Social engineering binnen de Nederlandse Rijksoverheid

Onderzoek naar het informatiebeveiligingsbeleid bij de Nederlandse Rijksoverheid inzake social engineering

Student:	Krijn van der Laan
Identiteitsnummer:	851212445

Datum rapport:	19 september 2016
Datum presentatie:	25 oktober 2016
Datum einde inschrijving:	01-02-2017

Social engineering binnen de Nederlandse Rijksoverheid

Onderzoek naar het informatiebeveiligingsbeleid bij de Nederlandse Rijksoverheid inzake social engineering

Social Engineering the Dutch Government

Research on the information security policy of the Dutch government for the subject of social engineering

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM9806 Afstudeertraject Business Process Management and IT
Student:	Krijn van der laan
Identiteitsnummer:	851212445
Datum:	25 oktober 2016
Afstudeerbegeleider	dr. ir. H.L. Jonker
Meelezer	dr. ir. H.P.E. Vranken
Derde beoordelaar	N.V.T.
Versie nummer:	1.4
Status:	definitief

Abstract

De opkomst van informatiesystemen en beschermingsmechanismen leek de beveiligingsproblemen te hebben opgelost. Echter, het cruciale element blijft het individu en niet de machine. Het installeren van de nieuwste beveiligingsmechanismen staat dan ook niet garant voor een volledige bescherming van het systeem. Het systeem met het beveiligingsmechanisme hoeft niet zelf geïnfiltreerd te worden, het is vaak gemakkelijker om de informatie te krijgen die nodig is met behulp van overtuigingskracht, manipulatie of goede wil. Social engineers vallen de zwakste schakel aan in de organisatie, namelijk de mensen.

Het doel van dit onderzoek is om te achterhalen wat het verschil is tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid omtrent de geïdentificeerde socialengineeringmaatregelen uit het literatuuronderzoek en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid?

Hiervoor is de volgende onderzoeksvraag opgesteld:
Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid omtrent de geïdentificeerde socialengineeringmaatregelen uit het literatuuronderzoek en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid?

Om een antwoord te kunnen geven op de onderzoeksvragen is een enquête, een case study en een archief onderzoek uitgevoerd waarvoor interviews met respondenten van de Rijksoverheid zijn gehouden in combinatie met online vragenlijsten aan respondenten van de Rijksoverheid.

Uit de antwoorden op de vragenlijsten en interviews in combinatie met het archiefonderzoek bleek dat er een wezenlijk verschil is in de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid. Vrijwel alle maatregelen tegen socialengineeringsaanvallen geïdentificeerd in het literatuuronderzoek zijn alleen indirect aanwezig in het informatiebeveiligingsbeleid van de Rijksoverheid. Dit informatiebeveiligingsbeleid dringt echter niet volledig door tot de werkvloer. De gemiddelde awareness van een medewerker op het informatiebeveiligingsbeleid tegen social engineering in dit onderzoek blijkt 64,82% te zijn, waarvan 5 van de 19 aspecten onder de 50 procent scoren en slechts één aspect de volledige 100 procent. Dit duidt erop dat de Rijksoverheid zich meer richt op het afvinken van opgesteld informatiebeveiligingsbeleid en minder op de doorvoering van de awareness op dit informatiebeveiligingsbeleid.
Tevens wordt er in het informatiebeveiligingsbeleid niet direct over social engineering gesproken.

De belangrijkste aanbevelingen op basis hiervan zijn:

- Er dient een gestructureerde oplossing/manier te komen om social engineering en soortgelijke informatiebeveiligingsaspecten onder de aandacht te brengen binnen de Rijksoverheid. In deze oplossing moeten de meestvoorkomende aanvallen en technieken met de maatregelen die ertegen genomen kunnen worden, worden beschreven. Een verwijzing naar deze gestructureerde oplossing inzage social engineering kan vervolgens worden opgenomen in de BIR.
- Het aanbieden van opleidingen en trainingen inzake social engineering en het informatiebeveiligingsbeleid om de bewustwording te vergroten.

Sleutelbegrippen

Social Engineering, Rijksoverheid, informatiebeveiligingsbeleid, medewerker awareness .

Woord vooraf

Deze scriptie met de titel ‘Social engineering binnen de Nederlandse Rijksoverheid’ is het eindresultaat van het empirisch afstudeeronderzoek. Deze scriptie dient ter afsluiting van de masteropleiding Business Proces Management & IT aan de Open Universiteit.
Het onderzoek is uitgevoerd binnen de Nederlandse Rijksoverheid.

Graag wil ik via deze weg alle mensen bedanken die deze scriptie mogelijk hebben gemaakt.
Als eerste dank ik mijn begeleider dr. ir. H.L. Jonker voor de constructieve samenwerking, zijn feedback en het enthousiasme voor het vakgebied.
Daarnaast ben ik alle geïnterviewde personen en respondenten van de enquête erkentelijk voor hun tijd en bijdrage.
Als laatste wil ik mijn werkgever, het SSC-ICT, bedanken voor de financiële bijdrage en tijd die hij mij ter beschikking heeft gesteld tijdens deze opleiding.

Ik wens allen die deze scriptie lezen veel leesplezier!

Krijn van der Laan,
September 2016

Samenvatting

De opkomst van informatiesystemen en beschermingsmechanismen leek de beveiligingsproblemen te hebben opgelost. Echter, het cruciale element blijft het individu en niet de machine. Het installeren van de nieuwste beveiligingsmechanismen staat dan ook niet garant voor een volledige bescherming van het systeem. Het systeem met het beveiligingsmechanisme hoeft niet zelf geïnfiltreerd te worden, het is vaak gemakkelijker om de informatie te krijgen die nodig is met behulp van overtuigingskracht, manipulatie of goede wil. Social engineers vallen de zwakste schakel aan in de organisatie, namelijk de mensen.

Dit onderzoek richt zich op het informatiebeveiligingsbeleid bij de Nederlandse Rijksoverheid inzake social engineering.

Doelstelling
De doelstellingen van dit empirisch onderzoek zijn:

- Onderzoeken in hoeverre er informatiebeveiligingsbeleid is opgesteld inzake social engineering binnen de Nederlandse Rijksoverheid.
- De dekkingsgraad van het informatiebeveiligingsbeleid inzake social engineering onderzoeken.
- De bewustwording van het informatiebeveiligingsbeleid inzake social engineering bij de medewerkers onderzoeken.
- Onderzoeken hoe bekend de medewerkers van de Rijksoverheid zijn met het begrip en de terminologie van social engineering.
- Onderzoeken of de Nederlandse Rijksoverheid te maken heeft gehad met aanvallen via social engineering in de afgelopen zes maanden.

Hoofdvragen
De hoofdvragen van het onderzoek luiden als volgt:

1. Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid inzake de geïdentificeerde socialengineeringmaatregelen uit het literatuuronderzoek en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid?

2. In hoeverre is de Rijksoverheid zelf het doelwit of slachtoffer van socialengineeringaanvallen geweest in de afgelopen 6 maanden?

Gevolgde onderzoeksstrategie
Als eerste is stapsgewijs een onderzoeksstrategie opgesteld. Dit stappenplan geeft de verschillende fasen weer van het empirisch onderzoekstraject en ziet er als volgt uit:

1. Opstellen/uitbreiden conceptueel raamwerk op basis van het literatuuronderzoek
2. Uitwerken onderzoeksplan
3. Eerste aanzet methode van onderzoek
4. Deskresearch beschikbare informatiebeveiligingsdocumenten
5. Afnemen interviews
6. Verwerken resultaten interviews
7. Afnemen enquêtes
8. Verwerken resultaten enquêtes
9. Afronden methode van onderzoek
10. Uitwerken van onderzoeksresultaten
11. Beantwoorden van hoofd- en deelvragen

12. Afronden scriptieverslag
13. Presentatie afstudeerscriptie.

Conclusie hoofdvraag 1
Er is een aanzienlijk verschil tussen de mate van bescherming in theorie en die in de praktijk bij de Rijksoverheid.

Om te kunnen concluderen dat er geen verschil is tussen de theorie en de praktijk moeten alle percentages van de awareness van het informatiebeveiligingsbeleid 100 procent zijn.
Zoals in de onderstaande tabel is weergegeven, komt dit maar bij één beveiligingsmaatregel voor, de fysieke beveiligingsmaatregel voor de invoering van bezoekerspasjes. Bij vijf maatregelen is minder dan de helft van de medewerkers op de hoogte van het informatiebeveiligingsbeleid.
Alle percentages onder de 50% zijn rood gemarkeerd om te verduidelijken dat hier de meeste winst te behalen is.

Administratieve beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**	**Awareness van de medewerkers van dit beleid**
Antivirus/antiphishing	Ja	71,4%
Arbeidsvoorwaarden	Ja	35,7%
Auditbeleid en -controles	Ja	Niet gevraagd
Blokkering toegangsrechten	Ja	89,3%
Clean desk	Ja	96,4%
Controle beschikbaarheid positieve referenties	Nee	21,4%
Controle juistheid van curriculum	Nee	60%
Disciplinaire maatregelen	Ja	32,1%
Documentafhandeling/-vernietiging	Ja	50%
E-mailfiltering	Ja	Niet gevraagd
Het beperken van datalekken	Ja	57,1%
Incidentafhandelingsstrategie	Ja	60,7%
Informatieclassificatie	Ja	42,9%
Locken van computer	Ja	92,6%
Retourneren van bedrijfsmiddelen	Ja	77,4%
Wachtwoordmanagement	Ja	96,4%

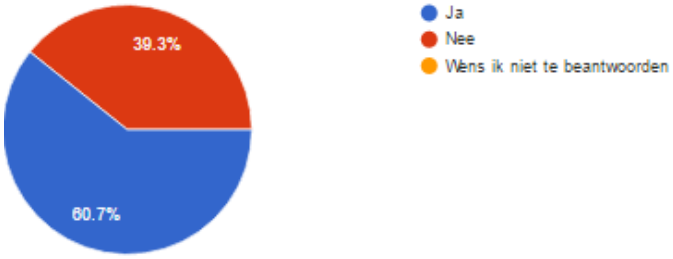
Tabel 1: Aanwezig administratief beleid inclusief de awareness van dit beleid

Fysieke beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**	**Awareness van de medewerkers van dit beleid**
Aanmeldformulieren bezoekers	Ja	96,4%
Beveiligingscamera's	Ja	67,9%
Bezoekerspasjes	Ja	100%
Biometrische toegangsdeuren	Nee	10,7%
Foto-identificatiepasjes	Ja	67,9%

Tabel 2: Aanwezig fysiek beleid inclusief de awareness van dit beleid

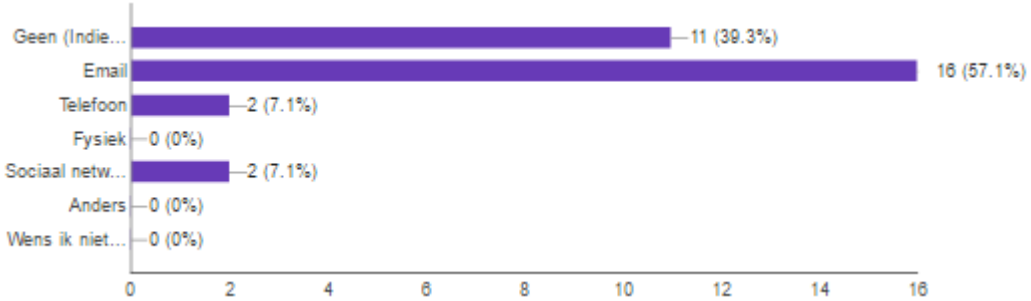
Het lijkt er dan ook op dat de Rijksoverheid te veel vertrouwt op de aanwezigheid van beleid om in theorie te kunnen aantonen dat zij aan alle eisen uit de BIR heeft voldaan. De Rijksoverheid neemt een afwachtende houding aan met de gedachte dat zij veilig is totdat het tegendeel is bewezen. Het invoeren van beleid zonder dat dit beleid bekend is bij de medewerkers betekent in feite dat het beleid nooit het gewenste resultaat zal hebben.

Conclusie centrale vraagstelling 2:
De Rijksoverheid is zelf veelvuldig het doelwit/slachtoffer van socialengineeringaanvallen. 60,7% van de respondenten denkt het doelwit/slachtoffer te zijn geweest van een socialengineeringaanval in de afgelopen zes maanden.



Figuur 1: Percentage medewerkers dat slachtoffer is geweest van een socialengineeringaanval in de afgelopen zes maanden

Hierbij geeft 57,1% van de respondenten aan dat de poging via e-mail verliep. 7,1% geeft aan via de telefoon en een sociaal netwerk te zijn benaderd.
Dit betekent dat ongeveer 10% van de medewerkers doelwit/slachtoffer is geweest van drie socialengineeringaanvallen via verschillende kanalen in de afgelopen zes maanden.



Figuur 2: Medium waarmee de aanval werd uitgevoerd

Eindconclusie:
Uit de conclusie van onderzoeksvraag twee wordt inzichtelijk dat 60,7% van de respondenten in de laatste zes maanden denkt slachtoffer te zijn geweest van een socialengineeringsaanval. Uit deze cijfers blijkt dat het probleem social engineering binnen de Rijksoverheid wel degelijk bestaat. De schade is in dit onderzoek niet onderzocht echter in het literatuuronderzoek kwam naar voren dat het opruimen van een incident in de betreffende onderzoeken gemiddeld 40.000 USD kost voor de onderzochte organisaties. Waarschijnlijk berokkent social engineering dan ook aanzienlijke schade aan de Rijksoverheid. Met deze cijfers zouden we verwachten dat social engineering een belangrijk punt is binnen de informatiebeveiligingsbeleid van de Rijksoverheid.

Niets is echter minder waar. Iedere Rijksdienst voert het op Rijksoverheid bepaalde informatiebeveiligingsbeleid door binnen hun organisatie. Hiermee proberen deze Rijksdiensten naar hun beste vermogen social engineering het hoofd te bieden. Social engineering wordt echter niet direct genoemd in de belangrijkste informatiebeveiligingsdocumenten van de Rijksoverheid. Indirect worden in deze informatiebeveiligingsdocumenten echter wel vrijwel alle onderzochte beveiligingsmaatregelen uit dit onderzoek tegen socialengineeringsaanvallen afgedekt.

De gemiddelde awareness van een medewerker op het informatiebeveiligingsbeleid tegen social engineering in dit onderzoek blijkt 64,82% te zijn, waarvan 5 van de 19 aspecten onder de 50 procent scoren en slechts één aspect de volledige 100 procent. Voor de Rijksoverheid en de Rijksdiensten valt op het awareness aspect dan ook de grootste winst te behalen.

Aanbevelingen voor wetenschappelijk vervolgonderzoek
Het onderzoek moet met een andere vraagstelling of andere scope worden uitgevoerd. De scope moet worden verbreed om de onderzoeksresultaten generaliseerbaarder te maken. Ook kunnen enkele vragen die tijdens dit onderzoek naar boven zijn gekomen worden uitgezocht.
Enkele voorbeelden hiervan zijn:

- Scopeaanpassing/-verbreding naar een heel ministerie, een volledige Rijksdienst of de volledige Rijksoverheid.
- Scopeaanpassing naar België of de Europese Unie (EU). Social engineering komt in alle EU-landen voor. Het zou dan ook interessant zijn om te bekijken hoe andere overheden en de EU hier mee omgaan en welke wetgeving/maatregelen zij hiertegen hebben ingevoerd.
- Hoe wordt het informatiebeveiligingsbeleid geüpdatet, hoe lang duurt het voordat het informatiebeveiligingsbeleid dat is opgesteld bij alle Rijksdiensten bekend is en is ingevoerd?
- Wordt het informatiebeveiligingsbeleid ook nageleefd? Het testen van het informatiebeveiligingsbeleid of het houden van interviews/enquêtes over het informatiebeveiligingsbeleid.
- Het testen van het informatiebeveiligingsbeleid door middel van aanvallen, zoals een mystery guest om binnen te komen of penetratietesten op de medewerkers (phishing mails etc.).
- Welke informatiebeveiligingsmaatregelen beschermen daadwerkelijk tegen de methoden of technieken van social engineering?
- Is er een verband tussen de awareness en het aantal jaar dat iemand werkzaam is in zijn functie? Zijn hier wezenlijke verschillen tussen?
- Is er een verband tussen de awareness van interne medewerkers en die van externe medewerkers? Zijn hier wezenlijke verschillen tussen?
- Hoe wordt het informatiebeveiligingsbeleid overgebracht op de medewerkers?

Hetzelfde onderzoek moet over een aantal jaar nogmaals worden uitgevoerd. De gebieden van informatiebeveiliging en social engineering veranderen continu. Over twee jaar kan het referentiemodel er totaal anders uitzien door nieuwe inzichten, aanvallen, maatregelen of de techniek. Ook zou het interessant zijn om te zien of na een aantal jaar de uitkomsten zijn verbeterd ten opzichte van dit onderzoek.

Aanbevelingen voor de praktijk (Rijksoverheid)
De volgende aanbevelingen zorgen ervoor dat de aspecten van social engineering bij de Rijksoverheid beter onder de aandacht worden gebracht:

- Er dient een gestructureerde oplossing/manier te komen om social engineering en soortgelijke informatiebeveiligingsaspecten onder de aandacht te brengen binnen de Rijksoverheid. In deze oplossing moeten de meestvoorkomende aanvallen en technieken met de maatregelen die ertegen genomen kunnen worden, worden beschreven. Een verwijzing naar deze gestructureerde oplossing inzake social engineering kan vervolgens worden opgenomen in de Baseline Informatiebeveiliging Rijksdienst (BIR).
- Een risicoanalyse uitvoeren van de drie maatregelen waar geen beleid voor is om te beslissen of hier beleid voor dient te komen.
- Het uitvoeren van een penetratietest met behulp van het referentiemodel social engineering teneinde de daadwerkelijke bescherming tegen social engineering vast te stellen.
- Het aanbieden van opleidingen en trainingen inzake social engineering en het informatiebeveiligingsbeleid om de bewustwording te vergroten.
- Informatiebeveiliging als vast onderwerp in functioneringsgesprekken opnemen om op de hoogte te blijven van de laatste updates.

Rijksdiensten kunnen zich pro-actiever opstellen jegens de bepaling van de inhoud van de BIR. Momenteel hebben de Rijksdiensten een afwachtende houding.

Inhoudsopgave

1 Context van het onderzoek

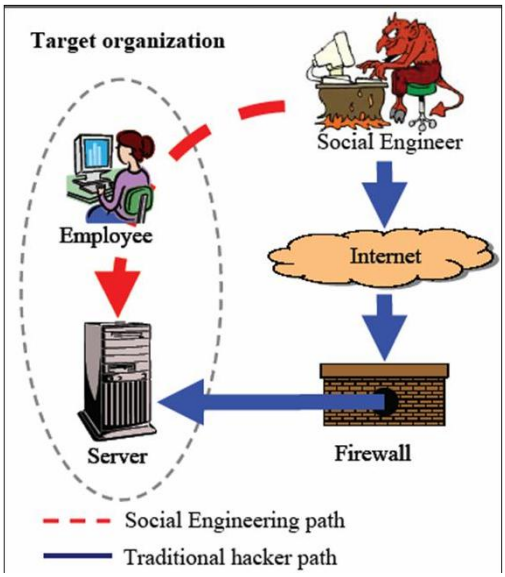
Dit afstudeeronderzoek is verricht in het kader van de masteropleiding Business Process Management and IT aan de Open Universiteit. Dit hoofdstuk bestaat uit de volgende onderdelen:

- De aanleiding voor het onderzoek
- De relevantie van het onderzoek
- De leeswijzer

1.1 Aanleiding voor het onderzoek

De hoeveelheid informatie waarover een individu of organisatie beschikt, is evenredig met de macht die een organisatie of individu over anderen kan hebben. Daarom is niet alleen de verwerving van informatie belangrijk maar is ook de bescherming van informatie tegen potentiële aanvallen van belang.

De opkomst van informatiesystemen en beschermingsmechanismen leek de beveiligingsproblemen te hebben opgelost. Echter, het cruciale element blijft het individu en niet de machine. Het installeren van de nieuwste beveiligingsmechanismen staat dan ook niet garant voor een volledige bescherming van het systeem. Het systeem met het beveiligingsmechanisme hoeft niet zelf geïnfiltreerd te worden, het is vaak gemakkelijker om de benodigde informatie te verkrijgen met behulp van overtuigingskracht, manipulatie of goede wil. Social engineers vallen dan ook de zwakste schakel aan in de organisatie, namelijk de mensen.



Figuur 3: The Social Engineer (Hermansson & Ravne, 2005)

Technologie alleen is weerloos als deze schakel wordt uitgebuit. Dit maakt dat socialengineeringaanvallen behoren tot de gevaarlijkste aanvallen voor een organisatie.

Uit het literatuuronderzoek dat eerder is verricht, is gebleken dat een aanzienlijk aantal organisaties te maken krijgt met social engineering. Uit het onderzoek dat is uitgevoerd door Research (Research, D. (2011)) blijkt dat 48% van de onderzochte grote bedrijven en 32% van de kleine bedrijven socialengineeringaanvallen hadden ondervonden. De gemiddelde kostprijs om een aanval af te wikkelen is 25.000 USD.

Uit onderzoek van Institute (Institute, 2014) blijkt dat 52% van de onderzochte organisaties een socialengineeringaanval heeft meegemaakt. De gemiddelde kostprijs om een aanval af te wikkelen is 46.000 USD bij de onderzochte bedrijven.

In Nederland is ook onderzoek gedaan naar socialengineeringaanvallen. Uit het onderzoek van Capgemini in Nederland (Capgemini, 2015) blijkt dat 37% van de bedrijven met een dergelijke aanval te maken heeft gehad. De gemiddelde kostprijs van een socialengineeringsaanval op een bedrijf is niet onderzocht in dit onderzoek.

De genoemde onderzoeken worden uitgebreider besproken in de literatuurstudie, die is toegevoegd als bijlage.

In dit empirisch onderzoek wordt onderzocht in welke mate de Nederlandse Rijksoverheid informatiebeveiligingsbeleid heeft ingevoerd inzake social engineering en in hoeverre dit informatiebeveiligingsbeleid bekend is bij de medewerkers in de praktijk.

1.2 Relevantie

Er liggen drie soorten relevantie ten grondslag aan de uitvoering van dit onderzoek, te weten wetenschappelijke relevantie, praktische relevantie en persoonlijke relevantie. Deze worden hieronder toegelicht.

1.2.1 Wetenschappelijke relevantie

Uit het uitgevoerde literatuuronderzoek blijkt dat social engineering leeft in de literatuur. De literatuur beschrijft de laatste ontwikkelingen en is compleet. De informatie is echter niet volledig in één model of op één plaats vastgelegd.
Tevens blijkt uit de studies die worden besproken in hoofdstuk 3 van het literatuuronderzoek dat een groot deel van de organisaties te maken krijgt met social engineering.

Voorafgaand aan dit onderzoek heeft literatuuronderzoek plaatsgevonden. De hoofdvraag daarin was: 'Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarin of wat ontbreekt?'
Deze vraag is met 'ja' beantwoord. Er ontbreekt een risicomanagementmodel dat specifiek social engineering aangaat. Ook ontbreekt een totaaloverzicht van alle essentiële controles en welke aanvallen/technieken/emoties worden afgedekt door gebruik te maken van deze controles.

Met deze conclusie uit het literatuuronderzoek ben ik op zoek gegaan naar empirische onderzoeken/praktijkonderzoeken inzake social engineering of bepaalde aspecten uit social engineering binnen de overheid (gemeenten, ministeries, rijksdiensten etc.). Ik ben zelf werkzaam binnen de Rijksoverheid waardoor de gedachte was om mijn positie binnen de overheid te gebruiken. Met behulp van een persoonlijk netwerk binnen een organisatie is het gemakkelijker deuren te openen dan als buitenstaander.

Uiteindelijk zijn twee relevante empirische onderzoeken en een aantal praktijkonderzoeken naar het bedrijfsleven gevonden. Deze praktijkonderzoeken beschrijven in hoeverre het bedrijfsleven slachtoffer is of te maken heeft gehad met socialengineeringaanvallen met bijkomende schade. Deze onderzoeken beschrijven niet welke maatregelen bedrijven hebben genomen en welk informatiebeveiligingsbeleid aanwezig is.

Het eerste empirische onderzoek is een onderzoek naar social engineering binnen de Limburgse gemeenten (Goes, 2012). Het tweede onderzoek is een onderzoek naar phishing binnen de Belgische overheid (Schoofs, 2014).
Deze onderzoeken beschrijven of een procedure, maatregel of informatiebeveiligingsbeleid aanwezig is tegen social engineering en phishing. De onderzoekers vergaten naar mijn mening echter het verschil tussen informatiebeveiligingsbeleid in theorie en in praktijk te onderzoeken. Een organisatie kan via procedures en maatregelen in theorie veel informatiebeveiligingsbeleid hebben opgesteld. Als de medewerkers in de praktijk echter niet op de hoogte zijn van dit informatiebeveiligingsbeleid zal de praktische uitwerking van dit beleid niet effectief zijn. Naar mijn mening zijn de genoemde onderzoeken dan ook onvolledig en zijn ze gedaan op een ander niveau (gemeenten en Belgische overheid) dan waar de Rijksoverheid voor staat.

Ik kwam tot de conclusie dat het op grond van de literatuur en vanuit wetenschappelijk oogpunt niet duidelijk/bekend is:

- Wat het informatiebeveiligingsbeleid is van de Nederlandse Rijksoverheid inzake social engineering
- Of de medewerkers van de Rijksoverheid zich bewust zijn van het geldende informatiebeveiligingsbeleid
- In welke mate de overheid zelf slachtoffer is van socialengineeringaanvallen.

Dit empirisch onderzoek vult dan ook een gat binnen de wetenschappelijke literatuur over het informatiebeveiligingsbeleid en de praktische uitwerking van dit informatiebeveiligingsbeleid inzake social engineering binnen de Nederlandse Rijksoverheid.

1.2.2 Praktische relevantie

Voor de Rijksoverheid heeft het resultaat van het onderzoek de onderstaande voordelen:

- ***Risicobeheersing inzake social engineering:*** door inzicht te krijgen in de mate van aanwezigheid van informatiebeveiligingsbeleid inzake social engineering kunnen risico's in kaart worden gebracht, om deze vervolgens indien nodig af te dekken.
- **Inzicht in de awareness van de medewerkers:** de aanwezigheid van informatiebeveiligingsbeleid wil niet zeggen dat alle medewerkers hiervan automatisch op de hoogte zijn. Met het onderzoek wordt inzichtelijk gemaakt in hoeverre de medewerkers op de hoogte zijn van het opgestelde informatiebeveiligingsbeleid.
- **Kennismaking met of opfrissing van de kennis van social engineering en de aspecten ervan:** de respondenten van de interviews en de enquête bouwen kennis op die ze nog niet hadden of die was verwaterd.

1.2.3 Persoonlijke relevantie

Inmiddels ben ik vier jaar bezig met de universitaire opleiding Business Proces Management and IT. Deze afstudeerscriptie betekent voor mij persoonlijk dan ook de afsluiting van mijn opleiding waarna een vervolgstap gezet kan worden in mijn carrière.

1.3 Doel van dit document

Het doel van dit document is drieledig. Ten eerste is dit document bestemd voor de examencommissie van de Open Universiteit met als doel: de beschrijving van het afstudeerproject die als bewijs moet dienen dat aan alle exameneisen is voldaan.

