstellen advies ministeries**
   Aan de hand van een analyse van de interviews en de vergelijking van de interviews met de begripsbepaling en het framework wordt er een algemeen advies opgesteld met aandachtspunten. Deze aandachtspunten dienen bij te dragen aan een verbeterde bescherming tegen Social Engineering.

7. **Schrijven eindscriptie**

[2] Onder andere IEEE, ACM.org, scholar.google.com, SANS en de universiteitsbibliotheek

De eindscriptie is een verslaglegging van de bevonden resultaten die voortkomen uit de hierboven genoemde stappen. Tevens geeft de eindscriptie antwoord op de onderzoeksvragen in de vorm van een conclusie en wordt in de reflectie teruggeblikt op het uitgevoerde onderzoek.

8. **Eindpresentatie**
   De eindpresentatie is het slotstuk van het afstudeeronderzoek. In deze presentatie zal op een bondige manier uitleg gegeven worden over ons onderzoek met daarin de belangrijkste bevindingen en conclusies.

1.6 Structuur van de scriptie

Hoofdstuk 2 is een beschrijving van Social Engineering die kaderstellend is voor het onderzoek. Aan de hand van de bestudeerde literatuur worden het begrip Social Engineering en de onderdelen die met het begrip samenhangen eenduidig beschreven en onderbouwd. Daarnaast dient hoofdstuk 2 als basis voor het framework beschreven in hoofdstuk 3.

Hoofdstuk 3 is een weergave van de poging te komen tot een overzichtelijk framework wat Social Engineering precies is. Door middel van verschillende modellen met bijbehorende beschrijving wordt het framework stap voor stap opgebouwd.

Hoofdstuk 4 beschrijft de analyse en bijbehorende resultaten van de verschillende interviews afgenomen bij de ministeries en het advies aan de ministeries. Het advies komt voort uit een vergelijking van de resultaten van de interviews met de begripsbepaling en het framework en beschrijft mogelijke aandachtspunten die kunnen bijdragen aan verbetering van de bescherming tegen Social Engineering bij de ministeries.

Hoofdstuk 5 beschrijft de conclusies die antwoord geven op de verschillende onderzoeksvragen en doet aanbevelingen voor verder onderzoek.

Hoofdstuk 6 is een reflectie van de onderzoekers op het uitgevoerde onderzoek.

1.7 Taakverdeling

In de onderstaande tabel staat de taakverdeling globaal weergegeven. De taken die zowel bij de kolom "Arjan" als bij de kolom "Robert" afzonderlijk zijn aangekruist houden in dat ieder apart aan een taak werkt maar dat deze taak meerdere producten oplevert. Zo bestaat de taak "Plan van Aanpak opstellen" uit verschillende producten die door ieder apart zijn opgesteld. Het brainstormen over de inhoud en opzet van het framework is een voorbeeld van een taak waar gezamenlijk aan gewerkt is.

Taak	Arjan	Robert	Arjan en Robert
Plan van Aanpak			
• Opstellen	X	X	
• Bijstellen		X	
Literatuuronderzoek			
• Verzamelen relevante literatuur	X	X	
• Opstellen bruikbare definitie Social Engineering		X	
• Vaststellen doelen Social Engineering		X	
• Vaststellen Social Engineering aanvallen en kenmerken	X		
• Vaststellen overige factoren Social Engineering	X		
Conceptueel framework			
• Brainstormen inhoud framework			X
• Brainstormen opzet framework			X
• Opstellen prototype modellen	X	X	
• Evalueren prototype modellen			X
• Opstellen definitieve modellen		X	
• Beschrijven framework	X	X	
Interviews bij Overheid			
• Acquisitie ministeries	X	X	
• Voeren oriënterende gesprekken	X	X	
• Opstellen geheimhoudingsclausule	X		
• Opstellen interviews			X
• Afnemen interviews			
o Ministerie A		X	
o Ministerie B		X	
o Ministerie C	X		
• Uitwerken interviews			
o Ministerie A		X	
o Ministerie B	X		
o Ministerie C	X		
• Analyse interview resultaten			
o Per onderdeel van ministerie			
▪ Ministerie A	X		

▪ Ministerie B		X	
▪ Ministerie C		X	
o Tussen ministeries			X
• Vergelijking resultaten met begripsbepaling	X		
• Vergelijking resultaten interviews met framework		X	
• Opstellen advies			X
Scriptie			
• Beantwoording hoofdonderzoeksvragen	X	X	
• Opstellen conclusies			X
• Opstellen aanbevelingen			X
• Opstellen reflectie onderzoek	X	X	
• "Fine tunen" van scriptie	X	X	
• Reviewen scriptie			X
Presentatie			
• Opstellen presentatie			X
• Houden van presentatie			X

2 Social Engineering: Een begripsbepaling

2.1 Opmerkingen vooraf

Overal waar mannelijk enkelvoud wordt gelezen kan ook vrouwelijk enkelvoud worden gelezen. Plaatsen waar de woorden aanval en doel worden genoemd zonder dat de term Social Engineering hieraan voorafgaat, hebben betrekking op Social Engineering.

2.2 Het begrip Social Engineering

2.2.1 Definitie

Social Engineering is een nogal ruim begrip dat op verschillende manieren ingevuld kan worden. Om voor dit onderzoek een eenduidige betekenis te hanteren zal in deze subparagraaf een definitie gegeven worden wat er onder dit begrip wordt verstaan.

In de wetenschappelijke literatuur zijn veel verschillende definities van Social Engineering te vinden. Hieronder worden enkele definities gegeven.

"the art and science of getting people to comply to your wishes" [54]

"Social Engineering is a social / psychological process by which an individual can gain information from an individual about a targeted organization" [56]

"Social Engineering is the term for using human deception as means for information theft." [47]

"Social engineering can be regarded as 'people hacking', basically its hacker jargon for soliciting unwitting participation from a person inside a company rather than breaking into the system independently" [37]

"breaking an organization's security by interactions with people" [49]

Al deze definities komen grotendeels op hetzelfde neer, namelijk het gebruik maken van en interactie met de mens om zo gevoelige informatie te verkrijgen.

De definitie van Social Engineering die in dit onderzoek gehanteerd wordt is:

"Het misleiden, manipuleren, gebruik maken van het niet bewust zijn van de mens en de voorbereiding daarop om gevoelige informatie te verkrijgen."

In dit onderzoek wordt er gebruik gemaakt van een andere definitie van Social Engineering dan in de bestaande literatuur. Reden hiervoor is dat de definities in de bestaande literatuur nogal ruim en globaal gesteld zijn waardoor ze geen duidelijk afgebakend kader stellen.

Hieruit is het moeilijk te bepalen of bepaalde informatie genoemd in een artikel wel of niet binnen het kader van de gestelde definitie valt. Om structuur in het begrip Social Engineering te kunnen aanbrengen is een definitie met een duidelijk kader nodig, om te bepalen welke informatie er wel of niet onder Social Engineering valt. Daarnaast hanteert de definitie een ruimere context waarin ook het niet bewust zijn van de mens en voorbereiding zijn opgenomen.

2.2.2 Terminologie en onderbouwing

Misleiden en manipuleren
De termen *misleiden* en *manipuleren* zijn dusdanig verschillend dat ze apart in de definitie worden genoemd. Misleiden heeft betrekking op het overtuigen van de mens van iets wat niet waar is (vertekend beeld geven, om de tuin leiden) en manipulatie heeft betrekking op het op slinkse wijze beïnvloeden van de mens. Beide termen zijn een vorm van beïnvloeding alleen de manier waarop de beïnvloeding in zijn werk gaat is anders.

Het niet bewust zijn van de mens
Het *niet bewust zijn van de mens* heeft betrekking op het niet stilstaan bij de gevolgen die bepaalde acties kunnen hebben. Een voorbeeld hiervan is een medewerker die gaat lunchen en nooit de deur van zijn kantoor op slot doet. Op zijn bureau in het kantoor liggen belangrijke documenten over de financiële stand van zaken van de organisatie. Deze documenten zijn daardoor voor iemand die zich in het gebouw bevindt relatief eenvoudig te bemachtigen waardoor er gevoelige informatie in verkeerde handen kan vallen.

Het niet op slot doen van het kantoor is simpelweg het gevolg van het niet bewust zijn van de gevolgen die dit zou kunnen hebben als een kwaadwillende zich toegang tot deze ruimte verschaft. Doordat Social Engineering aanvallen, besproken in subparagraaf 2.6.5 veelvuldig van deze eigenschap [52] gebruik maken wordt deze eigenschap opgenomen in de definitie.

Voorbereiding
In de bestudeerde literatuur wordt ook gesproken over *voorbereiding* (background research) die voorafgaat aan de misleiding, manipulatie en het gebruik maken van het niet bewust zijn van de mens, waarbij een goede voorbereiding cruciaal is [37][47][50][56].Voorbereiding heeft te maken met het verzamelen van informatie over een bepaald persoon en / of organisatie uit publieke bronnen.

Een voorbeeld van voorbereiding is het raadplegen van de corporate website van een bepaalde organisatie. Hierop staat bijvoorbeeld een organogram van de organisatie waarop de verschillende afdelingen binnen de organisatie af te leiden zijn. Daarnaast kunnen er ook gegevens van medewerkers op staan zoals functie, naam en telefoonnummer. Deze informatie kan gebruikt worden om iemand binnen de organisatie te misleiden door bijvoorbeeld iemand binnen de organisatie te bellen en je voor te doen als een collega waarvan je de gegevens via de website hebt achterhaald. Door het noemen van naam en afdeling wordt de geloofwaardigheid vergroot waardoor degene die gebeld wordt denkt te

maken te hebben met een collega. Hierdoor is de collega welwillender om bepaalde "gevoelige" informatie af te geven.

Het verschil is dus dat voorbereiding niet beoogt gevoelige informatie te verkrijgen en dat het misleiden, manipuleren en het gebruik maken van het niet bewust zijn van de mens naast het verkrijgen van gevoelige informatie ook kan dienen als voorbereiding. Vanwege dit verschil wordt voorbereiding als aparte term in de definitie genoemd.

Gevoelige informatie
Met *gevoelige informatie* wordt informatie bedoeld die een organisatie economische schade kan toebrengen. Hierbij moet bijvoorbeeld gedacht worden aan handelsgeheimen van een organisatie die de continuïteit, het imago en de reputatie in gevaar kunnen brengen [14].

Vertrouwelijkheid, integriteit en beschikbaarheid van informatie

In dit onderzoek wordt er vanuit gegaan dat Social Engineering zich vooral richt op het ondermijnen van het onderliggende beveiligingsdoel vertrouwelijkheid. Dit komt doordat Social Engineering probeert gevoelige informatie te verkrijgen die meestal vertrouwelijk van aard is. De Social Engineer kan echter wel door de beveiligingsdoelen integriteit en beschikbaarheid te ondermijnen een poging doen om de vertrouwelijkheid van informatie te compromitteren.

2.3 De Social Engineer

Social Engineering wordt uitgevoerd door een persoon die in dit onderzoek de Social Engineer genoemd wordt. De Social Engineer wordt beschouwd als een persoon die niet gerelateerd of verbonden is aan de doelwit organisatie. Medewerkers in de organisatie die Social Engineering aanvallen uit zouden kunnen voeren worden in dit onderzoek niet beschouwd als Social Engineers.

In dit onderzoek wordt er een onderscheid gemaakt tussen *gevoelige* en *niet-gevoelige* informatie waarbij gevoelige informatie economische schade kan toebrengen aan de organisatie als deze in verkeerde handen valt. Daarnaast wordt ook onderscheid gemaakt tussen *waardevolle* en *niet-waardevolle* informatie. Hiermee wordt aangegeven dat informatie die een organisatie als gevoelig of niet-gevoelig bestempelt *allebei* waardevol voor de Social Engineer kunnen zijn. Waardevolle informatie kan zowel het doel van Social Engineering verwezenlijken als gebruikt worden door de Social Engineer ter voorbereiding op het verkrijgen van gevoelige informatie.

De werkwijze van de Social Engineer hangt af van de drijfveer van de Social Engineer en het hebben van een specifiek doel. Een Social Engineer kan ook willekeurig te werk gaan zonder een concreet doel voor ogen te hebben. Voor een uitgebreide beschrijving van de verschillende drijfveren die een Social Engineer kan hebben wordt verwezen naar [48]. In dit onderzoek hebben de drijfveren van een Social Engineer geen toegevoegde waarde.

2.4 Het doel van Social Engineering

In de bestudeerde literatuur wordt aangegeven dat Social Engineering verschillende doelen kan hebben. Voorbeelden hiervan zijn:

- Het er toe aanzetten van een slachtoffer om "gevoelige" informatie af te geven [52].
- Het verkrijgen van directe toegang tot informatie over de organisatie of toegang krijgen tot een informatiesysteem in de organisatie [56].
- Ongeautoriseerde toegang verkrijgen tot systemen of informatie om fraude te plegen, netwerkstoringen te veroorzaken, industriële spionage uit te voeren of identiteitsdiefstal te plegen of simpelweg het netwerk plat te leggen [44][54].

In feite komt het er op neer dat de doelen van Social Engineering in de literatuur vaak in het verlengde liggen van het eigenlijke doel namelijk het verkrijgen van gevoelige informatie. Zoals in de bovenstaande opsomming is weergegeven wordt er vooral aangegeven welke economische schade er aangericht kan worden mocht er bepaalde gevoelige informatie verkregen zijn.

Het *doel* van Social Engineering dat in dit onderzoek gebruikt wordt komt naar voren in de gehanteerde definitie van Social Engineering namelijk: "het verkrijgen van gevoelige informatie". Afhankelijk van wat voor informatie is verkregen kan er op verschillende manieren economische schade aangericht worden. Bijvoorbeeld het verkrijgen van gebruikersnaam en wachtwoord voor een bepaald informatiesysteem kan toegang geven tot informatie over bijvoorbeeld de financiële positie van de organisatie of de ontwerptekeningen van nieuwe prototypes. Welke schade er met deze informatie aangericht kan worden is moeilijk te inventariseren en valt buiten het bereik van dit onderzoek.

2.5 Voorbereiding

Voordat een Social Engineering aanval goed kan worden uitgevoerd gaat er meestal een gedegen voorbereiding aan vooraf [37][47][50][56]. In de bestudeerde literatuur worden er verschillende manieren aangegeven waarop een Social Engineer informatie inzamelt als voorbereiding.

1. **Zoekmachine (Search engine)**
   Een zoekmachine is een specifiek ontworpen programma om informatie te zoeken die beschikbaar is op het Internet. De zoekmachine zoekt naar informatie die voldoet aan vooraf opgegeven zoekcriteria en produceert een lijst met referenties die hieraan voldoen.

   Een Social Engineer kan een zoekmachine gebruiken om onder andere organisatiegegevens te achterhalen. Voorbeelden hiervan zijn informatie over de organisatie zelf (locatie, organisatiestructuur, branche, bedrijfsprocessen), informatie over haar medewerkers (namen, telefoonnummers en functies) en informatie over zijn klanten.

Er worden op Internet ook diensten aangeboden door websites als de WayBackMachine [33] die over de jaren heen allerlei websites met de informatie die gepubliceerd werd op deze websites hebben gearchiveerd. Deze Internet archieven kunnen voor een Social Engineer op volledig legale wijze een schat van informatie opleveren [35][36][49][55].

2. **Nieuwsgroepen (newsgroups)**
   Een nieuwsgroep is een verzameling van berichten gepost door verschillende gebruikers met betrekking tot een bepaald onderwerp. Nieuwsgroepen zijn een onderdeel van het Usenet systeem, een netwerk voor het verspreiden van tekstberichten en binaire bestanden. Een nieuwsgroep kan geraadpleegd worden door de meeste webbrowsers en door nieuwslezers. Ook is het mogelijk om via zoekmachines zoals Google groups in verschillende nieuwsgroepen te zoeken [17][18][19][49].

   Een Social Engineer kan nieuwsgroepen gebruiken om bijvoorbeeld e-mail adressen te achterhalen van gebruikers of om uit de geposte berichten relevante informatie zoals medewerkerfuncties en namen te achterhalen om zo een bedrijfsprofiel te creëren.

3. **Vacature websites (Job-sites)**
   Dit zijn websites op het Internet met daarachter een grote database met vacatures van organisaties. Via een vacature website, zowel extern als op de website van de organisatie zelf, kan een Social Engineer er achter komen welke vacatures er bij een bepaalde organisatie openstaan. Deze gegevens kan de Social Engineer gebruiken voor latere aanvallen. Tevens kunnen bepaalde vacatures inzicht geven in welke systemen en functies er in de organisatie aanwezig zijn [49][55].

4. **Corporate website**
   De corporate website van een organisatie is het digitale visitekaartje van de organisatie op internet. Via de corporate website publiceert de organisatie algemene informatie zoals in welke branche zij actief is, contact informatie en huidige activiteiten. Behalve de publieke corporate website beschikken organisaties vaak ook over een intra- of extranet. Door de corporate website / intra- of extranet te bekijken kan de Social Engineer informatie verzamelen over bijvoorbeeld bedrijfsprocessen, afdelingen, medewerkers, vacatures en telefoonnummers [40][41][49][55].

Voorbereiding op een Social Engineering aanval is vrijwel risicoloos omdat het passief van aard is en er gebruik gemaakt wordt van publiek toegankelijke bronnen. Hierdoor is voorbereiding nauwelijks te detecteren voor organisaties.

2.6 Social Engineering aanvallen

2.6.1 Een Social Engineering aanval

Uit de literatuur zijn verschillende Social Engineering aanvallen geïnventariseerd die binnen de gestelde definitie van dit onderzoek vallen. Vervolgens zijn de aanvallen met elkaar vergeleken om zo de overeenkomstige en verschillende kenmerken te bepalen. Aan de hand van deze kenmerken is bepaald dat een Social Engineering aanval een actie is waarbij de mens direct of indirect betrokken is waarbij wel of niet gebruik gemaakt kan worden van een medium om één of meerdere doelen te realiseren

In deze paragraaf zal uitgelegd worden wat het verschil is tussen directe en indirect betrokkenheid van de mens, wat het gebruik van een medium inhoudt, welke doelen een Social Engineering aanval kan realiseren en welke Social Engineering aanvallen er zijn.

2.6.2 Directe en indirecte betrokkenheid van de mens

In dit onderzoek wordt er onderscheid gemaakt tussen directe en indirecte aanvallen. Bij directe aanvallen is er sprake van interactie tussen de mens en de Social Engineer. De Social Engineer probeert door in te spelen op de eigenschappen van de mens (zie subparagraaf 2.7.3), deze tot uiting te laten komen. Bij indirecte aanvallen speelt de Social Engineer in op het niet bewust zijn van de mens wat reeds tot uiting is gekomen in toegang, het omgaan met informatie, inter-persoonlijke relaties en het handelen. Iedere Social Engineering aanval, zowel direct als indirect, bevat een menselijke component.

Een voorbeeld van een directe aanval is een telefoongesprek met een medewerker in een organisatie waarbij de Social Engineer zich voordoet als iemand anders, ook wel Impersonation genoemd (zie subparagraaf 2.6.5). In deze aanval is een duidelijke interactie aanwezig tussen de Social Engineer en de mens.

Een voorbeeld van een indirecte aanval is het verkrijgen van documenten met informatie die iemand op zijn bureau heeft laten liggen. Dit kunnen belangrijke documenten zijn die niet in de handen van de Social Engineer mogen vallen. De medewerker is zich niet bewust van het feit dat deze documenten ook binnen de organisatie gecompromitteerd kunnen worden. Bij deze aanval maakt de Social Engineer indirect gebruik van het niet bewust zijn van de medewerker.

2.6.3 Gebruik van een medium bij een Social Engineering aanval

In bepaalde situaties kan een aanval fysiek uitgevoerd worden en kan er gebruik gemaakt worden van een medium. Een medium is een middel waardoor directe interactie tussen de Social Engineer en de mens mogelijk wordt zonder dat de Social Engineer fysiek in contact hoeft te staan met de mens. Een Social Engineer kan zowel binnen als buiten de organisatie

gebruik maken van verschillende media waarbij voor het gebruik van media binnen de organisatie fysieke toegang vereist is. Voorbeelden van media zijn onder andere de telefoon, fax en e-mail etc. [50].

2.6.4 Doelen van een Social Engineering aanval

Uit de in de literatuur geïnventariseerde Social Engineering aanvallen is bepaald dat een aanval één of meerdere van de onstaande doelen kan bereiken. In de volgende subparagraaf zal per aanval aangegeven worden welke doelen een aanval mogelijk kan realiseren.

Toegang verkrijgen
Onder toegang verkrijgen wordt verstaan, het fysiek toegang verkrijgen tot een bepaalde beschermde ruimte. In geval van een organisatie houdt dit in, het toegang verkrijgen tot de organisatie van buitenaf en het toegang verkrijgen tot ruimtes binnen de organisatie.

Informatie verkrijgen
Onder informatie verkrijgen wordt verstaan het bemachtigen van gevoelige informatie waarmee het beoogde doel van Social Engineering kan worden bereikt of informatie die gebruikt kan worden als voorbereiding op een volgende aanval.

Vertrouwensrelatie met de mens opbouwen
Onder een vertrouwensrelatie opbouwen wordt verstaan het investeren in een duurzame relatie tussen de Social Engineer en de mens ter voorbereiding op een volgende aanval.

Mens tot handelen aanzetten
Onder een handeling laten verrichten door de mens wordt verstaan het overhalen van de mens om een bepaalde handeling te verrichten ter voorbereiding op een volgende aanval. Het resultaat van een handeling bestaat niet uit het verkrijgen van toegang en / of informatie.

Elke aanval heeft één of meerdere doelen die bij een succesvolle uitvoering van de aanval bereikt kunnen worden. Elk doel levert een bijdrage aan het bereiken van het doel van Social Engineering, het verkrijgen van gevoelige informatie.

2.6.5 Social Engineering aanvallen

Uit de bestudeerde literatuur zijn verschillende aanvallen geïnventariseerd die betrekking hebben op de context waarin Social Engineering in dit onderzoek geplaatst is. Hiermee wordt aangegeven dat de aanvallen binnen de kaders en de definitie van Social Engineering van dit onderzoek vallen. In deze subparagraaf zullen de verschillende aanvallen uiteengezet worden waarin per aanval wordt aangegeven welk(e) doel(en) er bereikt kan / kunnen worden, of er gebruik gemaakt kan worden van een medium en of de mens direct of indirect hierbij betrokken is.

1. **Piggybacking**
   Piggybacking, (meeliften met een ander) is het fysiek toegang verkrijgen tot een beschermde ruimte door gebruik te maken van de mens. Door gebruik te maken van onder andere de behulpzaamheid en achteloosheid van de mens kan de Social Engineer zonder zijn werkelijke identiteit bekend te maken toegang verkrijgen tot een ruimte. De behulpzaamheid van mensen is uit te buiten door bijvoorbeeld een zware doos te dragen zodat mensen bij de ingang een deur voor je open houden [25][26][27][49][52][55].

   Door middel van een Piggybacking aanval kan de Social Engineer proberen fysieke toegang te verkrijgen tot een bepaalde ruimte. Er kan geen gebruik gemaakt worden van een medium omdat de Social Engineer bij een Piggybacking aanval fysiek aanwezig moet zijn. Daarnaast vindt er interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een directe benadering.

2. **Tailgating**
   Bij een Tailgating aanval (achtervolgen, bumperkleven) speelt de Social Engineer in op de achteloosheid van de mens. Door strak achter iemand aan te lopen kan geprobeerd worden om toegang te krijgen tot een bepaalde ruimte zonder dat de Social Engineer hiervoor zijn werkelijke identiteit bekend hoeft te maken. Een ander voorbeeld van een Tailgating aanval is het goede moment af te wachten en toe te slaan op het moment dat een persoon een bepaalde ruimte verlaat en er gelegenheid is om toegang te krijgen tot die ruimte [32][49].

   Door middel van een Tailgating aanval kan de Social Engineer proberen om fysieke toegang te verkrijgen tot een bepaalde ruimte. Er kan geen gebruik gemaakt worden van een medium omdat de Social Engineer bij een Tailgating aanval altijd fysiek aanwezig moet zijn. Tijdens de Tailgating aanval vindt er geen interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een indirecte benadering.

3. **Impersonation**
   Impersonation (voordoen als iemand anders) betekent in de breedste zin van het woord dat een Social Engineer zich voordoet of uitgeeft als een ander persoon. De Social Engineer neemt een andere identiteit aan en probeert te voorkomen dat zijn werkelijke identiteit achterhaald wordt [12][13][44][49][50][52][55][57].

   Door middel van een Impersonation aanval kan de Social Engineer proberen om toegang en / of informatie te verkrijgen, een vertrouwensrelatie op te bouwen en / of een handeling te laten verrichten. Een Impersonation aanval kan zowel fysiek plaatsvinden als via een medium. Tijdens een Impersonation aanval vindt altijd interactie plaats tussen de Social Engineer en de mens waardoor er altijd sprake is van een directe benadering.

4. **Reverse Social Engineering**
   Er is van een Reverse Social Engineering (omgekeerde Social Engineering) aanval sprake als de mens de Social Engineer om hulp vraagt. Reverse Social Engineering kan ook worden gezien als een Impersonation aanval maar vanwege het aanbiedende in plaats van vragende karakter van deze aanval kan er een wezenlijk onderscheid gemaakt worden. Een Social Engineer kan de hulpbiedende situatie op verschillende manieren bewerkstelligen maar de volledige aanval bestaat altijd uit een opeenvolging van een aantal fasen[41][44][47]. Deze fasen zijn de sabotage fase, de adverteerfase en de assistentie fase. In de sabotage fase zorgt de Social Engineer dat er een fout ontstaat waardoor de mens genoodzaakt is contact op te nemen met een expert. In de adverteerfase zorgt een Social Engineer ervoor dat de gebruiker met hem contact opneemt, dit kan bijvoorbeeld door zijn telefoonnummer te vermelden in de foutmelding of visitekaartjes uit te delen etc. In de assistentie fase zorgt de Social Engineer ervoor dat het probleem wordt opgelost. De Social Engineer kan in deze fase misschien al proberen informatie te verkrijgen maar bovenal wordt hij beschouwd als een held na het oplossen van het probleem en vergroot hiermee zijn vertrouwen [37][41][43][44][47][50].

   Door middel van een Reverse Social Engineering aanval kan de Social Engineer proberen om toegang en / of informatie te verkrijgen, een vertrouwensrelatie op te bouwen en / of een handeling te laten verrichten. Een Reverse Social Engineering aanval kan zowel fysiek plaatsvinden als via een medium. Tijdens een Reverse Social Engineering aanval vindt er altijd interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een directe benadering.

5. **Shoulder Surfing**
   Shoulder Surfing (over de schouder meekijken) is de kunst van het ongemerkt observeren van de mens door bij een persoon over zijn schouder mee te kijken om aan informatie te komen. Shoulder Surfing is vooral effectief op plaatsen waar het druk is en het redelijk eenvoudig is om dicht bij iemand in de buurt te gaan staan, zonder dat het opvalt. Het kan bijvoorbeeld gaan om meelezen van een document dat iemand leest of een formulier waarop iemand gegevens invult of invoer apparaten (keypad / toetsenbord) waar mensen een unieke persoonlijke code (gebruikersnaam / wachtwoord / pincode) invullen [29][49][50][52][57].

   Door middel van een Shoulder Surfing aanval kan de Social Engineer proberen om informatie te verkrijgen. Een Shoulder Surfing aanval vindt altijd fysiek plaats. De Social Engineer zou ook gebruik kunnen maken van apparatuur om op afstand een Shoulder Surfing aanval uit te voeren. In dit onderzoek wordt deze apparatuur niet als een medium beschouwd omdat de Social Engineer fysiek op de plaats van de aanval aanwezig moet zijn. Tijdens een Shoulder Surfing aanval vindt geen interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een indirecte benadering.

6. **Dumpster Diving**

Dumpster Diving (afval doorzoeken), ook wel dumpstering, binning, trash picking of trashing genoemd [5][55] is een term voor het doorzoeken van afval binnen en buiten een organisatie. Social Engineers maken gebruik van Dumpster Diving om zo informatie te verzamelen over een persoon of organisatie. Het afval kan door de Social Engineer op verschillende manieren worden verkregen. Bijvoorbeeld door 's nachts op pad te gaan en afval uit de afvalcontainers mee te nemen of door bepaalde personen zoals schoonmakers of vuilnismannen om te kopen. Dumpster Diving heeft zichzelf vaak als zeer waardevol bewezen, aangezien het weinig risico met zich meebrengt, niet verboden is bij de wet [55] en zeer waardevolle informatie kan opleveren [5][30][44][52][55].