Ten tweede is het de bedoeling dat het document van waarde is voor de wetenschap en de Rijksoverheid. Voor de wetenschap vult dit document een lacune op in de wetenschappelijke literatuur inzake het informatiebeveiligingsbeleid en de praktische uitwerking van dit informatiebeveiligingsbeleid inzake social engineering binnen de Nederlandse Rijksoverheid.

Ten derde beidt deze scriptie de Rijksoverheid een eerste inzicht in het aanwezige beleid omtrent social engineering, risicobeheersing inzake social engineering en de awareness van de medewerkers van het aanwezige informatiebeveiligingsbeleid.

1.4 Leeswijzer

In hoofdstuk 1 worden de aanleiding voor het onderzoek, de drie relevantievormen en het drieledige doel van het afstudeerdocument gepresenteerd.

In hoofdstuk 2 wordt de onderzoeksopzet beschreven, dus de wijze waarop het empirisch onderzoek is opgebouwd en uitgevoerd. Aspecten die voorbijkomen zijn de doelstelling, onderzoeksvragen, afbakening en scope, onderzoeksbenadering en de onderzoekspopulatie.

In hoofdstuk 3 komt de methode van onderzoek aan de orde. Dit hoofdstuk beschrijft de onderzoeksstrategie, welke onderzoeksmethoden bestaan, welke zijn gebruikt en de reden waarom hiervoor is gekozen. Vervolgens wordt de methode van dataverzameling beschreven. Andere onderzoekers moeten het onderzoek kunnen herhalen.

In hoofdstuk 4 worden de resultaten van het onderzoek gepresenteerd. De informatie die benodigd is voor de beantwoording van de onderzoeksvragen wordt weergegeven.

In hoofdstuk 5 wordt teruggekeken naar de doelstelling en onderzoeksvragen om deze vervolgens te beantwoorden en hier uiteindelijk conclusies uit te trekken.

In hoofdstuk 6 worden aanbevelingen voor verder onderzoek gedaan. Het gaat dan om wetenschappelijk vervolgonderzoek en onderzoek naar de praktijkomgeving (Rijksoverheid).

In hoofdstuk 7 wordt een product- en procesreflectie gepresenteerd. Hier wordt gereflecteerd op de kwaliteit van het onderzoek en de houdbaarheid van de conclusies. Tevens wordt besproken wat goed ging en wat beter kan in de toekomst, met de bijbehorende leerpunten.

De referenties staan in de bibliografie volgens de APA-6 standaard.

In de bijlagen staat additionele informatie die niet geschikt is om in het verslag op te nemen maar toch een wezenlijk onderdeel is van het onderzoek. Het gaat om onderzoeksdata als interview- en enquêtelijsten, uitgewerkte interviews en enquêtes etc.

2 Onderzoeksopzet

De onderzoeksopzet beschrijft het doel van dit empirisch onderzoek en de middelen die worden gebruikt voor de uitvoering van dit onderzoek.

2.1 Doelstelling

De doelstellingen van dit empirisch onderzoek zijn:

- Te onderzoeken in hoeverre er informatiebeveiligingsbeleid is opgesteld inzake social engineering binnen de Nederlandse Rijksoverheid.
- De dekkingsgraad van het informatiebeveiligingsbeleid inzake social engineering te beschrijven.
- De bewustwording van het informatiebeveiligingsbeleid inzake social engineering bij de medewerkers te bevorderen.
- Aan te geven hoe bekend de medewerkers van de Rijksoverheid zijn met het begrip social engineering en de terminologie van social engineering.
- Te onderzoeken of de Nederlandse Rijksoverheid te maken heeft gehad met aanvallen via social engineering in de afgelopen zes maanden.

Aan dit onderzoek ligt het uitgevoerde literatuuronderzoek ten grondslag dat als uitkomst een conceptueel model heeft van de verschillende aanvallen inzake social engineering. Dit conceptueel model wordt uitgebreid met de geïdentificeerde beveiligingsmaatregelen uit de literatuurstudie.

Met deze inzichten kan vervolgens worden bepaald in hoeverre de Nederlandse Rijksoverheid ten tijde van het onderzoek informatiebeveiligingsbeleid heeft inzake social engineering en in hoeverre de medewerkers van de organisatie zich bewust zijn van dit informatiebeveiligingsbeleid inzake social engineering.
Het onderzoek richt zich niet op het oplossen van de gevonden problemen.

2.2 Hoofd- en deelvragen

De eerste hoofdvraag in deze scriptie luidt:

Hoofdvraag 1: 'Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid omtrent de geïdentificeerde socialengineeringmaatregelen uit het literatuuronderzoek en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid?

De eerste hypothese in deze scriptie luid:

Hypothese 1: Het informatiebeveiligingsbeleid inzake social engineering binnen de Rijksoverheid komt niet over bij de medewerkers op de werkvloer.

De deelvragen behorend bij de eerste hoofdvraag luiden:

Deelvragen:

1. Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid?
2. Zijn de medewerkers van de Nederlandse Rijksoverheid inhoudelijk bekend met deze informatiebeveiligingsdocumenten?
3. Zijn de medewerkers van Nederlandse Rijksoverheid bekend met de terminologie van social engineering?
4. Welke socialengineeringmaatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de Rijksoverheid?
5. Wat is de mate van awareness van de medewerkers binnen de Rijksoverheid van het informatiebeveiligingsbeleid inzake social engineering?

De tweede hoofdvraag in deze scriptie luid:

Hoofdvraag 2: In hoeverre is de Rijksoverheid zelf het doelwit of slachtoffer van socialengineeringaanvallen geweest in de afgelopen zes maanden?

De tweede hypothese in deze scriptie luid:

Hypothese 2: Meer dan 50 procent van de onderzochte Rijksoverheid-medewerkers is in de afgelopen zes maanden slachtoffer geweest van een socialengineeringaanval.

De deelvragen behorend bij de tweede hoofdvraag luiden:
Deelvragen:

6. Van welke socialengineeringaanvallen is de Nederlandse Rijksoverheid in het afgelopen jaar slachtoffer geweest en welk medium gebruikten deze aanvallen?

2.3 Scope en afbakening

2.3.1 Scope

Om antwoord te kunnen geven op de hoofdvragen en deelvragen en het wetenschappelijke gat te dichten, wordt een empirisch onderzoek uitgevoerd binnen de Nederlandse Rijksoverheid.

De overheid en de Rijksoverheid zijn niet hetzelfde. Een overheid is het hoogste bevoegde gezag op een bepaald grondgebied. Zo bestaat de totale overheid uit de Rijksoverheid, provincies, gemeenten en waterschappen. Deze overheden nemen op tal van terreinen maatregelen, vaardigen wetten uit

en zien toe op de naleving ervan. In totaal maken meer dan 1.600 organisaties en instanties deel uit van de overheid, waaronder elf ministeries, twaalf provincies en 390 gemeenten.

De Rijksoverheid is onderdeel van de overheid en bestaat onder andere uit elf ministeries in Den Haag, de uitvoerende diensten die onder deze ministeries vallen en de Hoge Colleges van Staat. In totaal werken er bij de Rijksoverheid zo'n 100.000 rijksambtenaren, verspreid over heel Nederland. Bij de Rijksoverheid werken ook veel externe medewerkers die voor een bepaalde periode worden ingehuurd.

De ministeries zijn:

- Ministerie van Algemene Zaken
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Buitenlandse Zaken
- Ministerie van Defensie
- Ministerie van Economische Zaken
- Ministerie van Financiën
- Ministerie van Infrastructuur en Milieu
- Ministerie van Onderwijs, Cultuur en Wetenschap
- Ministerie van Sociale Zaken en Werkgelegenheid
- Ministerie van Veiligheid en Justitie
- Ministerie van Volksgezondheid, Welzijn en Sport

Onder de verantwoordelijkheid van de ministeries vallen veel ambtelijke organisaties en uitvoerende diensten, ook wel sectoren of Rijksdiensten genoemd, zoals de Belastingdienst, het Openbaar Ministerie en de Dienst Justitiële Inrichtingen. Ook heeft de Rijksoverheid verschillende inspecties, zoals de Onderwijsinspectie. Tot slot maken zelfstandige bestuursorganen deel uit van de Rijksoverheid.

Gegeven deze omvangrijke context en de beperkte tijd en onderzoekscapaciteit en het beperkte geld die beschikbaar zijn tijdens deze afstudeeropdracht, is besloten om in te zoomen op drie Rijksdiensten die vallen onder twee verschillende ministeries.

De ministeries en Rijksdiensten waarop wordt ingezoomd, worden op verzoek van de Rijksdiensten geanonimiseerd. Informatiebeveiliging en privacy is een combinatie die gevoelig ligt binnen de Rijksoverheid. Anonimisering van de resultaten was een harde voorwaarde van de Rijksdiensten om mee te werken aan dit onderzoek.

2.3.2 Afbakening

In dit onderzoek wordt niet onderzocht in hoeverre de Nederlandse Rijksoverheid beschermd is tegen social engineering. Het gaat in dit onderzoek om de aanwezigheid en het bewustzijn van het informatiebeveiligingsbeleid. Om te onderzoeken of de Nederlandse Rijksoverheid ook daadwerkelijk beschermd is tegen social engineering dient te worden getest of het informatiebeveiligingsbeleid bestand is tegen socialengineeringaanvallen door middel van praktijktesten.
Tevens is niet onderzocht in hoeverre het informatiebeveiligingsbeleid inzake social engineering wordt nageleefd door de medewerkers van de Nederlandse Rijksoverheid.

2.4 Onderzoekspopulatie

Een belangrijk onderdeel van het empirisch onderzoek is de samenstelling van de onderzoeksgroepen. De onderzoeksgroepen bestaan uit medewerkers van de participerende Rijksdiensten/ministeries. De representativiteit van de populatie was afhankelijk van de bereidheid van de verschillende ministeries, Rijksdiensten en medewerkers om deel te nemen aan het onderzoek. Idealiter namen alle ministeries, Rijksdiensten, afdelingen en medewerkers deel aan het onderzoek. In verband met de beperking in tijd, geld en capaciteit van zowel de onderzoeker als de ministeries was dit echter niet mogelijk.

Er zijn twee varianten om deze onderzoeksgroep te kiezen:

- **Aselecte steekproef:** iedereen in een bepaalde populatie heeft een gelijke kans om geïnterviewd te worden.
- **Selecte steekproef:** afhankelijk van de keuze van de onderzoeker worden bepaalde personen wel of niet geïnterviewd.

Voor dit empirisch onderzoek zijn twee onderzoeksgroepen samengesteld, waarbij verschillende varianten zijn gekozen om de onderzoeksgroep te bepalen.

Interview onderzoekspopulatie

De eerste groep bevat de medewerkers die hebben deelgenomen aan de interviews. Deze groep is selectief samengesteld. In de interviews diende ingegaan te worden op het informatiebeveiligingsbeleid inzake social engineering binnen de organisatie/afdeling. De medewerkers die zijn geselecteerd voor de interviews hebben een IT-, IT security- of managementfunctie.

Enquête onderzoekspopulatie

De tweede groep bevat medewerkers die de enquête toegestuurd hebben gekregen. Deze medewerkers zijn aselectief geselecteerd. Vanuit de deelnemende organisaties zijn bepaalde afdelingen aangewezen waar de enquête uitgezet kon worden. De onderzoeker had hier dan ook geen vrije keuze in.

3 Methode van onderzoek

Bij het maken van een ontwerp voor een onderzoek dient een beslissing genomen te worden over de te volgen aanpak oftewel de onderzoeksmethode. De keuze wordt voorafgegaan door afwegingen omtrent breedte of diepgang, kwalitatief of kwantitatief onderzoek, inductief of deductief, verklarend of verkennend onderzoek en de onderzoeksmethode. De literatuur beschrijft verschillende methoden van onderzoek. Elke methode bestaat uit een combinatie van afwegingen zoals die hierboven zijn genoemd.

3.1 Onderzoeksstrategie

Als eerste is stapsgewijs een onderzoekstrategie opgesteld. Dit stappenplan geeft de verschillende fasen weer van het traject van het empirisch onderzoek.

1. Opstellen/uitbreiden conceptueel raamwerk op basis van het literatuuronderzoek
2. Uitwerken onderzoeksplan
3. Eerste aanzet methode van onderzoek
4. Deskresearch beschikbare informatiebeveiligingsdocumenten
5. Afnemen interviews
6. Verwerken resultaten interviews
7. Afnemen enquêtes
8. Verwerken resultaten enquêtes
9. Afronden methode van onderzoek
10. Uitwerken van onderzoeksresultaten
11. Beantwoorden van hoofd- en deelvragen
12. Afronden scriptieverslag
13. Presentatie afstudeerscriptie.

3.2 Onderzoeksmethoden

Het boek 'Methoden en technieken van onderzoek' geschreven door Saunders en anderen (Saunders, Lewis, Thornhill, Booij, & Verckens, 2013) wordt geleverd bij de aanschaf van de afstudeercursus. In dit boek worden zeven onderzoeksmethoden onderscheiden die in deze paragraaf worden besproken. Van elk van deze zeven methoden wordt aangegeven of deze geschikt is voor dit empirisch onderzoek. De zeven onderzoekmethoden worden hieronder weergegeven, inclusief een korte vooruitblik op de conclusie of deze geschikt zijn:

Onderzoeksmethode	**Geschikt voor soort onderzoek**	**Geschikt (ja of nee)**
Experiment	Richt zich op causale verbanden	Nee
Enquête	Richt zich op kwalitatief en kwantitatief onderzoek door middel van vragenlijsten om feiten en meningen te achterhalen	Ja
Casestudy	Richt zich op een of meer specifieke situaties om daarin inzicht te krijgen of om deze op te lossen	Ja
Action research	Richt zich op het oplossen van een probleem in plaats van te onderzoeken of er een probleem is	Nee
Grounded theory	Richt zich op het bouwen van een model of theorie door een combinatie van inductie en deductie	Nee
Etnografie	Richt zich op het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, zoals zij die zouden beschrijven en verklaren	Nee
Archiefonderzoek	Richt zich op de stand van zaken van een bepaalde situatie in een bepaalde periode (door de tijd, huidig)	Ja

Tabel 3: Onderzoeksmethoden

3.2.1 Het experiment

Het doel van een experiment is het bestuderen van causale verbanden tussen verschillende groepen, om na te gaan of een verandering in één onafhankelijke variabele een verandering teweegbrengt in een andere, afhankelijke variabele.
In een klassiek experiment zijn er twee groepen, waarvan de leden willekeurig over de groepen zijn verdeeld. De leden uit de groepen komen uit een zogenoemde steekproef. Dit betekent dat de twee groepen exact gelijksoortig zijn in alle aspecten die relevant zijn voor het onderzoek, behalve dat de ene groep wel en de andere groep niet aan de geplande interventie of manipulatie wordt blootgesteld.

In het geval van dit onderzoek is deze methode niet geschikt. Bij experimenteel onderzoek worden gegevens verzameld over proefpersonen in een gecontroleerde situatie, om zodoende een hypothese te toetsen. Het doel van het experiment sluit dan ook niet aan op de doelstelling van dit onderzoek.
In dit onderzoek is het doel niet om een causaal verband aan te geven tussen verschillende groepen. In dit onderzoek wordt onderzocht in welke mate de organisatie informatiebeveiligingsbeleid heeft opgesteld tegen social engineering en wordt de mate van bewustzijn van dit informatiebeveiligingsbeleid onder de medewerkers onderzocht.

3.2.2 De enquête

Een enquête is een vragenlijst die aan meerdere personen wordt voorgelegd, om op deze manier onderzoek te doen. Dit kan schriftelijk, maar gebeurt tegenwoordig ook steeds meer digitaal.
Het doel van de enquête is om ‘wie’-, ‘wat’-, ‘waar’- en ‘hoeveel’-vragen te beantwoorden.
Met een enquête kunnen zowel kwantitatieve als kwalitatieve gegevens worden verzameld.
Een enquête kan worden uitgevoerd door middel van een vragenlijst of een interview.

Vragenlijsten maken het mogelijk om op zeer economische wijze uit een omvangrijke populatie informatie te verzamelen. Een vragenlijst bestaat meestal uit meerkeuzevragen en schalen. De respondenten kunnen alleen kiezen uit bepaalde antwoorden en kunnen vaak maar weinig eigen inbreng geven. De vragenlijsten kunnen telefonisch, schriftelijk, online of face-to-face worden afgenomen.
Vragenlijsten worden meestal ingezet voor kwantitatief onderzoek.

Interviews kunnen telefonisch of face-to-face worden afgenomen. De vragen en de volgorde waarin die worden gesteld staan in grote lijnen vast. De interviewer heeft echter in beperkte mate de ruimte om door te vragen naar aanleiding van de antwoorden van de respondent en om te variëren in de volgorde van de vragen. Er zijn verschillende soorten interviews, die elke een eigen mate van vooraf aangebrachte structuur hebben. In semigestructureerde interviews heeft de interviewer bijvoorbeeld veel vrijheid. Er worden vaak open vragen gesteld, waarna doorgevraagd kan worden om daarmee zo gedetailleerd mogelijke informatie te verzamelen. Semigestructureerde interviews worden gebruikt voor kwalitatief onderzoek.

Voor gestructureerde interviews zijn de vragen en vraagvolgorde vooraf bepaald en houdt de interviewer zich aan deze vraagvolgorde. Dit is de interviewsoort die gebruikt dient te worden in kwantitatief onderzoek (Saunders et al., 2013).

Het houden en uitwerken van interviews is tijdrovend. Ten eerste moet de tijd worden genomen om personen op een professionele manier te ondervragen. Ten tweede moet het interview worden uitgewerkt.

Deze methode is geschikt voor dit onderzoek en voor het beantwoorden van de hoofdvragen 1 en 2. Deze methode stelt de onderzoeker in staat in een korte periode tegen geringe kosten ruime, representatieve informatie te verzamelen.
Er kunnen zowel vragenlijsten als (semi)gestructureerde interviews binnen de Rijksdiensten worden afgenomen. Daarnaast sluit deze methode goed aan op de doelstelling en bij het achterhalen van de informatie die benodigd is om de onderzoeksvragen te beantwoorden.

3.2.3 De casestudy

Bij een casestudy wordt één of een klein aantal specifieke situaties intensief onderzocht. Het doel van een casestudy is vaak om inzicht in een situatie te krijgen of om een probleem te onderzoeken. De methode is voornamelijk geschikt voor de vraag 'waarom?', maar kan ook worden gebruikt voor de vragen 'hoe?' en 'wat?', al horen deze laatste vragen in het algemeen eerder bij de enquête. De casestudymethode kan zowel kwalitatieve als kwantitatieve data verzamelen en kan een combinatie van inductie en deductie bevatten.
In de casestudy is het mogelijk om een combinatie van dataverzameling te gebruiken. Dit kunnen zijn: (diepte-)interviews, groepssessies, waarneming, documentenanalyses en vragenlijsten.

Een casestudy onderscheidt vier casestudymodellen gebaseerd op twee discrete dimensies:

- Enkelvoudige case (één organisatie) en meervoudige case (meerdere organisaties)
- Holistische case (het bedrijf als geheel) en ingebedde case (onderscheid tussen teams en afdelingen).

In het geval van dit onderzoek is deze methode geschikt voor het beantwoorden van hoofdvraag 1. De methode sluit aan bij de doelstelling en onderzoeksvragen van dit onderzoek.
In dit onderzoek wordt een specifieke situatie onderzocht, namelijk of er informatiebeveiligingsbeleid is opgesteld inzake social engineering bij de Rijksoverheid.

3.2.4 Action research

Action research heeft als doel 'onderzoek in actie' in plaats van 'onderzoek over actie'. Dit betekent dat het onderzoek zich bezighoudt met het oplossen van een probleem in plaats van het probleem alleen te onderzoeken. Het oplossen van het probleem vindt plaats in een samenwerking tussen de onderzoekers en de medewerkers van de organisatie waarin het probleem zich bevindt. Dit gebeurt in verschillende cycli, zoals diagnose, plannen, actie ondernemen en beoordelen. Action research dient naast de oplossing ook implicaties te hebben buiten het directe onderzoek. Voor de onderzoekers komt dit neer op het ontwikkelen/opstellen van een model of theorie.

De grondlegger van deze methode, Lewin, stelde dat action research-onderzoek aan de volgende voorwaarden moet voldoen:

- Het onderzoek is gericht op het oplossen van een probleem
- Het probleem van het bedrijf staat centraal
- De omstandigheden en de omgeving van het probleem worden onderzocht
- Het onderzoek moet resultaten opleveren die wetenschappelijk te verantwoorden zijn
- De resultaten moeten passen in een theorie of een nieuwe theorie opleveren.

In het geval van dit onderzoek is deze methode niet geschikt. Het doel van de action research-methode sluit niet aan bij de doelstelling en de soort onderzoeksvragen van dit onderzoek. In dit onderzoek wordt namelijk geen probleem onderzocht. Er wordt juist onderzocht of er informatiebeveiligingsbeleid aanwezig is binnen de Rijksoverheid inzake social engineering en er wordt gekeken naar het bewustzijn van dit informatiebeveiligingsbeleid van de medewerkers.

3.2.5 De grounded theory

Het doel van onderzoek dat wordt uitgevoerd met behulp van de grounded theory-methode is voornamelijk om een model of theorie op te bouwen door een combinatie van inductie en deductie. De methode is vooral nuttig voor onderzoek waarin wordt geprobeerd om gedrag te voorspellen en te verklaren. In de grounded theory begint het verzamelen van informatie zonder dat de onderzoeker een theoretisch kader heeft opgesteld. De theorie of het model wordt ontwikkeld door een reeks waarnemingen, voornamelijk (uitgebreide) participerende waarnemingen, te doen.

Voor dit onderzoek is deze methode niet geschikt. Het doel van de grounded theory is met behulp van waarnemingen gedrag te voorspellen en te verklaren om hier vervolgens een model of theorie voor op te stellen. Dit doel sluit niet aan bij de doelstelling van dit onderzoek, waarin wordt onderzocht in welke mate de organisatie beschermd is tegen social engineering en waarin wordt gekeken naar het bewustzijn van social engineering onder de medewerkers. Dit is dan ook een totaal ander doel dan waarvoor de grounded theory is bedoeld.

3.2.6 De etnografie

Het doel van de etnografiemethode is het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, zoals zij die zelf zouden beschrijven en verklaren. Het onderzoeksproces dient flexibel te zijn om snel op veranderingen te kunnen anticiperen. Etnografie is een kwantitatieve en inductieve methode. Het is een methode die over een langere periode wordt gehanteerd en hierdoor veel geld en tijd kost voor de onderzoekers. In de meeste onderzoeken waarin etnografie de onderzoeksmethode is, wordt uitgebreide participerende waarneming gebruikt om de informatie te verzamelen.

In het geval van dit onderzoek is deze methode niet geschikt. Het doel van de etnografieonderzoeksmethode sluit niet aan bij de doelstelling en de soort onderzoeksvragen van dit onderzoek.
Tevens zijn voor dit onderzoek beperkte middelen en tijd beschikbaar waardoor het niet haalbaar is om gedurende een langere periode onderzoek te doen.

3.2.7 Archiefonderzoek

De archiefonderzoeksmethode maakt onderzoeksvragen mogelijk die gericht zijn op een bepaalde periode in het verleden en de veranderingen van gegevens in de loop van de tijd. Het is ook mogelijk om de methode te gebruiken om de huidige stand van zaken te achterhalen. Archiefonderzoek is voornamelijk een kwantitatieve en inductieve methode. Administratieve gegevens en documenten zijn de voornaamste bron bij archiefonderzoek. De documenten bevatten niet altijd de informatie waarnaar de onderzoeker op zoek is. Daarnaast zijn veel documenten vertrouwelijk waardoor toegang krijgen niet altijd mogelijk is.

In het geval van dit onderzoek is deze methode gedeeltelijk geschikt. Een aantal documenten inzake informatiebeveiliging bij de Rijksoverheid is vrij toegankelijk omdat het om ‘rijksbrede’ informatie gaat, terwijl andere informatie specifiek alleen door medewerkers van Rijksdiensten is op te vragen. Deze methode kan worden gebruikt om gedeeltelijk inzicht te krijgen in hoeverre de organisatie momenteel beschermd is tegen social engineering. Voor het inzicht in de mate van bewustzijn van social engineering bij de medewerkers is deze methode echter niet geschikt.

3.2.8 Gekozen onderzoeksmethoden

De keuze voor de onderzoeksmethode is bepaald door een combinatie van de volgende factoren: de doelstelling, de onderzoeksvragen, kennis van het onderwerpsgebied, de beschikbare tijd en de beschikbare middelen bij de organisatie waar het onderzoek wordt uitgevoerd. Van elke onderzoeksmethode is in de vorige paragraaf aangegeven of deze geschikt is voor dit onderzoek.

Het is mogelijk om bij een onderzoek meerdere methoden te gebruiken. Verschillende onderzoeksvragen of hypothesen kunnen een andere onderzoeksmethode vereisen om de vragen correct te kunnen beantwoorden of te bewijzen/ontkrachten. In dit onderzoek zijn twee hoofdvragen geformuleerd waarvoor dan ook potentieel meerdere onderzoeksmethoden benodigd zijn om deze correct te kunnen beantwoorden.
Zoals eerder beargumenteerd zijn meerdere onderzoeksmethoden geschikt voor dit onderzoek, dit zijn:

- De enquête
- De casestudy
- Het archiefonderzoek.

De kenmerken van de casestudy en enquête verschillen niet veel en zijn in meerdere opzichten elkaars gelijke. Het onderscheidende kenmerk tussen deze twee methoden is dat een casestudy werkt met een relatief klein aantal onderzoekseenheden en vaak verschillende dataverzamelingsmethoden combineert, waarbij meer in de diepte dan in de breedte wordt gewerkt. De enquête werkt juist met relatief grote onderzoekseenheden, waarbij meer in de breedte dan in de diepte wordt gewerkt.

Voor dit onderzoek wordt gekozen voor een combinatie van de enquête, casestudy en archiefonderzoek. De combinatie van deze drie onderzoeksmethoden maakt het mogelijk om zowel kwantitatieve als kwalitatieve data te verzamelen en te verwerken. Deze combinatie wordt triangulatie genoemd. Tevens zorgt de combinatie ervoor dat alle aspecten van het onderzoek afgedekt kunnen worden. De enquête zal in deze scriptie voor de onderstaande aspecten worden ingezet.

- De enquête zal worden gebruikt om informatie bij de medewerkers op te vragen
- Het archiefonderzoek en de casestudy richten zich op het aanwezige informatiebeveiligingsbeleid binnen de Rijksoverheid.

De informatie wordt verzameld door middel van de onderstaande dataverzamelingstechnieken, die typerend zijn voor de gekozen onderzoeksmethoden:

1. Documentenonderzoek
2. Semigestructureerde interviews
3. Vragenlijst (zonder open vragen).

Deze technieken zijn verkozen boven groepssessies en participerende observatie (waarneming). Zowel groepssessies als participerende observatie zijn niet geschikt en niet haalbaar binnen de te onderzoeken organisaties. Groepssessies zijn niet geschikt omdat wordt onderzocht of de Rijksoverheid informatiebeveiligingsbeleid heeft opgesteld inzake social engineering en de awareness van dit informatiebeveiligingsbeleid bij de medewerkers, waarvoor het noodzakelijk is om de medewerkers individueel te benaderen en te ondervragen.
Participerende observatie kost veel tijd en capaciteit, die er beide niet zijn voor dit onderzoek.

3.3 Referentieraamwerk social engineering

Een organisatie kan zich beschermen tegen socialengineeringdreigingen met behulp van informatiebeveiligingsmaatregelen/-beleid. Het onderstaande raamwerk is opgesteld door de dreigingen/aanvallen die zijn gevonden in het literatuuronderzoek af te zetten tegen de gevonden beveiligingsmaatregelen in het literatuuronderzoek. Per beveiligingsmaatregel is met een X aangegeven of deze maatregel de betreffende aanval helpt af te dekken.
Het raamwerk maakt duidelijk dat vaak meerdere beveiligingsmaatregelen dezelfde aanval helpen af te dekken. De combinaties tussen de aanvallen en maatregelen zijn door de onderzoeker gemaakt, in de literatuur worden deze combinaties niet beschreven. Er wordt telkens alleen aangegeven dat de beveiligingsmaatregelen helpen het gevaar van social engineering te verminderen. Bij de Rijksdiensten zal worden gekeken welke maatregelen zijn doorgevoerd.

Beveiligingsmaatregelen ==> / Aanvallen van Social engineering	Aanmeldformulier en bezoekers	Anti-virus/-phishing	Auditbeleid en -controles	Beveiligings camera's	Bezoekers pasjes	Biometrische toegangsdeuren	Blokkering toegangsrechten	Clean desk policy	Controle beschikbaarheid positieve referenties	Controle juistheid van Curriculum	Disciplinaire maatregelen	Documentafhandeling/-vernietiging	E-mail-filtering	Foto-identificatie pasjes	Informatie classificatie	Locken van computer	Management buy-in	Opleiding en bewustwording	Retouneren van bedrijfsmiddelen	Wachtwoord management
Advanced Persistent Threat		X	X			X											X	X		
Baiting		X	X			X											X	X		
Data leakage		X				X	X					X	X		X		X	X		
Direct approach	X		X	X	X	X							X	X		X	X	X		
Dumpster diving			X	X	X							X					X	X		
Fake profiles			X														X	X		
Fysieke imitatie	X		X	X	X	X											X	X		
Identity theft	X					X								X	X		X	X		X
Internal Threats	X						X	X	X	X	X	X		X	X	X	X	X	X	
Mail-outs		X															X	X		
Malicious software		X											X				X	X		
Manipulatie van emoties	X													X	X		X	X		X
Office snooping	X		X	X	X	X		X				X				X	X	X		X
People spotting																	X	X		
Phishing		X	X										X				X	X		X
Phreaking																	X	X		
Piggyback	X		X	X	X	X											X	X		
Pretexting	X		X		X							X		X	X		X	X		X
Reverse Social Engineering			X														X	X		
Shoulder surfing	X		X	X	X	X										X	X	X		
Water holing			X														X	X		
Web search			X														X	X		

Figuur 4: Referentiemodel social engineeringsmaatregelen tegen aanvallen

Per beveiligingsmaatregel wordt onderzocht of er informatiebeveiligingsbeleid voor is opgesteld binnen de Nederlandse Rijksoverheid.

Administratieve beveiligingsmaatregelen	Aanwezig
Antivirus/antiphishing	Ja of Nee
Arbeidsvoorwaarden duidelijk?	Ja of Nee
Auditbeleid en -controles	Ja of Nee
Blokkering toegangsrechten	Ja of Nee
Clean desk	Ja of Nee
Controle beschikbaarheid positieve referenties	Ja of Nee
Controle juistheid van curriculum	Ja of Nee
Disciplinaire maatregelen	Ja of Nee
Documentafhandeling/-vernietiging	Ja of Nee
E-mailfiltering	Ja of Nee
Het beperken van datalekken	Ja of Nee
Incidentafhandelingsstrategie	Ja of Nee
Informatieclassificatie	Ja of Nee
Locken van computer	Ja of Nee
Retourneren van bedrijfsmiddelen	Ja of Nee
Wachtwoordmanagement	Ja of Nee

Tabel 4: Administratieve beveiligingsmaatregelen

Fysieke beveiligingsmaatregelen	Aanwezig
Aanmeldformulieren	Ja of Nee
Beveiligingscamera's	Ja of Nee
Bezoekerspasjes	Ja of Nee
Biometrische toegangsdeuren	Ja of Nee
Foto-identificatiepasjes	Ja of Nee

Tabel 5: Fysieke beveiligingsmaatregelen

3.4 Bronnen

De geraadpleegde bronnen bestaan uit medewerkers en documenten van de drie participerende sectoren. De respondenten uit tabel 4 bestaan uit managers, IT-specialisten en beveiligingsspecialisten/-architecten en zijn geïnterviewd. Verder is een enquête gehouden onder een aantal medewerkers van de Rijksdiensten. De enquête is anoniem om de response te vergroten en om de bereidwilligheid van de Rijksdiensten te vergroten.

Organisatie	Functie van respondent
Blauw	Security Specialist
Blauw	Manager applicatiebeheer
Blauw	Manager servicedesk
Blauw	Manager ERP
Groen	Security Architect
Rood	IT Specialist
Groen	Informatiemanager
Rood	Solution Architect

Tabel 6: Interviewbronnen

3.5 Dataverzameling

3.5.1 Documentenanalyse

Tijdens de documentenanalyse zijn meerdere documenten doorgenomen. Dit zijn de Baseline Informatiebeveiliging Rijksdienst (BIR), NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002, een interne intranetpagina, het Algemeen Rijksambtenarenreglement (ARAR), Meldplicht datalekken in de Wet bescherming persoonsgegevens en de handreiking informatiebeveiliging.

De voor de overheid verplichte standaarden ISO 27001/ISO 27002 met aanvullingen zijn opgenomen in de BIR. De BIR is voor de Rijksoverheid verplicht, hierbij geldt het principe: pas toe of leg uit. De BIR:2012 is tevens de rijksimplementatie van de informatiebeveiligingsstandaarden NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. Beheerders van communicatie- en informatiesystemen leggen jaarlijks verantwoording af over de informatiebeveiliging van en binnen het systeem. De BIR is het leidende document voor informatiebeveiliging binnen de Rijksoverheid.

In de volgende paragrafen worden de gebruikte documenten kort beschreven.

3.5.1.1 NEN-ISO/IEC 27001

NEN-ISO/IEC 27001 specificeert eisen voor de vaststelling, implementatie, uitvoering, bewaking, beoordeling, het bijhouden en de verbetering van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden (NEN, 2014a).

3.5.1.2 NEN-ISO/IEC 27002

NEN-ISO/IEC 27002 geeft normen voor informatiebeveiliging voor organisaties en toepassingen inzake informatiebeveiligingsbeheer, waaronder de selectie, implementatie en het beheer van beheersmaatregelen die rekening houden met de omgeving(en) waarin de informatiebeveiligingsrisico's van de organisatie zich kunne voordoen. Deze Internationale Norm is ontworpen voor organisaties die voornemens zijn om beheersmaatregelen te selecteren in het implementatieproces van een managementsysteem voor informatiebeveiliging gebaseerd op ISO/IEC 27001, algemeen aanvaarde beheersmaatregelen inzake informatiebeveiliging te implementeren en hun eigen richtlijnen voor informatiebeveiligingsbeheer te ontwikkelen (NEN, 2014b).

3.5.1.3 Baseline Informatiebeveiliging Rijk (BIR)

Door de toename van gegevensuitwisseling tussen ministeries ontstond de behoefte aan een rijksbrede baseline: de Baseline Informatiebeveiliging Rijksdienst (BIR). De BIR Tactisch normenkader biedt één normenkader voor de beveiliging van de informatievoorziening van de Rijksdienst (Rijksoverheid, 2012a). Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de Rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld (Rijksoverheid, 2012b).

3.5.1.4 Algemeen Rijksambtenarenreglement (ARAR)

Het Algemeen Rijksambtenarenreglement, meestal afgekort tot ARAR, vormt de basis voor de rechtspositie van de Rijksambtenaren in Nederland. In het ARAR worden de arbeidsvoorwaarden voor en de rechtspositie van Rijksambtenaren beschreven (Rijksoverheid, 2015).

3.5.1.5 Intranet

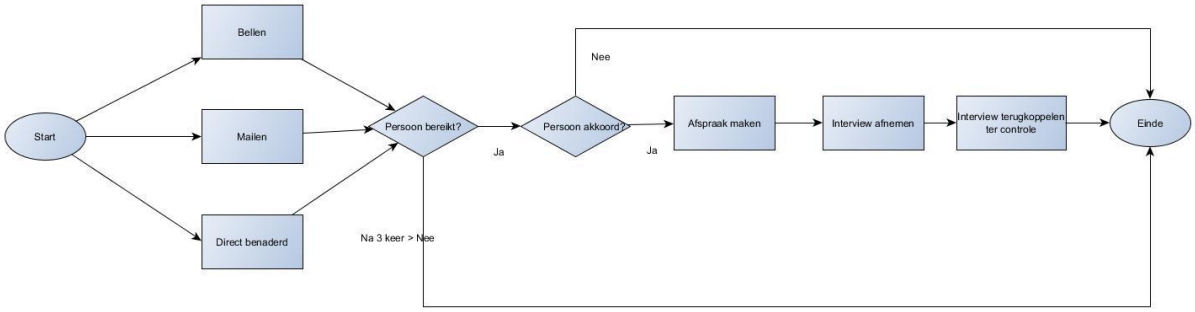
Er is gebruikgemaakt van verschillende beschrijvingen op de intranetpagina's van de Ministeries en Rijksdiensten. Dit zijn afgeschermde intranetlocaties waar alleen medewerkers van deze ministeries bij kunnen.

3.5.1.6 Meldplicht datalekken Wet bescherming persoonsgegevens

Op 1 januari 2016 is de meldplicht van datalekken ingegaan. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In een aantal gevallen moeten zij het datalek ook melden aan de mensen van wie de persoonsgegevens zijn gelekt (Persoonsgegevens, 2015) .

3.5.2 Semigestructureerde interviews

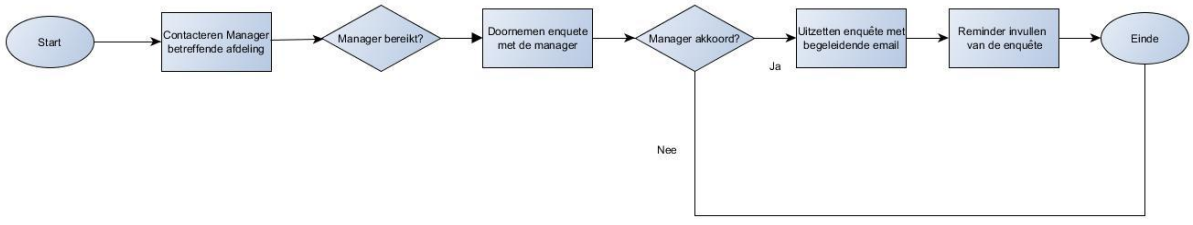
Als eerste zijn de interviewvragen opgesteld en doorgenomen met de begeleider van de Open Universiteit. De verbeteringen zijn doorgevoerd, waarna de medewerkers benaderd konden worden. Om een interview in te plannen met een respondent is gebruik gemaakt van een workflow. Respondenten zijn gebeld, gemaild of direct fysiek benaderd door de onderzoeker. Naar alle respondenten is een begeleidende e-mail gestuurd waarin het onderwerp social engineering, het doel van het onderzoek en de soort vragen kort werden beschreven. Vervolgens werden de afspraken ingepland, soms liep deze planning via een secretaresse. Op het ingeplande tijdstip is het interview afgenomen, waarna het interview is uitgewerkt en teruggekoppeld voor controle. Hierbij werd aangegeven dat de respondent correcties kon aanbrengen. Als een potentiële respondent niet kon worden bereikt, werd hij nogmaals benaderd. Als de respondent na drie keer nog niet was bereikt, kwam deze respondent te vervallen.



Figuur 5: Onderzoeksworkflow interviews

3.5.3 Enquête

Voor het uitzetten van de enquête is een andere workflow gebruikt. Een enquête mag namelijk niet zonder de expliciete toestemming van een afdelingsmanager bij medewerkers worden uitgezet. De manager dient zijn goedkeuring te verlenen, omdat het om capaciteit en dus geld gaat. Het kan ook om vertrouwelijke informatie gaan, waar ook toestemming voor nodig was.
Als eerste zijn de enquêtevragen opgesteld aan de hand van de gehouden interviews en uitwerkingen daarvan. Vervolgens zijn de vragen doorgenomen met de begeleider van de Open Universiteit, waarna de vragen zijn aangepast en nogmaals zijn besproken met de begeleider. De vragen zijn voorgelegd aan de manager van de organisatie. Zijn commentaar is verwerkt, waarna hij goedkeuring gaf.
Na het akkoord van de manager is de enquête bij de betreffende medewerkers uitgezet. Na een week is een reminder gestuurd. Met de managers is afgesproken dat zij ook toegang krijgen tot de uitkomsten van de enquête.



Figuur 6: Onderzoeksworkflow enquête

In deze enquête worden alleen gesloten vragen gesteld. De enquête is daarmee kwantitatief van aard en is online uitgezet. Er is gebruikgemaakt van verschillende soorten vragen: dichotome, multiple choice- en schaalvragen. Deze soorten vragen worden verderop in deze paragraaf kort besproken.
Bij elke vraag is een vluchtmogelijkheid aangeboden. De respondenten kunnen hierdoor de situatie die op hen van toepassing is beschrijven en als zij een vraag niet wensen te beantwoorden, kunnen

zij deze optie aanvinken. Wanneer een dergelijke optie niet wordt geboden, zal een respondent stoppen met antwoorden of zomaar iets invullen.

Een aantal vragen is niet geheel neutraal geformuleerd. Bij deze vragen wordt de respondent bewust een hulplijn geboden. Een voorbeeld is de vraag waarbij de respondent wordt gevraagd aan te geven met welke socialengineeringaanvallen hij bekend is. De verschillende soorten socialengineeringaanvallen worden in de vraag benoemd, de respondent een ervan aanvinken. In het interview wordt deze vraag als open vraag gesteld, zonder de antwoordmogelijkheden. In de enquête wordt aldus op een minder diep niveau getoetst hoe bekend de medewerkers zijn met social engineering dan in de interviews. In de beschikbare tijd kan echter een grotere groep mensen worden ondervraagd met de enquête dan met interviews.

Gesloten vragen brengen ook risico's met zich mee. De respondent is namelijk afhankelijk van de opties die hem worden voorgeschoteld. Hij heeft niet de mogelijkheid extra of andere informatie te vermelden.

- **Dichotome vraag:** een vraag waarbij de respondent uit twee antwoorden moet kiezen: ‘ja’ of ‘nee’.

- **Multiple choice-vraag/meerkeuzevraag:** een vraag waarbij de respondent één antwoord moet kiezen uit meerdere antwoorden. Een speciale vorm hiervan is de multiple response-vraag, waarbij de respondent meer dan een antwoord mag aankruisen.

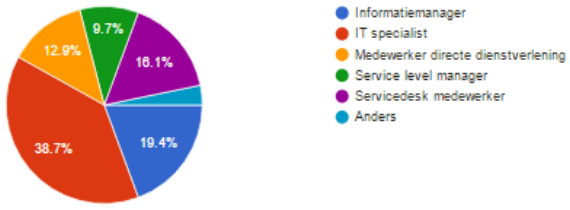
3.6 Antwoordbereidheid/respons

3.6.1 Respons interviews

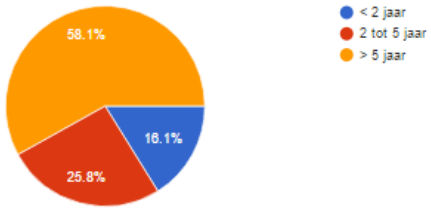
De representativiteit van deze populatie bleek uiteindelijk zeer goed. Van de twaalf personen die werden benaderd, bleken acht bereid te zijn mee te werken aan een interview, dit komt neer op 67%. De meeste van de geïnterviewde personen zijn bekenden van de onderzoeker, wat deze bereidwilligheid verklaart. In paragraaf 3.3 worden de verschillende functies van de geïnterviewden beschreven.

3.6.2 Respons enquête

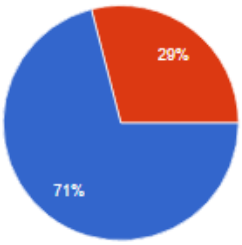
De representativiteit bleek lager voor de enquêtepopulatie. In totaal hebben 31 medewerkers de enquête ingevuld, terwijl deze naar in totaal 60 personen is verzonden. Dit komt neer op 51,67%. Later bleek dat drie enquêtes niet volledig waren ingevuld. Deze drie enquêtes zijn in hun geheel verwijderd, omdat de 100 procent-lijn per vraag anders zou zijn hierdoor. Uiteindelijk is met 28 medewerkers gerekend in de percentages.
Zoals hieronder is weergegeven in figuur 8 heeft het grootste deel van de respondenten de functie van IT-specialist. De overige functies zijn ook goed vertegenwoordigd. Het overgrote deel (58%) van de respondenten werkt langer dan vijf jaar in de huidige functie. Daarnaast is 71% van de respondenten intern en 29% extern. 80 % van de respondenten geeft aan toegang te hebben tot vertrouwelijke informatie vanuit zijn functie.



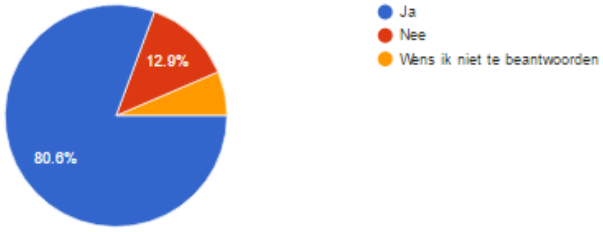
Figuur 7: Functies respondenten



Figuur 8: Jaren werkzaam in functie



Figuur 9: Intern/extern



Figuur 10: Toegang tot vertrouwelijke informatie

3.7 Betrouwbaarheid

Betrouwbaarheid is een schatting van de mate waarin een test vrij is van willekeurige meetfouten. Het gaat erom dat het gebruikte meetinstrument betrouwbare resultaten geeft, dat wil zeggen dat het meetinstrument steeds dezelfde resultaten geeft onder dezelfde condities. Dit wordt bekeken aan de hand van de onderstaande bronnen van toeval.

3.7.1 De onderzochte persoon

De respondenten moeten kunnen antwoorden zonder sociale wenselijkheid, dit wordt deelnemersvertekening genoemd. Het uitsluiten van deelnemersvertekening is gewaarborgd door anonimiteit in de enquête en de mogelijkheid om een vraag niet te beantwoorden in zowel de enquête als de interviews. Daarnaast is in het interview en de enquête aangegeven dat bij vragen contact kan worden opgenomen met de onderzoeker, zodat onduidelijke zaken verklaard kunnen worden. Verschillende personen hebben ook daadwerkelijk contact opgenomen met vragen over de enquête.
Voor het uitzetten van de enquête is toestemming van de managers gevraagd. Deze toestemming is door de managers overgebracht aan de respondenten. Het managementteam heeft toestemming gegeven voor de uitvoering van de enquête.

Naast deelnemersvertekening kunnen ook deelnemersfouten optreden: het gevaar bestaat dat de respondenten per ongeluk het verkeerde antwoord aankruisen in de enquête. Door de hoeveelheid afgenomen enquêtes is dit gevaar echter verwaarloosbaar.

De respondent heeft zelf de dag en het tijdstip bepaald waarop hij de enquête invulde of werd geïnterviewd. Hierbij is rekening gehouden met het feit dat er geen interviews net voor de lunch moeten worden gehouden. Dit heeft ervoor gezorgd dat de respondent ontspannen het interview in ging of de enquête heeft kunnen completeren. Aan de respondenten is een uiterste datum gesteld voor het invullen van de enquête en het inplannen van interviews.

3.7.2 De omstandigheden

Alle interviews zijn afgenomen in een vergaderruimte. De onderzoeker en de respondenten konden hierdoor in alle rust het interview voltooien.

3.7.3 De onderzoeker

Waarnemersfouten en waarnemersvertekening zijn beperkt door de enquête- en interviewvragen te baseren op het referentiemodel dat is voortgekomen uit het literatuuronderzoek. Iedere geïnterviewde kreeg de mogelijkheid te reageren op de uitgewerkte interviewantwoorden en correcties aan te brengen of vragen alsnog verder te beantwoorden. Als respondenten vragen hadden over de enquête konden zij deze stellen aan de onderzoeker.
Er zijn semigestructureerde interviews afgenomen. Alle interviews zijn door dezelfde onderzoeker gehouden. Hierdoor is elk interview vrijwel identiek verlopen.

3.8 Intersubjectief

Het onderzoek en het gevolgde proces zijn zo opgezet en beschreven dat dit onderzoek op dezelfde wijze opnieuw uitgevoerd kan worden door een andere onderzoeker om tot dezelfde resultaten te komen. Het onderzoek is dan ook herhaalbaar en zodanig uitgewerkt dat er overeenstemming zal zijn tussen onderzoekers over de resultaten. De onderstaande onderzoeksverslagstappen zijn uitgewerkt en aanwezig in het verslag.

Aanwezige processtappen in het empirisch onderzoek		
– Onderzoeksstrategie	– Onderzoeksplan	– Onderzoeksmethode
– Dataverzamelingsmethode	– Semigestructureerd interview	– Enquête
– Uitkomsten enquête	– Interviewresultaten	– Geanalyseerde documenten

Tabel 7: Processtappen in het onderzoek

3.9 Toetsbaarheid

Alle uitkomsten en vragen zijn toetsbaar. Er zijn alleen uitspraken gedaan over zaken die zijn waargenomen en controleerbaar zijn. Dit betekent dat alle onderzoeksresultaten kunnen worden bevestigd en openbaar zijn. Zowel de documenten, enquête-uitkomsten en uitgewerkte interviews zijn aanwezig in dit verslag.

3.10 Validiteit (extern en intern)

Door de validiteit van een onderzoek te controleren, worden de echtheid en het waarheidsgehalte gecontroleerd. Een onderzoeker wil er zeker van zijn dat hij meet wat hij wil weten en dat er geen systematische fouten zijn gemaakt in het onderzoek.

3.10.1 Interne validiteit

De resultaten van een onderzoek zijn intern valide als de resultaten die worden gemeten ook daadwerkelijk het gevolg zijn van de opzettelijke verandering en meten wat er gemeten moet worden.

Aan dit empirisch onderzoek ligt een uitgewerkt literatuuronderzoek ten grondslag. Dit literatuuronderzoek brengt de definitie van social engineering en de verschillende aspecten in kaart. Tevens zijn hierin de informatiebeveiligingsmaatregelen inzake socialengineeringaanvallen in een referentiekader in kaart gebracht. Het literatuuronderzoek, in combinatie met de gekozen/uitgewerkte onderzoeksstrategie en -methode specifiek voor het empirisch onderzoek, zorgt ervoor dat de interne validiteit gewaarborgd is en de juiste bronnen gebruikt zijn.

3.10.2 Externe validiteit

Als resultaten gegeneraliseerd kunnen worden, zijn ze extern valide. Generaliseren betekent dat mag worden gezegd dat de resultaten van het onderzoek ook gelden in vergelijkbare situaties.

Het onderzoek is verricht in drie sectoren vallende onder twee verschillende ministeries..
De resultaten van het aanwezige informatiebeveiligingsbeleid inzake social engineering is van toepassing op alle ministeries. Het beleid wordt namelijk op Rijksoverheidsniveau opgesteld. Wat niet onderzocht is en wat niet generaliseerbaar is, is of het beleid ook daadwerkelijk wordt uitgevoerd, getoetst en toegepast binnen de onderzochte sectoren.

De uitkomsten van de awareness van de medewerkers van het informatiebeveilingsbeleid inzake social engineering zijn niet generaliseerbaar binnen andere sectoren en de gehele ministeries. De

ministeries bestaan uit zoveel verschillende sectoren, afdelingen, specialismen en functies dat een te klein gedeelte van de totale populatie is onderzocht om de uitkomsten van dit onderzoek te kunnen generaliseren.

3.11 Ethiek

Onderzoekers hebben te maken met ethiek, wetenschappelijke integriteit en wetgeving.
De Open Universiteit gaat ervan uit dat onderzoekers die mensgebonden onderzoek doen op de hoogte zijn van de kaders en daarnaar handelen (Universiteit, 2016).
Belangrijke aspecten zijn onder andere dat:

- De deelnemers worden geïnformeerd over het doel van het onderzoek
- De deelname vrijwillig is en de deelnemer heeft ingestemd
- De (persoons)gegevens zorgvuldig worden gebruikt en beveiligd
- Het onderzoek controleerbaar en onafhankelijk is.

Alle deelnemers zijn mondeling en schriftelijk geïnformeerd over het doel van het onderzoek en de deelname aan de enquête en interviews was vrijwillig. De namen van de geïnterviewden zijn geanonimiseerd en alleen bekend bij de respondenten, onderzoeker en afstudeerbegeleiders. Tevens is de respondenten de mogelijkheid geboden om de interviewuitwerkingen te controleren, aan te passen of aan te geven dat gegevens/uitspraken niet gebruikt mogen worden.

Ook de enquête is geanonimiseerd. Er is op geen enkel moment inzichtelijk geweest voor de onderzoeker of anderen welke respondenten welke antwoorden hebben gegeven.

Alle onderzoeksgegevens zijn beschikbaar in dit verslag. De sectoren zijn echter geanonimiseerd met een fictieve naam zodat niet te achterhalen is in welke sectoren het onderzoek zich heeft afgespeeld. Deze gegevens zijn alleen bekend bij de onderzoeker, afstudeerbegeleiders en de betrokken sectoren. Dit was een voorwaarde van de sectoren, zij zouden anders hun medewerking niet verlenen.

Het onderzoek is zo onafhankelijk mogelijk uitgevoerd. De kaders zijn uitgezet door de onderzoeker, waarna de begeleiders op een aantal punten hebben bijgestuurd. Vanuit de sectoren kwam alleen de eis dat de resultaten van het onderzoek geanonimiseerd dienen te worden.

4 Resultaten van het empirisch onderzoek

Om antwoord te kunnen geven op de onderzoeksvragen dient eerst de vraag te worden beantwoord of de organisatie de beveiligingsmaatregelen uit het referentiemodel voldoende heeft afgedekt.

De BIR in combinatie met de uitkomsten van de interviews wordt gebruikt om te kunnen bepalen of de geïdentificeerde beveiligingsmaatregelen uit het referentiemodel voldoende wordt afgedekt.

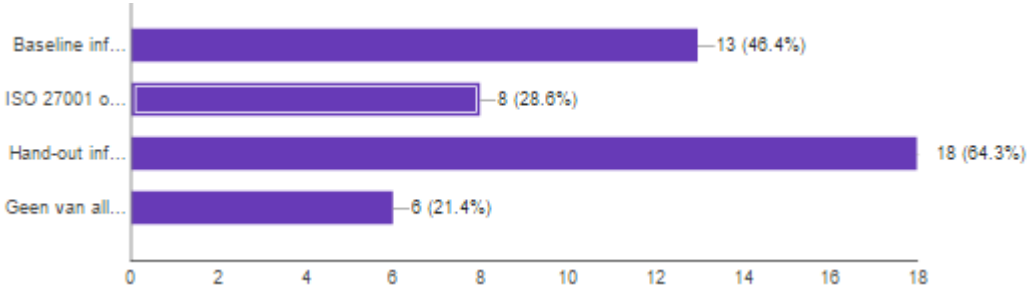
Alle respondenten hebben aangegeven dat de BIR leidend is voor de informatiebeveiliging binnen de organisaties en dat zij ten tijde van het onderzoek aan de punten uit de BIR voldoen. Hierdoor kan de BIR worden gebruikt om te bekijken of de beveiligingsmaatregelen worden afgedekt. Bij veel vragen uit de interviews komen de verschillende aspecten ook aan bod, waardoor de informatie is bepaald uit twee of meer bronnen. Een aantal aspecten staat echter zo duidelijk in de BIR dat niet om deze informatie is gevraagd in de interviews.