Door middel van een Dumpster Diving aanval kan de Social Engineer proberen om informatie te verkrijgen. Hierbij kan informatie ook voorkomen in de vorm van een item zoals een toegangsbadge, briefpapier, bedrijfslogo's, etc. Een Dumpster Diving aanval vindt fysiek plaats waarbij geen interactie plaatsvindt tussen de mens en de Social Engineer of de persoon die de Social Engineer heeft ingehuurd waardoor er sprake is van een indirecte benadering.

7. **Profiling**

Profiling (profiel maken) is het proces van informatieverzameling over een bepaald persoon die een relatie heeft met een organisatie om hiervan een profiel te creëren. Door het gedrag en bepaalde psychologische karakteristieken te analyseren kan een beeld over de desbetreffende persoon gevormd worden [31]. Het profiel kan gebruikt worden om in een bepaalde situatie de bekwaamheid van iemand te voorspellen of vast te stellen. De Social Engineer kan Profiling gebruiken om meer te weten te komen over het gedrag en routines van bijvoorbeeld een medewerker. Deze informatie kan dan weer gebruikt worden bij een vervolgaanval [28][31][37][48].

Door middel van een Profiling aanval kan de Social Engineer proberen om informatie over een persoon met een relatie tot een organisatie te verkrijgen door het gedrag van de mens te bestuderen. Een Profiling aanval vindt fysiek plaats. Tijdens een Profiling aanval vindt er geen interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een indirecte benadering.

8. **Desk Sniffing**

Desk Sniffing (rondsnuffelen op een bureau) heeft betrekking op het doorzoeken van een bepaalde ruimte naar iets van waarde. Een ruimte die extra gevoelig is voor deze aanval is de werkplek van de medewerker. Op de werkplek bevinden zich vaak spullen die nodig zijn om de dagelijkse werkzaamheden uit te kunnen voeren en daarom niet voortdurend netjes en veilig worden opgeborgen. De kans is dus groot dat er informatie aanwezig is op de werkplek die waardevol is voor de Social Engineer.

De Social Engineer kan door middel van een Desk Sniffing aanval proberen om informatie te verkrijgen op de werkplekken waar hij toegang tot heeft. De Social Engineer speelt hierbij in op de achteloosheid van de mens die allerlei spullen voor

"de snelle grijp" laat liggen. Een Desk Sniffing aanval vindt fysiek plaats. Tijdens een Desk Sniffing aanval vindt geen interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een indirecte benadering [43][52][53][57].

9. **Eavesdropping**

Eavesdropping (afluisteren), is het onderscheppen van gesprekken door onbedoelde ontvangers [7]. Iemand die stiekem meeluistert met een gesprek door gebruik te maken van afluisterapparatuur of simpelweg door dicht in de buurt te gaan staan van personen die een gesprek voeren wordt ook wel Eavesdropper genoemd. Door op plaatsen rond te hangen als bedrijfskantines, rookplaatsen of lobbies kan vaak zonder veel moeite een schat aan informatie worden verkregen [6][7][42][49].

De Social Engineer kan door middel van een Eavesdropping aanval proberen om informatie te verkrijgen door in te spelen op de achteloosheid van de mens. Een Eavesdropping aanval vindt fysiek plaats. De Social Engineer zou ook gebruik kunnen maken van apparatuur om op afstand een Eavesdropping aanval uit te voeren. In dit onderzoek wordt deze apparatuur niet als een medium beschouwd omdat de Social Engineer fysiek op de plaats van de aanval aanwezig moet zijn. Tijdens een Eavesdropping aanval vindt geen interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een indirecte benadering.

10. **Phishing**

Phishing (vissen naar gegevens), heeft betrekking op het oplichten van mensen door een vertrouwde omgeving te creëren waarin nietsvermoedende personen allerlei vertrouwelijke gegevens afgeven. Bekende methoden van Phishing zijn het klonen van een vertrouwde website, officieel uitziende e-mail gebruiken met een verzoek om gegevens terug te sturen naar de afzender en het versturen van enquêtes per e-mail en post. Bij het klonen van een vertrouwde website denken mensen dat de website authentiek is en hebben daarom geen argwaan bij het invullen van allerlei gegevens op de website. Het ervoor zorgen dat mensen de gekloonde website bezoeken kan op veel manieren. Veel voorkomende manieren zijn door E-mail en Instant Messaging in combinatie met DNS [4][22] en URL spoofing [22][23][24][30][35][43][47][50][57].

De Social Engineer kan door middel van een Phishing aanval proberen informatie te verkrijgen. Een Phishing aanval vindt alleen plaats via een medium. Tijdens een Phishing aanval vindt interactie plaats tussen de Social Engineer en de mens waardoor er sprake is van een directe benadering.

11. **Keylogger**

Een Keylogger is een softwarematig of hardwarematig apparaatje dat de toetsaanslagen van een keyboard van een computersysteem registreert. Een Social Engineer kan een softwarematige Keylogger installeren op het computersysteem of een hardwarematige Keylogger plaatsen tussen het keyboard en het computersysteem in.

Vanaf het moment van plaatsing zal de Keylogger alle toetsaanslagen van de gebruiker registreren. De kans is groot dat deze toetsaanslagen ook gebruikersnamen en wachtwoorden tot verschillende informatiesystemen bevatten. Na enige tijd zal de Social Engineer de softwarematige en / of hardwarematige Keylogger uitlezen waardoor er door de Social Engineer waardevolle informatie wordt verkregen.

De Social Engineer kan door middel van een Keylogger aanval proberen informatie te verkrijgen. De aanval vindt alleen fysiek plaats om dat de Social Engineer fysiek toegang moet hebben tot een informatiesysteem voor het plaatsen van de Keylogger. Er is bij deze aanval geen interactie met de mens waardoor deze aanval indirect plaatsvindt. De Social Engineer speelt in op het niet bewust zijn van de mens waardoor hij in staat is om de Keylogger te plaatsen [16][55].

12. **Item-dropping**
    Item-dropping (het neerleggen van spullen) heeft betrekking op het neerleggen van spullen op een specifieke plaats met de intentie dat het aanzet tot of deel uit maakt van een actie van de mens. Door bijvoorbeeld een cd-rom met aanlokkende titel op het bureau van de mens neer te leggen kan geprobeerd worden de nieuwsgierige mens te verleiden. Het gevolg kan zijn dat er een virus of trojan horse wordt geïnstalleerd op de computer van de mens waardoor er een direct gevaar met betrekking tot de informatiebeveiliging ontstaat [15][59].

    De Social Engineer kan door middel van een Item-dropping aanval proberen de mens een handeling te laten verrichten door in te spelen op de achteloosheid en nieuwsgierigheid van de mens. Een Item-dropping vindt altijd fysiek plaats zonder interactie tussen de Social Engineer en de mens waardoor er sprake is van een indirecte aanval.

2.6.6 Randgevallen

Er bestaan altijd randgevallen of een bepaalde Social Engineering aanval ook binnen de kaders van dit onderzoek als een aanval wordt beschouwd. De grens is in sommige gevallen dan ook flinterdun waardoor er discussie kan ontstaan.

Een voorbeeld van een randgeval is de Social Engineering aanval Profiling. De mens is bij deze aanval wel betrokken, wat deze aanval een Social Engineering aanval maakt. Het is echter moeilijk aan te geven of de aanval direct of indirect is. Er vindt geen interactie plaats en er wordt niet duidelijk ingespeeld op het niet bewust zijn van de mens. Dit maakt deze aanval een randgeval.

2.6.7 Aanvalsmatrix

In de onderstaande aanvalsmatrix zijn de verschillende Social Engineering aanvallen en de verschillende kenmerken hiervan overzichtelijk weergegeven. De vinkjes geven aan bij welke doelen per aanval bereikt kunnen worden, of de aanval direct of indirect is en de aanval fysiek of via een medium kan worden uitgevoerd.

			Doel							
			Toegang		Informatie		Relatie		Handeling	
			Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Aanval	Piggybacking	Fysiek	✓							
		Medium								
	Tailgating	Fysiek		✓						
		Medium								
	Impersonation	Fysiek	✓		✓		✓		✓	
		Medium			✓		✓		✓	
	Reverse Social Engineering	Fysiek			✓		✓		✓	
		Medium			✓		✓		✓	
	Shoulder Surfing	Fysiek				✓				
		Medium								
	Dumpster Diving	Fysiek				✓				
		Medium								
	Profiling	Fysiek				✓				
		Medium								
	Desk sniffing	Fysiek				✓				
		Medium								
	Eavesdropping	Fysiek				✓				
		Medium								
	Phishing	Fysiek								
		Medium			✓					
	Keylogger	Fysiek								
		Medium				✓				
	Item dropping	Fysiek								✓
		Medium								

2.7 Gereedschappen van de Social Engineer

Om een Social Engineering aanval kracht bij te zetten kan de Social Engineer gebruik maken van verschillende gereedschappen. In de volgende paragrafen zal uiteengezet worden welke gereedschappen de Social Engineer tot zijn beschikking heeft en op welke wijze de Social Engineer deze gereedschappen kan inzetten.

2.7.1 Technieken

Bij directe Social Engineering aanvallen kan de Social Engineer gebruik maken van technieken om te proberen de aanval succesvol uit te voeren. Uit de bestudeerde literatuur is gebleken dat een Social Engineer veel verschillende technieken ter beschikking heeft om te misleiden, te manipuleren en gebruik te maken van het niet bewust zijn van de mens. Elk artikel heeft zo zijn eigen visie over hoe een techniek ingezet kan worden en welke gevolgen dit heeft waardoor het moeilijk is om een eenduidige structuur aan te brengen. Daarom zal een algemene beschrijving gegeven worden van de geïnventariseerde technieken uit de bestudeerde literatuur. Een Social Engineer kan meerdere technieken in combinatie toepassen.

1. **Vleierij**
   Vleierij is een manier van interactie waarbij iemand overmatig of onoprecht wordt geprezen of gecomplimenteerd [11]. Door vleierij toe te passen probeert de Social Engineer in te spelen op bepaalde eigenschappen van de mens om zo een comfortabele situatie te creëren. De Social Engineer kan vervolgens proberen om deze comfortabele situatie uit te buiten [38][44].

2. **Intimidatie**
   Intimidatie is een manier van interactie waarbij iemand opzettelijk wordt bang gemaakt om hem er toe te zetten iets te doen. Dit kan bijvoorbeeld doordat de Social Engineer zich voordoet als een autoriteit. Intimidatie wordt gebruikt om een oncomfortabele situatie te creëren. De mens zal niet graag in zo´n situatie terecht komen en zal zo snel mogelijk uit deze situatie willen en daardoor eerder geneigd zijn aan bepaalde verzoeken te voldoen [38][41][49].

3. **Flirten**
   De Social Engineer kan deze manier van interactie gebruiken om avances te maken en de seksuele interesse van de mens op te wekken. Hierdoor wordt er een comfortabele situatie gecreëerd die uitgebuit kan worden [39][44].

4. **Vriendelijk zijn**
   Deze manier van interactie spreekt voor zich. Door vriendelijk te zijn speelt de Social Engineer in op de eigenschap van de mens dat hij graag gemogen wil worden. Het gaat hierbij om het creëren van een aangename situatie en het vergroten van de geloofwaardigheid waardoor de mens hulpvaardiger wordt [43][44].

5. **Bedrijfsjargon gebruiken**
   Door bedrijfsjargon te gebruiken zoals bedrijfsafkortingen, afdelingen, bedrijfsprocessen etc. kan de Social Engineer zijn geloofwaardigheid vergroten [41][56].

6. **Namedropping**
   Bij namedropping gebruikt de Social Engineer namen van medewerkers om een geloofwaardige identiteit bij de mens te creëren. Dit vergroot het vertrouwen van de mens waardoor de mens sneller zal voldoen aan bepaalde verzoeken van de Social Engineer [38][49][55][56].

7. **Diffusion of responsibility (verdeling van verantwoordelijkheid)**
   Dit is een techniek die de Social Engineer kan gebruiken om de mens te laten geloven dat hij niet alleen verantwoordelijk is voor bepaalde acties. Dit verlaagt voor de mens de drempel om te voldoen aan een verzoek van de Social Engineer [43][44][46][55].

8. **Urgency (urgentie)**
   De Social Engineer creëert een bepaalde situatie waaruit blijkt dat er haast achter een verzoek zit en dat dit met spoed moet worden uitgevoerd. De mens wordt met klem verzocht om te voldoen aan dit verzoek omdat er anders voor iedereen, dus ook voor de mens die beïnvloed wordt, negatieve consequenties aan verbonden zijn. Doordat de mens snel moet handelen, kan dit een mentale kortsluiting [55] als gevolg hebben waardoor de mens een onjuiste beslissing neemt omdat hij geconfronteerd wordt met de mogelijke gevolgen [42].

9. **Overloading (overbelasting)**
   Overloading houdt in het overladen van de mens met informatie waardoor hij niet in staat is deze informatie effectief te verwerken. De mens kan niet meer logisch redeneren [55] waardoor hij de informatie slechts tot zich neemt in plaats van deze te evalueren. Door overloading te gebruiken kan de Social Engineer de mens overhalen om te voldoen aan een verzoek. Een vorm van overloading is het beginnen van een discussie over een onderwerp waarvan de mens niet op de hoogte is. De mens heeft tijd nodig om bekend te worden met het onderwerp maar die tijd is er niet. De mens zal sneller argumenten accepteren zonder dat deze goed zijn doordacht [43][50].

10. **Strong affect (sterke beïnvloeding)**
    Strong affect is het veroorzaken van een verhoogde emotionele toestand van de mens door de Social Engineer. De mens wordt geconfronteerd met een gevoel van verassing, anticipatie, of boosheid waardoor hij minder goed met de door de Social Engineer aangedragen informatie omgaat. Er wordt bij strong affect ingespeeld op de verandering van de geestelijke toestand van de mens waardoor hij niet meer logisch kan denken [55] en daardoor toegeeft aan de verzoeken van de Social Engineer [56].

11. **Direct approach (directe benadering)**
    Onder direct approach wordt verstaan de directe benadering van de mens door de Social Engineer, en het zonder omweg vragen de mens te voldoen aan een verzoek. Deze benadering is het meest risicovol voor de Social Engineer omdat dit bij de mens argwaan kan opwekken waardoor het verzoek geweigerd kan worden [41][55].

12. **Authority (autoriteit)**
    Authority is een techniek die de Social Engineer kan gebruiken om de mens te intimideren. Door zich voor te doen als, of aan te geven dat hij een opdracht moet vervullen voor een belangrijk persoon zet de Social Engineer de mens onder druk om aan een bepaald verzoek te voldoen [38][41][44].

2.7.2 Situaties

Met behulp van de technieken kan de Social Engineer proberen bepaalde situaties te creëren. Deze situaties hebben betrekking op de gemoedstoestand van de mens. In de bestudeerde literatuur komt niet nadrukkelijk naar voren welke situaties er gecreëerd worden. Wel wordt er bij sommige technieken aangegeven op welke eigenschappen, waaronder emoties, wordt ingespeeld. Grofweg kan de Social Engineer twee situaties bij de mens creëren namelijk:

1. **Comfortabele situatie**
   De comfortabele situatie is een situatie waarin de mens een gevoel van controle heeft, zich veilig voelt en zich op zijn gemak voelt [52]. Door de mens zich op zijn gemak te stellen door bijvoorbeeld vleierij, flirten, vriendelijk te zijn of namedropping toe te passen kan de Social Engineer een comfortabele situatie creëren [41][55][56]. Hierna kan er op bepaalde eigenschappen van de mens worden ingespeeld om zo één of meerdere doelen te bereiken.

2. **Oncomfortabele situatie**
   Dit is een situatie waar de mens zich niet graag in bevindt en waar hij zo snel mogelijk uit wil. De mens voelt zich bedreigd, heeft de situatie niet meer in de hand, is bang om in de problemen te komen en kan meestal niet meer logisch redeneren [55][57]. Door bijvoorbeeld de mens te intimideren, overloading of authority toe te passen kan de mens onder druk gezet worden [52]. Omdat de mens zo snel mogelijk uit deze oncomfortabele situatie wil zal hij mogelijk sneller besluiten om aan een

verzoek van de Social Engineer te voldoen zonder dit besluit goed overwogen te hebben [43][56].

Als een Social Engineer een bepaalde aanval uitvoert dan probeert hij door het gebruik van verschillende gereedschappen een bepaalde situatie te creëren, die hij vervolgens probeert uit te buiten. De Social Engineer kan hierbij gestructureerd en ongestructureerd te werk gaan.

Een voorbeeld van een gestructureerde manier is dat de Social Engineer vooraf bepaalt of hij het slachtoffer in een comfortabele of oncomfortabele positie wil brengen. Door een bepaald slachtoffer op te bellen kan de Social Engineer gereedschappen zoals vleierij, strong affect en vriendelijk zijn gebruiken om zo het slachtoffer op zijn gemak te stellen. Hiermee bereikt de Social Engineer een comfortabele situatie en wint hij het vertrouwen van het slachtoffer waardoor hij één of meerdere doelen kan bereiken.

Een voorbeeld van een ongestructureerde manier is het opbellen van een slachtoffer, waar de Social Engineer het gebruik van gereedschappen af laat hangen van het verloop van het gesprek met het slachtoffer. De Social Engineer belt het slachtoffer op en constateert dat het slachtoffer erg behulpzaam is. Hij kan hiertoe authority, urgency en intimidatie gebruiken en zo het slachtoffer in een oncomfortabele positie brengen. Dit is dus een situatie die de Social Engineer naar aanleiding van het verloop van het gesprek creëert.

2.7.3 Eigenschappen van de mens

Met de kennis over de technieken en situaties kan de Social Engineer proberen om in te spelen op de eigenschappen van de mens of deze juist uit te buiten. Ieder mens kent behalve een aantal unieke eigenschappen ook een aantal eigenschappen waarvan gezegd kan worden dat iedereen die in meer of mindere mate bezit. De Social Engineer kan proberen hiervan gebruik te maken bij het voorbereiden en uitvoeren van een aanval. De literatuurstudie heeft een aantal algemene eigenschappen van de mens opgeleverd dat hieronder uiteengezet wordt, dit betekent echter niet dat hiermee het overzicht volledig is.

1. **Achteloosheid**
   Dit heeft betrekking op de onoplettendheid, nonchalance en onwetendheid van de mens. Omdat een mens, tenzij hij last heeft van achtervolgingswaanzin, niet voordurend bezig is de omgeving te observeren zal hij niet alles wat er in die omgeving gebeurt waarnemen. De nonchalance van de mens heeft betrekking op het negeren van de geldende regels en wat er in de omgeving gebeurt. Dit kan bewust zijn maar ook als gevolg van onwetendheid [42][52][55].

2. **Lage betrokkenheid**
   De mens voelt zich betrokken bij zaken die hem direct aangaan. Dat kan bijvoorbeeld zijn vanwege zijn positie binnen een organisatie. Bij zaken die niet direct betrekking hebben op de werkzaamheden behorende bij zijn functie of positie voelt de mens zich minder betrokken en bovendien kan de kennis op dit gebied ontbreken. In deze

situatie is de mens eerder geneigd om dingen aan te nemen van een andere persoon en bovendien is het moeilijk voor de mens om in te schatten wat de implicaties van een bepaalde actie kunnen zijn [49].

3. **Behulpzaam willen zijn**
   Mensen willen graag behulpzaam zijn [49]. Doordat de mens graag behulpzaam wil zijn kan de Social Engineer hier gebruik en of misbruik van maken door een beroep te doen op de mens [45].

4. **Mensen willen vertrouwen**
   Mensen willen graag andere mensen vertrouwen. Een Social Engineer kan hier gebruik en of misbruik van maken door met een overtuigend verhaal te komen. De mens zal bij een overtuigend verhaal snel aannemen dat het in orde is en de Social Engineer vertrouwen voor wie hij zegt te zijn [44].

5. **Gemogen willen worden**
   Over het algemeen willen mensen graag aardig gevonden worden. Als mensen je mogen betekent het dat je geaccepteerd en gerespecteerd wordt, wat je een goed gevoel geeft. Als iemand jou graag mag dan heb je voor die persoon ook vaak meer over [49].

6. **Integer willen zijn**
   Over het algemeen willen mensen graag integer overkomen. Integer zijn heeft betrekking op het doen wat je zegt, en zeggen wat je doet [21]. Een integer persoon houdt zich aan wat hij heeft gezegd, beloofd en wijkt ook in moeilijke tijden niet af van zijn principes, loyaliteit en afspraken [43][47].

7. **Emoties**
   Een Social Engineer kan het rationele denken van een slachtoffer beïnvloeden door in te spelen op de emoties van de mens. Emoties zijn persoonlijke interne ondervindingen waarmee een verzameling van lichamelijke reacties gepaard kan gaan [9]. Volgens Ekman [8], een professor psychologie aan de Universiteit van Californië zijn er zes basis emoties namelijk: woede, vreugde, angst, verdriet, verbazing en afschuw [9]. Daarnaast worden ook: acceptatie, afgunst, anticipatie, berouw, bewondering, haat, hoop, jaloezie, liefde, minachting, schaamte, schuldgevoel, spijt, trots, verveling, verwijt, wanhoop, medeleven en hebzucht als emoties beschouwd [2][37][43][56].

8. **Nieuwsgierigheid**
   Mensen zijn van nature nieuwsgierig [45]. Een Social Engineer kan hier dankbaar gebruik van maken door de interesse van de mens proberen te wekken. De mens zal zijn nieuwsgierigheid niet weten te bedwingen en zal doen wat de Social Engineer als vooropgezet plan had uitgedacht. Een goed voorbeeld hiervan wordt gegeven in artikel [15] waarbij USB-sticks willekeurig bij medewerkers op het bureau werden gelegd. Het eerste dat de medewerkers deden bij aankomst was de USB-stick op de computer aansluiten.

2.7.4 Psychologische principes

Behalve de technieken, situaties en eigenschappen van de mens zijn er psychologische principes die de Social Engineer kan volgen om te proberen een Social Engineering aanval succesvol uit te voeren. Om een beter inzicht te krijgen in hoe de mens gemanipuleerd en misleid kan worden wordt een uitstap gemaakt naar het vakgebied van de psychologie. In de bestudeerde literatuur [43][47] wordt verwezen naar het werk van Robert Cialdini [58]. Cialdini doet al meer dan dertig jaar onderzoek naar manipulatie, compliance[3] en onderhandeling en heeft een reputatie opgebouwd als expert op dit gebied. In zijn boek "Influence" [58] geeft Cialdini aan dat er duizenden tactieken bestaan om mensen naar je hand te zetten waarvan de meerderheid is onder te brengen binnen een zestal verschillende categorieën. Elk van deze zes categorieën wordt geleid door een fundamenteel psychologisch principe dat richting geeft aan het menselijk gedrag. Een Social Engineer kan deze principes toepassen in zijn Social Engineering aanvallen. Doordat de principes context onafhankelijk zijn dient de Social Engineer er zijn eigen invulling aan te geven.

De zes basis principes van Cialdini zijn:

1. **Wederkerigheid (Reciprocation, geven en nemen, voor wat hoort wat)**
   De beslissing om mee te werken aan een verzoek van een ander kan worden gemanipuleerd door wederkerigheid. Het wederkerigheidprincipe is zeer krachtig en overweldigt vaak alle andere factoren die normaal gesproken de beslissing bepalen. Bovendien kan het wederkerigheidprincipe gebruikt worden om een gunst van een ander uit te lokken. Door iemand een ongevraagde gunst te verlenen is die persoon op dat moment minder in staat om zelf te bepalen wie hij iets schuldig is. Voor wat hoort wat en als iemand jou een gunst verleent dan moet je een gunst terug verlenen. Tenslotte spoort het wederkerigheidprincipe aan tot ongelijke gunsten, door een schuldgevoel, oncomfortabele situatie of situatie waarin sociale omgangsvormen in het geding komen te creëren. Hierdoor zal een persoon eerder instemmen met een gunst die groter is dan de gunst die hij zelf heeft ontvangen.

   Behalve in de hierboven genoemde situaties waarbij er druk wordt uitgeoefend op de ontvanger van een gunst door een reeds gemaakte concessie is er nog een tweede variant. Bij deze tweede variant leidt het wederkerigheidprincipe tot een compromisproces. In dit compromisproces wordt een verzoek gedaan tot een grote gunst met de intentie om de andere persoon in te laten stemmen met een kleinere gunst. Deze techniek wordt ook wel *rejection-then-retreat* of *door-in-the-face* techniek genoemd. In de praktijk betekent dit dat er eerst een verzoek tot grote gunst aan een persoon wordt gedaan waarvan zeker is dat het verzoek geweigerd zal worden. Als het verzoek tot grote gunst geweigerd wordt zal de verzoeker een verzoek doen tot een kleinere gunst. Omdat de persoon in kwestie de verzoeker tegemoet zal willen komen is de kans groot dat hij akkoord gaat met het verzoek. Volgens Cialdini [58] werkt de rejection-then-retreat techniek ook bij verzoeken tot respectievelijk grote

[3] Compliance vertaald naar de Nederlandse taal betekent: Overeenstemming bereiken over, of aanpassen van bepaalde acties om te voldoen aan andermans wensen, regels of noodzaak.

gunsten, voorwaarde is echter wel dat de gunst altijd kleiner moet zijn dan de gunst in het voorgaande verzoek [20][47].

Een voorbeeld van het wederkerigheidprincipe bij Social Engineering is als een Social Engineer een Reverse Social Engineering aanval gebruikt. Hierbij biedt de Social Engineer zich aan als de redder in nood door het probleem van de mens (dat de Social Engineer opzettelijk zelf heeft veroorzaakt) op te lossen. Omdat de Social Engineer door een gunst te verlenen als een held wordt gezien, zal de mens nu eerder instemmen met een verzoek dat de Social Engineer aan de mens doet [49].

2. **Commitment en Consistentie**
Commitment en consistentie heeft betrekking op het feit dat wanneer je een belofte maakt, je deze ook moet nakomen en wanneer je een standpunt inneemt je bij dit standpunt moet blijven [21]. Mensen willen graag consistent overkomen in wat ze zeggen, waarin ze geloven, hoe ze zichzelf een houding geven en hoe ze handelen [58]. De sleutel om een persoon over te halen om te voldoen aan jouw wensen is door ervoor te zorgen dat een persoon een bepaald standpunt of positie inneemt dat in lijn ligt met een later verzoek tot een gunst. De kunst is om de persoon in kwestie te sturen naar een bepaald standpunt of positie. Hierdoor is de kans groot dat de desbetreffende persoon later instemt met het verzoek tot een gunst dat consistent is met zijn eerder ingenomen standpunt of positie [20][47][58].

De Social Engineer kan gebruik maken van het committent en consistentie principe door een slim standpunt of positie te bedenken dat hij het slachtoffer wil laten innemen. De Social Engineer zal dit standpunt of positie vervolgens geloofwaardig moeten proberen te maken. Als het slachtoffer zijn standpunt of positie heeft ingenomen kan de Social Engineer een poging doen om het consistente gedrag van het slachtoffer uit te buiten door een verzoek tot een gunst te doen dat in lijn ligt met het ingenomen standpunt of positie van het slachtoffer.

3. **Sociale bewijskracht (Social Proof)**
Sociale bewijskracht heeft betrekking op het feit dat als anderen iets doen dan ga jij dat ook doen [20]. Mensen bepalen in een bepaalde situatie wat goed is door te kijken naar hoe andere mensen in dezelfde situatie handelen. Een voorbeeld van dit principe in de praktijk is het vragen aan iemand om een gunst en hierbij aan te geven dat andere mensen in dezelfde situatie ook deze gunst hebben verleend. Sociale bewijskracht is in twee situaties het meest effectief. In de eerste situatie is er sprake van onzekerheid bij de mens waarbij de mens eerder geneigd is om de acties van anderen als correct aan te nemen. In de tweede situatie is er sprake van overeenkomstigheid waardoor de mens eerder geneigd is om andere mensen te volgen waarmee hij zich gelijkwaardig voelt [20][47][58].