4.1 Algemene awareness van het informatiebeveilingsbeleid

In deze paragraaf worden de uitkomsten weergegeven met betrekking tot de algemene vragen aan de respondenten inzake het informatiebeveiligingsbeleid.

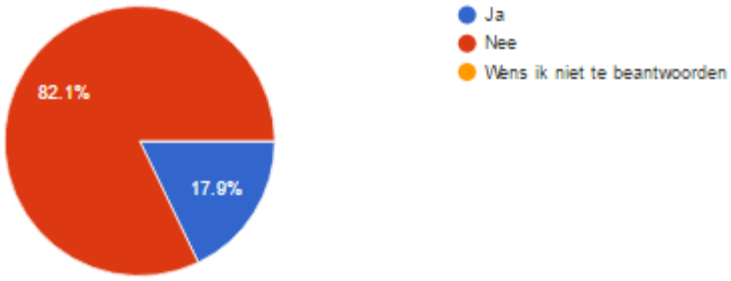
Hieronder wordt op elk van de vragen ingegaan.

Vraag 1: 'Met welke onderstaande informatiebeveiligingsdocumenten bent u inhoudelijk bekend?'
Hieruit komt naar voren dat bijna de helft (46,4%) van de respondenten inhoudelijk op de hoogte is van de BIR, het leidende informatiebeveiligingsdocument binnen de Rijksoverheid. 64,3 procent van de respondenten is inhoudelijk op de hoogte van de hand-out informatiebeveiliging en 21,4 procent is van geen van de informatiebeveiligingsdocumenten inhoudelijk op de hoogte.



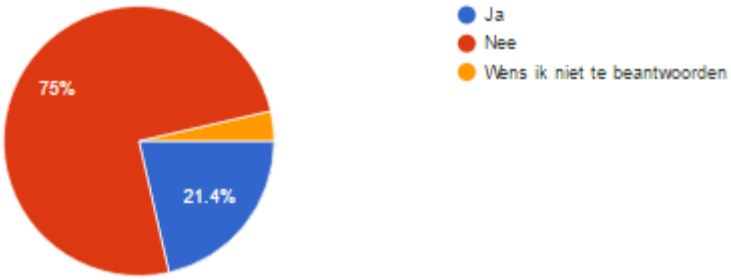
Figuur 11: Bekendheid informatiebeveiligingsdocumenten

Vraag 2: 'Heeft u ooit vanuit deze organisatie een cursus of training gevolgd inzake informatiebeveiliging?'
Hieruit komt naar voren dat slechts 17,9% van de respondenten wel een training heeft gevolgd inzake informatiebeveiliging en 82,1% van de respondenten geen training heeft gevolgd inzake informatiebeveiliging.



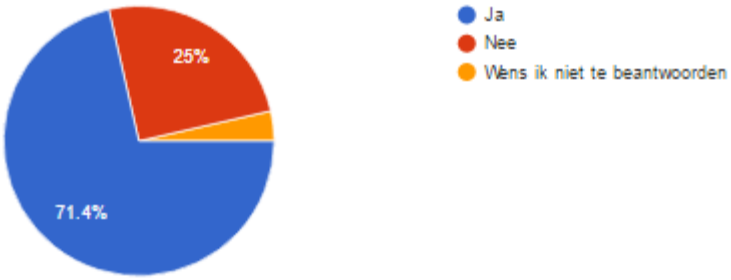
Figuur 12: Training gevolgd inzake informatiebeveiliging

Vraag 3: 'Is u ooit vanuit deze organisatie een cursus aangeboden inzake informatiebeveiliging?'
74,2% van de respondenten geeft aan dat hem of haar nooit een cursus of training is aangeboden inzake informatiebeveiliging binnen de Rijksdienst. 21,4% geeft aan wel een cursus aangeboden te hebben gekregen. Uit de vorige vraag is gebleken dat 17,9% daadwerkelijk een cursus inzake informatiebeveiliging heeft gevolgd, terwijl de cursus aan 21,4% is aangeboden. Er lijken dan ook respondenten te zijn die niet geïnteresseerd zijn in een cursus inzake informatiebeveiliging.



Figuur 13: Percentage respondenten dat een cursus is aangeboden

Vraag 4: 'Zou u als u de kans kreeg binnen de organisatie een training volgen over informatiebeveiliging/social enginering?'
Uit de gecombineerde resultaten van de vorige twee vragen is gebleken dat niet iedere respondent geïnteresseerd is in een training inzake informatiebeveiliging. Dit blijkt ook uit de resultaten van deze vraag. 25% van de respondenten geeft aan niet geïnteresseerd te zijn in een training, 71,4% geeft aan wel de training te zullen volgen indien deze kans zich voordoet. 3,6% van de respondenten wenst deze vraag niet te beantwoorden.



Figuur 14: Cursus volgen indien de kans wordt gegeven

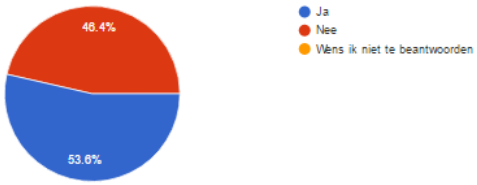
4.2 Algemene awareness van social engineering

In de literatuurstudie is de volgende definitie van social engineering gevonden die wordt gebruikt in het afstudeeronderzoek:
Social engineering is een set van methoden waarmee het gedrag van een individu of groep individuen zodanig wordt gemanipuleerd dat dit individu of deze groep de social engineer toegang verleent tot bepaalde informatie. De social engineer heeft als doel deze informatie te gebruiken om de slachtoffers uit te buiten. Deze techniek maakt gebruik van de aard van de mens om slachtoffers uit te buiten, om gevoelige informatie te verkrijgen en hen te manipuleren en ervan het overtuigen deze informatie te onthullen door het inzetten van uitzonderlijk goede communicatieve vaardigheden. Boven alles maakt social engineering gebruik van de zwakste schakel in de beveiliging: de menselijke factor.

In deze paragraaf worden de uitkomsten weergegeven met betrekking tot de algemene awareness van de respondenten inzake het informatiebeveiligingsbeleid.

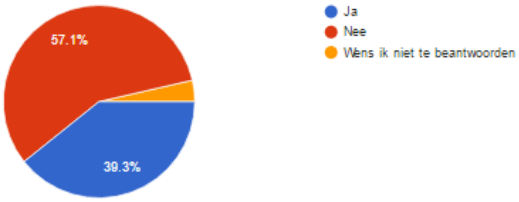
Hieronder wordt op elk van de vragen ingegaan.

Vraag 1: 'Bent u bekend met het begrip social engineering zoals dat in de bijgevoegde tekst is gedefinieerd?'
53,6% van de respondenten is bekend met de definitie van social engineering die in dit onderzoek wordt gebruikt.



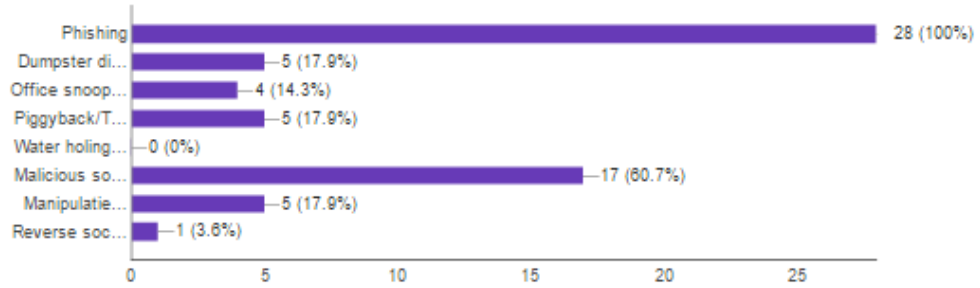
Figuur 15: Bekendheid definitie social engineering

Vraag 2: 'Kunt u beschrijven hoe een socialengineeringaanval wordt uitgevoerd?'
57,1% van de respondenten is niet bekend hoe een socialengineeringaanval wordt uitgevoerd.



Figuur 16: Percentage van de respondenten dat een socialengineeringaanval kan beschrijven

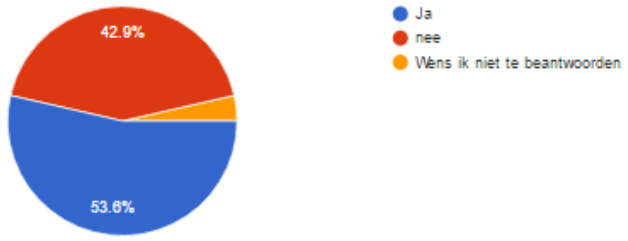
Vraag 3: 'Met welke van de genoemde socialengineeringaanvallen bent u bekend?'
In deze enquêtevraag is bewust naar de aanvallen als begrip gevraagd. Met deze vraag wordt getoetst in hoeverre de respondenten bekend zijn met de termen en dus niet of zij inhoudelijk bekend zijn met de aspecten van een bepaalde aanval. Het kan zijn dat wanneer een begrip wordt uitgelegd de respondenten hiermee wel bekend zijn en de vraag anders zullen beantwoorden.



Figuur 17: Met welke aanvallen is de respondent bekend?

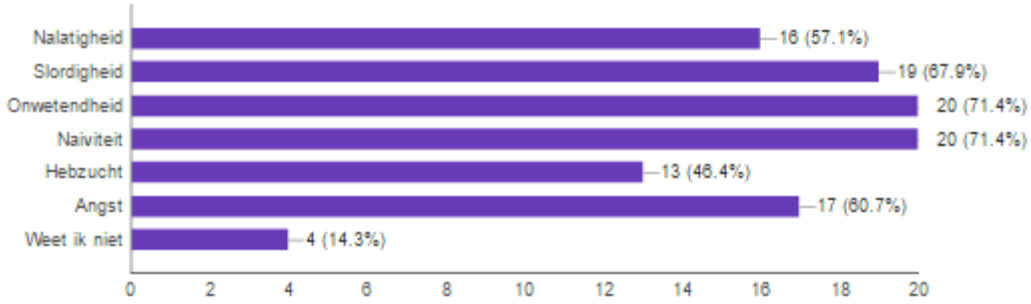
Phishing is bekend bij alle respondenten terwijl water holing en reverse social engineering bij vrijwel geen enkele respondent bekend is. Malicious software is ook bij veel respondenten bekend, deze aanvalsvorm valt echter niet onder social engineering.

Vraag 4: 'Bent u bekend met de meestvoorkomende motieven van social engineers?'
De helft van de respondenten geeft aan bekend te zijn met de meestvoorkomende motieven van een social engineer.



Figuur 18: Percentage van de respondenten dat bekend is met de motieven van social engineering

Vraag 5: 'Van welke menselijke aspecten maakt een social engineer misbruik?'
Bij alle menselijke aspecten is te zien dat minstens de helft van de respondenten op de hoogte is dat een social engineer hiervan misbruik probeert te maken. 14,3% van de respondenten geeft aan niet te weten van welke menselijke aspecten een social engineer gebruikmaakt.



Figuur 19: Awareness van de menselijke aspecten die een social engineer misbruikt

4.3 Het aanwezige informatiebeveiligingsbeleid en de awareness van de respondenten van dit informatiebeveiligingsbeleid

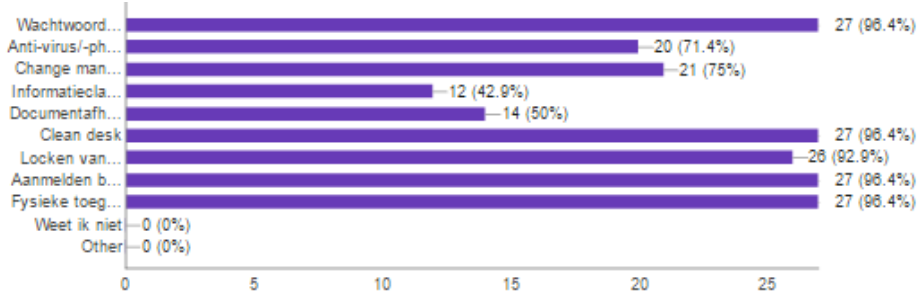
Aanmeldformulier bezoekers
Om een goed overzicht te behouden over welke mensen in een gebouw aanwezig zijn, is het noodzakelijk om aanmeldformulieren voor bezoekers te gebruiken. Aan de hand van deze formulieren is door de tijd inzichtelijk welke personen in het gebouw aanwezig waren/zijn.

De respondenten geven aan dat bezoekers uiterlijk een dag van tevoren schriftelijk dienen te worden aangemeld bij de receptie, die de verstrekking van de bezoekerspassen regelt. Het onderdeel (sector,

afdeling, team) dat als gastheer optreedt, zorgt zelf voor de begeleiding (ophalen, begeleiden en uitgeleiden door of namens de ontvangende partij).

Hieruit blijkt dat er aanmeldformulieren voor bezoekers aanwezig zijn bij de Rijksoverheid.

In de enquête is de respondenten de vraag gesteld voor welke aspecten er informatiebeveiligingsbeleid aanwezig is binnen hun Rijksdienst. Specifiek voor het aanmelden van bezoekers geeft 96,4 procent aan dat hiervoor beleid aanwezig is binnen hun Rijksdienst.



Figuur 20: Awareness van de aspecten op het informatiebeveiligingsbeleid

Hieruit blijkt dat een grote meerderheid (96,4%) van de medewerkers op de hoogte is van het informatiebeveiligingsbeleid inzake aanmeldformulieren voor bezoekers.

Antivirus/antiphishing

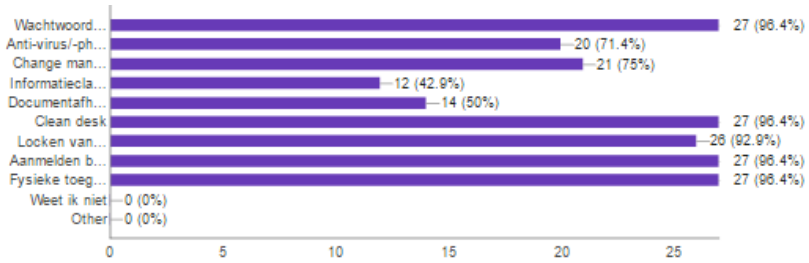
Er behoren maatregelen te worden getroffen voor de detectie, de preventie en het herstel om de organisatie te beschermen tegen virussen en phishing.

In het informatiebeveiligingsbeleid van de Rijksoverheid worden de onderstaande antivirus- en antiphishingmaatregelen beschreven (Rijksoverheid, 2012a):

- Bij het openen van bestanden wordt geautomatiseerd gecontroleerd op virussen, trojans en andere malware.
- Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware.
- Er zijn continuïteitsplannen voor het herstel na aanvallen met virussen, waarin minimale maatregelen voor back-ups en het herstel van gegevens en programmatuur zijn beschreven.

Hieruit blijkt dat er beleid inzake antivirus- en antiphishingmaatregelen aanwezig is bij de Rijksoverheid.

In de enquête is de respondenten de vraag gesteld voor welke aspecten er beveiligingsbeleid aanwezig is binnen hun Rijksdienst. Specifiek voor antivirus/antiphishing geeft 71,4% aan dat hiervoor beleid aanwezig is binnen zijn Rijksdienst.



Figuur 21: Awareness van de aspecten van het informatiebeveiligingsbeleid

Hieruit blijkt dat een grote meerderheid van de medewerkers op de hoogte is van het beleid inzake antivirus/antiphishing.

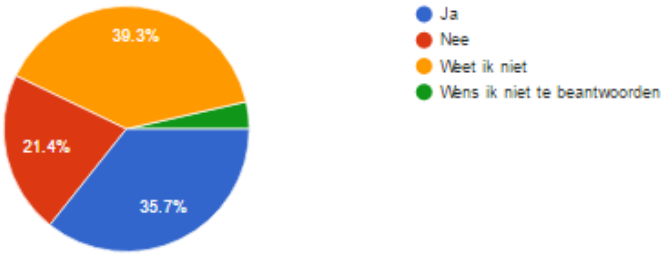
Arbeidsvoorwaarden

In de arbeidsvoorwaarden zijn de afspraken met de medewerker vastgelegd over de wettelijke verantwoordelijkheden, de wijze waarop met informatie dient te worden omgegaan en het handelen bij het constateren van een nalatigheid met betrekking tot de informatiebeveiliging.

Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de arbeidsvoorwaarden te aanvaarden en daarvoor te tekenen in hun arbeidscontract. In dit contract staan hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging. Hierdoor weet elke medewerker wat zijn verantwoordelijkheden zijn. Tevens worden de verantwoordelijkheden beschreven op het intranet, om de medewerkers hiervan nogmaals op de hoogte te stellen (Rijksoverheid, 2012a).

Hieruit blijkt dat er arbeidsvoorwaarden aanwezig zijn binnen de Rijksoverheid.

In de enquête is aan de respondenten de vraag gesteld of binnen hun Rijksdienst is vastgelegd welke verantwoordelijkheden bij welke persoon/welk team/welke functie horen, bijvoorbeeld met behulp van een RACI-matrix of Verix-matrix.
Slechts 35,7% geeft aan dat de verantwoordelijkheden formeel zijn vastgelegd. 21,4% geeft aan dat de verantwoordelijkheden niet worden vastgelegd en 39,3% geeft aan niet te weten of deze verantwoordelijkheden worden vastgelegd.



Figuur 22: Awareness arbeidsvoorwaarden

Hieruit blijkt dat 39,3% niet op de hoogte is van het beleid inzake arbeidsvoorwaarden. Daarnaast geeft 21,4% aan dat deze voorwaarden niet zijn opgenomen in de arbeidsvoorwaarden. Dit kan wellicht worden verklaard als bekeken wordt hoelang deze medewerkers reeds in dienst zijn bij de betreffende Rijksdienst. De BIR is sinds 2012 in gebruik en wordt jaarlijks bijgesteld. In paragraaf 3.5.2 wordt inzichtelijk gemaakt dat 58,1% van de respondenten al langer dan vijf jaar in de huidige functie werkt.

Auditbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging behoort onafhankelijk en met geplande tussenpozen of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging te worden beoordeeld. Het auditbeleid dient aan de volgende stappen te voldoen volgens de BIR:

- Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld (Rijksoverheid, 2012a).
- Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement (Rijksoverheid, 2012a).

Deze argumentatie uit de BIR wordt bevestigd door de informatie uit de interviews. De respondenten geven aan dat periodiek audits plaatsvinden.

Elke drie jaar vindt controle op basis van de BIR plaats, door de Auditdienst Rijk (ADR). Er wordt puntsgewijs gekeken of de afdelingen/Rijksdienst nog voldoen/voldoet aan de BIR. Als een bepaald punt is gecontroleerd en is afgedekt, wordt het niet opnieuw bekeken bij een ongewijzigde situatie.

Jaarlijks vindt een ISO 27001-audit plaats bij de Rijksdiensten. Daarnaast vinden per Rijksdienst/afdeling individuele audits plaats specifiek voor die organisatie/afdeling.

Hieruit blijkt dat een auditbeleid en auditcontroles aanwezig zijn bij de Rijksoverheid.

In de enquête is geen vraag gesteld over het auditbeleid.

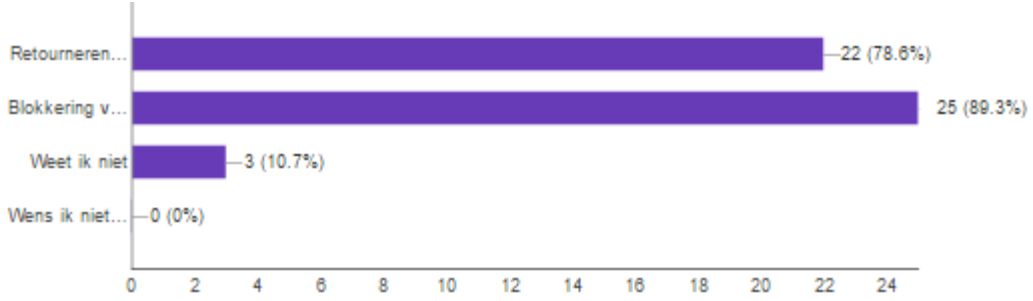
Blokkering van de toegangsrechten

De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatievoorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst of zij moeten na een wijziging worden aangepast.

De respondenten geven aan dat de toegangsrechten voor externen automatisch worden geblokkeerd als hun contract afloopt. In het personeelssysteem moet een einddatum zijn opgenomen. Dit levert bij de verlenging van de overeenkomsten met externen regelmatig problemen op, omdat de einddatum dient te worden aangepast in het personeelssysteem. Als de ingevoerde einddatum wordt bereikt, wordt automatisch de toegangspas tot het gebouw geblokkeerd evenals de active directory account (netwerkaccount) van de medewerker. De toegang tot de individuele systemen dient handmatig te worden afgesloten. De active directory account is echter benodigd om de individuele, onderliggende systemen te bereiken.

Hieruit blijkt dat er beleid aanwezig is inzake het blokkeren van de toegangsrechten binnen de Rijksoverheid.

In de enquête is aan de respondenten gevraagd met welke van de genoemde aspecten rekening wordt gehouden bij het beëindigen of wijzigen van het dienstverband binnen hun organisatie. Zoals is weergegeven in figuur 24 geeft 89,3% van de respondenten aan dat er beleid aanwezig is met betrekking tot de blokkering van toegangsrechten wanneer een dienstverband wordt gewijzigd of eindigt.



Figuur 23: Awareness blokkering toegangsrechten

Hieruit blijkt dat het merendeel van de respondenten (89,3%) op de hoogte is van het beleid inzake de blokkering van toegangsrechten binnen de Rijksoverheid.

Clean desk-procedure

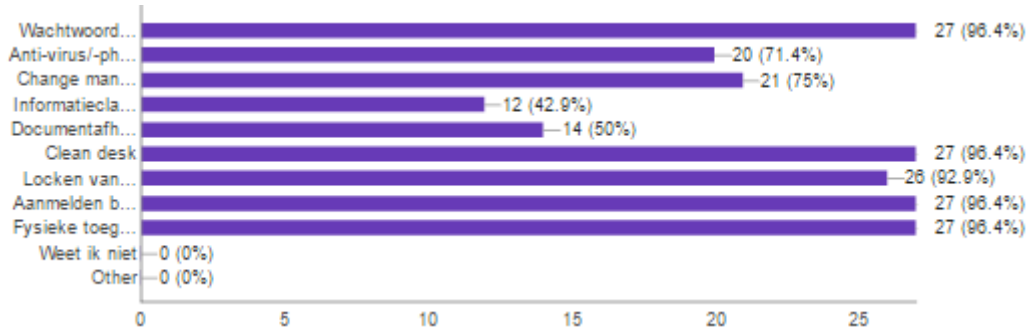
'Clean desk' betekent dat de bureaus van de medewerkers leeg dienen te zijn als zij niet aanwezig zijn. Documenten mogen niet open en bloot op de bureaus liggen. De documenten dienen veilig in kasten, achter slot en grendel, te worden opgeborgen. Hierdoor zou geen vertrouwelijke informatie moeten rondslingeren op de verschillende werkplekken.

De Rijksoverheid hanteert een 'clean desk, clear screen'-procedure. Deze procedure geldt ook voor medewerkers die hun werkzaamheden buiten de gebouwen en terreinen van de organisatie verrichten (Rijksoverheid, 2012a) (Interviews + Handreiking).

De respondenten geven wel aan dat niet iedereen voldoet aan clean desk. Het blijkt dat niet alle medewerkers de mogelijkheid hebben om hun spullen achter slot en grendel te bewaren. Mensen worden aangesproken op de resultaten van de clean desk-audit, naar aanleiding hiervan worden geen disciplinaire maatregelen genomen. Daarnaast vinden de clean desk-audits niet vaak genoeg plaats om de cultuur te kunnen veranderen, ze worden momenteel te sporadisch uitgevoerd.

Hieruit blijkt dat er een clean desk-beleid aanwezig is bij de Rijksoverheid. Dit beleid wordt/kan echter niet altijd worden nageleefd.

In de enquête is de respondenten gevraagd om aan te geven voor welke aspecten een beveiligingsbeleid aanwezig is binnen de organisatie. Specifiek voor clean desk geeft 96,4% van de respondenten aan van dit beleid op de hoogte te zijn.



Figuur 24: Awareness van de aspecten op het informatiebeveiligingsbeleid

Hieruit blijkt dat vrijwel alle medewerkers (96,4%) op de hoogte zijn van het beleid inzake clean desk.

Controle beschikbaarheid positieve referenties

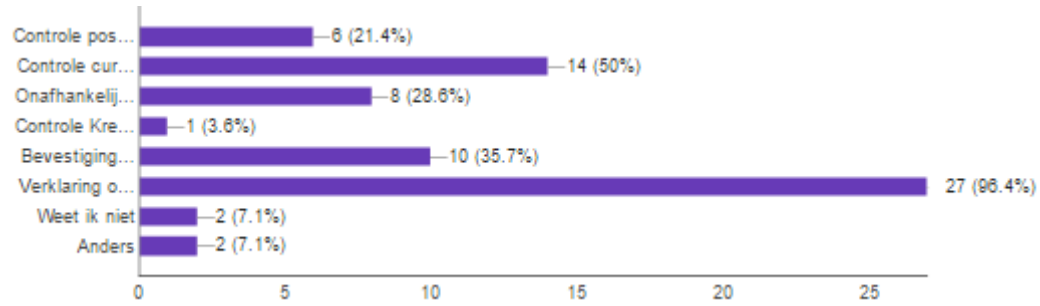
Er dient een controle plaats te vinden van de positieve referenties van sollicitanten. Als deze referenties niet worden nagetrokken, weet de organisatie niet of de sollicitant voldoet aan de functie-eisen en of deze sollicitant wellicht andere motieven heeft om te solliciteren.

In de BIR wordt dit punt niet besproken. Tevens geven de respondenten aan dat de referenties van een sollicitant zelden tot nooit worden nagetrokken.

Hieruit blijkt dat referenties niet worden nagetrokken bij de Rijksoverheid.

In de enquête is gevraagd aan de respondenten of er volgens hen een controle van de positieve referenties plaatsvindt en of hier beleid voor is.

21,4% van de respondenten geeft aan hier beleid voor is en dat deze controle wordt uitgevoerd binnen zijn Rijksdienst.



Figuur 25: Awareness van de aspecten uit het informatiebeveiligingsbeleid

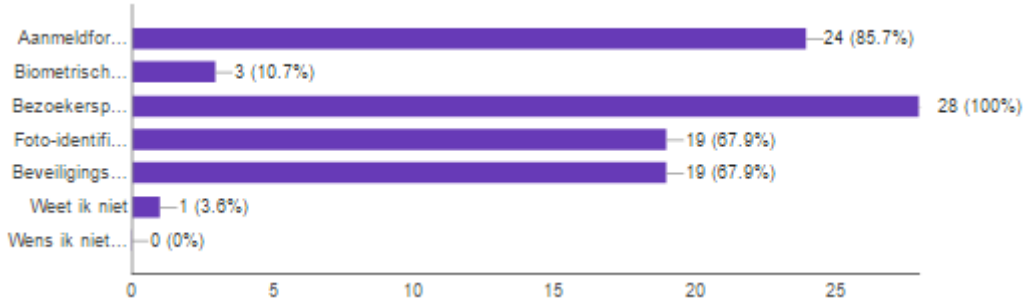
Bezoekerspasjes

Beveiligde zones behoren te worden beschermd door middel van geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
Bezoekers krijgen, nadat ze zich hebben aangemeld en gelegitimeerd, een bezoekerspas met autorisaties die geschikt zijn voor een bezoeker (Rijksoverheid, 2012a).