Een voorbeeld van het gebruik van het Social Proof principe wordt hieronder weergegeven. De Social Engineer belt een slachtoffer en probeert het slachtoffer over te halen om te voldoen aan zijn verzoek. De Social Engineer beweert dat de andere collega's van het slachtoffer nooit moeilijk doen bij hetzelfde verzoek. Bovendien

beweert de Social Engineer dat hij dit verzoek regelmatig doet en dat nooit iemand hier moeilijk over doet. Of het werkelijk lukt om het slachtoffer over te halen hangt af van de overtuigingskracht van de Social Engineer en de onzekerheid van het slachtoffer.

4. **Sympathie**

Mensen zeggen zeggen eerder ja tegen personen die ze kennen en sympathiek vinden. Hiervan kan een persoon die een ander persoon naar zijn hand wil zetten gebruik maken, door de nadruk te leggen op een aantal factoren die hun aantrekkelijkheid vergroten en hun innemende persoonlijkheid beter tot uiting laten komen[58]. De eerste factor die de sympathie opwekt is fysieke aantrekkingskracht. Hoewel altijd al werd gedacht dat fysieke schoonheid een voordeel oplevert in sociale interactie blijkt uit onderzoek [47] dat het voordeel zelfs groter is dan verwacht. Aantrekkelijke mensen zijn beter in het misleiden van mensen om zo te krijgen wat ze willen hebben en om de houding van anderen te veranderen. De tweede factor die symphatie opwerkt is gelijksoortigheid.Mensen zijn eerder geneigd om in te gaan op een verzoek dat wordt gedaan door mensen die net zo zijn als zij zelf. De derde factor is lof; door het geven van complimenten kan sympathie worden opgewekt. Deze complimenten mogen dan echter niet doorzichtig zijn omdat dit juist een tegengesteld effect kan hebben. De vierde factor kan sympathie bevorderen doordat mensen door herhaaldelijk contact met elkaar vertrouwd raken. Uitgangspunt hierbij is dat het contact onder positieve omstandigheden plaatsvindt. De vijfde factor om sympathie op te wekken is associatie. Mensen brengen zichzelf graag in verband met positieve dingen. [20][47][58].

Een Social Engineer probeert bijvoorbeeld in een telefoongesprek met een slachtoffer te achterhalen wat zijn interesses zijn (hobby's, sport, eten etc). De Social Engineer probeert vervolgens het slachtoffer te overtuigen dat hij ook deze interesses heeft waardoor sympathie door gelijksoortigheid wordt opgewekt. Vanwege de sympathie die het slachtoffer nu heeft voor de Social Engineer zal hij eerder geneigd zijn om in te gaan op een verzoek van de Social Engineer.

5. **Autoriteit**

Autoriteit heeft betrekking op het recht om acties van andere personen te beïnvloeden, te sturen en te controleren**.** Autoriteit kan worden bepaald door de wet, traditie, geldende morele regels, of door toestemming van de personen die onder gezag staan [1]. Uit onderzoek van onder andere Milgram in 1974 [58] is gebleken dat autoriteit een zeer sterk middel is om mensen te manipuleren. Autoriteit kan mensen ertoe aanzetten om acties te ondernemen waar ze niet achter staan. De oorsprong van het gehoorzamen aan autoriteiten ligt bij de opvoeding. Tijdens de opvoeding wordt geleerd dat gehoorzaamheid leidend is als goed gedrag. Autoriteit kan ook gebaseerd zijn op zogenaamde symbolen in plaats van de werkelijke inhoud [47]. Er wordt hierbij onderscheid gemaakt in een drietal symbolen. Het eerste symbool heeft betrekking op de titel die een bepaalde persoon heeft. Een titel kan aangeboren zijn zoals bij mensen van adel het geval is maar een titel kan ook resultaat zijn van een jarenlange investering in studie of onderzoek. Mensen zullen personen met een

bepaalde titel een hogere status toekennen waarmee zij automatisch een hogere autoriteit vertegenwoordigen. Het tweede symbool van autoriteit dat mensen kan beïnvloeden is kleding. Met kleding kan een bepaalde vorm van autoriteit worden uitgestraald, denk aan de politie, rechters, chirurgen, leger, etc. Het derde symbool is typisch Amerikaans en minder relevant in dit onderzoek. Het heeft betrekking op het respect dat eigenaren van prestigieuze auto's krijgen van anderen [1][47][58].

Helpdesks zijn volgens Impersonation casestudies het meest voorkomende doelwit van Social Engineering aanvallen [57]. De Social Engineer belt bijvoorbeeld de helpdesk van een organisatie en doet zich voor als een belangrijke werknemer, bijvoorbeeld de adjunct directeur of de secretaris van de adjunct directeur. De Social Engineer voegt hiermee een element van intimidatie toe. De desbetreffende helpdeskmedewerker zal niet snel een verzoek afslaan als het de adjunct directeur is die belangrijke informatie nodig heeft waar de toekomst van de organisatie vanaf hangt. De Social Engineer kan er bovendien nog een schepje bovenop doen door tegen de helpdeskmedewerker te zeggen dat weigering verstrekkende gevolgen voor hem kan hebben [57].

6. Schaarste

Schaarste zorgt ervoor dat mensen meer waarde hechten aan bepaalde kansen. Een bekend voorbeeld is de reactie van een klant als hij geïnformeerd wordt over het feit dat van een product nog maar een beperkt aantal op voorraad is. De klant zal eerder geneigd zijn om het product nu toch te kopen. Schaarste heeft de beslissing van de klant beïnvloed door het zwaarder mee te laten wegen in de eventuele aanschaf van het product. Deze techniek wordt ook wel *beperkt aantal g*enoemd [58]. Daarnaast bestaat er binnen het schaarste principe ook nog de techniek van "deadline" waarbij geprobeerd wordt een persoon ervan te overtuigen dat de kans die hem wordt geboden slechts voor beperkte tijd geldig is. Behalve de reden dat schaarste ervoor zorgt dat mensen meer waarde hechten aan bepaalde kansen, zorgt schaarste er ook voor dat de vrijheid van mensen beperkt wordt. Mensen reageren hierop door de schaarste zelfs meer dan daarvoor te willen opvullen en zo de vrijheid weer te vergroten. Het schaarsteprincipe is naast de waarde die er aan goederen wordt gehecht ook van toepassing op de waarde die aan informatie wordt gehecht. Onderzoek heeft aangetoond dat beperking van toegang tot informatie ervoor zorgt dat mensen deze juist willen hebben en er meer voor over hebben om deze te krijgen [47]. Het schaarste principe werkt het best bij nieuwe schaarse informatie en / of producten en wanneer er gestreden moet worden met andere mensen om schaarse informatie en / of producten [20][47][58].

De Social Engineer kan gebruik maken van het schaarsteprincipe door een schaars goed, bijvoorbeeld de laatste kaartjes van een concert als prijs weg te geven voor het volledig invullen van een enquête. Deze methode van werken wordt ook wel *phishing* genoemd. Het slachtoffer wil de kaartjes natuurlijk graag hebben en vult daarom zo volledig mogelijk het enquête formulier in. De Social Engineer heeft nu op slinkse wijze allerlei informatie van het slachtoffer weten los te krijgen. De kaartjes zal het slachtoffer waarschijnlijk nooit ontvangen.

2.8 Resultaten

In dit hoofdstuk is een begin gemaakt met de structurering van het begrip Social Engineering. Hierin is een onderbouwde definitie gegeven, is het doel van Social Engineering beschreven, is aangegeven welke waarde informatie kan hebben voor een Social Engineer en is aangegeven wat er onder voorbereiding wordt verstaan.

Vervolgens zijn de verschillende kenmerken van een Social Engineering aanval beschreven. Een mens kan bij een aanval direct of indirect betrokken zijn waarbij de aanval fysiek of via een medium plaatsvindt. Daarnaast kan de aanval kan één of meerdere doelen bereiken. Deze doelen zijn toegang verkrijgen, informatie verkrijgen, vertrouwensrelatie opbouwen en handeling laten verrichten. Uit de literatuurstudie zijn verschillende Social Engineering aanvallen geïnventariseerd die binnen de gestelde definitie vallen. Deze kort en bondig uiteengezet.

Tenslotte is er een overzicht gegeven van welke gereedschappen de Social Engineer kan gebruiken om een aanval kracht bij te zetten in een poging een aanval succesvol uit te voeren. Deze gereedschappen zijn onderverdeeld in technieken, situaties, en eigenschappen van de mens. Daarnaast zijn er ook nog psychologische principes die richting geven aan het menselijke gedrag waarvan de Social Engineer gebruik kan maken om de mens naar zijn hand te zetten.

De definitie en de verschillende onderdelen vormen de basis voor een verdere structurering van het begrip Social Engineering weergegeven in een conceptueel framework, beschreven in het volgende hoofdstuk.

3 Conceptueel Framework

3.1 Inleiding

Het conceptuele framework is een eerste poging Social Engineering te structureren en visueel weer te geven. Structuur is er reeds aangebracht in de begripsbepaling door de definitie en het doel van Social Engineering, Social Engineering aanvallen en gereedschappen in kaart te brengen. In het framework zal geprobeerd worden om Social Engineering verder te structureren door de onderdelen uit de begripsbepaling ten opzichte van elkaar te positioneren. Omdat het een eerste poging betreft zijn niet alle onderdelen van de begripsbepaling hierin terug te vinden en zal mogelijk niet alles consistent zijn. De toegevoegde waarde van dit conceptuele framework is het feit dat het een eerste poging is wat in de toekomst verfijnd en uitgebreid kan worden. Overal waar in deze scriptie het woord "framework" wordt gebruikt, wordt "conceptueel framework" bedoeld.

3.2 Uitgangspunten en aannames

Het framework is gebaseerd op de in hoofdstuk 2 beschreven begripsbepaling. Het framework is tot stand gekomen door het houden van brainstormsessies en door middel van prototyping getoetst aan de begripsbepaling. Aannames en uitgangspunten zullen waar nodig onderbouwd worden met behulp van literatuurbronnen.

3.2.1 De organisatie

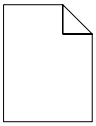
Het framework richt zich op de organisatie en haar omgeving. Hiermee wordt een doorsnee profit / non-profit organisatie bedoeld waarin mensen verschillende functies uitoefenen om zo een bijdrage te leveren aan het bereiken van een gezamenlijk doel . De organisatie wordt in dit framework fysiek opgedeeld in drie organisatiegebieden namelijk: *fysiek binnen de organisatie, fysiek buiten de organisatie* en *de organisatiegrens* waarbij de organisatiegrens de opdeling maakt tussen binnen en buiten.

Als objecten zich binnen de organisatie bevinden dan betekent dit dat zij zich fysiek binnen de organisatie bevinden. Objecten buiten de organisatie bevinden zich fysiek buiten de organisatie. Het is lastig om de precieze ligging van de organisatiegrens aan te geven. De organisatiegrens kan zowel liggen bij de toegang tot het terrein waar de fysieke organisatie (bijvoorbeeld het kantoorpand) zich op bevindt als bij de ingang tot de fysieke organisatie zelf (bijvoorbeeld de ingang(en) van het kantoorpand). In dit onderzoek is de organisatiegrens de overgang waar publieke toegang over gaat in beperkte toegang door bijvoorbeeld toegangscontrole. Daarnaast kan de organisatiegrens ook gelaagd zijn wat inhoudt dat er meerdere toegangscontroles kunnen zijn. Deze onderverdeling is gemaakt omdat zo beter aangegeven kan worden waar de Social Engineering aanvallen in de organisatie precies plaatsvinden.

3.2.2 Informatiedragers en informatie

Zowel binnen als buiten de organisatie als op de grens van de organisatie kunnen zich verschillende objecten bevinden. In dit framework worden deze objecten informatiedragers genoemd en wordt er onderscheid gemaakt tussen hardcopy, menselijke en informatiesysteem informatiedragers.

Hardcopy
Onder hardcopy informatiedragers wordt verstaan alle informatiedragers die tastbaar zijn voor de mens en niet in staat zijn om informatie zelfstandig te verwerken. De primaire taak van een hardcopy informatiedrager is het passief dragen van informatie. Voorbeelden van hardcopy informatiedragers zijn: papieren documenten, cd-rom's, diskettes, USB-sticks, posters en whiteboards. Een hardcopy informatiedrager zal in het framework worden aangegeven met het onderstaande symbool.



Mens
De menselijke informatiedrager spreekt voor zich. Het gaat hierbij om de mens als informatiedrager en informatie die is opgeslagen in het menselijk brein. Indien er gesproken wordt over een menselijke informatiedrager die een menselijke informatiedrager benadert er sprake van verschillende instanties van de menselijke informatiedrager. Een menselijke informatiedrager zal in het framework worden aangegeven met het onderstaande symbool.

Informatiesysteem
De informatiesysteem informatiedrager is een drager die in staat is zelfstandig met informatie om te gaan. In tegenstelling tot de hardcopy informatiedrager is bij een informatiesysteem één van de belangrijkste taken het creëren, bewerken, verwijderen en opslaan van informatie. Een informatiesysteem kan vaak grotere hoeveelheden informatie opslaan dan een hardcopy informatiedrager. Een netwerk maakt deel uit van een informatiesysteem. Het is geen op zichzelf staande informatiedrager omdat de informatie op een netwerk niet permanent wordt opgeslagen. Een netwerk wordt gebruikt om informatie te transporteren tussen verschillende instanties van informatiesysteem informatiedragers. Een informatiesysteem informatiedrager zal in het framework worden aangegeven met het onderstaande symbool.

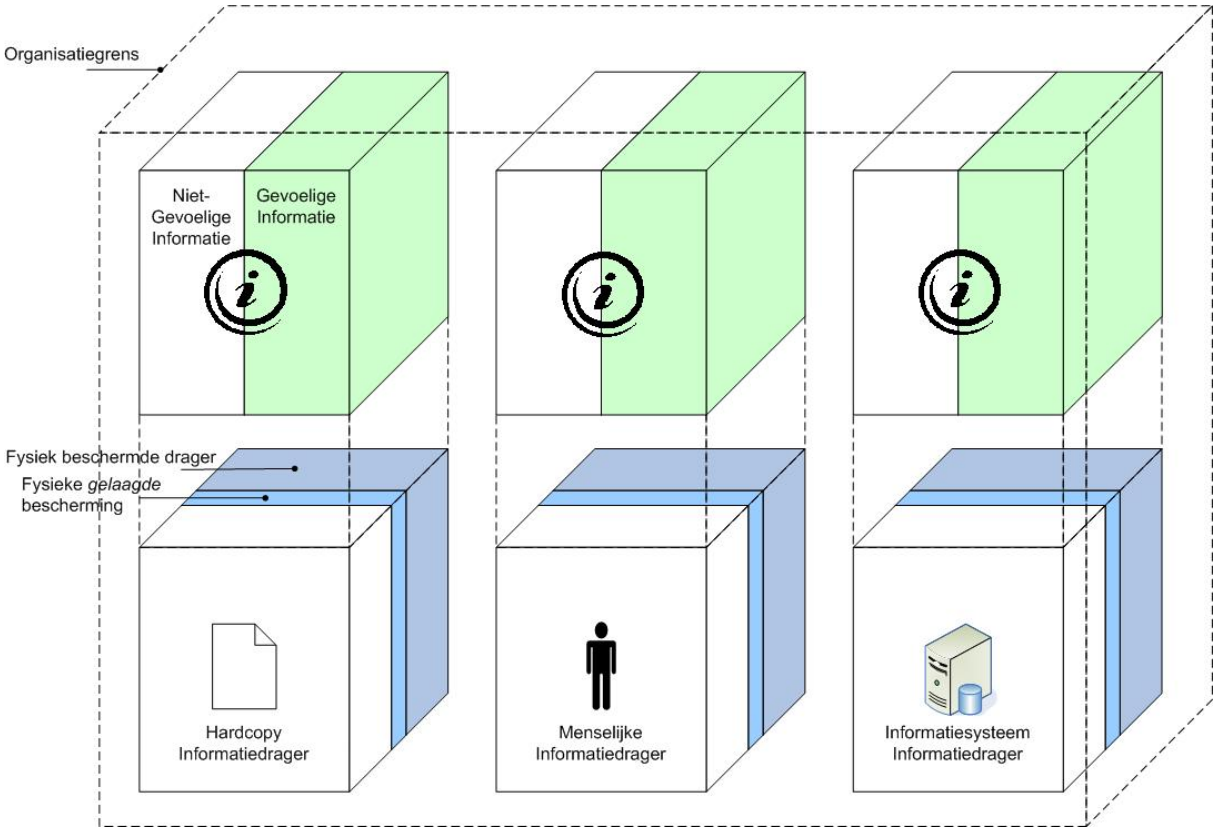
De reden dat het onderscheid in informatiedragers wordt gemaakt is dat verschillende aanvallen in de bestudeerde literatuur (zie subparagraaf 2.6.5) impliciet dit onderscheid ook al maken. Dumpster Diving, letterlijk prullenbak doorzoeken, heeft hoofdzakelijk als doel het verzamelen van informatie die staat op hardcopy informatiedragers. In de prullenbak zullen dit vooral papieren documenten zijn (tenzij je computers ook in de prullenbak gooit, een recent voorbeeld hiervan is Officier van Justitie Tonino die zijn computer bij de vuilnis zette [34]). Aanvallen zoals Impersonation en Piggybacking hebben direct betrekking op de mens en vallen daardoor eenduidig onder de menselijke informatiedrager. Aanvallen zoals de Keylogger hebben vanwege hun technisch mechanisme het duidelijk gemunt op het informatiesysteem als drager.

Gevoelige en niet gevoelige informatie

De informatie die op de verschillende informatiedragers staat wordt onderverdeeld in het type gevoelige en niet-gevoelige informatie. Dit onderscheid is fundamenteel voor Social Engineering en dit komt terug in de gebruikte definitie, uitgelegd in subparagraaf 2.2.1 en 2.2.2. Informatie wordt in het framework aangeduid met het onderstaande symbool.

Gelaagde bescherming informatiedragers

In subparagraaf 3.2.1 is aangegeven dat objecten, dus ook informatiedragers, binnen de organisatie beschermd zijn door de organisatiegrens. Hiermee wordt bedoeld dat informatiedragers fysiek binnen de organisatie niet voor iedereen toegankelijk zijn. Bescherming wordt daarom in dit framework gezien als beperkte toegang van mensen tot informatiedragers. Naast informatiedragers die beschermd worden door de organisatiegrens zijn er ook informatiedragers die voorzien zijn van *gelaagde* bescherming. Voorbeelden hiervan zijn papieren documenten in afsluitbare kasten en de opdeling van de organisatie in toegangszones waarbij beperkte toegang is toegestaan zoals serverruimtes en directiekamers.



Figuur 1: Opdeling gevoelige / niet-gevoelige informatie en gelaagde bescherming

In deze figuur is de informatiedrager met de informatie daarop uit elkaar getrokken om aan te geven dat de gevoelige en niet-gevoelige informatie haaks op de gelaagde bescherming van de informatiedrager staat. Hierdoor ontstaat een matrix waar er onderscheid gemaakt wordt tussen:

- Gevoelige informatie die gelaagd beschermd is.
- Gevoelige informatie die *niet* gelaagd beschermd is
- Niet-gevoelige informatie die gelaagd beschermd is
- Niet-gevoelige informatie die *niet* gelaagd beschermd is.

Dit onderscheid wordt gemaakt om aan te geven dat gevoelige en niet-gevoelige informatie wel of niet gelaagd beschermd kan zijn. Dit betekent dat gevoelige informatie niet per definitie altijd beschermd hoeft te zijn en in sommige gevallen relatief eenvoudig te verkrijgen is door de Social Engineer.

Verplaatsing van informatiedragers

Informatiedragers met daarop informatie kunnen zich binnen en buiten de organisatie bevinden. Een medewerker als menselijke informatiedrager kan zich bijvoorbeeld tijdens kantooruren buiten de organisatie bevinden. Een voorbeeld van de verplaatsing van de overige twee informatiedragers kan zijn een laptop of documenten die de medewerker meeneemt buiten de organisatie.

Ook kan er verplaatsing binnen een type informatiedrager plaatsvinden. Zo kan bijvoorbeeld een papieren document uit een kluis gehaald worden waardoor er geen gelaagde

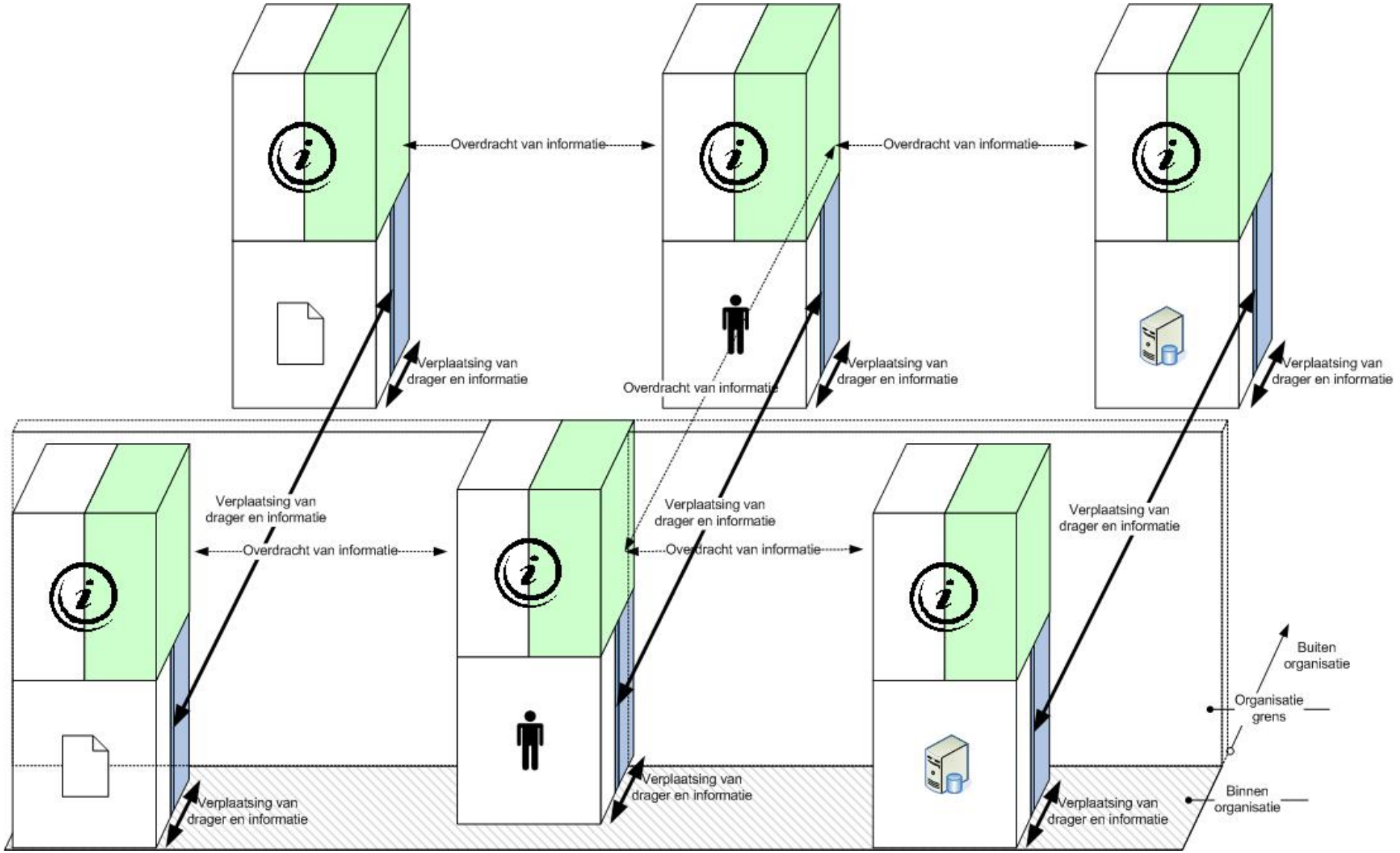
bescherming meer is. Hetzelfde geldt voor de mens en een informatiesysteem dat een bepaalde beveiligde zone verlaat.

Informatie overdracht
Naast de verplaatsing van informatiedragers is er overdracht van informatie tussen de informatiedragers mogelijk waarbij de menselijke informatiedrager het middelpunt vormt. Zo kan een mens bijvoorbeeld informatie op een document tot zich nemen en informatie op een document vastleggen of informatie uit een informatiesysteem opvragen en invoeren.

Directe overdracht van informatie van een hardcopy informatiedrager naar een informatiesysteem informatiedrager en vice versa is ook mogelijk maar niet van toegevoegde waarde voor dit framework. Deze overdracht van informatie verloopt in dit framework uitsluitend via de mens.

De reden dat de verplaatsing van informatiedragers en de overdracht van informatie is opgenomen in het framework is om aan te geven dat zowel binnen als buiten de organisatie Social Engineering aanvallen plaats kunnen vinden en dat de informatiedragers buiten de organisatie ook een belangrijk doelwit kunnen zijn voor de Social Engineer.

De verplaatsing van informatiedragers en de overdracht van informatie is schematisch weergegeven in onderstaande figuur.

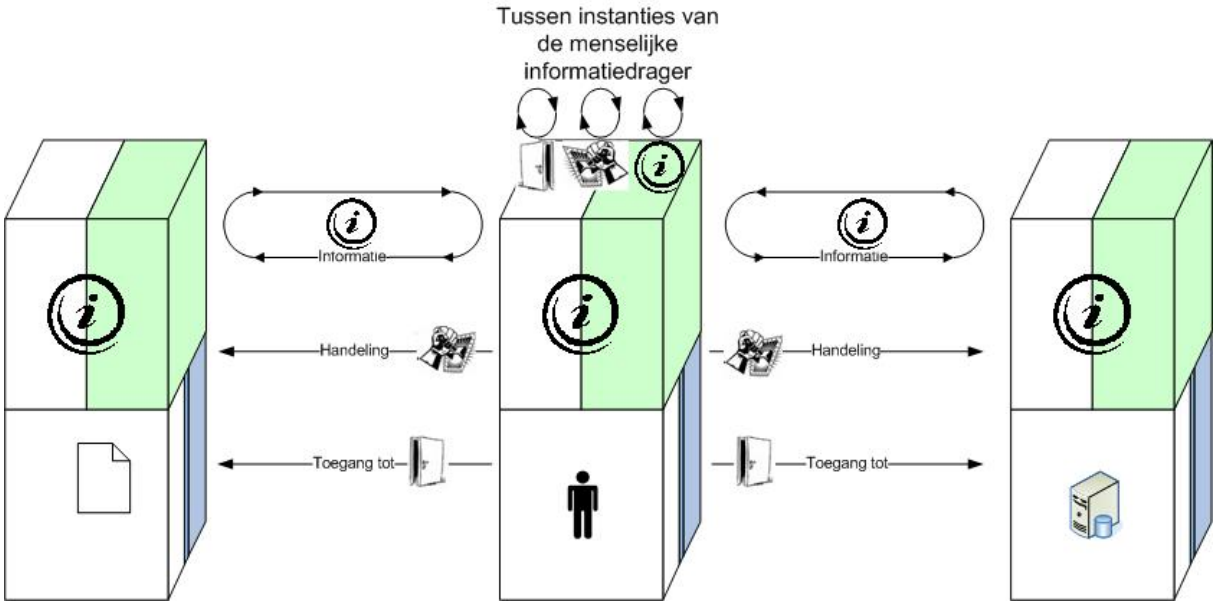


Figuur 2: Verplaatsing van informatiedragers en overdracht van informatie

Met de gestippelde pijlen wordt in figuur 2 de overdracht van informatie weergegeven. De dubbele pijl houdt in dat er van beide informatiedragers informatie over kan worden gedragen. De dikke pijlen geven de verplaatsing van de informatiedragers met informatie weer. De organisatiegrens wordt aangegeven met een transparante muur en het deel wat zich binnen de organisatie bevindt met de gearceerde ondergrond. In figuur 2 is aangegeven dat de menselijke informatiedrager voor een deel in de organisatiegrens staat. Dit heeft als reden dat Social Engineering aanvallen op de organisatiegrens alleen betrekking hebben op de menselijke informatiedrager.