De respondenten geven ook aan dat bezoekers zich altijd moeten melden bij de receptie en alleen worden toegelaten tot het gebouw als zij een geldig legitimatiebewijs (paspoort, rijbewijs of ID-kaart) kunnen tonen. De receptie geeft de bezoeker een bezoekerspas die hij zichtbaar moet dragen en bij het verlaten van het gebouw moet inleveren bij de receptie of in de zuil bij de deur van de uitgang moet gooien waardoor de deur automatisch opengaat. Bezoekers die toegang nodig hebben tot de beveiligde zones staan onder voortdurende begeleiding van een medewerker of de beveiliging.

Hieruit blijkt dat er bezoekerspasjes worden gebruikt bij de Rijksoverheid en hier beleid voor opgesteld is.

Aan de respondenten is gevraagd voor welke aspecten van de fysieke beveiliging er beleid aanwezig is binnen hun Rijksdienst. 100 procent van de respondenten geeft aan dat er beleid aanwezig is omtrent het fysieke aspect bezoekerspasjes.



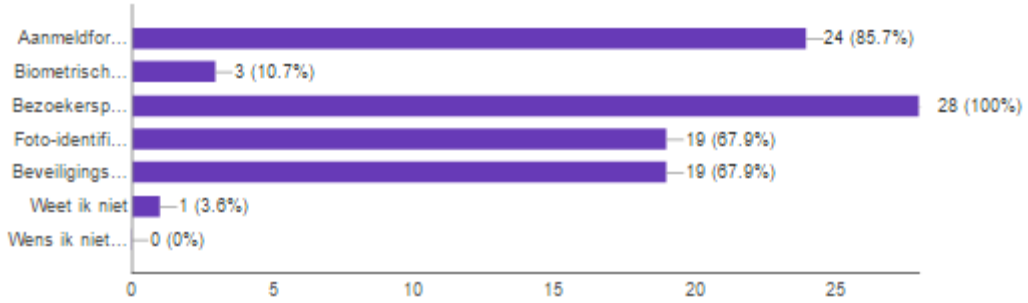
Figuur 26: Awareness op het fysieke toegangsbeleid

Hieruit blijkt dat alle medewerkers zich bewust zijn dat er beleid is omtrent bezoekerspasjes.

Beveiligingscamera's

In de beschikbare informatiebeveiligingsdocumenten staan geen gegevens over het informatiebeveiligingsbeleid inzake het gebruik van beveiligingscamera's. De geïnterviewden gaven daarentegen wel aan dat op vrijwel alle Rijksoverheid-locaties camera's hangen bij de ingangen van gebouwen en in belangrijke ruimten in gebouwen (bijvoorbeeld serverruimten).

Aan de respondenten van de enquête is gevraagd voor welke aspecten van de fysieke beveiliging er informatiebeveiligingsbeleid aanwezig is binnen hun Rijksdienst. Een van de fysieke aspecten is het gebruik van beveiligingscamera's. 67,9% van de respondenten geeft aan op de hoogte te zijn van het feit dat er camera's hangen en zich dus ervan bewust dat er beleid is inzake beveiligingscamera's voor hun Rijksdienst.



Figuur 27: Awareness van het camerabeleid

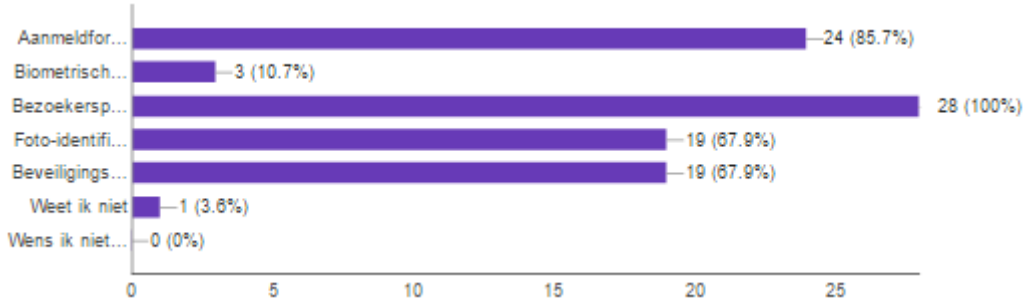
Hieruit blijkt dat er beleid is opgesteld binnen de Rijksoverheid omtrent het gebruik van beveiligingscamera's en dat een ruime meerderheid (67,9%) van de respondenten op de hoogte is van dit informatiebeveiligingsbeleid.

Biometrische toegangsdeuren
Biometrische technologie herkent iemand met behulp van zijn unieke biologische kenmerken, zoals vingerafdrukken, stem en gezicht.

De respondenten geven aan dat de medewerkers een toegangspas krijgen waarmee ze de gebouwen in en uit kunnen. Er wordt nog geen gebruik gemaakt van biometrische toegang tot de gebouwen. Ook in de BIR is nies te vinden over biometrische toegangsdeuren of het gebruik van biometrische techniek op andere onderdelen.

Hieruit blijkt dat de Rijksoverheid geen gebruik maakt van biometrische toegangsdeuren voor de toegang tot de gebouwen.

Aan de respondenten is gevraagd voor welke aspecten rondom de fysieke beveiliging beleid aanwezig is binnen hun Rijksdienst. Een van de aspecten van fysieke beveiliging is een biometrische toegangsdeur. Slechts 10,7% van de respondenten geeft aan dat er beleid aanwezig is inzake biometrische toegangsdeuren.



Figuur 28: Awareness van het fysieke toegangsbeleid

De exacte vraag die is gesteld, luidt: ‘Welke aspecten van de fysieke beveiliging zijn ingeregeld binnen de organisatie?’ Het kan zijn dat een bepaalde ruimte in een gebouw is beveiligd met biometrische technologie. In de enquête is gevraagd naar (de aanwezigheid van) beleid specifiek voor de toegang tot gebouwen, niet tot specifieke ruimten. De vraag blijkt dan ook een ander antwoord op te leveren dan verwacht.

Hieruit blijkt dat binnen een aantal afdelingen beleid aanwezig is inzake biometrische toegangsdeuren. Dit beleid komt echter niet terug in de BIR of enig ander informatiebeveiligingsdocument dat voor dit onderzoek is gebruikt.

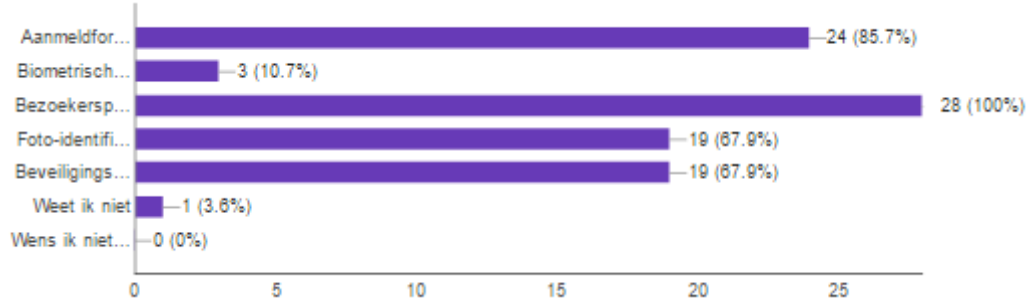
Toegangspas met foto-identificatie
De medewerkers beschikken over diverse autorisaties om hun taken te kunnen uitvoeren. Die autorisaties bepalen in welke delen van een gebouw zij mogen komen.

De respondenten geven aan dat iedere medewerker een op naam gestelde toegangspas krijgt, die voorzien is van een foto.
Het gebruik van deze toegangspas is strikt persoonlijk en bovendien gebonden aan het arbeidscontract. Per Rijksoverheid-locatie kan toegang worden gegeven aan de gebruiker van de pas door hem te autoriseren voor de betreffende locatie.

Figuur 29: Voorbeeld toegangspas

Hieruit blijkt dat er beleid aanwezig is met betrekking tot toegangspasjes en dat er toegangspasjes worden gebruikt bij de Rijksoverheid.

Aan de respondenten is gevraagd voor welke aspecten van de fysieke beveiliging er beleid aanwezig is binnen hun Rijksdienst. Toegangspassen met foto-identificatie zijn zo'n aspect. 67,9% van de respondenten geeft aan dat er beveiligingsbeleid aanwezig is inzake foto-identificatietoegangspassen.



Figuur 30: Awareness van het fysieke toegangsbeleid

Hieruit blijkt dat een kleine meerderheid van de respondenten op de hoogte is van het informatiebeveiligingsbeleid inzake foto-identificatietoegangspassen. Dit is een onverwachte uitkomst. De onderzoeker had hier 100% verwacht, omdat elke Rijksoverheid-medewerker (intern en extern) een Rijkspas krijgt met zijn foto erop. Zonder deze persoonlijke toegangspas kan alleen toegang worden verkregen met een bezoekerspas voor een dag (een 'dagpas'), waar geen foto op staat.

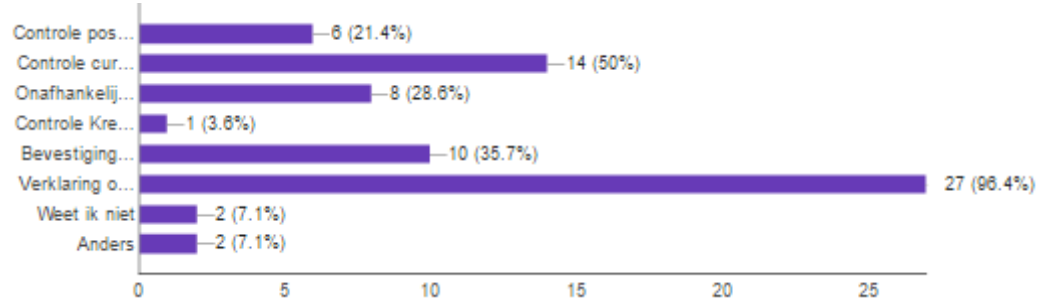
Controle juistheid van curriculum vitae
Er dient te worden gecontroleerd of het aangeleverde curriculum vitae correct is en dat hier niet mee is gesjoemeld. Er moet een onafhankelijke identiteitscontrole plaatsvinden en er dient een bevestiging van diploma's en certificaten plaats te vinden.

In de BIR wordt dit punt niet besproken. Tevens geven de respondenten aan dat het curriculum van een sollicitant zelden tot nooit volledig wordt nagetrokken. Als het gevoel goed is tijdens de sollicitatie dan is het goed. Het curriculum wordt nagekeken op relevante werkervaring en diploma's. Er vinden normaliter geen checks plaats van diploma's en referenties. De respondenten worden wel

geacht hun diploma's aan te leveren zodat deze aan hun personeelsdossier kunnen worden toegevoegd.

Hieruit blijkt dat het curriculum vrijwel niet wordt nagetrokken bij de Rijksoverheid en dat hier geen informatiebeveiligingsbeleid voor is opgesteld.

In de enquête is gevraagd aan de respondenten of er informatiebeveiligingsbeleid aanwezig is voor de controle van het curriculum, een onafhankelijke identiteitscontrole en de bevestiging van diploma's en certificaten. 50% van de respondenten geeft aan dat er informatiebeveiligingsbeleid aanwezig is voor de controle op curricula vitae van sollicitanten. 28,6% van de respondenten geeft aan dat er informatiebeveiligingsbeleid aanwezig is voor een onafhankelijke identiteitscontrole. 35,7% geeft aan dat er beleid aanwezig is voor de bevestiging/controle van diploma's en certificeringen.



Figuur 31: Awareness controle juistheid curriculum

Hieruit blijkt dat hier een verschil is tussen de aanwezigheid van informatiebeveiligingsbeleid en de perceptie van de aanwezigheid van dit beleid.
In de interviews hebben alle managers, IT-specialisten en beveiligingsspecialisten aangegeven dat er geen informatiebeveiligingsbeleid is omtrent de controle van het curriculum vitae, terwijl een aanzienlijk deel van de respondenten aangeeft dat hier wel degelijk beleid voor aanwezig is.

Disciplinaire maatregelen
Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die een inbreuk op de beveiliging hebben gemaakt.

Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligingsbeleid (Rijksoverheid, 2012a). De BIR verwijst vervolgens naar hoofdstuk 8 uit het Algemeen Rijksambtenarenreglement (ARAR). In het ARAR is het volgende opgenomen:

- De ambtenaar, die de hem opgelegde verplichtingen niet nakomt of zich overigens aan plichtsverzuim schuldig maakt, kan deswege disciplinair worden gestraft
- Plichtsverzuim omvat zowel het overtreden van enig voorschrift als het doen of nalaten van iets, hetwelk een goed ambtenaar in gelijke omstandigheden behoort na te laten of te doen.

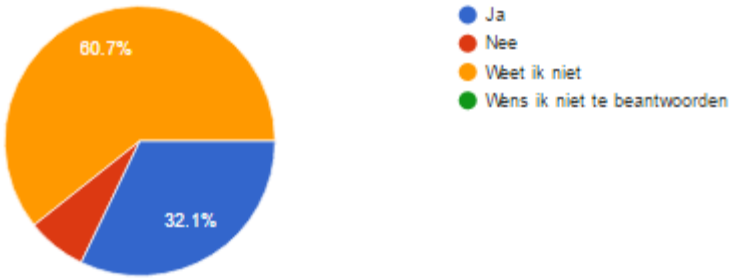
Enkele disciplinaire straffen die kunnen worden opgelegd, zijn:

- Schriftelijke berisping
- Vermindering van het recht op jaarlijkse vakantie met ten hoogste een derde van het aantal uren, waarop in het desbetreffende kalenderjaar aanspraak bestaat
- Gehele of gedeeltelijke inhouding van het salaris tot een bedrag van ten hoogste het salaris over een halve maand
- Het niet ontvangen van periodieke salarisverhogingen gedurende ten hoogste vier jaren

- Schorsing voor een bepaalde tijd met gehele of gedeeltelijke inhouding van bezoldiging
- Ontslag.

Hieruit blijkt dat er een formeel disciplinair proces met maatregelen is ingeregeld bij de Rijksoverheid.

In de enquête werd de respondenten gevraagd of binnen de Rijksdienst informatiebeveiligingsbeleid aanwezig is omtrent disciplinaire maatregelen tegen medewerkers bij een inbreuk op de informatiebeveiliging.



Figuur 32: Awareness van beleid inzake disciplinaire maatregelen

60,7% geeft aan niet te weten of hiervoor beleid aanwezig is. 7,1% geeft aan dat hiervoor geen beleid aanwezig is binnen zijn Rijksdienst.

Hieruit blijkt dat in totaal 67,8% van de medewerkers niet op de hoogte is van het aanwezige informatiebeveiligingsbeleid inzake disciplinaire maatregelen binnen de Rijksoverheid.

Documentafhandeling/-vernietiging
Media en documenten behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn.

In de BIR wordt aangegeven dat er procedures zijn vastgesteld en in werking zijn getreden voor verwijdering van vertrouwelijke data en de vernietiging van verwijderbare media. Voor het verwijderen van data wordt een Secure Erase gebruikt voor apparaten waarbij dit mogelijk is.

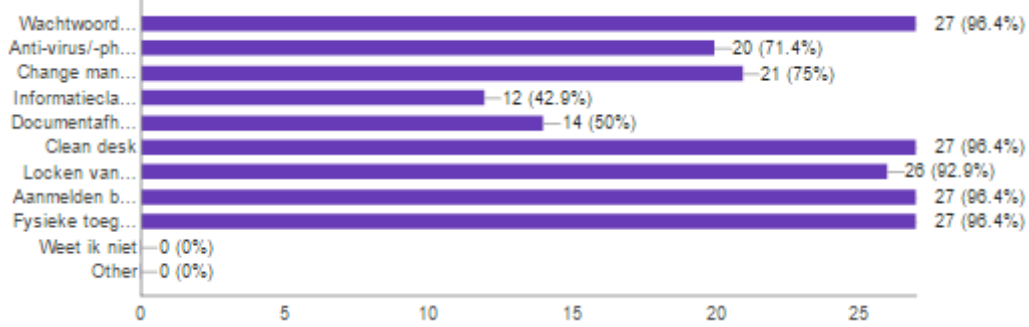
De geïnterviewden geven aan dat op elke verdieping een normale papierbak met daarop een shredder en een fysiek afgesloten papierbak aanwezig zijn. De afgesloten papierbak wordt opgehaald en de inhoud ervan wordt vernietigd door een externe partij. Op deze manier wordt het papier op een veilige en beveiligde manier vernietigd.

Alle mobiele apparaten en harde schijven worden na afschrijving vernietigd en dus niet doorverkocht als tweedehands goederen. Ook media worden op deze manier op een veilige en beveiligde manier vernietigd.

Hieruit blijkt dat de medewerkers van de Rijksoverheid over een veilige en beveiligde manier van documentafhandeling/-vernietiging beschikken en hier beleid voor is opgesteld. Het is aan de medewerkers zelf om te bepalen of informatie vertrouwelijk is en op welke wijze deze vervolgens vernietigd (shredder) of weggegooid (afgesloten papierbak) dient te worden.

In de enquête is de respondenten gevraagd om aan te geven voor welke aspecten een beveiligingsbeleid aanwezig is binnen de organisatie. Specifiek voor documentafhandeling en -

vernietiging geeft 50% van de respondenten aan van dit beleid op de hoogte te zijn.



Figuur 33: Awareness van de aspecten van het informatiebeveiligingsbeleid

Hieruit blijkt dat de helft van de medewerkers op de hoogte is van het informatiebeveiligingsbeleid inzake documentafhandeling en -vernietiging.

E-mailfiltering
Het opzetten en onderhouden van e-mailspamfilters zal ervoor zorgen dat gebruikers minder snel ten prooi vallen aan phishingaanvallen, ketting-e-mails, virussen of wormen die schade kunnen veroorzaken.

Binnen de Rijksoverheid wordt gebruikgemaakt van een spamfilter voor de e-mailberichten (Rijksoverheid, 2012a).
De respondenten geven aan dat de internetprovider ook een spamfilter heeft ingesteld voor het internetverkeer. Er zijn derhalve twee spamfilters actief voor e-mailfiltering: een bij de internetprovider en een bij de IT-dienstverlener van de Rijksdiensten zelf.

Hieruit blijkt dat binnen de Rijksoverheid e-mailfiltering plaatsvindt en hier informatiebeveiligingsbeleid voor is opgesteld.

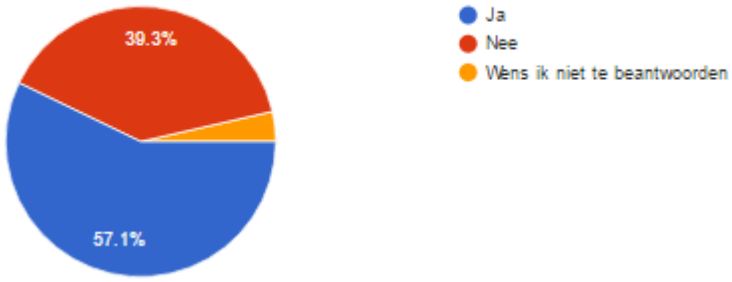
In de enquête is niet gevraagd of de respondenten op de hoogte zijn van dit informatiebeveiligingsbeleid, omdat dit informatiebeveiligingsbeleid technisch op de achtergrond zijn werk doet. De medewerkers krijgen hier niet veel van mee.

Het beperken van datalekken
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Voorbeelden van beveiligingsincidenten zijn het kwijtraken van een USB-stick met informatie, de diefstal van een laptop of een inbraak door een hacker.
Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan of als een onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten.

In de BIR staat niets over de beperking van datalekken of hoe om te gaan met datalekken. Datalekken worden zelfs niet genoemd in de BIR. De respondenten gaven echter aan dat voor de gehele overheid hetzelfde proces geldt inzake datalekken en dat hier een wet voor is. In deze wet wordt het proces dat door de overheidsinstanties dient te worden gevolgd uitgebreid beschreven. Bij het niet melden van een datalek krijgt de verantwoordelijke instantie een waarschuwing of aanzienlijke boete. Binnen de Rijksdiensten wordt het wettelijk voorgeschreven proces in een apart document beschreven, met de naam ‘Handboek voor de afhandeling van (vermoedelijke) datalekken’. Hierin is ook een stappenplan opgenomen.

Hieruit blijkt dat er informatiebeveiligingsbeleid aanwezig is voor het beperken en afhandelen van datalekken binnen de Rijksoverheid.

In de enquête is vervolgens gevraagd aan de medewerkers of zij weten hoe ze dienen om te gaan met een datalek. 39,3% van de respondenten weet niet hoe moet worden omgegaan met een datalek binnen zijn Rijksdienst.



Figuur 34: Awareness van het beleid inzake datalekken

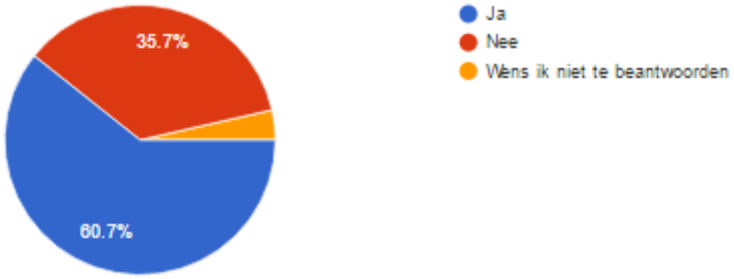
Hieruit blijkt dat een groot deel van de respondenten niet op de hoogte is van het informatiebeveiligingsbeleid inzake de omgang met datalekken.

Een incidentafhandelingsproces
Er moet een procedure voor het rapporteren van beveiligingsgebeurtenissen zijn vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten. Daarin worden de handelingen vastgelegd die moeten worden uitgevoerd na het ontvangen van een melding van een beveiligingsincident. Een gedocumenteerd incidentafhandelingsproces zal ervoor zorgen dat een gebruiker onder druk precies weet welke procedures hij dient te volgen.

In de handreiking informatiebeveiliging en de BIR wordt aangegeven dat incidenten altijd direct gemeld dienen te worden, er wordt niet aangegeven bij wie deze gemeld moeten worden.
De respondenten geven aan dat er een incidentafhandelingsproces aanwezig is bij de Rijksdiensten. Incidenten moeten te allen tijde gemeld worden bij de servicedesk en de directe lijnmanager van de medewerker die het incident constateert. De servicedesk maakt een melding aan van het incident en maakt een inschatting van de impact. Vervolgens zet de servicedesk de melding door naar de afdeling beveiliging en neemt bij spoed telefonisch contact op met haar.
De afdeling beveiliging zet vervolgens, indien nodig, vervolgacties uit. Zij kan het incident escaleren en het escalatieteam bijeenroepen. Het escalatieteam bestaat uit alle lijnmanagers en teammanagers. Elke maand rapporteert het beveiligingsteam over de incidenten in de afgelopen periode. Deze rapportages worden uitgebracht aan het managementteam en de directies.

Er is derhalve een incidentafhandelingsproces ingericht binnen de Rijksoverheid.

In de enquête werd vervolgens aan de medewerkers gevraagd of zij weten hoe zij dienen om te gaan met een beveiligingsincident binnen hun organisatie. Hieruit blijkt dat 35,7% van de ondervraagde medewerkers dit niet weet en niet op de hoogte is van het beleid inzake incidentafhandeling.



Figuur 35: Awareness van incidentafhandelingsbeleid

Hieruit blijkt dat een derde van de medewerkers niet op de hoogte is van het incidentafhandelingsinformatiebeveiligingsbeleid.

Informatieclassificatie

Informatie is een strategisch bedrijfsmiddel dat beveiligd moet worden. Niet alle soorten informatie hoeven echter op dezelfde manier behandeld te worden. Informatieclassificatie zorgt ervoor dat elke soort informatie een geschikt niveau van beveiliging krijgt. Het classificatiebeleid dient duidelijk te beschrijven welke informatie als gevoelig wordt beschouwd en hoe met deze informatie om moet worden gegaan.

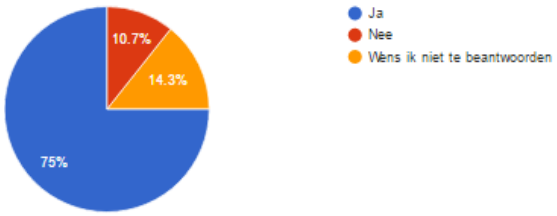
Binnen de Rijksoverheid bestaan verschillende niveaus van dataclassificatie. Figuur 35 is afkomstig uit de BIR en geeft de verschillende niveaus weer.
De respondenten gaven aan dat deze niveaus ook daadwerkelijk worden gebruikt. Binnen de organisatie is een lijst aanwezig van de verschillende informatiesystemen met de daarbij horende classificatie. Voor Word-documenten zijn templates aanwezig met de verschillende niveaus van classificatie.

Beveiligingsniveau / *Aard van de informatie:*	Baseline (BIR)	Baseline + aanvullende beveiligings maatregelen	Baseline + DWR-G beveiligings maatregelen
Openbare informatie	V	V	V
Niet gerubriceerde informatie	V	V	V
Departementaal Vertrouwelijke	V	V	V
Staatsgeheim – Confidentieel	X	V	V
Staatsgeheim – Geheim	X	O	V
Staatsgeheim – Zeer Geheim	X	X	X

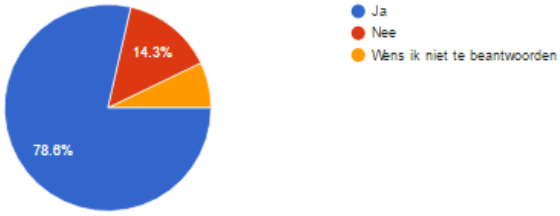
Figuur 36: Informatieclassificatie

Hieruit blijkt dat er informatieclassificatiebeleid is ingeregeld binnen de Rijksoverheid.

In de enquête is de respondenten gevraagd of zij vanuit hun functie toegang hebben tot vertrouwelijke informatie en of zij vanuit hun functie kunnen aangeven welke informatie vertrouwelijk is binnen hun Rijksdienst/afdeling.



Figuur 37: Percentage respondenten dat vertrouwelijke informatie kan identificeren



Figuur 38: Percentage respondenten met toegang tot vertrouwelijke informatie

75% van de respondenten zegt te kunnen aangeven welke informatie vertrouwelijk is binnen zijn afdeling. Als een medewerker weet welke informatie vertrouwelijk is dan dient hij op de hoogte te zijn van het informatieclassificatiebeleid om deze keuze te kunnen maken. 78,6% van de respondenten geeft aan met vertrouwelijke informatie te maken te hebben in zijn functie.

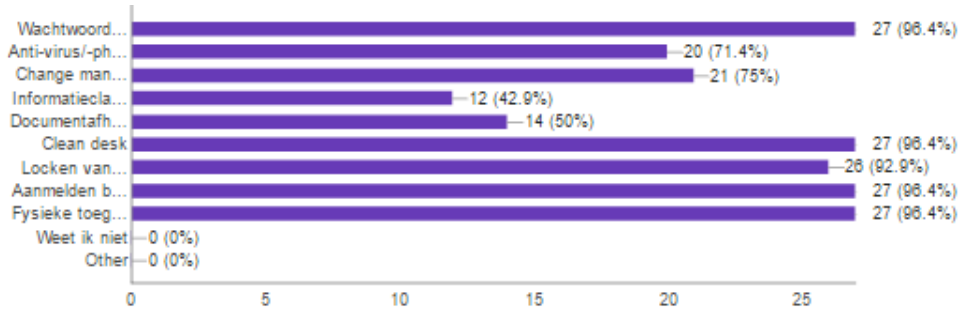
Hieruit blijkt dat 75% van de respondenten op de hoogte is van het informatieclassificatiebeleid binnen de Rijksoverheid.