3.2.3 De mens centraal bij toegang tot, handeling laten verrichten op, informatie verkrijgen uit informatiedragers

De menselijke informatiedrager speelt een belangrijke rol in het framework. Ten eerste kan de menselijke informatiedrager overdracht van informatie bewerkstelligen tussen zichzelf en de overige informatiedragers. Onder deze overige informatiedragers valt ook een andere instantie van de menselijke informatiedrager. Ten tweede kan de menselijke informatiedrager fysieke toegang hebben tot de overige informatiedragers. Zo kan de mens toegang hebben tot bepaalde hardcopy informatiedragers zoals documenten in een kluis als toegang tot informatiesystemen. De menselijke informatiedrager kan echter ook fysiek toegang hebben tot andere instanties van menselijke informatiedragers die wel of niet een gelaagde bescherming hebben. Een voorbeeld hierbij is een secretaresse die toegang heeft tot de kamer van de directeur waar de directeur zich in bevindt. Ten derde kan de menselijke informatiedrager een handeling verrichten op de overige twee informatiedragers of op een andere instantie van de menselijke informatiedrager. De menselijke informatiedrager staat centraal in het framework, dit wordt geïllustreerd aan de hand van de volgende figuur.



Figuur 3: De menselijke informatiedrager centraal

De iconen met pijlen getekend bovenop de menselijke informatiedrager houden in dat een instantie van de menselijke informatiedrager toegang heeft tot, een handeling kan verrichten op en informatieoverdracht kan plaats vinden tussen een andere instantie van de menselijke informatiedrager.

3.2.4 Plaats van de Social Engineer

In subparagraaf 3.2.1 is beschreven dat de organisatie in dit framework fysiek opgedeeld wordt in drie gebieden. De fysieke opdeling van de organisatie in drie gebieden levert in combinatie met de plaats van de Social Engineer een viertal scenario's op.

In het eerste scenario bevindt de Social Engineer Social Engineer zich buiten de organisatie en zal hij proberen één of meerdere doelen te bereiken door de menselijke informatiedrager in de organisatiegrens aan te vallen.

In het tweede scenario bevindt de Social Engineer zich buiten de organisatie en zal hij proberen één of meerdere doelen te bereiken door een informatiedrager buiten de organisatie aan te vallen. Voorwaarde hierbij is dat een informatiedrager een relatie heeft met de organisatie.

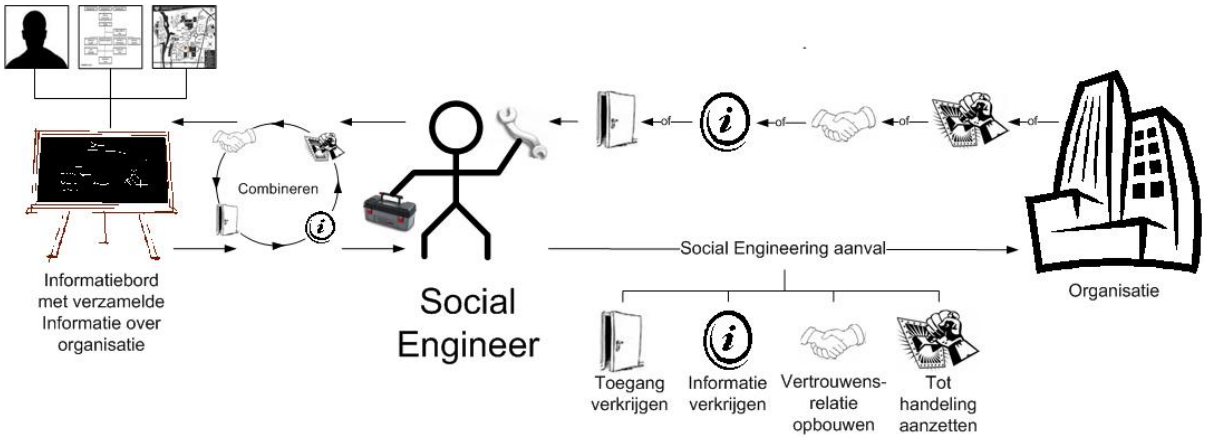
In het derde scenario bevindt de Social Engineer zich buiten de organisatie en probeert hij één of meerdere doelen te bereiken door een informatiedrager binnen de organisatie aan te vallen.

In het vierde scenario bevindt de Social Engineer zich binnen de organisatie en zal hij proberen om één of meerdere doelen te bereiken door een informatiedrager binnen de organisatie aan te vallen.

De plaats van een Social Engineer is van invloed op de strategie volgens welke de Social Engineer te werk gaat. Een Social Engineer die zich fysiek buiten een organisatie bevindt zal zich ten opzichte van een Social Engineer die zich fysiek binnen de organisatie bevindt op een andere manier voorbereiden en een andere invulling geven aan een mogelijke aanval.

3.3 Visualisatie van het Social Engineering proces

Om inzichtelijk te maken hoe in dit onderzoek invulling is gegeven aan het Social Engineering proces wordt er gebruik gemaakt van Figuur 4.



Figuur 4: Het Social Engineering "proces"

Elke Social Engineering aanval kent een voorbereidingsfase (zie paragraaf 2.5). Voor bepaalde aanvallen kan in tegenstelling tot andere aanvallen veel voorbereiding nodig zijn.

3.3.1 Aanvang

In een begin fase zal de Social Engineer nog weinig kennis hebben over de organisatie en alles wat daarmee in relatie staat. De Social Engineer zal daarom proberen zoveel mogelijk voorbereidende informatie te vergaren.

3.3.2 Voorbereiding

Om zich goed voor te bereiden op een aanval kan de Social Engineer alles wat hij op dat moment tot zijn beschikking heeft (zie het Informatiebord dat wordt weergegeven in figuur 4) proberen te combineren. Dit kunnen stukjes informatie zijn die schijnbaar op zichzelf geen waarde hebben maar in combinatie met elkaar wel waardevol (zie paragraaf 2.3) zijn.

3.3.3 Aanval

Als een Social Engineer alles wat hij tot zijn beschikking heeft voldoende acht om een aanval te kunnen uitvoeren zal hij een strategie bepalen. Deze strategie bestaat uit een vooraf opgesteld doel dat mogelijk bereikt kan worden door de wijze waarop de aanval in combinatie met de voorbereidende informatie wordt uitgevoerd. Een andere strategie die de Social Engineer kan toepassen is het willekeurig uitvoeren van een aanval waarbij het te bereiken doel niet vooraf vaststaat (zie paragraaf 2.3). De Social Engineer kan bij een aanval gebruik maken van een groot aantal gereedschappen (zie paragraaf 2.7).

3.3.4 Resultaat van een aanval

Het resultaat van een aanval heeft betrekking op het doel dat de aanval voor ogen heeft en het succes van een aanval. Dit resultaat kan de Social Engineer gebruiken om een vervolg aanval uit te voeren of als voorbereiding op een nieuwe, op zichzelf staande aanval.

In figuur 4 is te zien dat een Social Engineering aanval als resultaat toegang verkrijgen, informatie verkrijgen, een handeling uitvoeren, een vertrouwensrelatie opbouwen of een combinatie hiervan heeft. Het resultaat wordt aangegeven met de pijlen die van de organisatie naar de Social Engineer gaan. De Social Engineer kan dit resultaat combineren met informatie op het informatiebord om zo een vervolg aanval uit te voeren aangegeven met de pijlen naar de organisatie. Daarnaast kan het resultaat ook terecht komen op het informatiebord, aangegeven met de pijl van de Social Engineer naar het informatiebord, waarna het in de toekomst gebruikt kan worden voor andere aanvallen.

3.3.5 Social Engineering: een recursief proces

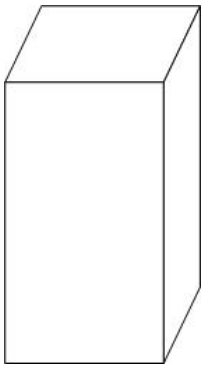
Social Engineering is een recursief proces wat betekent dat een Social Engineer voortdurend bezig is met het combineren van resultaten verkregen door voorbereiding of eerder uitgevoerde aanvallen voor het gebruik in vervolgaanvallen, om gevoelige informatie te verkrijgen. Een Social Engineer is continu bezig met het verkrijgen van inzichten en het combineren van ingrediënten om zo te bepalen welke aanval op welke manier het beste resultaat oplevert.

3.4 Het framework

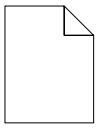
3.4.1 Gebruikte symbolen in het framework

Om Social Engineering inzichtelijk te maken zal het framework bestaan uit een aantal modellen. In deze modellen zal ter verduidelijking gebruik worden gemaakt van een aantal symbolen en matrices. De gebruikte symbolen en matrices worden hieronder beschreven.

Informatiedrager
Een informatiedrager (zie subparagraaf 3.2.2) wordt in het framework aangeduid met een rechthoek. Dit is een versimpelde weergave van een informatiedrager zoals weergeven in figuur 1 in subparagraaf 3.2.2.



Hardcopy informatiedrager
Hardcopy materiaal (zie subparagraaf 3.2.2) als informatiedrager wordt in het framework aangeduid met een A4 symbool.



Menselijke informatiedrager
De mens (zie subparagraaf 3.2.2) als informatiedrager wordt in het framework aangeduid met een symbool van een mens.

Informatiesysteem Informatiedrager
Een informatiesysteem (zie subparagraaf 3.2.2) als informatiedrager wordt in het framework aangeduid met het symbool van een server

Social Engineer
De Social Engineer als informatiedrager wordt in het framework aangeduid met een afbeelding van een van de meest bekende Social Engineers ter wereld, Face van The A-team.

Een goede beschrijving van Face wordt gegeven op één van de vele fansites van The A-team [10].

"Face was the A-Team's conman, often managing to cheat people out of everything they owned and still leave them smiling. Whatever was needed, be it a lawnmower engine (in the jungle) or an American Air Force Jet (in Peru) he could obtain it. And if the hapless victim was female it was all the easier for Face (nicknamed on account of his clean-cut good looks)"

Toegang

Een aanval kan resulteren in het fysiek toegang verkrijgen tot een bepaalde ruimte (zie subparagraaf 2.6.4). Toegang verkrijgen wordt aangegeven met het symbool van een deur. Toegang tot een bepaalde ruimte wordt als resultaat van een aanval *niet* in de framework modellen weergegeven door middel van een teruggaande pijl omdat toegang fysieke verplaatsing oplevert van de Social Engineer. In de modellen wordt wel aangegeven waar de Social Engineer zich binnen de organisatie mogelijk fysiek zou kunnen verplaatsen.

Ontvangen informatie
Een aanval kan resulteren in het verkrijgen van informatie (zie subparagraaf 2.6.4). Hiervoor wordt gebruik gemaakt van het symbool I dat staat voor informatie. Informatie als resultaat van een aanval zal in de framework modellen worden weergegeven met een teruggaande pijl aangezien de Social Engineer deze informatie kan verwerken en combineren waardoor de informatie op een later tijdstip van waarde kan zijn.

(Vertrouwens)relatie opbouwen
Een aanval kan resulteren in een verandering van de vertrouwensrelatie tussen de mens en de Social Engineer (zie subparagraaf 2.6.4), hiervoor wordt gebruikt gemaakt van het onderstaande symbool. Een verandering van de vertrouwensrelatie als resultaat van een aanval zal in de framework modellen worden weergegeven met een teruggaande pijl aangezien de Social Engineer deze verandering in de vertrouwensrelatie in de toekomst kan gebruiken voor een vervolg aanval.

Handeling
Een aanval kan resulteren in het laten verrichten van een handeling door de mens (zie subparagraaf 2.6.4). Een handeling wordt aangegeven met het onderstaande symbool. Een Social Engineer weet van te voren wat hij wil bereiken met het laten uitvoeren van een handeling. In de framework modellen wordt alleen aangegeven waar aanvallen om een handeling te laten verrichten kunnen worden uitgevoerd. Een voorbeeld van een handeling is de mens bepaalde informatie uit een informatiesysteem te laten verwijderen.

Aanval matrices
Voor de representatie van een aanval wordt gebruik gemaakt van een aanvalsmatrix. Deze matrix bestaat uit een identificatienummer om een unieke aanval te identificeren, de naam van de aanval, een kleur voor directe / indirecte benadering, rij voor fysiek, rij voor medium en tenslotte een kolom om de doelen aan te geven die met de aanval bereikt kunnen worden.

Het identificatienummer (1) van een aanval wordt weergeven in een cirkel met de kleur wit of zwart. Een zwarte cirkel heeft betrekking op een directe aanval, een witte cirkel heeft betrekking op een indirecte aanval.

Directe Aanval

Indirecte aanval

De aanval matrix kan worden ingevuld door vinkjes te zetten op de desbetreffende plaatsen die van toepassing zijn bij een aanval. De horizontaal geplaatste letters T, I, R, H staan voor **T**oegang, **I**nformatie, **R**elatie, **H**andeling. De verticaal geplaatste letters F en M staan voor de methode van Benadering **F**ysiek, **M**edium.

1

Naam van de aanval				
	T	**I**	**R**	**H**
F	✓		✓	
M		✓		✓

Aanval via de mens
Om een aanval aan te geven die via de mens verloopt naar een andere informatiedrager en waarvan het resultaat informatie verkrijgen of een vertrouwensrelatie opbouwen betreft, wordt gebruik gemaakt van de bij de aanval horende cirkel met identificatienummer waarvan de buitenste rand een onderbroken lijn is.

Directe Aanval

Indirecte aanval

3.4.2 Identificatie van Social Engineering aanvallen

In de onderstaande matrices wordt per Social Engineering aanval weergegeven welke doelen bereikt kunnen worden, of een aanval direct of indirect wordt uitgevoerd, of de aanval fysiek of via een medium wordt uitgevoerd en tenslotte wat het identificatienummer van de aanval is in dit onderzoek.

1 Piggybacking

	T	I	R	H
F	✓			
M				

2 Tailgating

	T	I	R	H
F	✓			
M				

3 Impersonation

	T	I	R	H
F	✓	✓	✓	✓
M		✓	✓	✓

4 Reverse SE

	T	I	R	H
F		✓	✓	✓
M		✓	✓	✓

5 Shoulder surfing

	T	I	R	H
F		✓		
M				

6 Dumpster diving

	T	I	R	H
F		✓		
M				

7 Profiling

	T	I	R	H
F		✓		
M				

8 Desk sniffing

	T	I	R	H
F		✓		
M				

9 Eavesdropping

	T	I	R	H
F		✓		
M				

10 Phishing

	T	I	R	H
F				
M		✓		

11 Keylogger

	T	I	R	H
F		✓		
M				

12 Item dropping

	T	I	R	H
F				✓
M				

3.4.3 De modellen

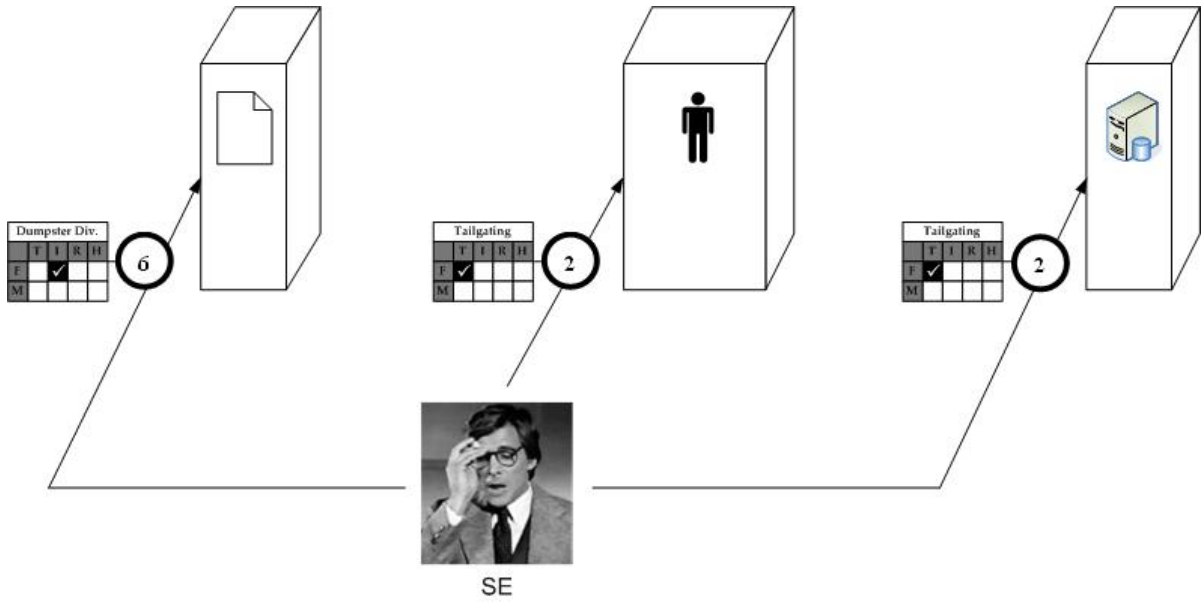
In subparagraaf 3.2.1 en 3.2.4 is aangegeven dat een organisatie fysiek kan worden opgedeeld in een aantal organisatiegebieden en dat een Social Engineering aanval afhankelijk is van de plaats van de Social Engineer. Dit leidt tot een framework dat bestaat uit vier modellen namelijk:

- Social Engineering aanvallen van buiten de organisatie op organisatiegrens
- Social Engineering aanvallen van buiten de organisatie op informatiedragers buiten de organisatie
- Social Engineering aanvallen van buiten de organisatie binnenin de organisatie
- Social Engineering aanvallen binnen de organisatie

In deze paragraaf wordt verduidelijkt hoe de modellen precies gelezen en geïnterpreteerd moeten worden.

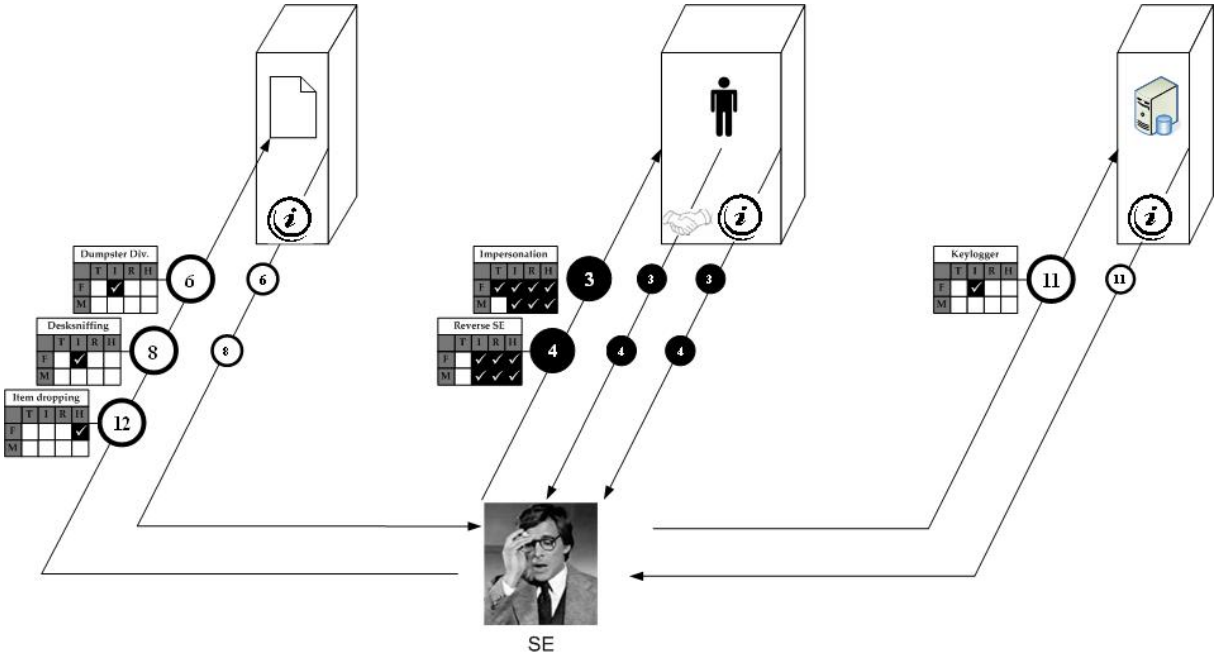
Om te beginnen wordt elk model beschouwd vanuit de invalshoek van de Social Engineer, in dit geval “Face” van the A-team [10].

Door de Social Engineer te positioneren tegenover de verschillende informatiedragers binnen en buiten de organisatie ontstaat er een driedimensionaal beeld. Hierin wordt door middel van pijlen vanuit de Social Engineer aangegeven welke aanvallen hij vanuit die positie kan uitvoeren. Een voorbeeld hiervan wordt in de volgende figuur weergegeven.



Figuur 5: Visualisatie van Social Engineering aanvallen op informatiedragers

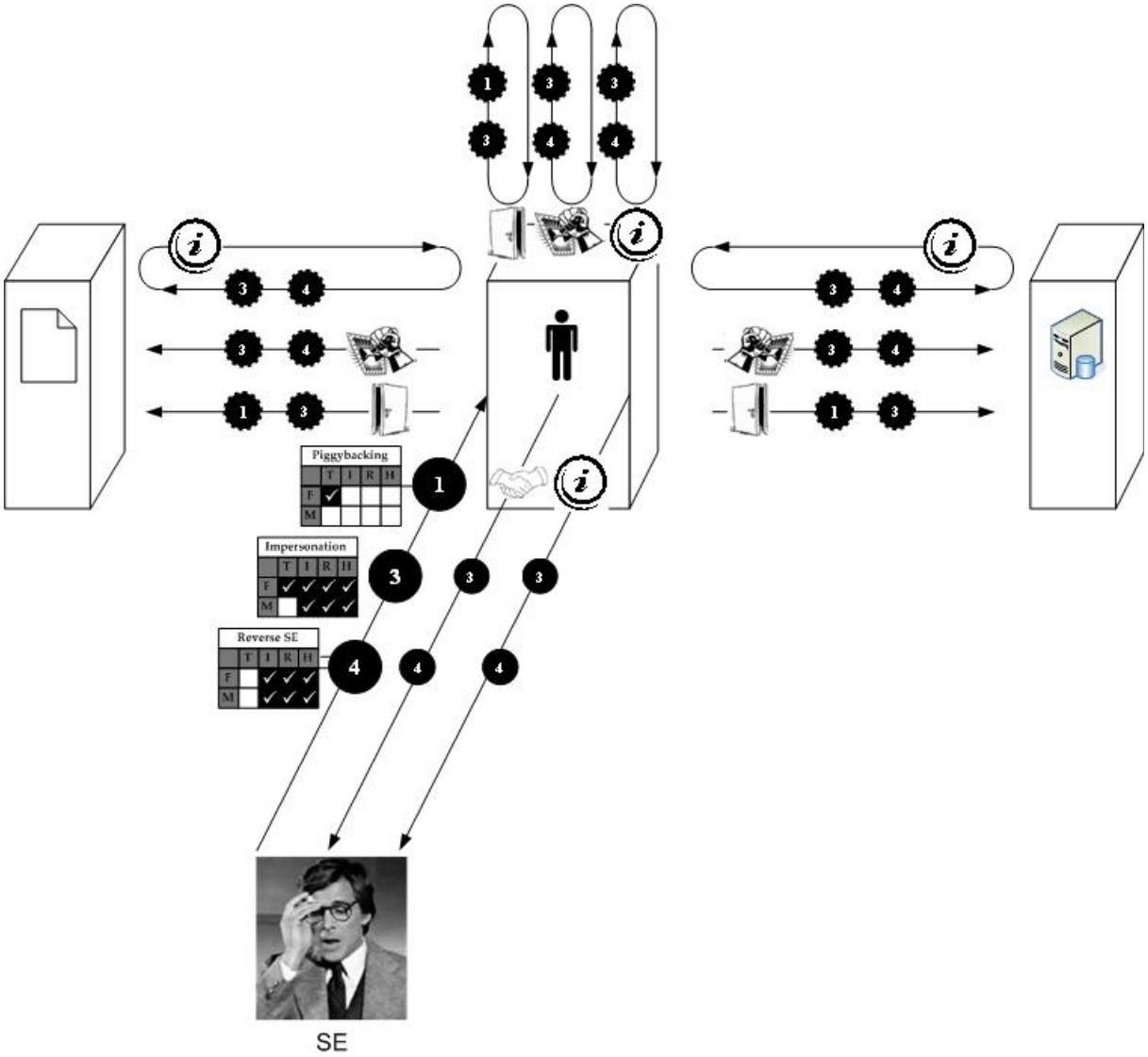
In figuur 6 geven de teruggaande pijlen van de verschillende informatiedragers richting de Social Engineer het resultaat aan van de verschillende aanvallen waarbij er informatie wordt verkregen of een vertrouwensrelatie wordt opgebouwd. Op deze pijlen wordt met behulp van cirkels met daarin identificatienummers aangegeven welke aanvallen dit resultaat bewerkstelligen. In de volgende figuur wordt een voorbeeld gegeven van hoe het resultaat van een aanval wordt weergegeven.



Figuur 6: Resultaat van Social Engineering aanvallen op informatiedragers

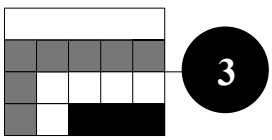
In figuur 7 wordt weergegeven dat de menselijke informatiedrager het middelpunt vormt in de verschillende framework modellen. Veel Social Engineering aanvallen verlopen via deze menselijke informatiedrager omdat deze toegang heeft tot, handelingen uit kan voeren op en informatie overdracht kan bewerkstelligen tussen de menselijke informatiedrager en de twee andere informatiedragers (zie subparagraaf 3.2.3). Om het verloop van deze aanvallen duidelijk weer te geven wordt er gebruik gemaakt van pijlen tussen de menselijke informatiedrager en de twee overige informatiedragers. Bij deze pijlen wordt door middel van een icoon aangegeven welk doel er wordt verwezenlijkt en wordt er door middel van identificatienummers aangegeven welke aanvallen hierop betrekking hebben. Bepaalde aanvallen hebben als doel het verkrijgen van informatie. Hoe deze informatie via de menselijke informatiedrager uit de twee overige informatiedragers wordt verkregen wordt aangegeven met een pijl richting de menselijke informatiedrager en een pijl terug met daarop het informatie icoon. Ook zijn er Social Engineering aanvallen tussen twee instanties van de menselijke informatiedrager mogelijk. Hierbij is het mogelijk om via de menselijke informatiedrager toegang te krijgen tot, informatie te verkrijgen van en een handeling te verrichten op een andere instantie van de menselijke informatiedrager. Zowel informatieoverdracht uit instanties van de mens als hardcopy en informatiesysteem informatiedragers vindt hierbij plaats via de menselijke informatiedrager waarna de informatie overgedragen wordt aan de Social Engineer. Informatieoverdracht uit hardcopy- en informatiesysteem informatiedragers vindt hierbij plaats via de mens waarna de

informatie overgedragen wordt aan de Social Engineer. Een voorbeeld hiervan wordt weergegeven in de volgende figuur.



Figuur 7: Social Engineering aanvallen via de mens op overige informatiedragers

Bepaalde aanvallen zijn contextspecifiek. Dit betekent dat de doelen die een aanval kan bereiken afhankelijk zijn van de positie van de Social Engineer ten opzichte van de organisatie en het organisatiegebied waarop de aanval betrekking heeft (zie subparagraaf 3.2.1). In elk model wordt er per aanval in de matrix aangegeven welke doelen in deze context mogelijk bereikt kunnen worden. De doelen die in deze context mogelijk bereikt kunnen worden zullen in de matrix met een zwarte achtergrond worden weergegeven (zie onderstaande figuur).



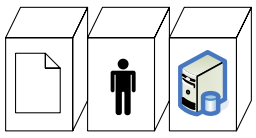
Figuur 8: Weergave matrix bereikbare doelen in context

Daarnaast zijn er nog enkele contextspecifieke eigenschappen die per model verschillend zijn. Deze worden per model beschreven.

3.4.4 Model 1: Social Engineering aanvallen op organisatiegrens

Opmerkingen bij model 1
In dit model worden de Social Engineering aanvallen aangegeven die uitgevoerd kunnen worden op het organisatiegebied "organisatiegrens" waarbij de Social Engineer zich in het organisatiegebied "buiten de organisatie" bevindt. In de organisatiegrens die met grijs is aangegeven is de menselijke informatiedrager weergegeven. Hiermee wordt aangegeven dat de menselijke informatiedrager zich in de organisatiegrens kan bevinden. Andere dragers hebben geen toegevoegde waarde in de organisatiegrens omdat er in dit scenario geen Social Engineering aanvallen op toepasbaar zijn. Er wordt per aanval in de bijbehorende matrix weergegeven welke doelen er bereikt kunnen worden en of de aanval fysiek plaatsvindt of via een medium verloopt en of de aanval indirect of direct is.

In deze situatie zijn alle aanvallen gericht op de menselijke informatiedrager in de organisatiegrens. Via de menselijke informatiedrager in de organisatie kan de Social Engineer toegang verkrijgen tot de organisatie waardoor hij in theorie ook toegang kan verkrijgen tot de drie verschillende informatiedragers binnen de organisatie. Behalve het verkrijgen van toegang kan de Social Engineer ook de menselijke informatiedrager in de organisatiegrens een handeling laten verrichten, er een vertrouwensrelatie mee opbouwen of er informatie van verkrijgen. De handeling die de Social Engineer de menselijke informatiedrager in de organisatiegrens wil laten verrichten heeft betrekking op de informatiedragers die zich binnen de organisatie bevinden. Daarnaast kan er ook een aanval uitgevoerd worden die via de menselijke informatiedrager in de organisatiegrens verloopt en waarbij er informatie wordt verkregen uit informatiedragers binnen de organisatie. Deze informatiedragers binnen de organisatie worden als volgt weergegeven:



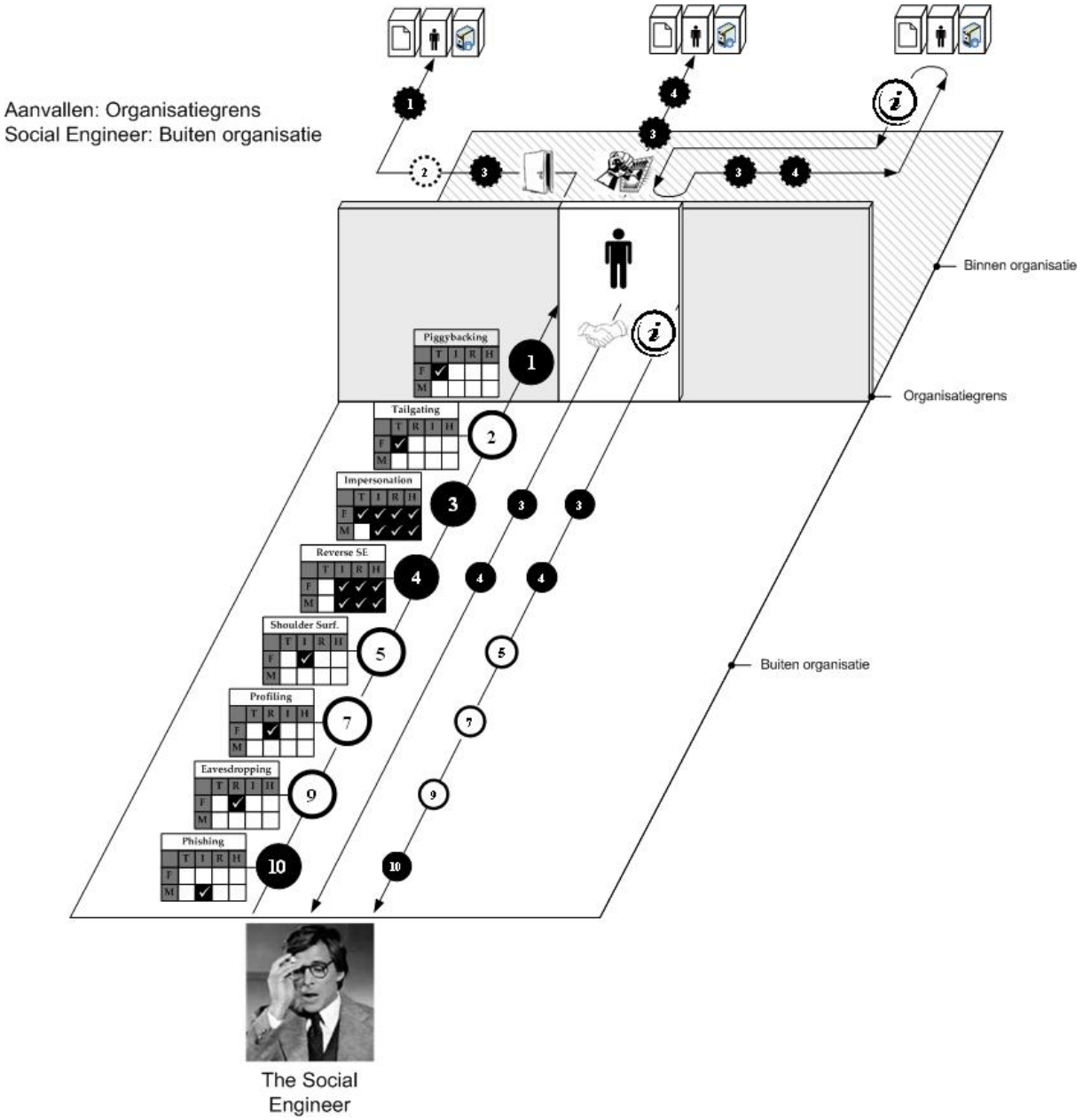
De weergave van model 1 wijkt af van de overige modellen. Dit heeft te maken met de overzichtelijkheid van het model.

Om te verduidelijken hoe een aanval precies in dit model verloopt, zal er een voorbeeld gegeven worden.

De Social Engineer wil zich toegang verschaffen tot het organisatiegebied "binnen de organisatie". Om dit voor elkaar te krijgen moet hij fysiek door de organisatiegrens heen gaan. Om dit voor elkaar te krijgen gebruikt hij de Impersonation aanval. Hij doet zich voor als iemand van de keuringsdienst van waren en meldt zich bij de receptie van de organisatie

die verantwoordelijk is voor de toegangscontrole. De Social Engineer geeft aan dat hij een onaangekondigde inspectie komt doen naar de kwaliteit van het eten in de bedrijfskantine. Omdat de receptionist constateert dat de inspectie aangekondigd is vraagt ze om identificatie of de inspecteur wel daadwerkelijk van de keuringsdienst van waren is. De Social Engineer heeft van te voren een officieel uitziende badge gemaakt met het logo van de keuringsdienst van waren erop. Hij laat de badge zien waarna hij door de receptioniste wordt doorgelaten. De Social Engineer bevindt zich nu in het organisatiegebied "binnen de organisatie".

Deze aanval is in het model weergegeven met nummer 3. Zoals te zien is in de matrix kan met deze aanval alleen fysiek toegang worden verkregen. De aanval vindt plaats op de menselijke informatiedrager in organisatiegebied "organisatiegrens". Vanuit deze informatiedrager, aangegeven met de witte rechthoek, verschaft de aanval in principe toegang tot alledrie de informatiedragers in de organisatie. Dit is aangegeven door middel van een pijl met het "toegang" icoon en het nummer van de aanval die wijst naar de afbeelding met de drie informatiedragers.



Figuur 9: Social Engineering aanvallen op organisatiegrens (model 1)

3.4.5 Model 2: Social Engineering aanvallen buiten de organisatie

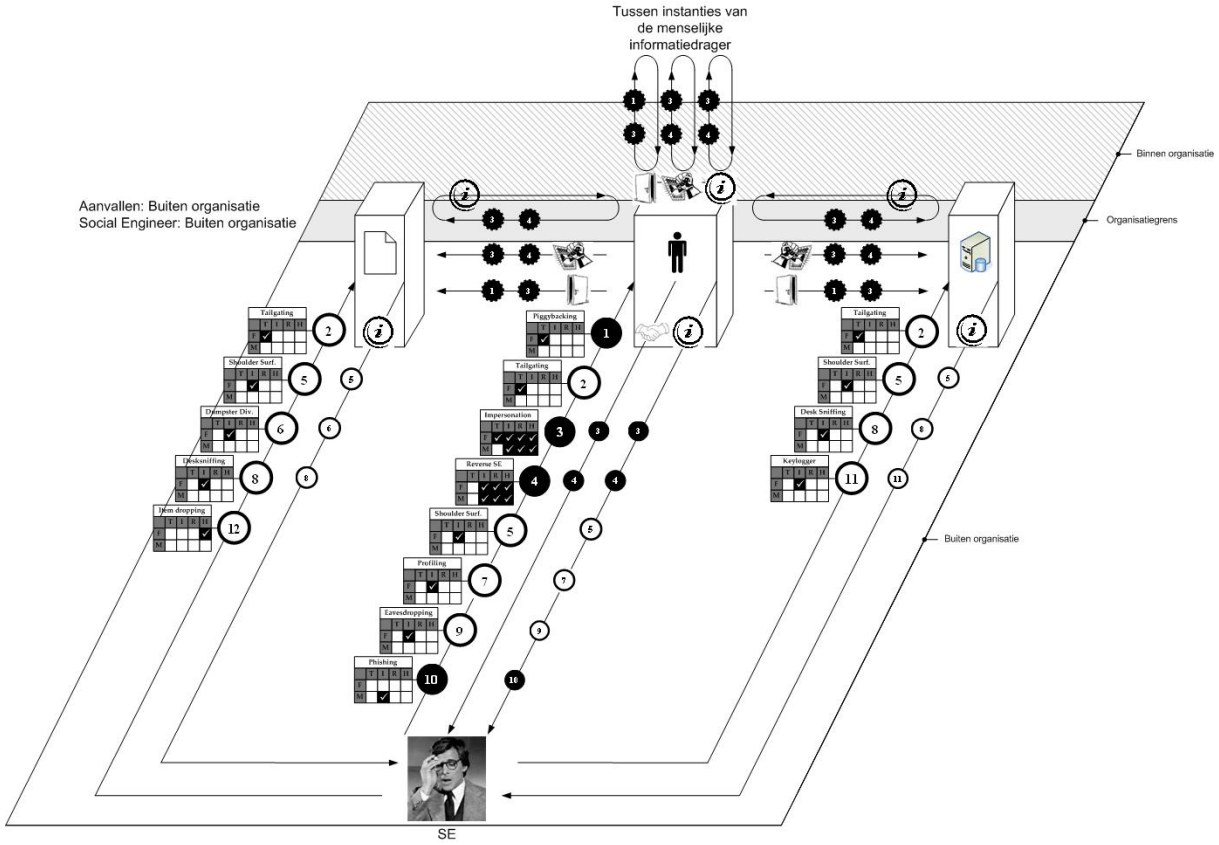
Opmerkingen bij model 2
In dit model worden de Social Engineering aanvallen aangegeven die uitgevoerd kunnen worden op het organisatiegebied "buiten de organisatie" waarbij de Social Engineer zich in het organisatiegebied "buiten de organisatie" bevindt. Er wordt per aanval in de bijbehorende matrix weergegeven welke doelen er bereikt kunnen worden en of de aanval fysiek plaatsvindt of via een medium verloopt en of de aanval indirect of direct is.

In dit model is te zien dat veel aanvallen via de mens verlopen en dat sommige aanvallen uitgevoerd kunnen worden op meerdere informatiedragers. Om te verduidelijken hoe een aanval die via de mens verloopt in dit model wordt weergegeven zal er door middel van een voorbeeld een aanval uitgewerkt worden.

Een medewerker zit in de trein te werken met gevoelige documenten. De Social Engineer kan naast of achter de medewerker gaan zitten om zo een Shoulder Surfing aanval uit te voeren. Door de gevoelige documenten ongemerkt te bekijken kan hij waardevolle informatie verkrijgen die hij wellicht in de toekomst kan gebruiken voor een vervolgaanval.

In het model is de aanval met nummer 5 door een witte cirkel aangegeven waaruit blijkt dat het om een indirecte aanval gaat. In de bijbehorende matrix staat dat deze aanval in deze situatie alleen fysiek uitgevoerd kan worden en dat enige doel wat bereikt kan worden het verkrijgen van informatie is.

Het resultaat van de aanval is aangegeven met de teruggaande pijl met het "ontvangen informatie"icoon waarmee is aangegeven dat de aanval met nummer 5 er voor zorgt dat er informatie bij de Social Engineer terugkomt. In het model is te zien dat Shoulder Surfing bij alledrie de informatiedragers kan plaatsvinden. In dit voorbeeld wordt er alleen informatie verkregen wat er in de gevoelige documenten staat en is dus alleen de aanval van toepassing op de hardcopy informatiedrager.



Figuur 10: Social Engineering aanvallen buiten de organisatie (model 2)

3.4.6 Model 3: Social Engineering aanvallen binnen de organisatie van buitenaf

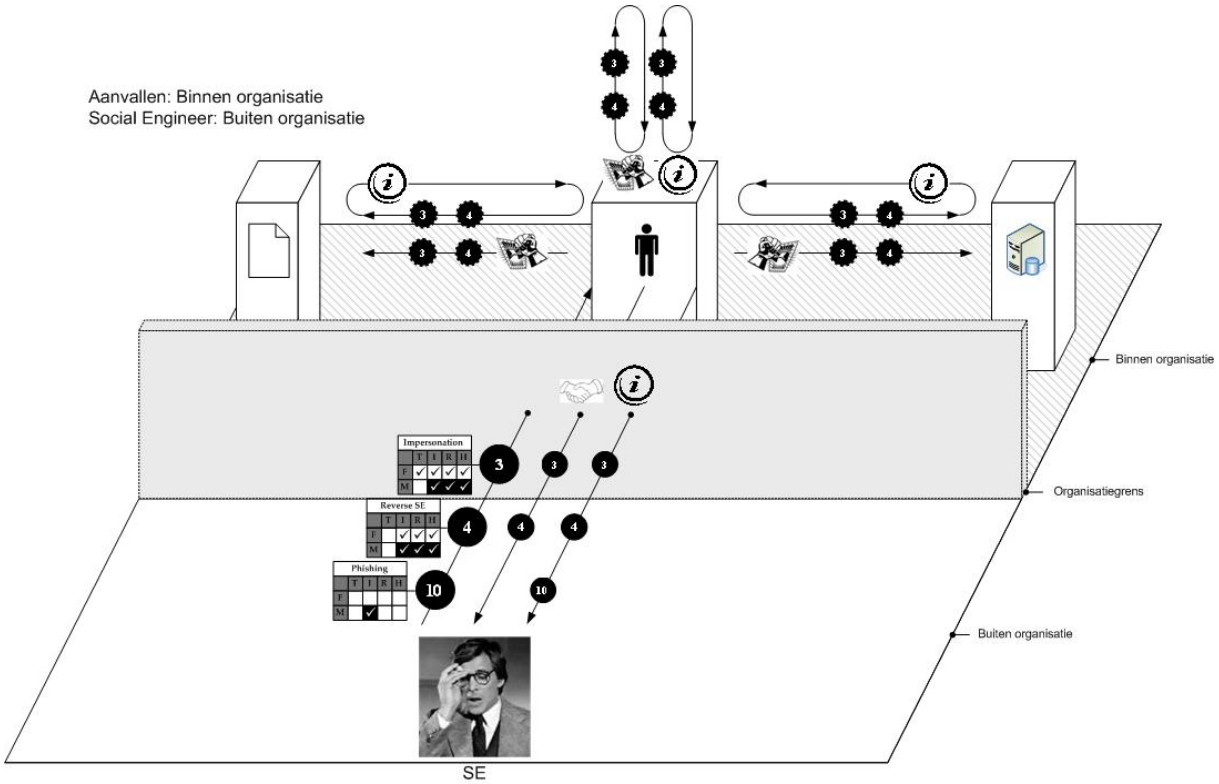
Opmerkingen bij model 3
In dit model worden de Social Engineering aanvallen aangegeven die uitgevoerd kunnen worden op het organisatiegebied "binnen de organisatie" waarbij de Social Engineer zich in het organisatiegebied "buiten de organisatie" bevindt. Er wordt per aanval in de bijbehorende matrix weergegeven welke doelen er bereikt kunnen worden en of de aanval fysiek plaatsvindt of via een medium verloopt en of de aanval indirect of direct is.

Er kunnen in dit scenario maar weinig aanvallen plaatsvinden. De aanvallen die hier uitgevoerd kunnen worden zijn alleen van toepassing op de menselijke informatiedrager. Ook is in de matrices bij de aanvallen te zien dat de aanvallen alleen kunnen plaatsvinden via een medium. Om het model te verduidelijken zal één aanval aan de hand van een voorbeeld beschreven worden.

Een Social Engineer kan een Phishing aanval uitvoeren om zo gevoelige informatie zoals inloggegevens van een medewerker te verkrijgen. Dit doet de Social Engineer door bijvoorbeeld een medewerker een e-mail te sturen met daarin de vraag of hij zich wil aanmelden voor het online smoelenboek van de organisatie. Aangegeven wordt dat dit een intern initiatief is om collega's dichter bij elkaar te brengen ter bevordering van de interne communicatie en bedrijfsvoering. De e-mail ziet er professioneel en authentiek uit waaruit de medewerker constateert dat deze ook daadwerkelijk bij de organisatie vandaan komt. In de e-mail wordt er gevraagd om naar een webpagina te gaan waar een online invulformulier staat en daar de gebruikersnaam en het wachtwoord wat de medewerker intern gebruikt in te vullen(b.v. voor het intranet), zodat de organisatie de medewerker kan identificeren. Hierna wordt aangegeven of de medewerker wel of niet is opgenomen in het smoelenboek.

De e-mail en de webpagina zijn niet van de organisatie maar van de Social Engineer waardoor hij in het bezit komt van gebruikersnamen en wachtwoorden. De medewerker heeft echter niets in de gaten.

Deze aanval is in het model weergegeven met nummer 10. Zoals te zien is kan de aanval alleen via een medium plaatsvinden en is het doel van de aanval het verkrijgen van informatie. Daarnaast is te zien dat de positie van de Social Engineer fysiek in het organisatiegebied "buiten de organisatie" is en dat de aanval plaatsvindt op een medewerker die zich fysiek in het organisatiegebied "binnen de organisatie" bevindt. Het medium zorgt er dus voor dat de Social Engineer organisatiegebieden kan overbruggen. Het resultaat van de aanval is weergegeven met teruggaande pijl met "verkregen informatie" icoon en het nummer van de aanval.



Figuur 11: Social Engineering aanvallen binnen organisatie van buitenaf (model 3)

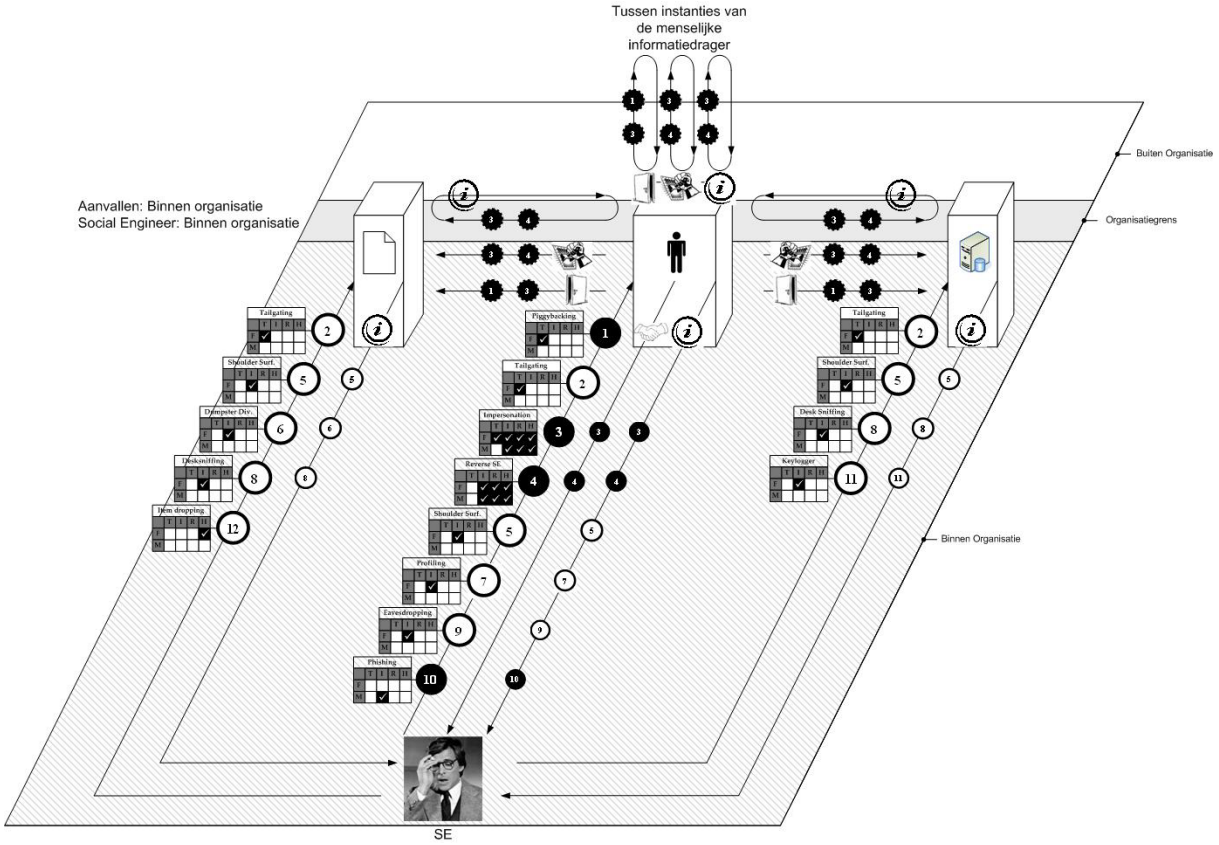
3.4.7 Model 4: Social Engineering aanvallen binnen de organisatie

Opmerkingen bij model 4
In dit model worden de Social Engineering aanvallen aangegeven die uitgevoerd kunnen worden op het organisatiegebied "binnen de organisatie" waarbij de Social Engineer zich in het organisatiegebied "binnen de organisatie" bevindt. Er wordt per aanval in de bijbehorende matrix weergegeven welke doelen er bereikt kunnen worden en of de aanval fysiek plaatsvindt of via een medium verloopt en of de aanval indirect of direct is.

In dit scenario zijn ook de meeste aanvallen gericht op de menselijke informatiedrager. Via deze informatiedrager kan de Social Engineer ook informatie, toegang tot of handeling verrichten op de andere twee informatiedragers. Om aan te geven hoe dit in zijn werk gaat zal het model aan de hand van een voorbeeld worden verduidelijkt.

Een Social Engineer wil toegang krijgen tot de archiefkamer van een organisatie die voorzien is van toegangscontrole door middel van een toegangspas. Om toegang te krijgen voert hij een Piggybacking aanval uit. Hij wacht zijn kans af totdat een andere medewerker van plan is de archiefkamer in te gaan. Net op dat moment komt de Social Engineer ook aangelopen met een groot aantal ordners. De medewerker ziet dat de Social Engineer zijn handen vol heeft en niet in staat is zijn pas te gebruiken om de deur te openen. Daarom maakt de medewerker de deur met zijn pas open zodat beide naar binnen kunnen. Op deze manier heeft de Social Engineer zichzelf toegang verschaft tot een beschermde ruimte.

Deze aanval is in het model weergegeven met nummer 1. Zoals te zien is in het model heeft deze aanval alleen als doel het fysiek toegang verkrijgen tot een ruimte. Ook is te zien dat de aanval zich richt op de menselijke informatiedrager. Via de mens is de Social Engineer in staat zich toegang te verschaffen tot een ruimte met daarin hardcopy informatiedragers, in dit geval de archiefkamer. Dit is in het model aangegeven met een pijl met het "toegang" icoon die naar de hardcopy informatiedrager wijst met daarop nummer 1.



Figuur 12: Social Engineering aanvallen binnen de organisatie (model 4)

3.5 Resultaten

In dit hoofdstuk is een poging gedaan om met de begripsbepaling als basis een verdere structuur aan te brengen in het onderwerp Social Engineering door een conceptueel framework op te stellen.

In het framework is aangegeven dat een organisatie kan worden opgedeeld in drie organisatiegebieden. Daarnaast wordt onderscheid gemaakt tussen drie verschillende informatiedragers met daarop informatie die gevoelig of niet-gevoelig kan zijn voor de organisatie. Ook wordt uiteengezet dat informatiedragers gelaagd beschermd kunnen zijn. Vervolgens is schematisch weergegeven dat informatiedragers zich tussen de verschillende organisatiegebieden kunnen verplaatsen. Deze gegevens zijn gecombineerd met de aanvallen uit de begripsbepaling en de positie van de Social Engineer, weergegeven in vier modellen. Per model wordt gevisualiseerd waar en welke Social Engineering aanvallen er plaats kunnen vinden, welke doelen per aanval bereikt kunnen worden en wat de positie is van de Social Engineer. Hieruit is te concluderen dat de positie van de Social Engineer en het organisatiegebied met daarin informatiedragers bepalend zijn voor welke aanvallen er uitgevoerd kunnen worden en welke doelen deze aanvallen kunnen bereiken.

In het volgende hoofdstuk wordt beschreven hoe de resultaten uit hoofdstuk 2 en 3 getoetst zijn bij de overheid.

4 De ministeries

4.1 Opzet en uitvoering interviews

Met de interviews gehouden bij de verschillende ministeries is geprobeerd door middel van gerichte vragen onderzoeksvraag 2 te beantwoorden. In deze paragraaf zal aangegeven worden hoe het interview is opgezet, welke voorwaarden er aan het interview gesteld zijn, hoe het acquisitieproces verlopen is en hoe de representativiteit van het interview gewaarborgd is

Opzet van het interview
In het eerste deel van het interview zijn vragen gesteld met betrekking tot de herkenning van en bescherming tegen Social Engineering. Het tweede deel van het interview richt zich vooral op maatregelen tegen Social Engineering en de naleving hiervan. In het derde deel van het interview is er een aantal scenario's voorgelegd. Afhankelijk van de mogelijkheid of een scenario zou kunnen plaatsvinden binnen een onderdeel van een ministerie worden er vanuit verschillende invalshoeken vragen gesteld. Het vierde deel van het interview richt zich op de locatie en waarde van informatie binnen het ministerie of onderdeel daarvan. De onderverdeling is gebaseerd op de begripsbepaling en het conceptueel framework.

Voorwaarden ministeries
De ministeries hebben een aantal voorwaarden gesteld waaraan voldaan moest worden voordat er medewerking werd verleend aan het onderzoek. Deze voorwaarden hebben betrekking op de omgang met de interview resultaten, goedkeuring over de uitwerking van de interviews en publicatie. Deze voorwaarden zijn opgenomen als bijlage 1 in deze scriptie.

Acquisitie
Om te onderzoeken of de overheid beschermd is tegen Social Engineering is een poging gedaan om alle ministeries waaruit de nationale overheid bestaat te benaderen voor medewerking aan dit onderzoek. Deze acquisitie leverde op dat slechts drie ministeries haar medewerking wilden verlenen. Omdat Social Engineering onderdeel uitmaakt van informatiebeveiliging is geprobeerd om voor dit onderzoek personen te interviewen met een beveiligingsachtergrond. Deze personen dienden betrokken te zijn bij de ontwikkeling en/of uitvoering van het informatiebeveiligingsbeleid. De tweede acquisitie ronde leverde vervolgens een aantal personen op dat bereid was mee te werken aan het onderzoek en voldeed aan de gewenste voorwaarden.

Representativiteit
Omdat slechts drie van de dertien ministeries bereid waren mee te werken is het lastig dan wel onmogelijk om uitspraken te kunnen doen over de gehele overheid. De uitkomsten van het interview om deelvraag 2.1 te beantwoorden en een algemeen advies op te stellen zijn daarom alleen van toepassing op de drie deelnemende ministeries. Dit betekent echter niet dat het antwoord op de onderzoeksvraag en het algemeen advies geen toegevoegde waarde kan hebben voor de overige niet deelnemende ministeries of organisaties in het algemeen.

Alle geïnterviewde personen zijn betrokken bij de informatiebeveiliging van een ministerie of onderdeel daarvan. Daarom wordt er in dit onderzoek vanuit gegaan dat de geïnterviewde personen op de hoogte zijn van alle zaken omtrent informatiebeveiliging. In de interviews wordt bij bepaalde vragen om de mening van de geïnterviewde(n) gevraagd. Omdat de wijze waarop zij tegen het onderwerp aan kijken bepalend zal zijn bij de ontwikkeling of uitvoering van het beleid wordt dit beschouwd als geldend voor het ministerie of onderdeel daarvan.