Locken van computer
Wie toegang heeft tot de pc van iemand anders, heeft de beschikking over tal van persoonlijke en vaak heel vertrouwelijke gegevens. Als een medewerker niet in de buurt van zijn computer is, dient hij de computer te locken zodat anderen hier geen gebruik van kunnen maken

De Rijksdiensten hanteren een clear screen-beleid. Dit beleid houdt het volgende in: log altijd uit of vergrendel de computer zodra je de werkplek (tijdelijk) verlaat.
De respondenten gaven aan dat dit periodiek gecontroleerd wordt.
(Bron: Handreiking informatievoorziening en interviews)

Hieruit blijkt dat er informatiebeveiligingsbeleid aanwezig is binnen de Rijksdiensten voor het locken van de computer indien de medewerker niet op zijn werkplek aanwezig is.

In de enquête is aan de respondenten gevraagd voor welke aspecten er informatiebeveiligingsbeleid aanwezig is binnen hun Rijksdienst. 92,9% van hen geeft aan dat er informatiebeveiligingsbeleid aanwezig is voor het locken van de computers.



Figuur 39: Awareness van de aspecten van het informatiebeveiligingsbeleid

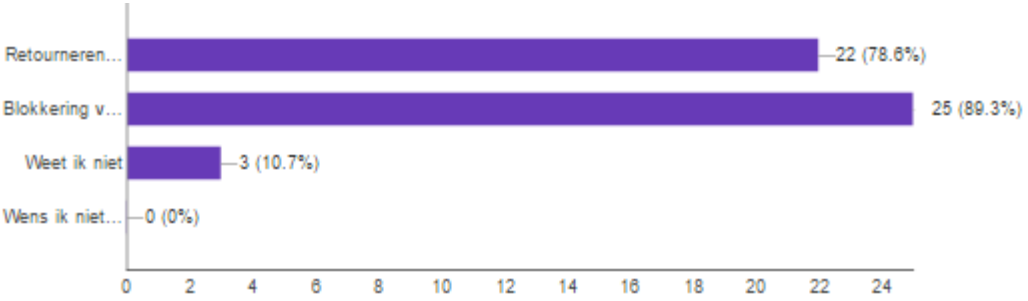
Hieruit blijkt dat bijna alle medewerkers (92,9%) bij de Rijksoverheid op de hoogte zijn van het informatiebeveiligingsbeleid inzake het locken van computers.

Retourneren van bedrijfsmiddelen

Wanneer een medewerker de Rijksdienst verlaat, moet hij alle bedrijfsmiddelen, zoals een mobiele telefoon of een laptop, retourneren.

Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband. Het lijnmanagement heeft een procedure vastgesteld voor de beëindiging van het dienstverband waarin minimaal aandacht besteed is aan het intrekken van de toegangsrechten en de inname van bedrijfsmiddelen (Rijksoverheid, 2012a).

Hieruit blijkt dat binnen de Rijksoverheid informatiebeveiligingsbeleid is opgesteld voor het retourneren van bedrijfsmiddelen bij de beëindiging van een dienstverband of overeenkomst.
In de enquête is de respondenten de vraag gesteld met welke van de onderstaande aspecten rekening wordt gehouden bij de beëindiging of wijziging van het dienstverband binnen de organisatie.
78,6% van de respondenten geeft aan dat bij de beëindiging van een dienstverband rekening wordt gehouden met het retourneren van bedrijfsmiddelen.



Figuur 40: Retourneren van bedrijfsmiddelen

Hieruit blijkt dat een ruime meerderheid van de medewerkers van de Rijksoverheid op de hoogte is van het informatiebeveiligingsbeleid inzake het retourneren van bedrijfsmiddelen.

Wachtwoordmanagement
Onder wachtwoordmanagement worden richtlijnen voor de samenstelling van wachtwoorden verstaan, zoals het aantal karakters dat elk wachtwoord moet bevatten en de aard daarvan. Ook wordt aangegeven hoe vaak een wachtwoord moet worden gewijzigd. Wachtwoordmanagement kan ook een eenvoudige verklaring inhouden dat de medewerkers geen wachtwoorden mogen prijsgeven aan anderen.

De medewerkers binnen de Rijksoverheid moeten de volgende gedragsregels naleven:

- Wachtwoorden worden niet opgeschreven
- Gebruikers delen hun wachtwoord nooit met anderen
- Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde
- Nadat voor een bepaalde gebruikersnaam vijf keer een foutief wachtwoord ingegeven is, wordt het account geblokkeerd.

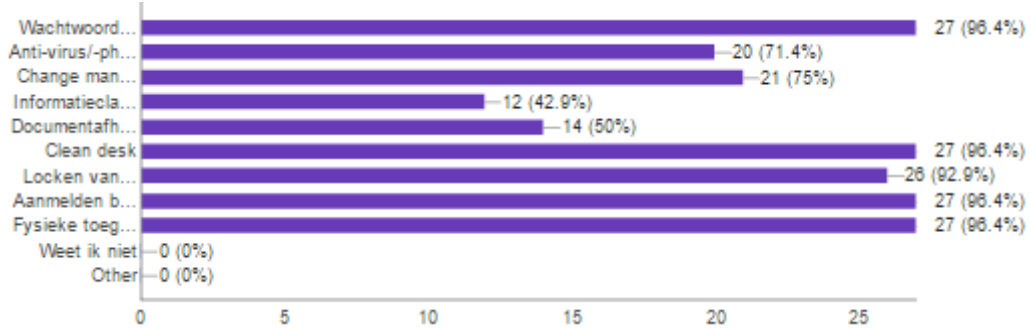
Daarnaast gelden de onderstaande regels in de onderzochte Rijksdiensten met betrekking tot het wachtwoordmanagement:

- Er wordt automatisch gecontroleerd op correct gebruik van wachtwoorden (sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord etc.)
- Wachtwoorden hebben een geldigheidsduur van maximaal drie maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd
- Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd
- De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen

(Rijksoverheid, 2012a); (Handreiking informatievoorziening)

Hieruit blijkt dat er informatiebeveiligingsbeleid inzake wachtwoordmanagement is ingeregeld en geborgd binnen de Rijksoverheid.

In de enquête is aan de respondenten gevraagd voor welke aspecten er informatiebeveiligingsbeleid aanwezig is binnen hun Rijksdienst. 96,4% van de respondenten geeft aan dat er specifiek voor wachtwoordmanagement informatiebeveiligingsbeleid aanwezig is binnen zijn Rijksdienst.

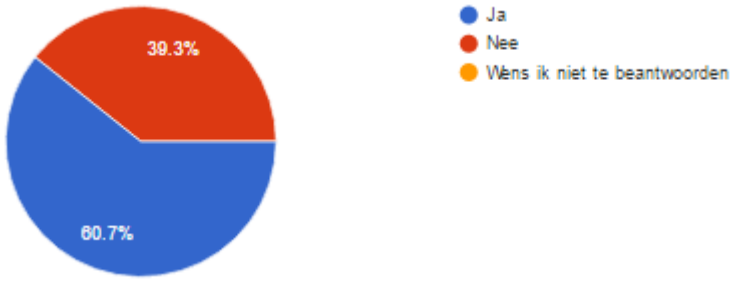


Figuur 41: Awareness van de aspecten van het informatiebeveiligingsbeleid

Hieruit blijkt dat vrijwel alle medewerkers (96,4%) binnen de Rijksoverheid op de hoogte zijn van het informatiebeveiligingsbeleid inzake wachtwoordmanagement.

4.5 In welke mate is de Rijksoverheid zelf het doelwit van social engineeringaanvallen?

In de enquête is onderzocht hoeveel respondenten denken het doelwit/slachtoffer te zijn geweest van een socialengineeringaanval in de afgelopen zes maanden. Vervolgens is de vraag gesteld via welk medium deze aanval/poging is ondernomen.
60,7% van de respondenten denkt het doelwit/slachtoffer te zijn geweest van een socialengineeringaanval in de afgelopen zes maanden.



Figuur 42: Percentage respondenten dat denkt slachtoffer te zijn geweest van een socialengineeringaanval in de afgelopen zes maanden

Vervolgens werd de vraag gesteld via welk kanaal deze poging werd ondernomen.
Hierbij geeft 57,1% van de respondenten aan dat de poging via e-mail werd gedaan. Daarnaast geeft 7,1% aan via telefoon en een sociaal netwerk te zijn benaderd. Dit betekent dat ongeveer 7% van de medewerkers doelwit/slachtoffer is geweest van drie socialengineeringaanvallen via verschillende kanalen in de afgelopen zes maanden.

Figuur 43: Via welk kanaal verliepen de socialengineeringaanvallen?

Hieruit blijkt dat meer dan de helft van de medewerkers van de Rijksoverheid te maken met een socialengineeringaanval in een periode van zes maanden. Een klein gedeelte krijgt zelfs te maken met meerdere aanvallen in deze periode. Het kanaal dat het meest wordt gebruikt voor de aanvallen is e-mail.

4.6 Samenvatting van het aanwezige informatiebeveiligingsbeleid en het percentage van de medewerkers dat op de hoogte is van dit informatiebeveiligingsbeleid

Administratieve beveiligingsmaatregelen	Informatiebeveiligingsbeleid aanwezig	Awareness van de medewerkers van dit beleid
Antivirus/antiphishing	Ja	71,4%
Arbeidsvoorwaarden	Ja	35,7%
Auditbeleid en auditcontroles	Ja	Niet gevraagd
Blokkering toegangsrechten	Ja	89,3%
Clean desk	Ja	96,4%
Controle beschikbaarheid positieve referenties	Nee	21,4%
Controle juistheid van curriculum	Nee	60%
Disciplinaire maatregelen	Ja	32,1%
Documentafhandeling/-vernietiging	Ja	50%
E-mailfiltering	Ja	Niet gevraagd
Het beperken van datalekken	Ja	57,1%
Incidentafhandelingsstrategie	Ja	60,7%
Informatieclassificatie	Ja	42,9%
Locken van computer	Ja	92,6%
Retourneren van bedrijfsmiddelen	Ja	78,6%
Wachtwoordmanagement	Ja	96,4%

Tabel 8: Administratieve beveiligingsmaatregelen

Fysieke beveiligingsmaatregelen	Informatiebeveiligingsbeleid aanwezig	Awareness van de medewerkers van dit beleid
Aanmeldformulieren bezoekers	Ja	96,4%
Beveiligingscamera's	Ja	67,9%
Bezoekerspasjes	Ja	100%
Biometrische toegangsdeuren	Nee	10,7%
Foto-identificatiepasjes	Ja	67,9%

Tabel 9: Fysieke beveiligingsmaatregelen

5 Conclusie en aanbevelingen

In dit hoofdstuk worden de onderzoeksresultaten uit hoofdstuk 4 gebruikt om antwoord te geven op de hoofd- en deelvragen. Als eerste wordt antwoord gegeven op de deelvragen, waarna de hoofdvragen beantwoord worden om uiteindelijk de hypothesen aan te nemen of te verwerpen.

5.1 Deelvraag 1: Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid?

Binnen de Nederlandse Rijksoverheid is de Baseline Informatiebeveiliging Rijksdienst (BIR) leidend. Alle Rijksdiensten die vallen onder de Rijksoverheid dienen te voldoen aan alle voorgeschreven punten in de BIR. Als een Rijksdienst niet kan voldoen aan een bepaald punt moet worden beargumenteerd waarom hier niet aan voldaan kan worden. Dit is het zogeheten 'comply or explain'-principe.

Aan de basis van de BIR ligt ISO 27001. ISO 27001 wordt dan ook gebruikt om de BIR up-to-date te houden.

Naast de BIR en ISO27001 is een Hand-out informatiebeveiliging opgesteld en verspreid binnen de Rijksdiensten. Op deze hand-out worden de belangrijkste aspecten van informatiebeveiliging beschreven. De hand-out is toegevoegd als bijlage.

5.2 Deelvraag 2: Zijn de medewerkers van de Nederlandse Rijksoverheid inhoudelijk bekend met deze informatiebeveiligingsdocumenten?

Alle medewerkers die zijn geïnterviewd zijn inhoudelijk bekend met de bij deelvraag 1 genoemde documenten. Dit is te verklaren omdat voor de interviews medewerkers zijn geselecteerd van wie werd verwacht dat zij hiervan op de hoogte waren.

In de enquête is de vraag gesteld met welke van de informatiebeveiligingsdocumenten de medewerkers inhoudelijk bekend zijn.

Hieruit is gebleken dat niet alle medewerkers van de Rijksoverheid inhoudelijk bekend zijn met de belangrijkste informatiebeveiligingsdocumenten:

- 46,4% van de medewerkers is inhoudelijk bekend met de BIR
- 28,6% van de medewerkers is inhoudelijk bekend met ISO 27001
- 64,3% van de medewerkers is inhoudelijk bekend met de Hand-out informatiebeveiliging
- 21,4% van de medewerkers is met geen van de informatiebeveiligingsdocumenten bekend

De verschillende Rijksdiensten hebben veel medewerkers die geen enkele affiniteit met ICT hebben. Hun werk is voornamelijk financieel of operationeel van aard of zij werken op beleidsniveau. Van de gemiddelde medewerker kan dan ook niet worden verwacht dat hij inhoudelijk op de hoogte is van de BIR, omdat zijn functie en kerntaken hier niet op zijn gericht. Van de medewerkers kan wel worden veracht dat zij op de hoogte zijn van de Hand-out informatiebeveiliging. Deze hand-out is een A4, waardoor deze snel te lezen is.

Het is interessant om te zien dat slechts 17,9% van de medewerkers een training inzake informatiebeveiliging heeft gevolgd. Toch is 46,4% inhoudelijk op de hoogte van de BIR. Dit betekent

dat medewerkers uit eigen indicatief de BIR hebben bekeken en geïnteresseerd zijn in het onderwerp informatiebeveiliging.

5.3 Deelvraag 3: Zijn de medewerkers van Nederlandse Rijksoverheid bekend met de terminologie van social engineering?

53,6 procent van de respondenten is bekend met de gegeven definitie van social engineering, die ook in dit onderzoek wordt gebruikt.
57,1 % van de respondenten is niet bekend hoe een social engineeringsaanval wordt uitgevoerd.

In de enquête is bewust naar de bekendheid van de aanvallen als begrip/terminologie gevraagd. Met deze vraag is getoetst in hoeverre de respondenten bekend zijn met de terminologie en dus niet inhoudelijk met de aspecten van een bepaalde aanval. Het kan zijn dat wanneer een begrip wordt uitgelegd de respondenten hiermee wel bekend zijn en de vraag anders zullen beantwoorden.

Phishing is bekend bij alle respondenten terwijl water holing en reverse social engineering bij vrijwel geen enkele respondent bekend is. Malicious software is ook bij veel respondenten bekend. Dit is echter geen aanval die onder social engineering valt.
De helft van de respondenten geeft aan bekend te zijn met de meestvoorkomende motieven van een socialengineeringaanval.

Minstens de helft van de respondenten weet dat een social engineer misbruik probeert te maken van bepaalde menselijke aspecten. 14,3% van de respondenten geeft aan niet te weten van welke menselijke aspecten een social engineer gebruikmaakt.

De conclusie is dat ongeveer de helft van de medewerkers bekend is met de definitie van social engineering en weet wat het begrip inhoudt. Ook geeft ongeveer de helft aan te weten wat de meestvoorkomende motieven zijn van social engineerings.

De conclusie is dat de medewerkers van de Rijksoverheid onvoldoende op de hoogte zijn van de terminologie en aspecten van social engineering.

5.4 Deelvraag 4: Welke socialengineeringbeveiligingsmaatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de Rijksoverheid?

In de onderstaande tabellen wordt per beveiligingsmaatregel weergegeven of hier wel of geen informatiebeveiligingsbeleid voor aanwezig is binnen de Rijksoverheid.

Administratieve beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**
Antivirus/antiphishing	Ja
Arbeidsvoorwaarden	Ja
Auditbeleid en auditcontroles	Ja
Blokkering toegangsrechten	Ja
Clean desk	Ja
Controle beschikbaarheid positieve referenties	Nee
Controle juistheid van curriculum	Nee
Disciplinaire maatregelen	Ja
Documentafhandeling/-vernietiging	Ja
E-mailfiltering	Ja
Het beperken van datalekken	Ja
Incidentafhandelingsstrategie	Ja
Informatieclassificatie	Ja
Locken van computer	Ja
Retourneren van bedrijfsmiddelen	Ja
Wachtwoordmanagement	Ja

Tabel 10: Administratieve beveiligingsmaatregelen

Fysieke beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**
Aanmeldformulieren bezoekers	Ja
Beveiligingscamera's	Ja
Bezoekerspasjes	Ja
Biometrische toegangsdeuren	Nee
Foto-identificatiepasjes	Ja

Tabel 11: Fysieke beveiligingsmaatregelen

De conclusie is dat voor 18 van de 21 socialengineeringbeveiligingsmaatregelen (85,71 %) op beleidsniveau direct of indirect worden afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de Rijksoverheid.

5.5 Deelvraag 5: Wat is de mate van awareness van de medewerkers binnen de Rijksoverheid van het informatiebeveiligingsbeleid inzake social engineering?

In de onderstaande tabellen is de mate van awareness van de medewerkers van het informatiebeveiligingsbeleid inzake de beveiligingsmaatregelen aangegeven.
Er zijn in totaal 21 beveiligingsmaatregelen. Van twee maatregelen is de awareness niet bekend. Van de overige 19 maatregelen is een awareness-percentage weergegeven. De gemiddelde awareness is 64,82% (alle percentages opgeteld en vervolgens gedeeld door 19), van alle beveiligingsmaatregelen die zijn onderzocht in dit onderzoek.

Administratieve beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**	**Awareness van de medewerkers van dit beleid**
Antivirus/antiphishing	Ja	71,4%
Arbeidsvoorwaarden	Ja	35,7%
Auditbeleid en -controles	Ja	Niet gevraagd
Blokkering toegangsrechten	Ja	89,3%
Clean desk	Ja	96,4%
Controle beschikbaarheid positieve referenties	Nee	21,4%
Controle juistheid van curriculum	Nee	60%
Disciplinaire maatregelen	Ja	32,1%
Documentafhandeling/-vernietiging	Ja	50%
E-mailfiltering	Ja	Niet gevraagd
Het beperken van datalekken	Ja	57,1%
Incidentafhandelingsstrategie	Ja	60,7%
Informatieclassificatie	Ja	42,9%
Locken van computer	Ja	92,6%
Retourneren van bedrijfsmiddelen	Ja	78,6%
Wachtwoordmanagement	Ja	96,4%

Tabel 12: Administratieve beveiligingsmaatregelen

Fysieke beveiligingsmaatregelen	**Informatiebeveiligingsbeleid aanwezig**	**Awareness van de medewerkers van dit beleid**
Aanmeldformulieren bezoekers	Ja	96,4%
Beveiligingscamera's	Ja	67,9%
Bezoekerspasjes	Ja	100%
Biometrische toegangsdeuren	Nee	10,7%
Foto-identificatiepasjes	Ja	67,9%

Tabel 13: Fysieke beveiligingsmaatregelen

5.6 Deelvraag 6: Van welke socialengineeringaanvallen is de Nederlandse Rijksoverheid in de afgelopen zes maanden het slachtoffer geweest en welk medium gebruikten deze aanvallen?

60,7% van de respondenten denkt het doelwit/slachtoffer te zijn geweest van een socialengineeringsaanval in de afgelopen zes maanden.

57,1% van de respondenten zegt dat de poging via e-mail verliep, 7,1% zegt ook via telefoon en een sociaal netwerk te zijn benaderd. Dit betekent dat ongeveer 10% van de medewerkers doelwit/slachtoffer is geweest van drie socialengineeringaanvallen via verschillende kanalen in de afgelopen zes maanden.

5.7 Hypothese 1: Het informatiebeveiligingsbeleid inzake social engineering binnen de Rijksoverheid komt niet over bij de medewerkers op de werkvloer

Deze hypothese houdt stand. De gemiddelde awareness van een medewerker van de beveiligingsmaatregelen tegen social engineering in dit onderzoek blijkt 64,82% te zijn.

5.8 Hypothese 2: Meer dan 50 procent van de onderzochte Rijksoverheid-medewerkers is in de afgelopen zes maanden het slachtoffer geweest van een socialengineeringaanval

Deze hypothese houdt stand. Het blijkt dat 60,7 % van de medewerkers van de Rijksoverheid het doelwit/slachtoffer is geweest van een socialengineeringaanval in de afgelopen zes maanden.

5.9 Hoofdvraag 1: Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid inzake de geïdentificeerde socialengineeringmaatregelen uit het literatuuronderzoek en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid?

Er is een aanzienlijk verschil tussen de mate van bescherming in theorie en praktijk bij de Rijksoverheid.

Om te kunnen concluderen dat er geen verschil tussen de theorie en praktijk is dienen alle percentages van de awareness van het informatiebeveiligingsbeleid 100% te zijn.
Zoals uit de onderstaande tabel blijkt, komt dit echter maar bij één beveiligingsmaatregel voor, de fysieke beveiligingsmaatregel voor de invoering van bezoekerspasjes. Bij vijf maatregelen is minder dan de helft van de medewerkers op de hoogte van het informatiebeveiligingsbeleid.
Alle percentages onder de 50% zijn rood gemarkeerd om te verduidelijken dat hier de meeste winst te behalen is.

Administratieve beveiligingsmaatregelen	Informatiebeveiligingsbeleid aanwezig	Awareness van de medewerkers van dit beleid
Antivirus/antiphishing	Ja	71,4%
Arbeidsvoorwaarden	Ja	35,7%
Auditbeleid en -controles	Ja	Niet gevraagd
Blokkering toegangsrechten	Ja	89,3%
Clean desk	Ja	96,4%
Controle beschikbaarheid positieve referenties	Nee	21,4%
Controle juistheid van curriculum	Nee	60%
Disciplinaire maatregelen	Ja	32,1%
Documentafhandeling/-vernietiging	Ja	50%
E-mailfiltering	Ja	Niet gevraagd
Het beperken van datalekken	Ja	57,1%
Incidentafhandelingsstrategie	Ja	60,7%
Informatieclassificatie	Ja	42,9%
Locken van computer	Ja	92,6%
Retourneren van bedrijfsmiddelen	Ja	77,4%
Wachtwoordmanagement	Ja	96,4%

Tabel 14: Awareness administratieve beveiligingsmaatregelen

Fysieke beveiligingsmaatregelen	Informatiebeveiligingsbeleid aanwezig	Awareness van de medewerkers van dit beleid
Aanmeldformulieren bezoekers	Ja	96,4%
Beveiligingscamera's	Ja	67,9%
Bezoekerspasjes	Ja	100%
Biometrische toegangsdeuren	Nee	10,7%
Foto-identificatiepasjes	Ja	67,9%

Tabel 15: Awareness fysieke beveiligingsmaatregelen

Het lijkt er dan ook op dat de Rijksoverheid te veel vertrouwt op de aanwezigheid van beleid om in theorie te kunnen aantonen dat zij aan alle eisen uit de BIR heeft voldaan. De Rijksoverheid leunt achterover en neemt een afwachtende houding aan met de gedachte dat ze veilig is totdat het tegendeel is bewezen. Het invoeren van beleid zonder dat dit beleid bekend is bij de medewerkers betekent in feite dat het beleid nooit het gewenste resultaat zal hebben.

5.10 Hoofdvraag 2: In hoeverre is de Rijksoverheid zelf het doelwit of slachtoffer van socialengineeringaanvallen?

De Rijksoverheid is zelf veelvuldig het doelwit/slachtoffer van socialengineeringaanvallen.
60,7% van de respondenten denkt het doelwit/slachtoffer te zijn geweest van een socialengineeringaanval in de afgelopen zes maanden.

57,1% van de respondenten gaf aan dat de poging via e-mail verliep en 7,1% zegt via telefoon en een sociaal netwerk te zijn benaderd.
Dit betekent dat ongeveer 10% van de medewerkers doelwit/slachtoffer is geweest van drie socialengineeringaanvallen via verschillende kanalen in de afgelopen zes maanden.

5.11 Eindconclusie

Uit de conclusie van onderzoeksvraag twee blijkt dat 60,7% van de respondenten in de laatste zes maanden denkt slachtoffer te zijn geweest van een socialengineeringsaanval. Uit deze cijfers blijkt dat het probleem social engineering binnen de Rijksoverheid wel degelijk bestaat. De schade is in dit onderzoek niet onderzocht echter in het literatuuronderzoek kwam naar voren dat het opruimen van een incident in de betreffende onderzoeken gemiddeld 40.000 USD kost voor de onderzochte organisaties. Waarschijnlijk berokkent social engineering dan ook aanzienlijke schade aan de Rijksoverheid. Met deze cijfers zouden we verwachten dat het aspect social engineering een belangrijk punt is binnen het informatiebeveiligingsbeleid van de Rijksoverheid.

Niets is echter minder waar. Iedere Rijksdienst voert het op Rijksoverheid bepaalde informatiebeveiligingsbeleid door binnen hun organisatie. Hiermee proberen deze Rijksdiensten naar hun beste vermogen social engineering het hoofd te bieden. Social engineering wordt echter niet direct genoemd in de belangrijkste informatiebeveiligingsdocumenten van de Rijksoverheid. Indirect worden in deze informatiebeveiligingsdocumenten echter wel vrijwel alle onderzochte beveiligingsmaatregelen uit dit onderzoek tegen socialengineeringsaanvallen op beleidsniveau afgedekt.

De gemiddelde awareness van een medewerker op het informatiebeveiligingsbeleid inzake social engineering in dit onderzoek blijkt 64,82% te zijn, waarvan 5 van de 19 aspecten onder de 50 procent scoren en slechts één aspect de volledige 100 procent. Voor de Rijksoverheid en de Rijksdiensten valt op het awareness aspect dan ook de grootste winst te behalen.

6 Aanbevelingen voor vervolgonderzoek

Hieronder worden aanbevelingen gedaan voor vervolgonderzoek.

6.1 Aanbevelingen voor wetenschappelijk vervolgonderzoek

6.1.1 Andere of bredere scope

Het onderzoek moet met een andere vraagstelling of andere scope worden uitgevoerd. De scope moet worden verbreed om de onderzoeksresultaten generaliseerbaarder te maken. Ook kunnen enkele vragen die tijdens dit onderzoek naar boven zijn gekomen, worden uitgezocht.
Enkele voorbeelden hiervan zijn:

- Scopeaanpassing/-verbreding naar een heel ministerie, een volledige Rijksdienst of de volledige Rijksoverheid.
- Scopeaanpassing naar België of de Europese Unie (EU). Social engineering komt in alle EU-landen voor. Het zou interessant zijn om te bekijken hoe andere overheden en de EU hiermee omgaan en welke wetgeving/maatregelen zij hiertegen hebben ingevoerd.
- Hoe wordt het informatiebeveiligingsbeleid geüpdatet, hoe lang duurt het voordat het informatiebeveiligingsbeleid dat is opgesteld bij alle Rijksdiensten bekend is en is ingevoerd?
- Wordt het informatiebeveiligingsbeleid ook nageleefd? Het testen van het informatiebeveiligingsbeleid of het houden van interviews/enquêtes over het informatiebeveiligingsbeleid.
- Het testen van het informatiebeveiligingsbeleid door middel van aanvallen, bijvoorbeeld een mystery guest die probeert binnen te komen of penetratietesten op de medewerkers (phishing mails etc.).
- Welke informatiebeveiligingsmaatregelen beschermen daadwerkelijk tegen de methoden of technieken van social engineering?
- Is er een verband tussen de awareness en het aantal jaar dat iemand werkzaam is in zijn functie? Zijn hier wezenlijke verschillen tussen?
- Is er een verband tussen de awareness van interne medewerkers en die van externe medewerkers? Zijn hier wezenlijke verschillen tussen?
- Hoe wordt het informatiebeveiligingsbeleid overgebracht op de medewerkers?