4.2 Verwerking interviewresultaten

In deze paragraaf wordt beschreven hoe de resultaten uit de verschillende interviews verwerkt zijn. Nadat de verschillende interviews zijn afgenomen, zijn de resultaten per interview vastgelegd in een interviewverslag. Omdat de interviews gebaseerd zijn op open interviewvragen is bij de vastlegging van de interviewresultaten vooral gekeken naar de relevantie van het antwoord ten opzichte van de vraag. Overbodige informatie per vraag is alleen opgenomen als het een bijdrage leverde aan antwoorden op andere interviewvragen.

De verschillende interviewverslagen zijn teruggekoppeld naar de geïnterviewden zodat zij hun goedkeuring konden geven voor het gebruik van deze informatie voor het onderzoek. Nadat iedere geïnterviewde zijn reactie op het interviewverslag heeft gegeven is waar nodig het interviewverslag bijgewerkt.

Nadat alle interviewverslagen zijn goedgekeurd wordt er bepaald wat de verschillende ministeries tegen Social Engineering doen om zo onderzoeksvraag 2.1 te beantwoorden. Om uitspraken te kunnen doen over wat de drie ministeries tegen Social Engineering doen wordt als eerste bepaald wat de overeenkomsten en verschillen zijn tussen de onderdelen binnen een ministerie. De overeenkomsten tussen de verschillende onderdelen zijn gebruikt om resultaten te verkrijgen over wat er per ministerie gedaan wordt tegen Social Engineering. Hierna wordt bepaald welke overeenkomsten er tussen de verschillende ministeries zijn om zo een uitspraak te kunnen doen over wat zij alle drie doen tegen Social Engineering. De resultaten en de beantwoording van onderzoeksvraag 2.1 worden beschreven in paragraaf 5.1.

Ook zullen de overeenkomsten tussen de drie ministeries vergeleken worden met de begripsbepaling en het conceptueel framework. De resultaten die hieruit volgen zullen verwerkt worden in een algemeen advies voor de betrokken ministeries waarin zal staan aan welke punten met betrekking tot Social Engineering er nog (extra) aandacht moet worden besteed. Vanwege de voorwaarden die de ministeries stellen aan het gebruik en de verwerking van de interviewresultaten zal het advies een algemeen karakter hebben (zie paragraaf 4.1). Dit betekent dat afdelingen en ministeries niet bij naam en toenaam worden genoemd zodat niet kan worden afgeleid van welk ministerie en welk onderdeel de verschillende resultaten afkomstig zijn. Dit heeft de volgende gevolgen voor de manier waarop de resultaten verwerkt worden.

Alle overeenkomsten tussen de ministeries zullen per interviewdeel worden samengevat. De overeenkomsten zullen vervolgens vergeleken worden met de begripsbepaling en het framework waaruit verschillende conclusies getrokken worden. De conclusies worden gebruikt in het opstellen van het advies weergegeven in paragraaf 4.4.

De reden dat de overeenkomsten tussen de ministeries worden vergeleken met de begripsbepaling en het framework is om vast te stellen wat de afwijkingen bij de ministeries zijn. Door eerst alle overeenkomsten per ministerie te bepalen hoeft er vanwege de algemene aard van het advies maar één keer de vergelijking met de begripsbepaling en het framework gemaakt te worden. Alle afwijkingen die worden geconstateerd zijn automatisch toe te kennen aan minstens één van de drie ministeries waardoor het in lijn is met de voorwaarde dat het advies algemeen van aard moet zijn. De ministeries weten zelf wel of deze afwijkingen wel of niet op haar van toepassing zijn.

Per onderdeel van een ministerie zijn er ook verschillende scenario's voorgelegd met daarbij vier vragen over het betreffende scenario. De scenario's zijn in de interviewvragen opgenomen om te dienen als optioneel toetsmiddel om te kijken of de antwoorden op deze vragen consistent zijn met eerder gestelde vragen.

Elke vraag van een scenario wordt gesteld vanuit een bepaalde invalshoek om de geïnterviewde zich te laten inleven in de situatie van een ander. Zo wordt geprobeerd de geïnterviewde actief na te laten denken of eerdere uitspraken wel daadwerkelijk het beeld van de medewerker en de organisatie weergeven en niet van de geïnterviewde zelf.

De scenario's zijn alleen gebruikt wanneer hiervoor tijd en ruimte was in het interview. In geval van tijdsgebrek zijn de scenario's gedeeltelijk of helemaal weggelaten. Doordat de scenario's niet in elk interview zijn behandeld is hierdoor geen goede vergelijking tussen de verschillende onderdelen per ministerie en tussen de ministeries als geheel mogelijk. Hierdoor worden de resultaten van de scenario's niet gebruikt in het advies.

4.3 De overheid en Social Engineering

In deze paragraaf zal onderzoeksvraag 2.1 beantwoord worden, "wat doet de overheid tegen Social Engineering?". Dit zal gedaan worden aan de hand van de overeenkomsten die gevonden zijn tussen de drie ministeries voortkomend uit de interviewverslagen. Als eerste zullen, zoals aangegeven is in de opzet van het interview, de overeenkomsten tussen de ministeries per onderwerp besproken worden. Hierna zal onderzoeksvraag 2.1 beantwoord worden waarbij het antwoord gebaseerd is op de volgende onderwerpen:

- Herkenning en bescherming tegen Social Engineering
- Maatregelen tegen Social Engineering en naleving van deze maatregelen
- Locatie en waarde van informatie binnen en buiten de ministeries

4.3.1 Herkenning en bescherming tegen Social Engineering

De ministeries herkennen Social Engineering in de zin dat zij bekend zijn met het begrip Social Engineering. Dit is echter alleen van toepassing op medewerkers binnen de ministeries die in het kader van hun functie betrokken zijn bij informatiebeveiliging. Voor de overige medewerkers is dit vaak niet het geval. Er wordt wel geprobeerd het begrip Social Engineering bekend te maken in heel de organisatie door aandacht te besteden aan het onderwerp Social Engineering in onder andere bewustwordingssessies en -campagnes.

De ministeries als geheel hanteren geen eenduidige definitie van het begrip Social Engineering maar is per onderdeel verschillend. Wel staat de mens als zwakste schakel en het verkrijgen van "gevoelige" informatie bij elk ministerie centraal in haar definitie. De ministeries geven globaal aan dat zij de werkwijze van een Social Engineer zien als een persoon die zich voordoet als een ander persoon door gebruik te maken van zijn communicatieve vaardigheden.

Op dit moment zijn er nog geen gevallen van Social Engineering bekend of herkend als zodanig die hebben bijgedragen tot concrete acties binnen de verschillende ministeries. Dit betekent niet dat er geen Social Engineering aanvallen hebben plaatsgevonden. Buiten de ministeries zijn er ook geen specifieke gevallen van Social Engineering bekend die hebben bijgedragen aan concrete acties. Wel zijn er landelijke incidenten geweest die als trigger hebben gediend voor het evalueren, aanscherpen en herzien van bestaande maatregelen en het promoten van informatiebeveiliging onder de medewerkers. De ministeries geven aan dat er geen formele uitwisseling plaatsvindt tussen de ministeries over informatiebeveiligingsincidenten.

Tussen de verschillende ministeries is er een duidelijk verschil in de mate waarin zij beschermd zijn tegen Social Engineering. Sommige ministeries zijn verder in het uitrollen van hun informatiebeveiliging dan andere. Bij sommige ministeries is de bescherming zich nog aan het vormen. Dit betekent niet dat de andere ministeries automatisch voldoende beschermd zijn. Informatiebeveiliging is een groeiproces dat voortdurend in beweging is. Op medewerkerniveau geven de ministeries aan dat zij op dit moment nog niet voldoende beschermd zijn tegen Social Engineering. De ministeries geven aan te werken aan de bewustwording van informatiebeveiliging onder haar medewerkers. Wat bij alle ministeries overeenkomt is dat zij aangeven dat een "echte" Social Engineer met de juiste vaardigheden toch wel de organisatie binnenkomt.

4.3.2 Maatregelen tegen Social Engineering en naleving van deze maatregelen

Elk ministerie heeft algemene maatregelen op het gebied van informatiebeveiliging welke deels ook Social Engineering tegengaan en de medewerkers beschermen. Deze maatregelen zijn onder andere gebaseerd op de Code voor Informatiebeveiliging, het VIR en het VIR-BI, A&K analyses, CAO, ambtenarenwet en het gezonde verstand.

De code voor informatiebeveiliging is een internationale standaard voor informatiebeveiliging in organisaties en dient als naslagwerk waarin normen en doelstellingen zijn opgenomen die dienen als basis voor het implementeren van een beveiligingsbeleid [3].

Het VIR wat staat voor Voorschrift Informatiebeveiliging Rijksdienst en het VIR-BI wat staat voor Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie, zijn leidend op het gebied van de beveiliging van de informatievoorziening binnen de overheid. Het VIR geeft door middel van een kader algemene regels aan voor de beveiliging van informatie binnen de rijksoverheid [60]. Het VIR-BI geeft regels voor de beveiliging van bijzondere informatie bij de rijksdienst [61].

A&K analyses zijn analyses die de afhankelijkheid van bedrijfsprocessen van informatiesystemen en kwetsbaarheid van informatiesystemen analyseren om aan de hand hiervan maatregelen op te stellen om informatiesystemen te beschermen.

De CAO en de ambtenarenwet hebben vooral betrekking op maatregelen waar de medewerker zich aan moet houden. Hieronder vallen ook maatregelen met betrekking hebben op informatiebeveiliging.

Maatregelen worden gecommuniceerd door middel van bewustwordingsessies en -campagnes, intranet en e-mail en via afdelingshoofden naar de medewerkers. Bij de introductie van een nieuwe medewerker worden de maatregelen gecommuniceerd door middel van de aflegging van de eed en belofte, de ambtenarenwet waaraan de medewerker moet voldoen en huisregels. Daarnaast worden er in het normale werkproces ook maatregelen gecommuniceerd.

Controle op de naleving van maatregelen vindt plaats door middel van audits en een onaangekondigde mystery guest. De mystery guest is een door het ministerie ingehuurd persoon die probeert kwetsbaarheden in de organisatie te vinden. Controle valt onder de eindverantwoordelijkheid van de lijnmanager. Een lijnmanager is meestal geen informatiebeveiligingsexpert.

Voor het niet naleven van maatregelen binnen de organisatie zijn algemeen geldende sancties van toepassing welke ook gelden voor het niet naleven van informatiebeveiligingsmaatregelen. Het streven is dat het niet naleven van maatregelen wordt opgenomen in het persoonlijk dossier en meegenomen wordt in het functioneringsgesprek. Wat deze sancties precies zijn, is tijdens de interviews niet naar voren gekomen. Omdat sancties ervoor kunnen zorgen dat informatiebeveiligingsincidenten niet worden gemeld is het van belang tussen melding en sanctionering een balans te vinden.

Invoering van maatregelen en dus ook van informatiebeveiligingsmaatregelen leidt vaak tot verzet van medewerkers omdat het nut van deze maatregelen vaak niet duidelijk is. Daarom proberen de ministeries het besef van het nut van informatiebeveiliging te vergroten door hieraan actief aandacht te besteden.

4.3.3 Locatie en waarde van informatie binnen en buiten de ministeries

Binnen de ministeries bestaat er een eenduidige classificatie van informatie volgens het VIR-BI. De ministeries hanteren een beleid dat aangeeft hoe er omgegaan moet worden met de verschillende informatiedragers en de informatie daarop. De naleving van dit beleid is grotendeels de verantwoordelijkheid van de medewerker zelf. De naleving en controle hierop vindt niet tot nauwelijks plaats. De ministeries geven aan dat onder andere bewustwordingssessies moeten bijdragen aan hoe medewerkers met informatiedragers binnen en buiten de organisatie omgaan.

Het besef dat "niet waardevolle" informatie voor de medewerker juist wel waardevol kan zijn voor anderen is niet tot nauwelijks aanwezig. Medewerkers beschouwen informatie als waardevol wanneer deze informatie betrekking heeft op een belangrijk component van zijn of haar functie, dit is het beste uit te leggen door middel van een voorbeeld.

Een financieel medewerker beschouwt informatie over de begroting van zijn ministerie als waardevolle informatie omdat deze informatie belangrijk is voor het uitvoeren van zijn werkzaamheden en de resultaten die hij oplevert. Een notulen met afspraken van een belangrijke vergadering zal hij, omdat deze niet echt functie gerelateerd zijn, minder belangrijk vinden waardoor hij hier minder waarde aan hecht en deze informatie beschouwt als niet waardevol.

Hieruit volgt dat de medewerker zorgvuldiger om zal gaan met informatie die waardevol voor hem is dan informatie die niet waardevol voor hem is. Informatie over de begroting zal hij bijvoorbeeld zorgvuldig op bergen terwijl de notulen gewoon op zijn bureau rondslingert. Dit kan als gevolg hebben dat deze informatie gecompromitteerd kan worden door kwaadwillenden waarvoor de informatie wel waardevol is.

4.3.4 Wat doet de overheid tegen Social Engineering?

Uit de verschillende interviews zijn de volgende conclusies getrokken die aangeven wat de overheid doet tegen Social Engineering.

1. De ministeries erkennen de dreiging die uitgaat van Social Engineering. Deze dreiging is echter niet bij elke medewerker in de organisatie bekend.
2. De ministeries hanteren geen eenduidige definitie voor Social Engineering. Wel staan de mens als zwakste schakel en het verkrijgen van "gevoelige" informatie centraal.
3. Social Engineering maakt bij elk ministerie onderdeel uit van het informatiebeveiligingsbeleid.
4. Ministeries reageren actief op incidenten die direct of indirect met Social Engineering te maken hebben. Incidenten dienen als trigger om bestaande maatregelen te evalueren, aan te scherpen of te herzien.
5. De ministeries hebben algemene informatiebeveiligingsmaatregelen die deels bijdragen aan de bescherming tegen Social Engineering. Informatiebeveiligingsmaatregelen worden op verschillende manieren

gecommuniceerd naar de medewerker. Controle op naleving van informatiebeveiligingsmaatregelen vindt plaats door audits en de mystery guest.

6. Medewerkers binnen de ministeries worden bekend gemaakt met het begrip en de inhoud van Social Engineering door middel van bewustwordingssessies en -campagnes.

4.4 Advies aan ministeries

Dit advies zal bestaan uit een opsomming van aandachtspunten die kunnen leiden tot een betere bescherming tegen Social Engineering. Het advies is gebaseerd op overeenkomsten tussen de ministeries vergeleken met de begripsbepaling en het framework. Daarnaast zijn ook aandachtspunten opgenomen over zaken die op zijn gevallen tijdens en bij de uitwerking van de interviews. Elk aandachtspunt zal waar nodig kort worden verduidelijkt.

Vanwege de algemene aard van dit advies hoeft niet elk aandachtspunt op elk ministerie van toepassing te zijn.

1. **Het per ministerie hanteren van een eenduidige definitie van Social Engineering**
   De ministeries als geheel hanteren geen eenduidige definitie van het begrip Social Engineering maar is per onderdeel verschillend. Een eenduidige definitie binnen een ministerie zorgt voor een afgebakend kader. Dit kader legt de basis voor maatregelen, betere afstemming van onderdelen op elkaar en een verbeterde herkenning en afhandeling van incidenten met betrekking tot Social Engineering.

2. **Beschouw voorbereiding als een essentieel onderdeel van Social Engineering**
   Voorbereiding houdt in dat de Social Engineer informatie over de organisatie haalt uit publieke bronnen en deze gebruikt voor verschillende Social Engineering aanvallen (zie paragraaf 2.5). Evalueer daarom vanuit het oogpunt van Social Engineering welke informatie er over de organisatie publiek toegankelijk is. Ook Social Engineering aanvallen kunnen als voorbereiding dienen. Het gaat hierbij om het verkrijgen van voorbereidende informatie die relatief eenvoudig over een organisatie te verkrijgen is maar niet publiek toegankelijk is. Voorbereiding en aanvallen die als voorbereiding kunnen dienen zijn opgenomen in de begripsbepaling en / of het framework.

3. **Vergroot de scope van Social Engineering**
   Social Engineering vindt niet alleen fysiek binnen de organisatie en op de organisatiegrens plaats maar ook buiten de organisatie. Informatiedragers met informatie kunnen zich ook buiten de organisatie begeven waardoor zij ook hier het doelwit kunnen zijn van de Social Engineer. Door het vergroten van de scope wordt er een nieuw gebied zichtbaar waar informatiedragers met informatie van de organisatie zich in kunnen bevinden. Wil de organisatie zich in zijn geheel beschermen dan zullen de informatiedragers met informatie in dit gebied ook beschermd moeten worden. Hiervoor kunnen extra maatregelen getroffen worden en moet er bovendien voor gezorgd worden dat deze maatregelen worden nageleefd. De verschillende gebieden, de verplaatsing hiertussen van de informatiedragers met informatie en de aanvallen die er kunnen plaatsvinden zijn weergegeven in de verschillende modellen van het conceptueel framework.

4. **Beschouw Social Engineering vanuit het oogpunt van de Social Engineer met behulp van het conceptueel framework**
   Voor de Social Engineer kan informatie een andere waarde hebben dan voor de organisatie en haar medewerkers. Door de organisatie te beschouwen vanuit het oogpunt van de Social Engineer kan een beter inzicht worden verkregen in welke informatie er beschermd dient te worden tegen Social Engineering. Om dit inzicht te verkrijgen moet de waarde van gevoelige en niet-gevoelige informatie en de waarde van informatiedragers voor de Social Engineer bepaald worden. Vervolgens moet er geïnventariseerd worden welke Social Engineering aanvallen betrekking hebben op deze informatie en informatiedragers die waardevol zijn voor de Social Engineer. Evalueer tenslotte de bestaande maatregelen ter bescherming van deze informatie en informatiedragers. Hiervoor kan het framework van toegevoegde waarde zijn. Daarnaast is het belangrijk de medewerkers bewust te maken van het feit dat informatie die zij waarderen als "niet-waardevol" juist wel waardevol kan zijn voor anderen waaronder de Social Engineer zodat zij in de toekomst zorgvuldiger om gaan met informatie.

5. **Wissel informatie over informatiebeveiligingsincidenten op onderdeel niveau met elkaar uit.**
   Uit de interviews is gebleken dat er formeel geen uitwisseling plaatsvindt van informatie over informatiebeveiligingsincidenten tussen de verschillende onderdelen binnen een ministerie. Door informatie over informatiebeveiligingsincidenten uit te wisselen met elkaar kunnen de onderdelen van elkaar leren en kan het algehele informatiebeveiligingsniveau van de ministeries worden verhoogd. De informatie die uitgewisseld wordt kan onder andere bestaan uit maatregelen om incidenten te voorkomen of te beperken, procedures om incidenten af te handelen en best-practices.

6. **Gebruik meerdere methoden voor de controle op de naleving en dekking van de maatregelen.**
   Alle ministeries maken gebruik van een mystery guest om de informatiebeveiliging te testen. Aan de hand van de resultaten van deze test kan er worden afgeleid of de bestaande maatregelen afdoende zijn en of deze maatregelen goed worden nageleefd. De mystery guest kan echter een vertekend beeld geven omdat de test slechts een moment opname is. Daarnaast wordt er maar een klein deel van de maatregelen gecontroleerd op naleving en volledigheid. Om de informatiebeveiliging gerichter te testen moet een ministerie hiervoor meerdere methoden gebruiken. Voorbeelden hiervan zijn, overleg met de mystery guest welke beveiligingspunten getest worden, als ministerie zelf regelmatig zelf controles uitvoeren en medewerkers belonen die actief met informatiebeveiliging bezig zijn.

7. **Geef nieuwe medewerkers een introductie op het gebied van informatiebeveiliging.**
   Nieuwe medewerkers binnen het ministerie zijn vaak nog niet goed bekend met het reilen en zeilen van de informatiebeveiliging in de organisatie. Hierdoor vormen ze een relatief eenvoudig doelwit voor de Social Engineer. Uit de verschillende interviews is naar voren gekomen dat de ministeries wel procedures hanteren bij de introductie van nieuwe medewerkers maar dat informatiebeveiliging hier niet specifiek een onderdeel van uit maakt Een introductie waar onder andere de voorgeschreven maatregelen te vinden zijn en bij welke personen ze terecht kunnen kan bijdragen aan de verhoging van het informatiebeveiligingsniveau waar Social Engineering betrekking op heeft.

8. **Gebruik de gereedschappen uit de begripsbepaling en het conceptueel framework in bewustwordingssessies.**
   Alle ministeries houden bewustwordingssessies om het bewust zijn met betrekking tot informatiebeveiliging bij de medewerker te vergroten. Ook wordt hierin aandacht geschonken aan het onderwerp Social Engineering. Vaak wordt door middel van voorbeelden uit de praktijk aangegeven hoe een Social Engineering aanval in zijn werk gaat. In de begripsbepaling is aangegeven welke gereedschappen de Social Engineer tot zijn beschikking heeft bij het uitvoeren van een aanval. Zo kan de Social Engineer technieken gebruiken om de mens te misleiden en te manipuleren, kan er gebruik gemaakt worden van de situatie waarin de mens zich bevindt en kan er ingespeeld worden op verschillende eigenschappen van de mens. Daarnaast zijn er nog psychologische principes die richting geven aan het menselijke gedrag waarvan de Social Engineer gebruik kan maken om de mens naar zijn hand te zetten.

   De Social Engineer kan bij een soortgelijke aanval gebruik maken van verschillende gereedschappen wat betekent dat er meerdere manieren zijn om een aanval uit te voeren. Wat echter vaak niet verschilt, is het psychologische principe dat aan de aanval ten grondslag ligt. Door tijdens de bewustwordingssessies de medewerkers te wijzen op de psychologische principes achter de verschillende Social Engineering aanvallen wordt het bereik van de bewustwording tegen Social Engineering aanvallen vergroot. Als een medewerker zich bewust is van de psychologische principes is hij in staat meerdere aanvallen te doorgronden.

   Daarnaast is het belangrijk aandacht te besteden in de bewustwordingsessies aan de verschillende technieken omdat deze relatief eenvoudig te herkennen zijn. Ook de situatie waarin de mens zich op het moment van de aanval bevindt is van belang omdat, afhankelijk van de situatie, de mens anders reageert. Als laatste dienen de verschillende eigenschappen van de mens in beschouwing genomen te worden. Het is vaak moeilijk een natuurlijke reactie tegen te gaan maar bij voldoende herhaling is dit zeker mogelijk.

   Het conceptueel framework kan van toegevoegde waarde zijn in de bewustwordingssessies doordat het inzichtelijk maakt waar in de organisatie aanvallen plaats kunnen vinden en dat de mens de informatiedrager is die bij deze

aanvallen het middelpunt vormt. Deze inzichten kunnen gebruikt worden om medewerkers in te laten zien dat zij ook buiten de organisatie het doelwit van Social Engineering kunnen zijn en dat zij verbindende factor vormen om bij andere informatiedragers te komen.

Samengevat betekent dit dat de ministeries meer bereiken met haar bewustwordingssessies als er meer aandacht wordt besteed aan de beschreven gereedschappen van de Social Engineer en de inzichten verkregen uit het framework in plaats van alleen voorbeelden te noemen van veel voorkomende Social Engineering aanvallen.

4.5 Verantwoording en onderbouwing adviespunten

Bepaalde adviespunten uit de vorige paragraaf zijn het resultaat van een vergelijking van de begripsbepaling en het conceptueel framework met de overeenkomsten tussen de ministeries uit de interviewverslagen. Sommige adviespunten zullen in deze paragraaf extra onderbouwd worden omdat in het advies niet duidelijk naar voren komt wat de relatie met de begripsbepaling en het framework is.

Adviespunt 1: Het per ministerie hanteren van een eenduidige definitie van Social Engineering
In de begripsbepaling is de definitie van het begrip Social Engineering gegeven die gebruikt is bij de uitvoering van dit onderzoek. Deze definitie is opgesteld met de bedoeling een duidelijk kader te stellen wat Social Engineering wel en niet is. Tijdens de uitvoering van het onderzoek is geconstateerd dat het hebben van duidelijke definitie leidend is voor het aanbrengen van structuur in wat Social Engineering omvat.

In subparagraaf 4.3.1 is aangegeven dat de onderdelen binnen een ministerie onderling niet dezelfde definitie van Social Engineering hanteren. Daarnaast zijn sommige definities erg ruim van aard en is er geen duidelijke kaderstelling.

Uit deze twee constateringen volgt het adviespunt om per ministerie eenduidige definitie te hanteren zodat er afgebakend kader is waarin wordt aangegeven wat Social Engineering wel en niet is. Het kader kan zorgen voor een basis voor maatregelen, betere afstemming van onderdelen op elkaar en verbeterde herkenning en afhandeling van incidenten.

Adviespunt 2: Beschouw voorbereiding als een essentieel onderdeel van Social Engineering
In de interviews is er gevraagd welke definitie de verschillende onderdelen van de ministeries voor het begrip Social Engineering hanteren en of voorbereiding een deel uitmaakt van Social Engineering. In subparagraaf 4.3.1 is aangegeven dat de overeenkomst tussen de definities van de ministeries is dat de mens als zwakste schakel centraal staat. Voorbereiding wordt echter door verschillende onderdelen buiten beschouwing gelaten.

In subparagraaf 2.5 van de begripsbepaling is aangegeven dat voorbereiding cruciaal is voor de succesvolle uitvoering van een Social Engineering aanval. Het is daarom van belang voor de ministeries om voorbereiding te beschouwen als essentieel onderdeel van Social Engineering. Hierdoor wordt er met een andere bril gekeken naar informatie over het ministerie die publiek toegankelijk is en kan waar mogelijk de toegankelijkheid van informatie worden aangepast. Daarnaast kunnen er maatregelen genomen worden die voorbereiding tegengaan met als resultaat dat deze Social Engineering aanvallen kunnen vertragen.

Adviespunt 3: Vergroot de scope van Social Engineering
Het vergroten van de scope van Social Engineering heeft te maken met de verschillende plaatsen waar Social Engineering aanvallen kunnen plaatsvinden. Uit de interviews is geconstateerd dat de ministeries aannemen dat Social Engineering aanvallen vooral in het gebouw en bij de toegang tot het gebouw plaatsvinden waarbij de Social Engineer zich fysiek op deze twee plaatsen bevindt.

In subparagraaf 3.2.1 van het framework wordt aangegeven dat een organisatie opgedeeld kan worden in drie organisatiegebieden en dat verschillende informatiedragers met daarop informatie zich kunnen verplaatsen tussen deze verschillende gebieden. Vervolgens is er geconstateerd dat in sommige gevallen de plaats van de Social Engineer en het organisatiegebied bepalend zijn voor welke Social Engineering aanvallen er uitgevoerd kunnen worden en welke doelen bereikt kunnen worden (zie subparagraaf 3.2.4).

Door de scope te vergroten worden er nieuwe organisatiegebieden met daarin informatiedragers zichtbaar die ook beschermd moeten worden. Door maatregelen te treffen om deze nieuwe gebieden te beschermen wordt de bescherming tegen Social Engineering in zijn geheel vergroot.

Adviespunt 4: Beschouw Social Engineering vanuit het oogpunt van de Social Engineer

Uit de interviews is nauwelijks af te leiden of Social Engineering door de ministeries ook vanuit het oogpunt van de Social Engineer wordt beschouwd om zo een inzichten te verkrijgen welke informatie er beschermd dient te worden tegen Social Engineering. Wel wordt er in subparagraaf 4.3.3 aangegeven dat medewerkers alleen vanuit hun functie informatie waarderen als “waardevol” of “niet-waardevol” waaruit blijkt dat niet iedereen met dezelfde ogen naar informatie kijkt.

Deze twee argumenten zijn de reden om Social Engineering te beschouwen vanuit het oogpunt van de Social Engineer te noemen in het advies. Het framework is opgebouwd vanuit dit oogpunt en kan daardoor een belangrijke bijdrage leveren in de bepaling welke “gevoelige” en “niet-gevoelige” informatie en informatiedragers waardevol kunnen zijn voor de Social Engineer. Daarnaast dienen medewerkers bewust gemaakt te worden van het feit dat informatie die zij waarderen als “niet waardevol” juist wel waardevol kan zijn voor anderen zoals de Social Engineer (zie paragraaf 2.3) zodat zij hier zorgvuldiger mee omgaan.

5 Conclusie

5.1 Antwoord op onderzoeksvragen

In deze paragraaf worden de twee onderzoeksvragen beantwoord die in de probleemstelling (zie paragraaf 1.4) zijn gesteld.

Voordat deze vragen beantwoord kunnen worden moeten eerst de verschillende deelvragen beantwoord worden. Sommige deelvragen zijn al indirect in verschillende paragrafen beantwoord. Op deze vragen zal een kort antwoord gegeven worden en waar nodig verwezen worden naar de gerelateerde hoofdstukken.

In subparagraaf 5.1.1 t/m 5.1.5 worden de deelvragen van hoofdvraag één beantwoord. In subparagraaf 5.1.7 t/m 5.1.9 worden de deelvragen met betrekking tot hoofdvraag twee beantwoord. In subparagraaf 5.1.6 en 5.1.10 worden de hoofdvragen van dit onderzoek beantwoord.

5.1.1 Deelvraag 1.1: Wat is een bruikbare definitie van het begrip Social Engineering voor dit onderzoek?

De definitie die in dit onderzoek wordt gebruikt is:

"Het misleiden, manipuleren, gebruik maken van het niet bewust zijn van de mens en de voorbereiding daarop om gevoelige informatie te verkrijgen."

Deze definitie is bruikbaar omdat:

1. **De definitie een ruimere context hanteert van het begrip Social Engineering dan de definities gesteld in de bestaande literatuur.**

   Naast misleiding en manipulatie neemt de definitie ook het niet bewust zijn van de mens mee, wat betekent dat de mens zich niet bewust is van de mogelijk negatieve gevolgen van bepaalde acties. Dit kan uitgebuit worden door de Social Engineer. Daarnaast wordt er ook aandacht besteed aan de voorbereiding die benodigd is voor Social Engineering.

2. **De definitie stelt een duidelijk kader waarbinnen onderscheid wordt gemaakt wat Social Engineering wel en niet is.**

   Het kader geeft richting aan het onderzoek waardoor er een werkbaar geheel ontstaat om het onderzoek uit te voeren.

3. **De geïnventariseerde Social Engineering aanvallen en gereedschappen vallen binnen het kader dat door de definitie van Social Engineering wordt gesteld.**

4. **Het doel van Social Engineering, het verkrijgen van gevoelige informatie is duidelijk uit de definitie af te leiden**

5. **Met behulp van de definitie is een eerste opzet van een conceptueel framework mogelijk.**

De definitie wordt uitgebreid beschreven en onderbouwd in paragraaf 2.2

5.1.2 Deelvraag 1.2: Wat zijn de belangrijkste doelen van Social Engineering?

Het doel van Social Engineering is het verkrijgen van gevoelige informatie wat duidelijk is af te leiden uit de gestelde definitie van Social Engineering. Het doel van Social Engineering kan bereikt worden door Social Engineering aanvallen uit te voeren.

5.1.3 Deelvraag 1.3: Welke mogelijke Social Engineering aanvallen zijn er en wat zijn de kenmerken hiervan?

Uit de literatuur zijn de volgende Social Engineering aanvallen geïnventariseerd:

- Piggybacking
- Tailgating
- Impersonation
- Reverse Social Engineering
- Shoulder Surfing
- Dumpster diving
- Profiling
- Desk-sniffing
- Eavesdropping
- Phishing
- Keylogger
- Item-dropping

Deze Social Engineering aanvallen vallen allemaal binnen de in dit onderzoek gestelde definitie van Social Engineering. Daarnaast staat elke aanval op zichzelf wat betekent dat een aanval in principe niet afhankelijk is van andere aanvallen. Echter door aanvallen met elkaar te combineren is het doel van Social Engineering mogelijk sneller te bereiken. Social Engineering aanvallen hebben de volgende kenmerken:

Direct of indirect
De mens is bij een Social Engineering aanval direct of indirect betrokken. Hierdoor wordt er onderscheid gemaakt tussen directe en indirecte Social Engineering aanvallen. Bij directe aanvallen is er sprake van interactie tussen de mens en de Social Engineer. Bij indirecte aanvallen speelt de Social Engineer in op het niet bewust zijn van de mens waarbij er geen interactie plaatsvindt.

Fysiek en/of via medium
De uitvoering van een Social Engineering aanval kan zowel fysiek als via een medium plaatsvinden. Het verschil is dat er via een medium interactie kan plaatsvinden zonder dat de Social Engineer fysiek in contact hoeft te staan met de mens. Bij een fysieke aanval staat de Social Engineer fysiek in contact met de mens. Een voorbeeld hiervan kan zijn dat ze elkaar "letterlijk" in de ogen kijken.

Doelen
Een Social Engineering aanval kan één of meerdere doelen realiseren. Deze doelen zijn toegang verkrijgen, informatie verkrijgen, een vertrouwensrelatie opbouwen en handeling laten uitvoeren. Het realiseren van het doel informatie verkrijgen kan rechtstreeks leiden tot de verwezenlijking van het doel van Social Engineering, het verkrijgen van gevoelige informatie.

5.1.4 Deelvraag 1.4: Zijn er overige factoren die invloed hebben op Social Engineering?

Naast de geïnventariseerde Social Engineering aanvallen heeft de literatuurstudie een aantal factoren opgeleverd die bijdragen aan de invulling en uitvoering van een Social Engineering aanval. De factoren worden in dit onderzoek gereedschappen genoemd die de Social Engineer tot zijn beschikking heeft. Deze gereedschappen zijn onderverdeeld in *technieken* om de mens te misleiden, te manipuleren en gebruik te maken van het niet bewust zijn van de mens, *situaties* waar de mens zich in kan bevinden, verschillende *eigenschappen van de mens* waarop ingespeeld kan worden en *psychologische principes* die richting geven aan het menselijke gedrag. Deze gereedschappen worden beschreven in paragraaf 2.7

5.1.5 Deelvraag 1.5: Is Social Engineering te structureren in een framework zodat het inzichtelijker wordt?

In dit onderzoek is een eerste poging gedaan om structuur aan te brengen in het onderwerp Social Engineering door een framework op te stellen. De gevonden literatuur over dit onderwerp is in veel gevallen onvolledig, ongeordend en niet goed onderbouwd. Met het opstellen van een framework is geprobeerd orde te creëren en volledig te zijn over wat Social Engineering nou precies omvat.

Concluderend kan gesteld worden dat het mogelijk is Social Engineering te structureren in een framework. In dit onderzoek is aan de hand van de begripsbepaling in hoofdstuk 2 een

eerste opzet gegeven hoe het framework er uit zou kunnen zien. Hierbij is gebleken dat het erg lastig is om structuur aan te brengen en alle aspecten van Social Engineering hierin te verwerken. Daarom beperkt deze eerste opzet zich in het weergeven van de volgende punten:

- Opdeling van organisatie in informatiedragers met informatie
- Onderscheid tussen gevoelige en niet gevoelige informatie
- Gelaagde bescherming van informatiedragers
- Positie van informatiedragers met informatie ten opzichte van de organisatie
- Overdracht van informatie en verplaatsing van informatiedragers met informatie
- Opdeling van organisatie in organisatiegebieden
- Plaats van Social Engineer ten opzichte van de organisatie
- Aanvallen en doelen afhankelijk van de positie van de Social Engineer en organisatiegebieden

5.1.6 Hoofdvraag 1: Wat omvat Social Engineering?

In dit onderzoek is er een poging gedaan te beschrijven wat Social Engineering nou precies omvat. Hiervoor is uitgebreid gezocht naar beschikbare literatuur over dit onderwerp waarna deze gebruikt is om de definitie (deelvraag 1.1), de doelen (deelvraag 1.2), de aanvallen (deelvraag 1.3) en de overige factoren (deelvraag 1.4) van Social Engineering te bepalen. Tenslotte is met deze informatie een eerste poging gedaan om een framework (deelvraag 1.5) op te stellen dat Social Engineering visueel inzichtelijk maakt.

5.1.7 Deelvraag 2.1: Wat doet de overheid tegen Social Engineering?

De volgende punten geven aan wat de overheid (in dit geval de drie ministeries) doen tegen Social Engineering:

1. De ministeries erkennen de dreiging die uitgaat van Social Engineering. Deze dreiging is echter niet bij elke medewerker in de organisatie bekend.
2. De ministeries hanteren geen eenduidige definitie voor Social Engineering. Wel staan de mens als zwakste schakel en het verkrijgen van “gevoelige” informatie centraal.
3. Social Engineering maakt bij elk ministerie onderdeel uit van het informatiebeveiligingsbeleid.
4. Ministeries reageren actief op incidenten die direct of indirect met Social Engineering te maken hebben. Incidenten dienen als trigger om bestaande maatregelen te evalueren, aan te scherpen of te herzien.
5. De ministeries hebben algemene informatiebeveiligingsmaatregelen die deels bijdragen aan de bescherming tegen Social Engineering.
6. Informatiebeveiligingsmaatregelen worden op verschillende manieren gecommuniceerd naar de medewerker. Controle op naleving van informatiebeveiligingsmaatregelen vindt plaats door audits en de mystery guest.

7. Medewerkers binnen de ministeries worden bekend gemaakt met het begrip en de inhoud van Social Engineering door middel van informatiebeveiliging bewustwordingssessies en -campagnes.

5.1.8 Deelvraag 2.2: Is de overheid bestand tegen de verschillende soorten aanvallen uit ons framework?

De beantwoording van deze vraag blijkt alleen mogelijk wanneer alle aanvallen uit het framework daadwerkelijk zouden worden getoetst bij de verschillende ministeries. Binnen het kader van dit onderzoek was dit vanwege de volgende redenen echter niet mogelijk:

Gebrek aan tijd
Het kost veel tijd om alle Social Engineering aanvallen uit het framework te kunnen toetsen.De tijd in dit onderzoek is beperkt waardoor dit niet mogelijk is.

Gebrek aan informatie over de ministeries
Om een Social Engineering aanval toe te kunnen spitsen op de ministeries is specifieke informatie over de ministeries nodig. Hiervoor is een grondige voorbereiding nodig waar geen tijd voor is in dit onderzoek. Bovendien is niet gegarandeerd dat er voldoende informatie over de ministeries kan worden verzameld om een Social Engineering aanval succesvol uit te voeren.

De onderzoekers hebben niet de juiste vaardigheden
Om een Social Engineering aanval met succes uit te kunnen voeren moet een Social Engineer beschikken over de juiste vaardigheden. Beide onderzoekers hebben deze vaardigheden niet.

Grote variatie in de uitvoering van Social Engineering aanvallen
De Social Engineer kan op verschillende manieren invulling geven aan de uitvoering van een Social Engineering aanval. Hierbij kan hij gebruik maken van verschillende gereedschappen (zie subparagraaf 2.7). Door de gereedschappen te combineren wordt het aantal manieren om een aanval uit te voeren zo groot dat het in de praktijk onmogelijk is deze allemaal te toetsen.

Om toch een bevredigend antwoord te kunnen geven op deze onderzoeksvraag is de invalshoek aangepast. In plaats van te bepalen of de overheid bestand is tegen aanvallen uit het framework is er geprobeerd te achterhalen hoe de overheid probeert de Social Engineering aanvallen uit het framework te voorkomen of te beperken. Hiervoor worden in het interview gerichte vragen gesteld over de aard van de bestaande informatiebeveiligingsmaatregelen en wordt er niet ingegaan op de inhoud. Daarnaast worden er verschillende scenario's voorgelegd met daarin aanvallen die gebruikt kunnen worden extra informatie te achterhalen.

Met behulp van de interviews is achterhaald dat de ministeries geen specifieke maatregelen, maar algemene maatregelen hebben getroffen om de aanvallen uit het framework te voorkomen of te beperken. Een voorbeeld hiervan is de clean-desk policy, een algemene

maatregel die Social Engineering aanvallen zoals desk-sniffing, dumpster-diving en keylogging beperkt of zelfs voorkomt.

Concluderend kan er gesteld worden dat het niet gelukt is om vast te stellen of de overheid bestand is tegen de verschillende soorten Social Engineering aanvallen in ons framework. Wel heeft de overheid algemene maatregelen tegen getroffen die ook Social Engineering moeten tegengaan. Hieruit is echter niet af te leiden of deze voldoende zijn om alle Social Engineering aanvallen uit het framework te voorkomen of te beperken.

5.1.9 Deelvraag 2.3: Is het framework van toegevoegde waarde voor een verbeterde bescherming tegen Social Engineering?

De toegevoegde waarde van het framework heeft betrekking op de wetenschap, de analyse bij de overheid en organisaties in het algemeen. Wat de toegevoegde waarde per punt precies is zal in deze paragraaf worden uitgelegd.

Wetenschap
Het conceptueel framework is van toegevoegde waarde voor de wetenschap omdat zover bekend is, het framework de eerste geslaagde poging is om wat Social Engineering omvat gestructureerd weer te geven. Het framework vormt een solide basis dat gebruikt kan worden als uitgangspunt voor verder onderzoek naar dit begrip.

Analyse bij de overheid
De toegevoegde waarde van het framework bij de analyse van de overheid is:

1. Dat de onderdelen uit het framework de basis vormen om gerichte vragen te stellen over Social Engineering bij de overheid.
2. Door de inhoud van het framework als norm te beschouwen en te vergelijken met de interviewresultaten is het mogelijk om afwijkingen bij de overheid te constateren.
3. Dat de geconstateerde afwijkingen omgevormd kunnen worden tot een algemeen advies wat de overheid kan gebruiken om zich beter te beschermen tegen Social Engineering.

Organisaties
Het framework kan ook van toegevoegde waarde zijn voor organisaties omdat het naar Social Engineering kijkt vanuit het oogpunt van de Social Engineer. Hierdoor verschaft het framework inzicht in de volgende punten:

1. **Informatiedragers en informatie.**
2. **Gevoelige en niet-gevoelige informatie.**
3. **Bescherming van informatiedragers.**
4. **De positie van informatiedragers in de organisatiegebieden**
5. **De verplaatsing van informatiedragers met informatie tussen de organisatiegebieden.**
6. **Onderscheid in organisatiegebieden.**

7. **Aanvallen met bijbehorende doelen afhankelijk van de positie van de Social Engineer en het organisatiegebied.**

Door deze verschillende punten in beschouwing te nemen kan een organisatie haar informatiebeveiliging evalueren en mogelijk herzien waardoor zij in staat is om zich beter te beschermen tegen Social Engineering.

5.1.10 Hoofdvraag 2: Is de overheid beschermd tegen Social Engineering?

De vraag of de overheid[4] beschermd is tegen Social Engineering kan op meerdere manieren geïnterpreteerd worden. De vraag kan als doel hebben een antwoord te krijgen of de overheid beschermd is, waarbij "beschermd zijn tegen" inhoud dat de overheid zich bewust is van Social Engineering en dat zij concrete acties heeft ondernomen om deze dreiging tegen te gaan. Een tweede interpretatie is dat "beschermd zijn tegen" betekent dat de overheid bestand is tegen alle aanvallen op alle plaatsen in het framework. In dit onderzoek zullen de hierboven genoemde interpretaties met behulp van deelvraag 2.1. en 2.2 beantwoord worden.

De eerste interpretatie kan beantwoord worden door te verwijzen naar deelvraag 2.1 "Wat doet de overheid tegen Social Engineering".

De tweede interpretatie van de vraag kan vanwege verschillende redenen niet eenduidig beantwoord worden. Hiervoor is er te weinig informatie verkregen uit de verschillende interviews om te bepalen of de overheid beschermd is tegen de aanvallen uit het framework (zie deelvraag 2.2).

De overheid onderneemt verschillende acties tegen Social Engineering om de organisatie en haar medewerkers te beschermen. Echter een 100% bescherming tegen Social Engineering is in de praktijk niet haalbaar. De mens blijft bij informatiebeveiliging altijd de zwakste schakel. Daarnaast is de organisatie en haar omgeving continu aan veranderingen onderhevig waardoor de bescherming tegen Social Engineering continu geëvalueerd en bijgesteld moet worden. Bescherming tegen Social Engineering is een groeiproces en is daarom nooit af.

Het framework dat opgesteld is in dit onderzoek kan van toegevoegde waarde zijn voor een organisatie om zich beter te beschermen tegen Social Engineering. Door de verschillende aspecten die opgenomen zijn in het framework (zie deelvraag 2.3) in beschouwing te nemen kunnen er mogelijk nieuwe inzichten verkregen worden over wat Social Engineering omvat. Deze nieuwe inzichten kunnen gebruikt worden ter verbetering van de bescherming tegen Social Engineering.

Echter, de enige organisatie die zich 100% kan beschermen tegen Social Engineering is een organisatie zonder mensen.

[4] Hiermee worden de drie geanalyseerde ministeries bedoeld.

5.2 *Aanbevelingen*

Dit onderzoek onderscheidt zich van andere omdat het probeert een algemene beschrijving te geven wat Social Engineering omvat. Daarnaast is er een eerste poging gedaan om Social Engineering inzichtelijk te maken door het te structureren in de vorm van een framework.

Omdat het framework een eerste poging is om Social Engineering te structureren zijn nog niet alle onderdelen, afkomstig uit de begripsbepaling (hoofdstuk 2), hierin opgenomen. Voor de verdere uitbereiding en structurering is vervolgonderzoek noodzakelijk op de volgende gebieden:

1. **Uitbreiding van Social Engineering aanvallen en gereedschappen**
   De begripsbepaling is gebaseerd op bestaande literatuur. Door voortdurend onderzoek op het gebied van Social Engineering zal de bestaande literatuur zich uitbreiden waardoor er weer nieuwe inzichten over Social Engineering aanvallen en gereedschappen verkregen worden. Deze inzichten moeten wanneer zij van toegevoegde waarde zijn opgenomen worden in de begripsbepaling en framework om deze up-to-date te houden.

2. **Relaties tussen Social Engineering aanvallen en gereedschappen**
   De Social Engineer maakt bij een Social Engineering aanval gebruik van verschillende gereedschappen. Aangenomen wordt dat een Social Engineering aanval een beperkte set aan gereedschappen gebruikt die in iedere situatie hetzelfde zijn. Wellicht dat onderzoek kan aantonen wat precies de relatie tussen Social Engineering aanvallen en gereedschappen is.

3. **Relaties tussen de verschillende gereedschappen**
   In dit onderzoek is een onderscheid gemaakt tussen technieken, situaties, menselijke eigenschappen en psychologische principes. Vervolgonderzoek is nodig om de mogelijke relaties tussen de verschillende gereedschappen te bepalen. Hierdoor ontstaat er mogelijk een beter inzicht in het gebruik van de gereedschappen door de Social Engineer.

4. **Uitbereiding van framework met gereedschappen uit begripsbepaling**
   In het framework zijn alleen de Social Engineering aanvallen en de bijbehorende doelen uit de begripsbepaling opgenomen. Vervolgonderzoek kan uitwijzen of de verschillende gereedschappen mogelijk in het framework kunnen worden opgenomen

5. **Toespitsen van framework op organisatiestructuren**
   Wellicht is het mogelijk het framework aan te passen zodat het beter aansluit op bepaalde organisatiestructuren. Dit vereenvoudigt de toepasbaarheid bij organisaties. Vervolgonderzoek is daarom op dit gebied nog nodig.

6. **Het toekennen van variabelen aan Social Engineering aanvallen**
   Vervolgonderzoek is nodig om te bepalen of het mogelijk is variabelen toe te kennen aan de Social Engineering aanvallen die weergegeven zijn in het framework. Voorbeelden van variabelen kunnen zijn: kans van slagen, kosten en risico.

6 Reflectie

6.1 Oorspronkelijk onderzoek

Het onderzoek zoals beschreven in deze scriptie is niet het onderzoek zoals we dit oorspronkelijk hadden willen uitvoeren. Ons oorspronkelijke onderzoek had als doelstelling het vaststellen van kritieke succesfactoren die moeten leiden tot een succesvolle integratie van de informatiebeveiligings policy met betrekking tot Social Engineering. Deze kritieke succesfactoren hadden als doel bij te dragen aan de bescherming tegen Social Engineering door het bewustzijn met betrekking tot informatiebeveiliging te verhogen.

Na twee maanden bleek om verschillende redenen het onderzoek in huidige vorm niet meer haalbaar te zijn. Dit kwam doordat de acquisitie bij de overheid minder voorspoedig verliep dan gedacht. Ten eerste verliep de communicatie bij de overheid langzaam waardoor het moeilijk was om een ingang te vinden en in contact te komen met de juiste personen binnen de ministeries. Ten tweede verliep de besluitvorming om mee te werken aan ons onderzoek langzaam. Dit had te maken met het feit dat Social Engineering een gevoelig onderwerp is binnen de overheid. Ten derde was het niet mogelijk per ministerie zowel managers als medewerkers te interviewen waardoor de resultaten, noodzakelijk voor het oorspronkelijke onderzoek, niet met elkaar vergeleken konden worden. De reden hiervoor was dat onze contactpersonen bij de ministeries niet de tijd konden claimen van andere medewerkers binne het desbetreffende ministerie. Door deze redenen is er besloten het onderzoek aan te passen naar de huidige vorm waarbij de ministeries wel voldoende medewerking konden verlenen.

6.2 Acquisitie ministeries

Het acquisitieproces heeft relatief veel tijd in beslag genomen. Het vinden van de juiste contactpersonen was hierbij erg moeilijk. Van de ministeries die wij hebben benaderd haakte een groot deel na bestudering van ons onderzoeksplan af of liet simpelweg niets meer van zich horen. Dit had waarschijnlijk te maken met het onderwerp van ons onderzoek en het feit dat ministeries niet graag de vuile was buiten hangen. Enkele ministeries hebben we kunnen overtuigen van de toegevoegde waarde van ons onderzoek waarna zij instemden met het afnemen van verschillende interviews. Deze interviews moesten voldoen aan verschillende voorwaarden met betrekking tot de omgang met en publicatie van informatie.

6.3 Globale tijdsinvulling

Ons onderzoek is globaal opgedeeld in drie delen namelijk literatuurstudie, het conceptueel framework en onderzoek bij de ministeries. Van deze drie delen heeft het framework ons de meeste tijd gekost. Het bleek erg moeilijk om de juiste vorm te vinden waarin we Social

Engineering konden structureren. Hier zijn vele brainstorm- en prototypingsessies aan vooraf gegaan, welke niet zijn weergegeven in het onderzoek maar veel tijd hebben gekost.

Daarnaast heeft ook het onderzoek bij de ministeries meer tijd in beslag genomen dan vooraf was aangenomen. Dit kwam vooral omdat we het afnemen en uitwerken van de interviews enigszins hadden onderschat.

6.4 Bereikte resultaat

Wij zijn tevreden over de behaalde resultaten in dit onderzoek. We zijn dan ook van mening dat structurering van het begrip Social Engineering resulterend in een begripsbepaling en conceptueel framework van toegevoegde waarde kan zijn. Bijvoorbeeld voor mensen die zich bezig houden met informatiebeveiliging, als basis voor verder onderzoek en voor een beter inzicht in wat Social Engineering omvat.

De onderzoeksvraag of de overheid beschermd is tegen Social Engineering hebben we in dit onderzoek helaas niet eenduidig kunnen beantwoorden.

6.5 Persoonlijke reflectie

6.5.1 Reflectie Arjan Kieskamp

Met een tevreden gevoel kijk ik terug op het onderzoek dat Robert en ik de afgelopen maanden hebben uitgevoerd. Dit betekent echter niet dat het onderzoek altijd vlekkeloos is verlopen, in tegendeel zelfs. Het feit dat Robert en ik hebben besloten om ons afstudeer onderzoek samen uit te voeren heeft twee redenen. Ten eerste kennen Robert en ik elkaar van de Hogeschool den Bosch waar we de opleiding Bedrijfskundige Informatiesystemen hebben gevolgd en in 2004 zijn afgestudeerd. Destijds hebben we regelmatig met succes samen projecten uitgevoerd waardoor we precies weten wat we aan elkaar hebben. Later tijdens de opleiding Informatiekunde aan de Radboud Universiteit hebben we ook nog dikwijls samen of in groepsverband aan een project of opdracht gewerkt. Ten tweede zijn Robert en ik afzonderlijk altijd al geïnteresseerd geweest in de menselijke factor van ICT en informatiebeveiliging. We waren wel op de hoogte van het fenomeen Social Engineering maar de cursussen Security en Security in Organisations die deel uitmaken van de opleiding Informatiekunde hebben ons er toe bewogen om onderzoek naar dit onderwerp te gaan doen.

We hebben dr. Martijn van Oostdijk en ir. drs. Wolter Pieters gevraagd of zij ons wilden begeleiden tijdens het afstudeeronderzoek. Martijn van Oostdijk was onze docent bij de cursus Security in Organisations en Wolter Pieters was onze docent bij de cursus Security. Beide docenten hebben veel kennis op het gebied van informatie- en computerbeveiliging en waren bovendien toegankelijk.

Het oorspronkelijke onderzoek hebben we net zoals het huidige onderzoek zelf opgezet. We hebben door ons te verdiepen in het onderwerp zelf vragen opgesteld waarvan wij vonden

dat deze relevant waren om te onderzoeken en waarop bovendien niet direct een antwoord te vinden was in de literatuur. Helaas hebben we het oorspronkelijke onderzoek (zie paragraaf 6.1) vanwege een aantal redenen moeten staken. Hoewel dit een enorme tegenslag was, hebben we hiervan geleerd en geprobeerd om de moed niet te laten zakken. We hebben het onderzoek opnieuw opgezet door een ander aspect van Social Engineering te gaan onderzoeken.

Het huidige onderzoek heeft ook nog een aantal tegenslagen gekend. De acquisitie bij de ministeries heeft veel meer tijd gekost dan we hadden gepland. Daarnaast was het erg moeilijk om ministeries over te halen om mee te werken aan ons onderzoek. De drie ministeries die wel medewerking hebben verleend aan ons onderzoek ben ik daarom dankbaar. Het is enorm frustrerend als je oponthoud hebt tijdens je onderzoek zonder er iets aan te kunnen doen, behalve de planning voortdurend vooruit te schuiven. Uiteindelijk zijn we twee maanden uitgelopen op de oorspronkelijke planning, wat ongeveer evenredig staat met de tijd die de gehele acquisitie ons gekost heeft. Het moeilijkste onderdeel uit het onderzoek was het opstellen van het conceptueel framework. De onderzoeksvraag luidde: “Is Social Engineering te structureren in een framework zodat het inzichtelijker wordt?”. We hebben deze vraag beantwoord door een eerste concept versie te maken van een Social Engineering framework. Het proces van inventariseren, brainstormen, structureren, prototyping en realisatie is zeer tijdrovend geweest en heeft ons veel zweetdruppels gekost. Over het resultaat ben ik tevreden hoewel het slechts een eerste versie is waar nog aan gesleuteld moet worden.

De samenwerking met Robert heb ik als zeer prettig ervaren. Behalve dat we elkaar goed konden aanvullen, waren we beide niet terughoudend om kritiek op elkaar te geven. Omdat we allebei met een positieve instelling het onderzoek uitvoerden, heeft er zich geen enkel moment voorgedaan waarbij de continuïteit van het onderzoek in gevaar was.

De beide begeleiders hebben voldoende tijd vrij kunnen maken om ons te begeleiden tijdens het onderzoek. Door periodiek af te spreken was het mogelijk om de voortgang van ons onderzoek in de gaten te houden en inhoudelijk mee te denken over hoe we bepaalde zaken moesten gaan aanpakken. We hebben veel aan deze informatie gehad om ons onderzoek in goede banen te leiden en tot het uiteindelijke resultaat te komen.

Samenvattend ben ik tevreden over het verloop en de uitkomst van ons onderzoek. We hebben het hele onderzoek zelf opgezet en het is ons bovendien gelukt om een deel van het onderzoek te mogen uitvoeren bij de overheid (lees ministeries). Dit heeft ons wel extra tegenslagen opgeleverd. Deze tegenslagen maken deel uit van het onderzoeksproces en leren je om hiermee om te gaan.

Naar mijn mening heeft het onderzoek een toegevoegde waarde voor de wetenschap en organisaties omdat we geprobeerd hebben Social Engineering als complex geheel inzichtelijk te maken. De wetenschap kan op basis van dit onderzoek verder onderzoek doen, organisaties kunnen de resultaten van dit onderzoek gebruiken om zich beter te beschermen tegen Social Engineering.

Ten slotte wil ik alle personen die betrokken waren bij dit onderzoek bedanken voor hun bijdrage. Een extra woord van dank gaat uit naar Robert die het vol wist te houden om elke dag samen met mij in één ruimte te moeten werken.

6.5.2 Reflectie Robert Smit

In deze persoonlijke reflectie zal ik weergeven hoe ik het afstudeeronderzoek heb ervaren. Hierin komen de volgende onderwerpen aan bod: de aanleiding en invulling van het onderzoek, de uitvoering van het onderzoek, de samenwerking met Arjan, de overheid, de begeleiding bij het onderzoek en de opgeleverde resultaten.

De aanleiding om onderzoek te doen naar Social Engineering heeft te maken met onze gezamenlijke interesse in informatiebeveiliging. Al vroeg stond vast dat we onderzoek wilden doen naar een onderwerp in dit gebied. We hebben er toen voor gekozen om zelf ons onderwerp te kiezen en hierbij een onderzoeksplan te schrijven. Van deze keuze heb ik geleerd dat het komen tot een goed onderzoek veel tijd kost en dat het een groeiproces is wat continu moet worden bijgesteld. Echter het feit dat het onderzoek iets is wat je zelf hebt verzonnen en niet is voorgekauwd door anderen geeft het onderzoek een zekere meerwaarde.

De uitvoering van het onderzoek is over het algemeen goed verlopen. Wel zijn we verschillende obstakels tegengekomen die ons onderzoek met twee maanden hebben vertraagd. Ons oorspronkelijke onderzoek met als doel het bepalen van kritieke succesfactoren voor integratie van maatregelen op het gebied van Social Engineering bij de mens hebben we moeten herzien. Dit kwam doordat aan de ene kant ons onderzoek wellicht te ambitieus was en aan de andere kant doordat de verschillende ministeries niet de medewerking konden verlenen die nodig was om ons onderzoek succesvol uit te voeren. We hebben toen besloten ons onderzoek aan te passen zodat deze wel haarbaar zou zijn bij de overheid. Ik vond het jammer dat we deze aanpassing moesten doen omdat ik het oorspronkelijke onderzoek interessanter vond vanwege de grotere praktische component die hier in zat. Een tweede obstakel was het komen tot een overzichtelijk framework wat uiteindelijk veel meer tijd gekost heeft dan verwacht. Dit was werkelijk een hersenkraker. Het laatste obstakel was de acquisitie bij de overheid en het afnemen van de verschillende interviews. De acquisitie verliep trager dan verwacht en het afnemen en uitwerken van de interviews hebben we onderschat.

Over de resultaten van ons onderzoek ben ik zeer te spreken. Vooral de literatuurstudie vastgelegd in de begripsbepaling vind ik solide in elkaar zitten. Er is een duidelijke structuur aangebracht in het begrip Social Engineering en er is een volledig overzicht te geven wat Social Engineering nou precies omvat. Daarnaast zijn enkele onderdelen van Social Engineering gevisualiseerd door middel van een framework waardoor men zich een betere voorstelling kan maken hoe Social Engineering zich manifesteert. Ik vind ook dat de resultaten uit dit onderzoek een duidelijke bijdrage kunnen leveren voor organisaties die zich beter willen beschermen tegen Social Engineering. Ten eerste kan een organisatie zich snel bekend maken met het begrip Social Engineering door dat deze helder beschreven is.

Ten tweede kan een organisatie zowel de begripsbepaling als het framework gebruiken om haar informatiebeveiliging te verbeteren en waar nodig te herzien.

De samenwerking met Arjan is goed verlopen. Eigenlijk had ik niet anders verwacht omdat ik als sinds mijn HBO opleiding Hogere Informatica en mijn opleiding aan de universiteit regelmatig en succesvol met Arjan heb samengewerkt. De reden om dit onderzoek gezamenlijk uit te voeren heeft te maken dat je met z'n tweeën op een andere manier tegen bepaalde zaken aankijkt en elkaar aanvult waar nodig. Daarnaast kan je met twee man een groter onderzoek uitvoeren waarvan de resultaten een grotere impact kunnen hebben.

Wat me tegenviel is de trage besluitvorming bij sommige ministeries en hun houding tegenover wetenschappelijk onderzoek. In sommige gevallen is gebleken dat de overheid schuchter is om onderzoekers een kijkje in de keuken te laten nemen, ook wanneer de overheid er beter van kan worden. Dit geldt echter niet voor iedereen. Uiteindelijk heeft één ministerie ons erg geholpen door ons onderzoek interdepartementaal te bespreken waaruit uiteindelijk drie ministeries bereid waren mee te werken.

Onze begeleiders hebben ons gedurende het onderzoek inhoudelijk goed begeleid. De tijd die zij ter beschikking hebben gesteld en de inhoudelijke feedback die zij ons hebben gegeven is meer dan voldoende. Door periodiek te overleggen konden zij de voortgang van ons onderzoek goed bewaken, en wanneer wij problemen hadden, ons hier bij helpen. Ik vind wel dat beide begeleiders wat kritischer hadden mogen zijn over de inhoud en de aanpak van het onderzoek. Hiermee bedoel ik dat ik liever hoor wanneer iets fout dan dat er hier en daar nog iets verbeterd moet worden. Het was hierdoor moeilijk te peilen of we op de goede weg waren of niet.

Samenvattend kijk ik terug op een geslaagd afstudeeronderzoek voor de opleiding Informatiekunde en een succesvolle samenwerking met Arjan die het toch weer met mij heeft weten vol te houden. Ik heb mede door de tegenslagen die we hebben overwonnen, het bereikte resultaat bij de overheid en het opstellen van het framework veel geleerd. Social Engineering blijft een moeilijk onderwerp om onderzoek naar te doen, zeker bij de overheid.

7 Literatuurlijst

Internet Bronnen (Alfabetisch gesorteerd op onderwerp / titel)

[1] Autoriteit
http://www.historycentral.com/Civics/a.html
[2] Basisemoties
http://www.lichaamstaal.nl/lichaamstaal.html?emotie.html
[3] Code voor Informatie Beveiliging
http://www.cvib.nl/cvibnew/
[4] DNS spoofing
http://www.securesphere.net/download/papers/dnsspoof.htm
[5] Dumpster Diving
http://en.wikipedia.org/wiki/Dumpster_diving
[6] Eavesdropping
http://www.flashback.se/archive/BT/btcsmg.html
[7] Eavesdropping
http://en.wikipedia.org/wiki/Eavesdropping
[8] Eckman, Paul
http://www.paulekman.com
[9] Emotie
http://nl.wikipedia.org/wiki/Emotie
[10] Face
http://www.ateamshrine.co.uk/face.php
[11] Flattery
http://www.websters-online-dictionary.org/definition/flattery
[12] Impersonation
software.allindiansite.com/java/ijava.html
[13] Impersonation
http://en.wikipedia.org/wiki/Impersonation
[14] Information sensivity
http://en.wikipedia.org/wiki/Information_sensitivity
[15] Item-dropping
http://www.darkreading.com/document.asp?doc_id=95556&print=true
[16] Keystroke logging
http://en.wikipedia.org/wiki/Keylogger
[17] Nieuwsgroepen
http://nl.wikipedia.org/wiki/Usenet
[18] Nieuwsgroepen
http://www.breekpunt.nl/artikel.asp?id=1072
[19] Nieuwsgroepen
http://www.computerwoorden.nl/
[20] Overtuigen en beïnvloeden
http://www.leren.nl/cursus/sociale-vaardigheden/overtuigen-beinvloeden/beinvloedingsstrategieen.html

[21] Persoonlijke integriteit
http://www.heinpragt.com/menswerk/integriteit.php
[22] Phishing and Pharming
http://169.244.116.227/~tech/e-mail.html
[23] Phishing
http://en.wikipedia.org/wiki/Phishing
[24] Phishing
http://www.consumentenbond.nl/thema/elektronica_en_communicatie/553726/2660958/2660966/2661002/?ticket=nietlid
[25] Piggybacking
http://www.gbc.t-online.hu/english/bszotare3.htm
[26] Piggybacking
http://en.wikipedia.org/wiki/Piggybacking
[27] Piggybacking
http://www.nve.vt.edu/cias/Resources/glossary.htm
[28] Profiling / footprinting
http://it.ojp.gov/documents/asp/glossary/index.htm
[29] Shoulder-surfing
http://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29
[30] Social Engineering
http://en.wikipedia.org/wiki/Social_engineering_(computer_security)
[31] Surveillance / Profiling
http://en.wikipedia.org/wiki/Surveillance
[32] Tailgating
http://en.wikipedia.org/wiki/Tailgating
[33] The WayBackMachine
http://www.archive.org/web/web.php
[34] Tonino
http://www.nu.nl/news.jsp?n=423176&c=50
[35] URL spoofing
http://en.wikipedia.org/wiki/URL_spoofing
[36] Zoekmachine
http://en.wikipedia.org/wiki/Searchengine

Artikelen (Alfabetisch gesorteerd op auteur achternaam)

[37] M. Allen (2003). *The Use of 'Social Engineering' as a means of Violating Computer Systems.*
Online beschikbaar: http://www.sans.org/rr/whitepapers/engineering/529.php
[38] W. Arthurs (2001). A *Proactive defence to Social Engineering.*
Online beschikbaar: http://www.sans.org/rr/whitepapers/engineering/511.php
[39] Bernz, *The Complete Social Engineering FAQ!*
Online beschikbaar: http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt
[40] M. Bruck (2003). *Social Engineering a little known threat.*
Online beschikbaar: http://www.entrepreneur.com/article/0,4621,309221,00.html
[41] A. Dolan (2004). *Social Engineering Tools of the Trade.*
Online beschikbaar: http://www.sans.org/rr/whitepapers/engineering/1365.php

[42] S. Gaudin (2002). *Social Engineering The Human Side of Hacking.* Online beschikbaar: http://itmanagement.earthweb.com/secu/print.php/1040881/

[43] D. Gragg (2002). A *Multilevel defense against Social Engineering.* Online beschikbaar: http://www.sans.org/rr/whitepapers/engineering/920.php

[44] S. Granger (2001). *Social Engineering Fundamentals.* Online beschikbaar: http://www.securityfocus.com/infocus/1527

[45] S. Granger (2006). *Social Engineering Reloaded.* Online beschikbaar: http://www.securityfocus.com/infocus/1860

[46] Harl (1997). *The psychology of Social Engineering.* Op: Access All Areas III conference. Online beschikbaar: http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html

[47] M. Hermansson, R. Ravne (2005). *Fighting Social Engineering.* Master Thesis. Online beschikbaar: http://www.dsv.su.se/research/seclab/pages/pdf-files/2005-x-281.pdf

[48] D. Janssen (2005). *Social engineering: de menselijke schakel in de informatiebeveiliging.* Master Thesis. Online beschikbaar: http://www.niii.ru.nl/onderwijs/afstudereninfo/scripties/2005/DickJanssenScriptie.pdf

[49] C. Jones (2003). *Social Engineering Understanding and Auditing.* Online beschikbaar: http://www.sans.org/rr/whitepapers/engineering/1332.php

[50] F. Kanters (2005). *Misleiden, intimideren en manipuleren*. In: IT Beheer magazine. Online beschikbaar: http://www.le-platane.nl/Publicaties/Pub%20Social%20eng%20ITBM%204-2005.pdf

[51] L. Kuunders (2001). *Bruce Schneier.* Op: website Code voor Informatiebeveiliging Online beschikbaar: http://www.cvib.nl/cvibnew/2001/10/bruce_schneier.php

[52] C.E. Lively (2003). *Psychological Based Social Engineering.* Online beschikbaar: http://www.giac.org/certified_professionals/practicals/gsec/3547.php

[53] G.L. Orgill, G.W. Romney, M.G. Bailey and P.M. Orgill (2004). *The urgency for effective user privacy-education to counter Social Engineering attacks on secure computer systems*. In: Proceedings of the 5th conference on Information technology education, New York: ACM Press, pp. 177-181, ISBN:1-58113-936-5. Online beschikbaar: http://delivery.acm.org/10.1145/1030000/1029577/p177-orgill.pdf

[54] C. Paradowski (2001). The Cyber Con Game - Social Engineering. Online beschikbaar: http://www.giac.org/practical/gsec/Christopher_Paradowski_GSEC.pdf

[55] K.C. Redmon (2006). Mitigation of Social Engineering Attacks in Corporate America. Online beschikbaar: http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_KRedmon.pdf

[56] T. Thornburgh (2004). *Social Engineering: The "Dark Art"*. In: Proceedings of the 1st annual conference on Information security curriculum development, New York: ACM Press, pp. 133-135, ISBN:1-59593-048-5. Online beschikbaar: http://delivery.acm.org/10.1145/1060000/1059554/p133-thornburgh.pdf?key1=1059554&key2=8345461411&coll=GUIDE&dl=GUIDE&CFID=66643222&CFTOKEN=56148982

[57] R. Tims (2001). Social Engineering: *Policies and Education a Must.*

Online beschikbaar:
http://www.giac.org/certified_professionals/practicals/gsec/0452.php

Boeken

[58] Cialdini, R.B. (1993). *Influence*, HarperCollins College Publishers, ISBN 0673467511
[59] Mitnick, Kevin (2002). The *Art of Deception*, Wiley Publishing, ISBN 076454280X
[60] Ministerie van Binnenlandse Zaken (2004). *Voorschrift Informatiebeveiliging Rijksdienst*
[61] Ministerie van Binnenlandse Zaken (2004). *Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie*

8 Bijlagen

8.1 Bijlage I Geheimhouding en publicatie van gevoelige informatie

8.1.1 Over deze bijlage

Informatie van het type *bijzonder* of *gevoelig*[5] dat verkregen wordt bij de verschillende overheidsinstellingen in geschreven of digitale vorm, zal gedurende en na afronding van dit onderzoek zorgvuldig worden behandeld. De mogelijkheid tot misbruik van deze informatie door derden wordt hiermee voorkomen. In deze bijlage zal uiteen worden gezet hoe aan de waarborging van de geheimhouding van deze informatie invulling wordt gegeven. Er zal een onderverdeling gemaakt worden naar de wijze waarop bijzondere of gevoelige informatie wordt opgeslagen en verschillende mogelijkheden waarop bepaalde onderzoeksresultaten zullen worden gepubliceerd.

8.1.1.1 Vervoer schriftelijk materiaal

Vervoer van geschreven informatie van het type bijzonder of gevoelig zal zo veel mogelijk worden vermeden. Indien deze situatie zich toch voordoet dan zal het materiaal in een afgesloten tas met de grootste zorgvuldigheid worden vervoerd.

8.1.1.2 Vervoer digitaal materiaal

Informatie van het type bijzonder of gevoelig kan in digitale vorm op verschillende manieren worden vervoerd. In geval van een geheugendrager met directe toegang als USB-stick, floppy disk, Compact Disk, etc. zal informatie versleuteld worden opgeslagen met een algemeen bekend en geaccepteerd algoritme. (zie paragraaf opslag digitaal materiaal). In geval het van vervoer van informatie van het type bijzonder of gevoelig op een laptop zullen hiervoor de nodige voorzorgsmaatregelen worden getroffen (zie paragraaf opslag digitaal materiaal).

8.1.1.3 Opslag digitaal materiaal

Gedurende dit afstudeerproject wordt slechts gebruikt gemaakt van 2 laptops die beide zijn voorzien van een beveiligde bios, beveiligde hardeschijf, beveiligd Windows XP besturingssysteem voorzien van de laatste updates en anti virus / spyware. Daarnaast wordt er gebruik gemaakt van een beveiligde Linux server met slechts toegang voor de

[5] Met bijzondere of gevoelige informatie wordt verwezen naar niet-publieke informatie waarvan het uitlekken ervan in meer of mindere mate nadelige gevolgen kan hebben voor de overheid of overheidsinstelling.

onderzoekers van dit onderzoek, waarop informatie van het type bijzonder of gevoelig versleuteld kan worden opgeslagen.
De toegang tot informatie van elk type op de harde schijf van de laptop is altijd beveiligd met een sterk wachtwoord, zelfs bij verwijdering van de harde schijf is deze informatie niet toegankelijk. Informatie van het type bijzonder of gevoelig zal slechts onversleuteld op de harde schijf bestaan als daar een reden voor is. Materiaal op harddisk of ander medium dat bijzondere of gevoelige informatie bevat zal slechts worden opgeslagen door het te versleutelen met een algemeen bekend en geaccepteerd algoritme in combinatie met een voldoende lange willekeurige sleutel. Deze sleutel zal worden opgeslagen in een met sterk wachtwoord beveiligd bestand op de harde schijf.

8.1.1.4 Opslag schriftelijk materiaal

De opslag van geschreven informatie van het type bijzonder of gevoelig zal zoveel mogelijk worden beperkt. Materiaal dat niet nodig is voor onbepaalde tijd zal worden vernietigd (zoals aangegeven in paragraaf vernietiging schriftelijk materiaal). Informatie van het type bijzonder of gevoelig dat met reden bewaard moet blijven voor een bepaalde tijd zal zorgvuldig worden opgeslagen (lees buiten handbereik opgeborgen) in de werkkamer van de onderzoekers op de Radboud Universiteit. De werkkamer is slechts toegankelijk voor beide onderzoekers. Overige individuen hebben slechts toegang tot de werkkamer op uitnodiging van en bij aanwezigheid van minimaal een van de onderzoekers.

8.1.1.5 Vernietiging schriftelijk materiaal

Informatie van het type bijzonder of gevoelig zal worden vernietigd in geval er geen reden tot voortdurende opslag is. Het materiaal zal worden vernietigd door gebruik te maken van een papiervernietiger die het materiaal dusdanig vernietigt dat herstel praktisch gezien onmogelijk is. Bij kleinschalige vernietiging of herkenbaarheid wordt er gebruik gemaakt van het toevoegen van vergelijkbaar random dummy materiaal en een verspreide afvoer van het afval.

8.1.1.6 Vernietiging digitaal materiaal

Informatie van het type bijzonder of gevoelig zal slechts onversleuteld op de harde schijf bestaan als daar een reden voor is. Deze informatie zal worden vernietigd in geval er geen reden tot voortdurende opslag is. Permanente verwijdering zal ervoor zorgen dat het niet in verkeerde handen kan vallen. Ondanks dat bijzondere of gevoelige gegevens versleuteld worden opgeslagen zal in geval van goedkope verwijderbare media deze dusdanig vernietigd worden dat hergebruik onmogelijk is. In geval van bijvoorbeeld een USB-stick kan er een methode gebruikt worden om het geheugen vol te schrijven waardoor sporen worden verwijderd.

8.1.2 Publicatie

8.1.2.1 Non-publieke informatie

Non-publieke documentatie / informatie die wordt ontvangen van de verschillende overheidsinstellingen zal slechts in bezit blijven van beide onderzoekers en op geen enkele wijze worden verspreid aan derden, zelfs als deze derde een andere overheidsinstelling betreft. De vragende overheidsinstelling zal worden doorverwezen naar de overheidsinstelling die de documentatie heeft verstrekt.

8.1.2.2 Non-publieke informatie en afstudeerbegeleiders

Indien het wenselijk is in het belang van het onderzoek om non-publieke informatie te gebruiken in een overleg met beide afstudeerbegeleiders zal hiervoor eerst toestemming worden gevraagd bij de desbetreffende overheidsinstelling. Dan en slechts dan zal na goedkeuring een specifiek deel non-publieke informatie worden overlegd.

8.1.2.3 Publicatie resultaten

Elke overheidsinstelling krijgt een week de tijd om goedkeuring te geven of om mogelijke problemen aan te geven voordat een rapportage in de vorm van een thesis, abstract of presentatie zal worden gepubliceerd. Hierbij zal onderscheid worden gemaakt naar:

Openbare versie
Een publicatie met onderzoeksresultaten die openbaar toegankelijk is, dit kan eventueel een gecensureerde versie zijn van een vertrouwelijke versie. Er zal nimmer met naam en toenaam naar een overheidsinstelling worden verwezen, wel kan er in een bepaalde situatie gesproken worden over een specifieke overheidstelling als X, Y of Z. Hieruit zal vervolgens op geen enkele wijze afleidbaar zijn over welke overheidsinstelling in deze situatie wordt gesproken. (Afstudeer scriptie / abstract)

Vertrouwelijke versie
Onderzoekers en overheidsinstellingen

- *Vertrouwelijk per overheidsinstelling*
  De gepubliceerde rapportage zal zodanig worden opgesteld dat de resultaten niet herleidbaar zijn naar een specifieke overheidsinstelling. Wel kan er in een bepaalde situatie gesproken worden over een bepaalde overheidstelling als X, Y of Z. Specifieke informatie over de desbetreffende overheidsinstelling wordt in deze publicatie wel vermeld. (Verslag interviews)

- *Vertrouwelijk onder de meewerkende overheidsinstellingen*

De gepubliceerde rapportage is vertrouwelijk onder de meewerkende overheidsinstellingen. De overheidsinstellingen hebben onderling geen geheimen voor elkaar. (Advies ministeries)

Universiteit
Per hierboven genoemde twee punten kan onderscheid gemaakt worden of de beide afstudeerbegeleiders en eventueel een derde onafhankelijke lezer toestemming krijgen om de desbetreffende publicatie in zien. Hierover zal overleg gepleegd worden met de desbetreffende overheidsinstelling(en). Indien er geen toestemming verleend wordt bestaat er de mogelijkheid om censuur toe te passen waarna een nieuw verzoek tot leesrecht voor afstudeerbegeleiders en derde onafhankelijke lezer zal worden ingediend. (Beoordeling afstudeerscriptie door Universiteit)

8.2 Bijlage 2: Interviewvragen

8.2.1 Social Engineering: Herkenning en bescherming tegen

1. Is het ministerie bekend met het begrip Social Engineering?
2. Wat verstaat het ministerie precies onder het begrip Social Engineering?
3. Hoe denkt u dat een Social Engineer te werk gaat?
4. Zijn er concrete gevallen van Social Engineering bij het ministerie bekend die in het verleden hebben plaatsgevonden?
5. Zijn er gevallen van Social Engineering bekend buiten het ministerie die hebben bijgedragen tot concrete acties binnen het ministerie?
6. Is het ministerie voldoende beschermd tegen Social Engineering?

8.2.2 Maatregelen tegen Social Engineering en naleving

1. Wat doet het ministerie tegen Social Engineering?
2. Zijn er maatregelen getroffen die het Ministerie en haar medewerkers beschermt tegen Social Engineering? Zijn deze algemeen of concreet van aard?
3. Hoe zijn/worden maatregelen met betrekking tot Social Engineering gecommuniceerd naar de medewerkers?
4. Hoe wordt er gecontroleerd dat maatregelen met betrekking tot Social Engineering worden nageleefd?
5. Hoe staan medewerkers tegenover informatiebeveiliging waar Social Engineering onderdeel vanuit maakt?

8.2.3 Scenario's

Hier worden per ministerie een x (afhankelijk van de tijd) aantal scenario's voorgelegd met daarbij de volgende vragen.

Impersonation

Telefoon

Een medewerker wordt opgebeld door een medewerker van de helpdesk. Ze zijn bezig met een interne controle of de wachtwoorden van de medewerkers voldoen aan de nieuwe beveiligingseisen.

`Wilt u voor ons enkele vragen beantwoorden waardoor de beveiliging van informatie bij het ministerie kunnen verbeteren?'

`We hebben recentelijk nieuwe beveiligingsmaatregelen versneld doorgevoerd naar aanleiding van verschillende incidenten die onlangs hebben plaatsgevonden`. `Eén van deze maatregelen betreft de samenstelling van wachtwoorden´. We hebben inmiddels de helft van alle medewerkers van het ministerie al gecontroleerd en er is gebleken dat maar 10% een wachtwoord heeft wat aan de eisen voldoet. `Graag willen we wat vragen stellen om te kijken of uw wachtwoord aan de nieuwe eisen voldoet´.

1. Hoe zou u deze aanval beperkt/voorkomen hebben?
2. Welke acties zou u ondernemen?
3. Heeft het ministerie maatregelen die deze aanval kunnen beperken/ voorkomen?
4. Had een medewerker deze aanval kunnen herkennen en beperken/voorkomen?

Fysieke toegang

De Social Engineer is onder valse voorwendselen binnen gekomen bij het ministerie. Hij bevindt zich nu binnen het gebouw en kan zich hier vrij rond bewegen en toegang verschaffen tot verschillende gegevensdragers en informatiesystemen.

Bijvoorbeeld:

- Hij gaat een niet afgesloten kantoor binnen en vindt daar diverse documenten op het bureau of in de afvalbak(wachtwoord op postit, rapporten, usbstick).
- Hij plaats een keylogger die hij op een later tijdstip weer ophaalt.
- Hij loopt de printerruimte binnen en vindt daar verschillende uitgeprinte documenten die hij meeneemt of vastlegt.
- Hij kopieert gegevens van het prikbord zoals namen, adressen, telefoonnummers, verjaardagen, agenda's etc.
- Hij legt een cdrom met een aanlokkelijke titel neer bij op een bureau dat in werkelijkheid een trojan bevat.
- Hij gebruikt een intern toestel om zich voor te doen als iemand anders
- Hij voert een fysieke Impersonation uit door zich voor te doen als een collega

1. Hoe zou u deze aanval beperkt/voorkomen hebben?
2. Welke acties zou u ondernemen?
3. Heeft het ministerie maatregelen die deze aanval kunnen beperken/ voorkomen?
4. Had een medewerker deze aanval kunnen herkennen en beperken/voorkomen?

Phishing

Een medewerker krijgt een e-mail met daarin de vraag of hij zich wil aanmelden voor het online smoelenboek van het ministerie. Aangegeven wordt dat dit een intern initiatief is om collega's dichter bij elkaar te brengen ter bevordering van de interne communicatie en bedrijfsvoering. Dit initiatief is goedgekeurd door de directie van het ministerie. In de e-mail staat een link die toegang geeft tot het smoelenboek. Hiervoor is de gebruikersnaam en het wachtwoord wat de medewerker gebruikt voor intern gebruik (bv Intranet) vereist. Dit om de medewerker te identificeren als medewerker van het ministerie. Er wordt gevraagd om op deze pagina persoonlijke gegevens in te vullen en een foto achter te laten.

Alternatief: Om zich aan te melden moeten ze een account aanmaken door een gebruikersnaam plus wachtwoord te kiezen. Hierna hebben ze toegang tot het smoelenboek.

1. Hoe zou u deze aanval beperkt / voorkomen hebben?
2. Welke acties zou u ondernemen?
3. Heeft het ministerie maatregelen die deze aanval kunnen beperken / voorkomen?
4. Had een medewerker deze aanval kunnen herkennen en beperken / voorkomen?

8.2.4 Locatie en waarde van informatie binnen het ministerie

1. Is er binnen het ministerie een systeem wat de gevoeligheid van informatie aangeeft?
2. Is er een beleid hoe er met informatiedragers moet worden omgegaan?
3. Hoe wordt ervoor gezorgd dat dit beleid wordt nageleefd door de medewerkers?
4. Is er een besef bij de medewerker dat onbelangrijke informatie voor iemand anders juist wel waardevol kan zijn?

8.3 Bijlage 3: Contactpersonen

Naam: Arjan Kieskamp
Organisatie: Radboud Universiteit
Functie: Student
Telefoonnr.: 06-26030890
E-mail: a.a.kieskamp@student.ru.nl
Relatie: Onderzoeker

Naam: Robert Smit
Organisatie: Radboud Universiteit
Functie: Student
Telefoonnr.: 06-24537481
E-mail: crsmit@student.ru.nl
Relatie: Onderzoeker

Naam: ir. drs. Wolter Pieters
Organisatie: Radboud Universiteit
Functie: Junior onderzoeker
Telefoonnr.: +31 24 3652599
E-mail: w.pieters@cs.ru.nl
Relatie: Supervisor

Naam: dr. Martijn Oostdijk
Organisatie: Radboud Universiteit
Functie: Assistent Professor
Telefoonnr.: +31 24 3652713
E-mail: martijno@cs.ru.nl
Relatie: Supervisor