6.1.2 Verder in de tijd

Hetzelfde onderzoek moet over een aantal jaar nogmaals worden uitgevoerd. De gebieden van informatiebeveiliging en social engineering veranderen continu. Over twee jaar kan het referentiemodel er totaal anders uitzien door nieuwe inzichten, aanvallen, maatregelen of de techniek. Ook zou het interessant zijn om te zien of na een aantal jaar de uitkomsten verbeterd zijn ten opzichte van dit onderzoek.

6.2 Aanbevelingen voor de praktijk

De volgende aanbevelingen zorgen ervoor dat de aspecten van social engineering bij de Rijksoverheid beter onder de aandacht worden gebracht:

- Er dient een gestructureerde oplossing/manier te komen om social engineering en soortgelijke informatiebeveiligingsaspecten onder de aandacht te brengen binnen de Rijksoverheid. In deze oplossing moeten de meestvoorkomende aanvallen en technieken met de maatregelen die ertegen genomen kunnen worden, worden beschreven. Een verwijzing naar deze gestructureerde oplossing inzage social engineering kan vervolgens worden opgenomen in de BIR.
- Een risicoanalyse uitvoeren op de twee maatregelen (auditbeleid en emailfiltering) waar geen beleid voor is om te beslissen of hier beleid voor dient te komen.

- Het uitvoeren van een penetratietest met behulp van het referentiemodel social engineering teneinde de daadwerkelijke bescherming tegen social engineering vast te stellen.
- Het aanbieden van opleidingen en trainingen inzake social engineering en het informatiebeveiligingsbeleid om de bewustwording te vergroten.
- Informatiebeveiliging als vast onderwerp in functioneringsgesprekken opnemen om op de hoogte te blijven van de laatste updates.
- Rijksdiensten kunnen zich pro-actiever opstellen jegens de bepaling van de inhoud van de BIR. Momenteel hebben de Rijksdiensten in een afwachtende houding.

7 Reflectie

7.1 Productreflectie

De conclusies en aanbevelingen tonen duidelijk aan dat de kennis bij de Rijksoverheid van social engineering en het informatiebeveiligingsbeleid onvoldoende is. De BIR wordt opgesteld op een hoog niveau en opgelegd aan de Rijksdiensten. De Rijksdiensten zorgen vervolgens dat ze puntsgewijs aan de BIR voldoen of kunnen verklaren waarom ze er niet aan kunnen voldoen. Het informatiebeveiligingsbeleid komt vervolgens onvoldoende bij de medewerkers terecht.
Dit kan te maken hebben met de focus op de technische informatiebeveiliging en het feit dat zo veel medewerkers van de Rijksoverheid zo ver van informatiebeveiliging en IT afstaan.
Het is echter belangrijk om een informatiebeveiligingscultuur te hebben, omdat social engineers de medewerkers benaderen in plaats van de techniek doorbreken.

Dit onderzoek maakt dan ook pijnlijk inzichtelijk dat het informatiebeveiligingsbeleid niet goed bij de medewerkers overkomt. De resultaten van dit onderzoek geven aan waar de Rijksoverheid nog de nodige winst kan behalen ten aanzien van de beveiliging tegen de methoden of technieken van social engineering. Het onderzoek is dan ook niet bedoeld om de Rijksoverheid in een kwaad daglicht te stellen.

Het referentiemodel social engineering kan de Rijksoverheid helpen om informatiebeveiligingsmaatregelen tegen de methoden of technieken van social engineering in te voeren. Het geeft een duidelijk en overzichtelijk startpunt op het gebied van social engineering met de bijbehorende aspecten, aanvallen en beveiligingsmaatregelen.

De waarde van het onderzoek heeft dan ook drie belangrijke aspecten:

1. Er is een duidelijk referentiekader gecreëerd op basis van een uitgebreide literatuurstudie.
2. Het onderzoek maakt inzichtelijk dat de kennis en aanwezigheid van het aspect social engineering niet naar voren komt in de BIR, terwijl 56% van de medewerkers met socialengineeringaanvallen worden geconfronteerd.
3. Het geldende informatiebeveiligingsbeleid is slechts in beperkte mate bekend bij de medewerkers in de praktijk.

De resultaten van het onderzoek zouden een stuk sterker zijn als voor alle informatiebeveiligingsmaatregelen de awareness zichtbaar zou zijn gemaakt.
Het aantal geïnterviewden en enquêterespondenten van dit onderzoek is beperkt. Slechts 31 respondenten hebben meegedaan aan het onderzoek terwijl de enquête bij 60 personen is uitgezet. De resultaten zouden sterker en generaliseerbaar zijn als de scope was uitgebreid naar één volledige Rijksdienst of één geheel ministerie met respondenten van alle afdelingen. Gezien de beschikbare tijd en capaciteit ben ik wel tevreden met de scope van het onderzoek.

Er is tijdens dit onderzoek geen contact geweest met de Rijksdienst en de medewerkers die verantwoordelijk zijn voor het opstellen en bijhouden van de BIR. Er is meerdere malen gepoogd contact te leggen. Aangezien de BIR het leidende informatiebeveiligingsdocument is, had dit een belangrijke aanvulling op het onderzoek kunnen zijn.

De beperkingen van het onderzoek zijn dan ook:

1. Naar de awareness van het informatiebeveiligingsbeleid inzake drie maatregelen is niet gevraagd in de enquête. Hierdoor is geen volledig beeld verkregen.
2. Het aantal respondenten is beperkt, de generaliseerbaarheid en de externe validiteit zijn hierdoor verkleind.
3. Er is geen contact geweest met de Rijksdienst of de medewerkers die de BIR heeft/hebben opgesteld of deze up-to-date houdt/houden.

7.2 Procesreflectie

7.2.1 Literatuurstudie

Samen met mijn begeleider ben ik op zoek gegaan naar een relevant afstudeeronderwerp. Het was van belang dat het voor ons beiden een interessant onderwerp zou zijn met een goede wetenschappelijke relevantie. Na een overleg over mogelijke afstudeeronderwerpen heb ik mij in de verschillende onderwerpen verdiept. Uiteindelijk zijn we voor het literatuuronderzoek uitgekomen op de hoofdvraag: 'Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarin en wat ontbreekt?' Deze onderzoeksvraag raakt het aspect social engineering en het aspect risicomanagement. De afstemming van het onderwerp en de start van het afstuderen liep dan ook voorspoedig.

Kort na het begin van het afstudeertraject diende ik de literatuur in te duiken om relevante wetenschappelijke documenten/gegevens te verzamelen. Ik liep hier tegen het probleem aan dat mijn inschrijving pas aan het begin van de volgende maand (twee weken) verwerkt zou zijn en ik tot die tijd geen toegang zou hebben tot de bibliotheek van de Open Universiteit. In deze periode had ik veel tijd vrijgemaakt op mijn werk en privé om een goede start te maken. In het vervolg wacht ik dan ook altijd tot de inschrijving officieel is verwerkt, zodat ik niet tegen nare vertragingen aanloop en vakanties dien om te zetten.

Vervolgens liep ik tegen het probleem aan dat veel literatuur vijf tot tien jaar oud was en dat nieuwe literatuur alleen beschikbaar was tegen betaling. Via omwegen heb ik soms alsnog toegang gekregen tot de literatuur als ik kon aantonen dat ik een student was. Ik had mij beter moeten voorbereiden en moeten controleren of het onderwerp leeft binnen de wetenschap. Het zoeken van literatuur heeft veel tijd gekost. Het was wel een verademing dat alle literatuur inmiddels digitaal toegankelijk is. In het verleden, tijdens mijn hb0-studie moest ik nog fysiek naar de bibliotheek om boeken of documenten te lenen en kopietjes te maken.

Het boek 'Methoden en technieken van onderzoek', de BPM & IT-afstudeerhandleiding en de goede feedback van de docent hebben ervoor gezorgd dat het proces duidelijk en gestructureerd uitgevoerd kon worden. De mijlpaaldocumenten zorgden er vervolgens voor dat het verslag stapsgewijs opgebouwd kon worden om tot een goed eindresultaat te komen.

De feedback van de eerste begeleider was stipt en correct. Dat maakte de samenwerking prettig. Hij was ook enthousiast over het onderwerp en ging inhoudelijke discussies niet uit de weg, wat tot een beter eindresultaat heeft geleid.

Uiteindelijk is het literatuurverslag ingeleverd ter beoordeling, waarna ook de tweede begeleider voor het eerst inhoudelijk naar het verslag keek. Hierbij kwam naar voren dat het verslag niet aan alle punten van de beoordelingsmatrix voldeed. Helaas had ik deze beoordelingsmatrix nog nooit gezien of er iets over gehoord. Ook mijn eerste begeleider was er niet mee bekend. Het onderdeel dat ontbrak was echter lastig achteraf – correct en onderbouwd – toe te voegen. Een groot leerpunt is dan ook om goed te bekijken en af te stemmen met de begeleider op welke punten het verslag/proces uiteindelijk wordt beoordeeld.

7.2.2 Empirisch onderzoek

Aan het begin van het empirisch onderzoek ben ik op zoek gegaan naar een opdracht die ik binnen de organisatie waarin ik werk kon uitvoeren. Ik ben begonnen met het opstellen van de doelstelling, de hoofd- en deelvragen, de onderzoeksstrategie en het vinden van de juiste onderzoeksmethoden. Het boek 'Methoden en technieken van onderzoek', de BPMIT-afstudeerhandleiding en de feedback van de docent hebben ervoor gezorgd dat het verslag duidelijk en gestructureerd geschreven kon worden. De eerste aanzet tot het verslag en de opdracht was dan ook goed.

Achteraf bleek dat de scope niet breed genoeg was en dat met een bredere scope de wetenschappelijke relevantie aanzienlijk groter zou worden. De vraag bij een empirisch onderzoek is altijd of het onderwerp wetenschappelijk gezien relevant genoeg is. Er wordt echter nergens beschreven waar een onderwerp aan moet voldoen om wetenschappelijk relevant te zijn. Het was dan ook lastig om tot een onderwerp te komen dat wetenschappelijk relevant is en daarnaast relevant is voor de organisatie waar het onderzoek wordt uitgevoerd. Deze twee aspecten kunnen elkaar weleens bijten, omdat de scope beperkt is vanwege de capaciteit en de beschikbare tijd voor het afstudeeronderzoek.

Omdat de voorbereiding op het afstuderen (literatuuronderzoek) en afstuderen (empirisch onderzoek) als twee verschillende vakken en verslagen worden gezien door de BPM&IT-opleiding heb ik dit ook op deze manier aangepakt. Ik liep echter tegen het probleem aan bij het afstuderen (empirisch onderzoek) dat ik niet alle benodigde literatuur/data had om de empirische vragen te kunnen beantwoorden. Tevens waren niet alle data uit de literatuurstudie relevant voor het empirisch onderzoek. De twee verslagen zijn dan ook niet volledig consistent met elkaar en dienen dan ook als aparte verslagen gelezen te worden. Uiteraard is de basis gelegd in de literatuurstudie, maar er is slechts een gedeelte van gebruikt. In het vervolg zou ik het afstuderen dan ook als één geheel zien en eerst de opdrachtomschrijvingen van zowel het literatuuronderzoek als het empirisch onderzoek opstellen en afstemmen met de betrokkenen. Dit zorgt ervoor dat niet op de helft van het afstuderen een andere kant wordt opgegaan en dat alle benodigde literatuurgegevens aanwezig zijn.

Op mijn werk had ik van een aantal afdelingsmanagers toestemming gekregen om een enquête op hun afdeling uit te zetten en interviews te houden met een aantal medewerkers. Toen ik bezig was met de interviews kreeg ik van de Chief Information Officer (CIO) te horen dat ik toestemming nodig had van hem en het managementteam om een enquête uit te zetten bij de medewerkers van de Rijksdiensten. Tevens werd toen de eis gesteld dat het verslag volledig geanonimiseerd dient te worden opgeleverd. Als niet aan deze eisen werd voldaan, zou ik geen toestemming en medewerking

krijgen van de betrokken Rijksdiensten. In het vervolg zou ik dan ook zorgen dat ik vooraf bij de onderwerpbeschrijvingen de benodigde toestemming zou vragen. Het had zomaar kunnen gebeuren dan ik geen toestemming had gekregen van het managementteam, terwijl ik al meer dan honderd uur in het afstuderen had gestoken.

Het opstellen van de enquête en de interviews heeft vrij veel tijd gekost. Ik had daar nauwelijks ervaring mee. In het boek 'Methoden en technieken' wordt hier wel een handvat voor gegeven, maar deze twee technieken worden tijdens de masteropleiding BPM&IT alleen in het schakeljaar kort behandeld. De afstudeerders moeten zich binnen korte tijd deze skills eigen maken.

Het houden van de interviews ging daarentegen goed. De respondenten werkten goed mee en gaven duidelijke antwoorden. Indien zaken onduidelijk waren, kon hier goed op worden doorgevraagd. Tijdens de interviews schreef ik niet mee waardoor ik mij ook goed kon focussen op het interview zelf, de interviews werden opgenomen met een recorder.

Voor mijn werk zit ik vaak sollicitaties voor, waardoor interviews mij goed afgaan.

De antwoordbereidheid en welwillendheid van zowel de enquêterespondenten als de geïnterviewden waren prima. Veel medewerkers lieten na het invullen van de enquête een bericht achter waarin ze schreven dat ze het een zeer leerzaam en interessant onderwerp vonden.

Het uitwerken van de interviews heeft veel meer tijd gekost dan ik had ingeschat, dit heb ik dan ook zwaar onderschat. Een interview duurde ongeveer 1,5 uur en het koste het mij ongeveer vijf uur om dit volledig uit te werken. Hierna werd het interview voorgelegd aan de respondenten die met aanpassingen kwamen. In het vervolg zal ik hier aanzienlijk meer tijd voor reserveren.

Het uitwerken van de onderzoeksresultaten en het schrijven van de conclusies hiervan verliep goed. Reeds in een eerder stadium had ik de opzet van het eindverslag gemaakt, waardoor de hoofdstukken vervolgens alleen nog ingevuld hoefden te worden.

Het afstuderen heeft mij aanzienlijk meer tijd gekost dan de tijd die de opleiding voorschrijft. Alle andere vakken heb ik kunnen afsluiten binnen de gestelde tijd. Ik denk dan ook dat de inschatting niet realistisch is en bijgesteld dient te worden. Het kan ook zijn dat mijn begeleider en ik te enthousiast zijn geweest en te veel hooi op onze vork hebben genomen, waardoor de voorgeschreven tijd is overschreden.

De manier waarop wetenschappelijk onderzoek plaatsvindt, was niet geheel nieuw voor mij als onderzoeker. Tijdens mijn hbo-studie heb ik ook een afstudeeronderzoek verricht, waarvan een literatuuronderzoek een onderdeel was. Tijdens mijn premaster zijn alle facetten van een wetenschappelijk onderzoek naar voren gekomen en behandeld. Toch zit er een wereld van verschil tussen de facetten bespreken tijdens een premaster en daadwerkelijk zelfstandig een wetenschappelijk onderzoek uitvoeren. De nadruk ligt meer op de methodiek en de verantwoording van beslissingen dan op het eindresultaat. Bij mijn hbo-opleiding waren de uitkomsten van het praktijkonderzoek juist het belangrijkste beoordelingspunt.

Het onderwerp social engineering was voor mij niet compleet nieuw. Indirect had ik hier wel mee te maken gehad, maar ik had vrijwel geen kennis over het onderwerp. Het was dan ook zeer leerzaam om meer over dit actuele onderwerp te weten te komen.

Bibliografie

Literatuur gebruikt in aanvulling op de literatuurstudie:

Capgemini. (2015). *Cybersecurity in het MKB (techreport)* (Interpolis Ed.): Interpolis.

Goes, L. J. v. d. (2012). *SOCIAL ENGINEERING EN DE LIMBURGSE GEMEENTEN.* (Master), Open Universiteit. Retrieved from http://dspace.ou.nl/bitstream/1820/4578/1/INF_20121211_Goes.pdf

Hermansson, M., & Ravne, R. (2005). Fighting social engineering: University of Stockholm: Royal Institute of Technology.

Institute, P. (2014). *2014 Global Report on the Cost of Cyber Crime*: Ponemon Institute.

NEN. (2014a). NEN-ISO/IEC 27001. Retrieved from https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001

NEN. (2014b). NEN-ISO/IEC 27002. Retrieved from https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27002

Persoonsgegevens, A. (2015). De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

Rijksoverheid. (2012a). Baseline Informatiebeveiliging Rijksdienst Tactisch Normenkader (TNK). Retrieved from https://www.nationaleombudsman.nl/system/files/bijlage/BIR_TNK_1_0_definitief.pdf

Rijksoverheid. (2012b). Overzicht Baseline Informatiebeveiliging Rijksdienst (BIR 2012). Retrieved from http://www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012)

Rijksoverheid. (2015, 2015). Algemeen Rijksambtenarenreglement. Retrieved from https://www.rijksoverheid.nl/onderwerpen/overheidspersoneel/inhoud/werknemer-bij-de-overheid/arbeidsvoorwaarden-rijksoverheid

Saunders, M., Lewis, P., Thornhill, A., Booij, M., & Verckens, J. P. (2013). *Methoden en technieken van onderzoek* (5 ed.): Pearson.

Schoofs, P. (2014). *Phishing bij de overheid in Belgie.* (Master), Open Universiteit, Heerlen. Retrieved from http://dspace.ou.nl/bitstream/1820/4578/1/INF_20121211_Goes.pdf

Universiteit, O. (2016). Ethiek, wetenschappelijke integriteit en wetgeving. Retrieved from https://www.ou.nl/web/onderzoek/ethiek-wetenschappelijke-integriteit-en-wetgeving

Bijlagen 1: Interview en Enquête vragen

Als eerst wordt in deze paragraaf het ontwerp van het interview besproken. De interview vragen vallen onder één van de vier gekozen categorieën, dit zijn algemeen, informatie beveiligingsbeleid, social engineering en audit. Onder de categorie algemeen worden algemene vragen gesteld aan de respondent. Onder het kopje informatie beveiligingsbeleid worden vragen gesteld over het informatiebeveiligingsbeleid, welk beleid is er, hoe wordt dit vastgelegd, wie is verantwoordelijk hiervoor en hoe komt social engineering hierin naar voren. Vervolgens worden onder de categorie social engineering vragen gesteld inzake social engineering en incidentafhandeling.

De vragen zijn ontworpen met de gedachte om eerst te vragen naar wat men weet (kennis) binnen de organisatie om vervolgens indien de gewenste informatie niet is genoemd een gerichte vervolgvraag te stellen waarin directer om bepaalde informatie wordt gevraagd. Als men het antwoord niet weet of niet bekend is met de materie zal de kennis worden gegeven om erna de vraag te stellen hoe men nu tegen de materie aankijkt en of men deze materie herkend.
Door eerst te vragen naar wat men weet wordt geprobeerd zo min mogelijk bias in het interview aan te brengen.

In het interview worden vragen gesteld om; kennis te toetsen, een situatie te omschrijven en persoonlijke mening vragen.

De bias wordt niet volledig uit de vragen worden gehaald aangezien de uitkomsten van de interviews met elkaar na het transcriberen dienen te worden vergeleken.

Interview vragen

Algemene vragen
1. Wat is uw functie en kunt u deze in het kort omschrijven?
2. Hoeveel jaar werkt u in uw huidige functie?
3. Aan hoeveel medewerkers geeft u leiding?
4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van uw functie?

Informatie beveiligingsbeleid
6. Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat?
Is er binnen de organisatie bekend welke informatie het belangrijkst is?
8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001?
9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven?
10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?
11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?
12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?
13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?
14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?

Social engineering
15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering?
16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.*
17. Welke motieven zou een social engineer kunnen hebben?
18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
19. Waar maakt een social engineer misbruik van?
20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website.
23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?
26. Hoe groot is de kans dat een medewerker in een phishing mailt trapt?
27. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
28. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt.

Audit:
29. Hoe gaat men binnen de organisatie om met het verwijderen van vetrouwelijke documenten?
30. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
31. Weet je welke trends er spelen op het gebied van social engineering.
32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?
33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?

Enquete vragen

Deze enquête bestaat uit 26 multiplechoicevragen waarbij één of meerdere antwoorden gekozen dienen te worden. De enquête richt zich op het awareness van de medewerkers op het informatiebeveiligingsbeleid. Hiermee wordt dan ook getracht inzicht te krijgen in hoe de praktijk aansluit bij de theorie. Een bedrijf kan voor alle gevaren maatregelen en procedures hebben genomen, als deze maatregelen en procedures echter niet bekend zijn bij de medewerkers hebben deze niet het effect wat wordt verwacht.
Rondje = één antwoord mogelijk
Vierkant = meerdere antwoorden mogelijk
De vragen zijn onder te verdelen in drie categorieën, algemene vragen, informatiebeveiligingsvragen en social engineeringsvragen. De verwachte duur van de enquête is +- 15 minuten.

Algemene vragen
1. In welke categorie zou u uw functie plaatsen? *
- Informatiemanager
- IT specialist
- Medewerker directe dienstverlening
- Service level manager
- Anders

2. Hoeveel jaar werkt u in uw huidige functie? *
   - < 2 jaar
   - 2 tot 5 jaar
   - >5 jaar
3. Bent u een interne of externe medewerker? *
   - Intern
   - Extern
4. Worden nieuwe medewerkers gescreend voor ze worden aangenomen? *
   - Ja
   - Nee
   - Weet ik niet
   - Anders
5. Op welke onderstaande aspecten worden de nieuwe medewerkers gescreend? *
   - Controle positieve referenties
   - Controle curriculum vitae
   - Onafhankelijke identiteitscontrole
   - Controle Kredietwaardigheid
   - Bevestiging van diploma's/certificaten
   - Verklaring omtrent goed gedrag
   - Weet ik niet
   - Anders
6. Heeft u toegang tot vertrouwelijke informatie vanuit uw functie? *
   - Ja
   - Nee
   - Wens ik niet te beantwoorden

Informatiebeveiligingsbeleid

7. Met welke onderstaande informatiebeveiligingsdocumenten bent u inhoudelijk bekend? *
   - Baseline informatiebeveiliging Rijksdienst (BIR)
   - ISO 27001 of ISO 27002
   - Hand-out informatiebeveiliging
   - Geen van allen
   - Required
8. Voor welke aspecten heeft de organisatie een beveiligingsbeleid *
   - Wachtwoordmanagement
   - Anti-virus/-phishing
   - Change management
   - Informatieclassificatie
   - Documentafhandeling/-vernietiging
   - Clean desk
   - Locken van computer
   - Weet ik niet
9. Bent u in staat aan te geven welke informatie vertrouwelijk is op uw afdeling? *
   - Ja
   - Nee
   - Wens ik niet te beantwoorden
10. Heeft u ooit vanuit deze organisatie een cursus of training gevolgd inzake informatiebeveiliging of social engineering? *
   - Ja
   - Nee
   - Wens ik niet te beantwoorden

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. *

- De afdeling beveiliging onder leiding van de CIO
- Het lijnmanagement
- De directeur in combinatie met het MT
- Weet ik niet

12. Heeft u ooit vanuit deze organisatie een cursus aangeboden gekregen inzake informatiebeveiliging of social engineering? *

- Ja
- Nee
- Wens ik niet te beantwoorden?

13. Zou u als u de kans kreeg binnen de organisatie een training volgen m.b.t. informatiebeveiliging/social enginering? *

- Ja
- Nee
- Wens ik niet te beantwoorden

14. Met welke van de onderstaande aspecten wordt rekening gehouden bij het beëindigen of wijzigen van het dienstverband. *

- Retourneren van bedrijfsmiddelen
- Blokkering van de toegangsrechten
- Weet ik niet
- Wens ik niet te beantwoorden

15. Bent u bekend hoe u dient om te gaan met een beveiligingsincident binnen uw afdeling/organisatie? *

- Ja
- Nee
- Wens ik niet te beantwoorden

16. Wordt het beveiligingsbeleid actief uitgedragen/verspreid binnen de afdeling en organisatie? *

- Ja
- Nee
- Weet ik niet
- Wens ik niet te beantwoorden

Social engineering

Social engineering is een set van methoden waarmee het gedrag van een individu of groep individuen wordt gemanipuleerd zodanig dat dit individu of deze groep toegang verleent tot bepaalde informatie, met als doel deze informatie te gebruiken om de slachtoffers uit te buiten. Deze techniek maakt gebruik van de intrinsieke aard van de mensheid om slachtoffers uit te buiten, om gevoelige informatie te verkrijgen en hen te manipuleren en van het overtuigen van mensen om deze informatie te onthullen door het inzetten van uitzonderlijk goede communicatieve vaardigheden. Boven alles maakt social engineering gebruik van de zwakste schakel in de beveiliging: de menselijke factor

17. Bent u bekend met het begrip social engineering? *

- Ja
- Nee

Wens ik niet te beantwoorden

18. Met welke onderstaande aanvallen bent u bekend? *

- Phishing
- Dumpster diving
- Office snooping

- Piggyback/Tailgaiting
- Water holing/baiting
- Malicious software
- Manipulatie van emoties
- Reverse social engineering

19. Kunt u beschrijven hoe een social engineeringsaanval wordt uitgevoerd? *
    - Ja
    - Nee
    - Wens ik niet te beantwoorden
20. Bent u in de afgelopen 6 maanden benaderd via email, brief, fysiek, social netwerk of via de telefoon waarvan u denkt dat dit een poging was tot het verkrijgen van (gevoelige)informatie voor frauduleuse doeleinden? *
    - Ja
    - Nee
    - Wens ik niet te beantwoorden
21. Via welk kanaal werd deze poging ondernomen? *
    - Email
    - Telefoon
    - Fysiek
    - Sociaal netwerk
    - Anders
    - Wens ik niet te beantwoorden
22. Bent u bekend met de meest voorkomende motieven van social engineers? *
    - Ja
    - nee
    - Wens ik niet te beantwoorden
23. Van welke menselijke aspecten maakt een social engineer misbruik? *
    - Nalatigheid
    - Slordigheid
    - Onwetendheid
    - Naiviteit
    - Hebzucht
    - Weet ik niet
24. Hoe groot is de kans dat één of meerdere medewerkers in een phishing mail trappen? *
    - Klein
    - Middel
    - Groot
25. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft? *
    - Klein
    - Middel
    - Groot
26. Hoe groot is de kans dat, wanneer een medewerker een data container (USB) vindt, deze ook daadwerkelijk probeert te bekijken? *
    - Klein
    - Middel
    - Groot

Bijlagen 2: Uitgewerkte Interviews

Uitwerking interview 1:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Technisch applicatiebeheer en Informatiebeveiligingscoördinator(IB) van de afdeling ERP

2. Binnen welke afdeling valt u?
Afdeling ERP

3. Hoeveel jaar werkt u in uw huidige functie?
1 jaar als IB en 14 jaar als technisch applicatiebeheerder

4. Aan hoeveel medewerkers geeft u leiding?
Geen directe leiding, wel overkoepelende aansturing voor wijzigingen.

5. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Ja, alle medewerkers worden gescreend. Het niveau van de screening is afhankelijk van de functie. Voor alle functies is een verklaring van goed gedrag vereist (VOG), zowel voor externen als internen.

6. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, voor een deel toegang. Door functiescheiding wordt dit waar mogelijk ingeperkt.

Informatie beveiligingsbeleid
7. Hoe wordt binnen het BLAUW omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
Er wordt momenteel een Security Operation Center (SOC) binnen de organisatie ingericht. Het SOC voldoet nog niet aan alle eisen welke vanuit de BIR worden opgelegd. In het SOC worden risico impact analyses bepaald. De informatiebeveiliging zelf is vastgelegd in de Baseline Informatie Rijk (BIR), de basis van de BIR is ISO27001.

9. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?
Alle afdelingen weten wat voor hun de waardevolle informatie is. Daarnaast wordt eens per drie jaar een information risk assesment gehouden binnen het BLAUW volgens de IRAM 2 methodiek.
Kees verwacht dat het MT op de hoogte is van het niveau van de beveiliging binnen de organisatie met de bijbehorende risicofactoren.

10. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
Er is een intern beleid voor de verschillende vestigingen van de organisatie, dit wordt uitgedragen in de vorm van aanbevelingen. De aanbevelingen worden in de praktijk niet altijd uitgevoerd, dit is aan de afdelingen/organisatie zelf om te beslissen. De organisatie dient volgens de BIR te werken. De BIR is in de basis ISO 27001 met een aantal toevoegingen. Dit betekend dat voor de interne wijze van automatiseren de BIR gevolgd dient te worden. Ook de diensten die worden aangeboden als generieke diensten dienen te voldoen aan de BIR. Daarnaast worden ook applicaties beheert voor klanten waarbij de klanten zelf verantwoordelijk zijn voor het zich houden aan de BIR.

11. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? Social engineering wordt niet direct benoemd in de BIR, wel kort in ISO 27001.

Indirect wordt wel aangegeven dat de awareness van het personeel inzake informatiebeveiliging moet worden aangeleerd.

12. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid. Er is een CIO aangewezen binnen de organisatie welke verantwoordelijk is voor het invoeren en uitvoeren van de BIR binnen het BLAUW. De directe lijnverantwoordelijke dient het beleid of de punten welke door de CIO worden aangedragen uit te voeren. Kees is als coördinator degene bij wie dit door de manager van team ERP is belegd.

13. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Dit is de CIO en de lijnmanagers, beveiligingscoördinatoren.

14. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt? Jaarlijks wordt een sessie gehouden waarbij een risico analyse wordt gemaakt en waaruit vervolgens acties uit kunnen voortkomen. Alle afdelingmanagers en de informatiebeveiligings specialisten worden hierbij aangesloten.

Daarnaast wordt voor de Leonardo applicatie elke drie jaar een risico impact analyse gemaakt door de klant (systeemeigenaar van het ERP systeem).

15. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk? Bij alle incidenten dient de servicedesk te worden ingeschakeld. De servicedesk maakt vervolgens een incidentrapport aan en zet deze door naar de beveiligingscoördinator. De beveiligingscoördinator bepaalt vervolgens hoe het incident wordt afgehandeld en welke acties er dienen te worden ondernomen/uitgezet.

16. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen? Er worden hand-outs verspreid binnen de organisatie met algemene informatie aangaande informatiebeveiliging.
Bij incidenten of risico's worden mails verstuurd vanuit de servicedesk. Daarnaast is per afdeling een informatiebeleidcoördinator aangesteld welke binnen de afdeling het aanspreekpunt is m.b.t. informatiebeveiliging. Het beleid zou wel actiever uitgedragen kunnen worden. Momenteel wordt er sporadisch aandacht aan besteed, bijvoorbeeld voor een audit of controle.

Social engineering
17. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering? Mensen worden actief benaderd met het oog om misbruik van hun te maken. Met als doel het verkrijgen van wachtwoorden, pincodes etc. Kees kan zich vinden in mijn opgestelde definitie. Hij geeft echter wel aan dat niet altijd de gemanipuleerde persoon het slachtoffer is, de klanten van een organisatie kunnen het echte slachtoffer zijn.

18. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.* Nee, de vier verschillende fasen tijdens een aanval zijn niet bekend bij de respondent. Indirect beschrijft Kees wel de eerste twee fasen. Na het zien van het aanvalsschema kan kees zich hier in vinden en komt dit bekend voor. Hij geeft wel aan dat bij chantage het schema niet op lijkt te gaan. De stap van het creëren van een relatie lijkt hier niet op te gaan.

19. Welke motieven zou een social engineer kunnen hebben? Hoeven niet altijd criminelen te zijn, kunnen ook journalisten zijn die informatie proberen in te winnen. Financieel, concurrentievoordeel, criminaliteit, espionage.

20. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Phishing, namen noemen en het zich voordoen als iemand anders worden genoemd.

21. Waar maakt een social engineer misbruik van. De eenvoud waarbij mensen te benaderen zijn tegenwoordig via telefoon, email, internet. Het noemen van namen.
Medewerkers van de organisatie worden niet getraind om het misbruik van deze menselijke eigenschappen te voorkomen. Naar aanleiding van de commissie oosting wordt nu wel aandacht besteed aan het omgaan met de pers. Medewerkers worden geïnformeerd hoe met de pers om te gaan.

22. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Er bestaat altijd de kans dat eigen personeel wordt verleid om over de scheef te gaan. Alle medewerkers worden gescreend en dienen een VOG aan te leveren. Als medewerkers worden ontslagen, wordt de toegang geblokkeerd tot de gebouwen, applicaties en werkstations. Voor externen gaat dit zelfs automatisch bij het eindigen van de dienstverband. Bij internen is het een handmatige handeling. Zowel de toegang tot de gebouwen als de accounts worden op dezelfde wijze geblokkeerd als in het PMS systeem het dienstverband wordt beëindigd.
Hiernaast is er ook kans op imagoschade als medewerkers informatie aan de pers lekken. Hier zitten dan ook risico's waarop momenteel wordt geacteerd.

23. Zijn er recent incidenten geweest rondom social engineeringsaanvallen?
Ja Kees geeft aan dat hij bewust is van drie aanvallen in het afgelopen jaar.
1. Medewerkers van de organisatie kregen telefoontjes vanuit Afghanistan waarbij om informatie werd gevraagd.
2. Phising mails om inloggegevens van applicaties te bemachtigen.
3. Als test was een bedrijf ingehuurd waarbij vreemden het gebouw werden ingelaten, er werd getoetst hoe lang het duurde voordat deze mensen werden aangesproken door medewerkers wie ze waren en of zij zich konden identificeren.

24. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Telefoon, email, fysiek.

25. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Nee, niet alle medewerkers zijn zich bewust van social engineering. Social engineering komt ook niet direct terug in het informatiebeveiligingsbeleid. Alleen de vormen van social engineering welke in het nieuws komen zijn algemeen bekend. Denk hierbij aan phishing mails.

26. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Nee, medewerkers worden wel geïnformeerd via hand-outs en de email.
Mensen hebben echter geen training gehad en veel medewerkers hebben geen tijd om het informatiebeveiligingsbeleid of de e-mails volledig te lezen.

Medewerkers actief informeren tegen social engineering zal dan ook benodigd zijn in de vorm van een training of presentatie.

27. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Voornamelijk imagoschade, financiële schade en persoonlijke schade van inwoners van Nederland. Als er Kamervragen worden gesteld naar aanleiding hiervan kan het ook personen of de minister/staatssecretaris hun baan kosten.

Audit:
30. Worden nieuwe medewerkers binnen uw afdeling gescreend voordat ze worden aangenomen?
Ja, alle medewerkers worden gescreend en dienen een VOG aan te leveren.

31. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten? Op alle afdelingen zijn schredders en gesloten papierbakken aanwezig. Alle documenten worden dan ook vernietigd of afgeschermd weggegooid.

32. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten? Elke drie jaar wordt een informatie risico analyse uitgevoerd vanuit de klant voor de Leonardo applicatie. Daarnaast wordt jaarlijks een risico analyse uitgevoerd binnen de afdeling ERP door de organisatie zelf. De BIR wordt bijgesteld wanneer de noodzaak ertoe is.

Er zijn voor Leonardo diverse audits uitgevoerd in 2015:

- Verlenging ISO 27001 certificering voor BLAUW vestiging Zoetermeer, o.a. aandacht voor ERP Leonardo beheer, en het Leonardo change/release management proces.
- ADR audit inzake de Leonardo infrastructuur in opdracht van DFEZ (klant/opdrachtgever)
- Jaarlijkse audit betalingsverkeer Leonardo door de ADR i.v.m. accountantsverklaring

Ook beveiliging is bij de bovengenoemde audits aan bod gekomen. Impliciet heeft dit betrekking op het gevoerde beveiligingsbeleid.
In de ADR Audit inzake de Leonardo Infrastructuur kwam dit expliciet naar voren, bijvoorbeeld inzake netwerkbeveiliging/scheiding en de werking van het SOC.

Uitwerking interview 2:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Lijnmanager van de afdeling applicatiebeheer. Vanuit deze functie is de informant verantwoordelijk voor vier teams: ERP, ECM, Identiteit & Acces Management en Vernieuwing Grensmanagement.

2. Hoeveel jaar werkt u in uw huidige functie?
In de huidige functie 3 maanden. In totaal 16 jaar werkzaam binnen de organisatie in verschillende functies zoals manager ERP en technisch applicatie beheerder.

3. Aan hoeveel medewerkers geeft u leiding?
Direct aan vier teammanagers met in totaal +- 150 medewerkers onder deze team managers.

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Alle medewerkers moeten een verklaring omtrent goed gedrag overleggen. Voor verschillende rollen/functies binnen de organisatie is een screening benodigd. De BVA neemt hierin de lead.

Diploma's en referenties van sollicitanten worden bekeken, niet nagetrokken.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, vanuit de huidige functie heeft de informant toegang tot personele informatie.
De informant heeft geen toegang tot klantinformatie en informatiesystemen met vertrouwelijke informatie. Hij heeft deze toegang in het verleden wel gehad.

Informatie beveiligingsbeleid

6. Hoe wordt binnen de organisatie omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?

De organisatie is ISO gecertificeerd. Daarnaast wordt gewerkt om de organisatie en de klanten volledig BIR compliant te maken. Daar waar de organisatie nog niet compliant is worden explains opgesteld. De organisatie heeft een in control verklaring voor een deel van de organisatie, voor applicatiebeheer is deze nog niet behaald, er wordt naar gestreefd deze z.s.m. te behalen.
Er worden verschillende audits uitgevoerd: vanuit de eigen organisaties, vanuit de klanten en vanuit de gebruikersorganisatie.

In periodieke organisatiebijeenkomsten worden medewerkers op de hoogte gebracht van informatiebeveiliging, ook over social engineering. Ook is een flyer/hand-out verspreid binnen de organisatie om medewerkers bewust te maken van het informatiebeveiligingsbeleid.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?

Er is geen lijst/matrix bij de informant bekend van de verschillende informatiesystemen met bijbehorende graad van vertrouwelijkheid. Misschien dat deze lijst op een andere afdeling wel aanwezig is, dit weet de informant niet.
De medewerkers van de afdelingen zijn voor hun eigen afdelingen bewust wat de waardevolle/vertrouwelijke informatie is en hoe zij hier mee om dienen te gaan. Medewerkers zijn zich wellicht niet volledig bewust van de risico's als deze informatie verspreid wordt.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.

De BIR is de leidende maatstaf binnen de organisatie. Momenteel is de organisatie ISO 27001 gecertificeerd echter door omstandigheden zal dit in de nabije toekomst veranderen.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? De informant is op grote lijnen bekend met de inhoud van de BIR. Hiernaast wordt de informant regelmatig met bepaalde aspecten van de BIR geconfronteerd door de medewerkers van het team informatiebeveiliging en de IB-coordinatoren.

De informant weet niet of in de BIR wordt ingegaan op social engineering.

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid.

De informant vervult nog niet lang genoeg zijn huidige functie om hier op in te kunnen gaan. Hij verwacht dat zijn leidinggevende regelmatig contact heeft met de CIO.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid.

Binnen de organisatie is een informatiebeveiligingsteam aanwezig waar ook de CIO deel van uit maakt. Dit team is verantwoordelijk voor het volgen van de processen en van het beveiligen van de organisatie. Verder ligt er verantwoordelijkheid bij de afdelingshoofden, teammanagers en zelfs bij de medewerkers zelf om aan het informatiebeveiligingsbeleid te voldoen.
Er is duidelijk aangegeven/gecommuniceerd binnen de organisatie dat de managers verantwoordelijk zijn voor hun afdelingen. Vaak hebben managers een informatiebeveiligingscoordinator aangesteld welke het beleid controleert en doorvoert, het wordt dan ook naar beneden toe gedelegeerd.
De eindverantwoordelijke is uiteindelijk de directeur.
De organisatie is samen met de klant verantwoordelijk om volledig aan de BIR te voldoen. Als één van deze partijen niet compliant is, is automatisch de andere partij dit ook niet.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?
Wellicht dat dit gebeurd bij het team informatiebeveiliging/security. Onder de afdelingen waar de informant leiding aan geeft worden wel R&I's gemaakt echter zijn deze niet specifiek op het gebied van informatiebeveiliging. Informatiebeveiliging wordt wel meegenomen waar nodig/bekend.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?
De informant geeft aan hiervan niet op de hoogte te zijn. Er is naar zijn weten niet een eenduidig proces aanwezig hiervoor binnen de organisatie. Daarnaast heeft de informant nog niet eerder te maken gehad met een informatiebeveiligingsincident binnen de organisatie.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?
Het beleid wordt op verschillende manieren uitgedragen, de informant noemt: periodieke organisatiebijeenkomsten, per email, hand-outs en door IB coördinatoren.
Niet alle afdelingen dragen het beleid op dezelfde manier uit. De managers beslissen zelf of zij het werk delegeren naar een IB coördinator. Zaken zoals de hand-out, e-mails en de informatiebijeenkomsten zijn voor alle medewerkers beschikbaar.

Social engineering
15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering?
Mensen proberen zich voor te doen als iemand die ze niet zijn met kwaadwillige intenties.
Ze doen zich voor als instantie of vriend/kennis met goede intenties om vervolgens misbruik van het slachtoffer te maken. Ze maken vooral misbruik van de goedgelovigheid en van menselijke eigenschappen om dingen voor elkaar te krijgen die het slachtoffer niet wilt.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?
Een aanval begint met het stukje engineering, namelijk weten met wie je te maken hebt. Als eerste wordt informatie over een bedrijf/persoon opgezocht, vervolgens wordt gekeken naar de zwakke plekken van deze persoon/organisatie. Als laatste wordt iets aangeleverd waar de persoon dient in te trappen waarna bij de gegevens kan worden gekomen.

17. Welke motieven zou een social engineer kunnen hebben?
Financiële en seksuele motieven worden genoemd.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Phishing, een datalek en namen noemen wordt genoemd.

19. Waar maakt een social engineer misbruik van?
Nalatigheid, slordigheid, onwetendheid, naïviteit, hebzucht, omkoopbaarheid en vertrouwen worden genoemd.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Nee, in principe niet. Als medewerkers echter in een benarde financiële situatie terecht komen is het risico groter dat zij chantabel of over te halen zijn om iets te doen wat ze normaliter niet zouden doen.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?

Ja, er is informatie gelekt naar de pers. (datalek)

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering? Welke verbeteringen kunnen worden doorgevoerd?

Het mag/kan een tandje scherper dan het momenteel is. Er hoeft niet altijd aandacht aan besteed te worden indien de medewerkers maar wel met regelmaat worden wakker gemaakt.
Voorvallen uit de praktijk kunnen worden medegedeeld om de medewerkers bewuster te maken. Medewerkers dienen te worden geïnformeerd met praktijkvoorbeelden inzake social engineeringsaanvallen. Hierdoor krijgen medewerkers inzicht in de aanval, gevolgen en risico's. Praktijkvoorbeelden zullen veel meer aanspreken dan theorie.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?

De informant kan zich voorstellen dat hier en daar bewustwording nog verder kan worden vergroot.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Het kan de minister welke verantwoordelijk is voor de organisatie zijn baan kosten. Medewerkers verantwoordelijk voor de beveiliging/managers kan het hun functie kosten. Daarnaast kunnen personen gevaar lopen als klantinformatie op straat komt te liggen.

26. Hoe groot is de kans dat een medewerker in een phishing mailt trapt?

De kans dat 1 of meerdere medewerkers hier in trapt is zo goed als 100 procent. Het zal wel afhangen van de kwaliteit van de phishing mail. De mails zijn tegenwoordig zo kwalitatief hoog dat het lastig is om dit volledig af te vangen.

27. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.

Het ligt aan de locatie. Op de ene locatie is de kans groot aangezien een achterdeur aanwezig is zonder fysieke beveiliging. Op de andere locatie is de kans klein, de fysieke beveiliging in combinatie met toegangspassen vangt dit risico af. Voor de volgende fysieke beveiligingsonderdelen zijn er procedures.

1. autoriseren van medewerkers voor toegang tot (kritische) ruimten;
2. uitgeven van toegangsmiddelen aan vaste medewerkers;
3. uitgeven van toegangsmiddelen aan externe medewerkers;
4. het intrekken van toegangsmiddelen bij uitdiensttreding of beëindiging van het contract;
5. het blokkeren van toegangsmiddelen na uitdiensttreding of beëindiging van het contract;
6. de registratie van toegangsmiddelen, waarin ten minste de volgende gegevens moeten worden vastgelegd: namen van de personen die een toegangsmiddel bezitten; datum van uitgifte van de toegangsmiddelen; nummers van de toegangsmiddelen die in gebruik en in bewaring zijn;
7. hoe te handelen indien er sprake is van verlies, diefstal of misbruik

28. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt.

De kans dat een persoon deze uitleest is gemiddeld echter staan de USB poorten dicht waardoor de USB stick niet kan worden uitgelezen op het werk. Niet alle medewerkers zullen zich bewust zijn dat het planten van een USB stick een social engineeringsaanval kan zijn.

De kans dat een medewerker een bestand opent met een aantrekkelijke naam op de gedeelde netwerkschijf is groot. Er zal bij vrijwel geen enkele medewerker een lampje gaan branden dat dit een social engineerings aanval kan zijn. Om een bestand op de netwerkschijf te krijgen dienen echter wel een aantal beveiligingsmaatregelen te zijn ontweken, ook is het de kunst het bestand op een

locatie te krijgen waar de gebruikers vaak komen. De kans is dan uiteindelijk in deze organisatie dan ook klein dat een bestand op de netwerkschijf wordt geplaatst. Mocht dit toch lukken dan is de kans groot dat medewerkers het zullen openen.

Audit:

29. Hoe gaat men binnen de organisatie om met het verwijderen van vetrouwelijke documenten?
Op alle afdelingen staat een schredder, een afgesloten aluminiumbak en normale papierbakken. De medewerkers dienen zelf te bepalen hoe de betreffende documenten worden verwijderd en zijn dan ook zelf verantwoordelijk hiervoor.

30. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
Ja, er is een clean desk audit geweest. Hieruit bleek dat niet iedereen voldeed aan clean desk. Het bleek toen ook dat niet alle medewerkers de mogelijkheid hebben/hadden om hun spullen achter slot en grendel te bewaren. Mensen worden aangesproken op de resultaten van de audit, hier worden geen disciplinaire maatregelen op genomen. De audits gebeuren niet vaak genoeg om de cultuur te kunnen veranderen, ze worden momenteel dan ook te sporadisch uitgevoerd.

31. Weet je welke trends er spelen op het gebied van social engineering.
Nee, niet specifiek/momenteel. In het verleden zijn wel eens een aantal trends gedeeld binnen de organisatie. Ook is er wel eens iets in het nieuws over social engineering.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
De informant kan hier geen uitspraak over doen. Wel geeft hij aan dat het aan het soort ontwikkeling ligt en welke waarde hier aan wordt toegekend vanaf hogeraf. Dit kan het MT zijn of een andere instantie binnen de overheid.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Het is niet bekend/duidelijk bij de informant wie verantwoordelijk is voor het retourneren van de bedrijfsmiddelen. Hij gaat er van uit dat degene die de bedrijfsmiddelen uitgeven deze ook weer dienen in te nemen. Het is inzichtelijk bij de managers welke medewerkers welke bedrijfsmiddelen bezitten. Hiervan zijn overzichten beschikbaar.

Uitwerking interview 3:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Teammanager ERP: De aansturing van een IT afdeling gespecialiseerd in het beheer van ERP systemen. Voor deze functie Senior SAP specialist.

2. Hoeveel jaar werkt u in uw huidige functie?
Twee maanden in de huidige functie. Hiervoor 17 jaar SAP specialist.

3. Aan hoeveel medewerkers geeft u leiding?
+- 35 internen en +-65 externen.

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Diploma's worden geverifieerd bij een arbeidsvoorwaardengesprek. Vaak wordt navraag gedaan bij andere medewerkers over de nieuwe medewerker. Voor sommige functies is een A of B screening benodigd. In een A of B screening valt ook een financiële screening. Bij een A screening wordt ook de familie en vriendengroep bekeken.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, er is toegang tot vertrouwelijke informatie maar maakt hier geen gebruik van in de huidige functie. Zowel personele vertrouwelijke informatie als systeem vertrouwelijke informatie.

Informatie beveiligingsbeleid
6. Hoe wordt binnen het BLAUW omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
Steeds strikter, de afgelopen jaren wordt informatiebeveiliging steeds belangrijker. Er worden handouts uitgedeeld, clean desk policy is ingericht en wordt regelmatig gecontroleerd. Data lekken worden ook belangrijker, hier is ook beleid voor opgesteld. Tevens worden tests uitgevoerd, bijvoorbeeld is er een phishing mail test verspreidt om de medewerkers bewust te maken.
De informatiebeveiliging wordt vastgelegd in de Baseline Informatiebeveiliging Rijksdienst (BIR).

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?
Er wordt vanuit gegaan dat alle medewerkers weten welke informatie vertrouwelijk is binnen de organisatie. Er is geen lijst of systeem aanwezig waarin de informant voor zijn afdeling de verschillende soorten informatiebronnen met classificering kan inzien.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De BIR is lijdend voor informatiebeveiliging.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? De informant is alleen op hoog niveau bekend met de BIR en kan hierom niet aangeven of in de BIR informatiebeveiligingsmaatregelen zijn opgenomen tegen social engineering.

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid. De directe leidinggevende van de informant heeft regelmatig een overleg met de Chief Information Officer (CIO) van de organisatie waarin het informatiebeveiligingsbeleid wordt besproken en waar nodig acties worden uitgezet. Nieuwe ontwikkelingen op het gebied van beveiliging worden geïntegreerd binnen de organisatie door de CIO met behulp van de security coördinatoren.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. De Chief Information Officer (CIO) is eindverantwoordelijk binnen de organisatie voor het informatiebeveiliginsbeleid. De managers van de verschillende afdeling zijn verantwoordelijk voor het uitdragen van het beleid binnen hun afdelingen. Het werk op operationeel niveau is gedelegeerd naar informatiebeveiligingscoordinatoren.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt? Binnen de afdeling ERP wordt het kopje beveiliging altijd meegenomen met wijzigingen die dienen te worden doorgevoerd op de ERP applicaties. De afdeling security is verantwoordelijk voor de teamoverstijgende risico analyses en informatiebeveiliging incident afhandeling.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk? Als het om data van een klant gaat, wordt de klant geïnformeerd en de servicedesk. Vaak wordt eerst de afdelings beveiligingscoördinator benaderd om informatie van de laatste gang van zaken na te vragen. Mocht er een incident plaatsvinden dan is het momenteel niet

gelijk inzichtelijk wat de impact is op een afdeling. De informant gaat ervanuit dat het team security dit wel inzichtelijk zou moeten hebben.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen? De CIO bepaalt het informatiebeveiligingsbeleid. De CIO gaat vervolgens in gesprek met de afdelingmanagers en de informatiebeveiligingscoordinatoren om het beleid uit te dragen binnen de organisatie.

Social engineering

15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering? De informant weet niet wat social engineering precies inhoud maar denkt dat het te maken heeft met aanvallen via sociale media. Na het bespreken van mijn definitie van social engineering kan hij zich hier goed in vinden en is het begrip social engineering duidelijk.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? ***Als vervolg het aanvalsschema doorlopen.*** Nee, de informant is niet op de hoogte van een specifiek aanvalspatroon/schema.

17. Welke motieven zou een social engineer kunnen hebben? Financieel, chantage en een kick voor de social engineer worden genoemd.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Phishing wordt genoemd.

19. Waar maakt een social engineer misbruik van?
Van de goedgelovigheid en onwetendheid van mensen.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
In principe niet, echter hoe goed ken je alle medewerkers. De screening zou dit moeten afvangen.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
Verschillende Phishing e-mails, +- 4 keer in de afgelopen twee jaar.

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Een bepaalde kleine groep wel, veel andere medewerkers niet. In het totaal zou de bewustwording hoger kunnen. Er wordt regelmatig aandacht besteed aan phishing echter is dat maar een klein aspect van social engineering.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Nee, de bescherming kan beter. Met enige regelmaat zouden tests uitgevoerd dienen te worden waarbij de resultaten worden gedeeld en besproken. Bij vervolgtest zal dan waarschijnlijk blijken dat mensen niet meer in de aanvallen trappen en zich bewust zijn geworden van social engineering. Mensen dienen zelf geconfronteerd te worden met een aanval om ze bewust te maken en vervolgaanvallen af te slaan.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Het zou grote gevolgen kunnen hebben voor de organisatie. Dan hebben we gefaald als organisatie. Een minister kan hier zelfs voor uit zijn functie worden gezet.

Audit:

27. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten?
Er is beveiligde papierbak aanwezig welke op slot zit. Daarnaast is een schredder aanwezig. Harde schijven en andere hardware worden vernietigd na afschrijving.

28. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
Ja, er wordt regelmatig gekeken of de afdeling nog voldoet aan de BIR. Hiernaast worden verschillende ISO certificering behaald waarvoor regelmatig audits benodigd zijn om de certificering te behouden.

29. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt. Als het om een usb stick gaat is de kans klein, tevens zijn de usb poorten dichtgezet waardoor het niet kan voorkomen. Als het om een bestand op de netwerkschijf staat met een verleidende naam is de kans groot dat medewerkers deze bekijken. De kans is uiteindelijk vrij klein aangezien meerdere lagen van beveiliging dienen te worden doorbroken om een bestand op de shared netwerkschijf te krijgen.

30. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is klein bij de hoofdingangen, niet zozeer omdat mensen bewust zijn van de gevaren van piggybacking maar omdat er fysieke beveiliging aanwezig is. Bij sommigen achterdeuren is de kans aanzienlijk groter echter zijn de afdelingen zelf ook nog beveiligd en alleen toegankelijk met de juiste autorisaties.

31. Hoe groot is de kans dat een medewerker van de organisatie/afdeling in een phishing mail trapt? De kans is redelijk groot.

31. Weet je welke trends er spelen op het gebied van social engineering.
Nee, dit is niet de verantwoordelijkheid van de informant. Het inde gaten houden van trends en hierop reageren is belegd op een hoger niveau bij beveiligingsspecialisten.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
De informant staat hier te ver vanaf om hier iets over te kunnen zeggen. Dit zijn ontwikkelingen die op hoger niveau worden besproken waarna de uitvoering wordt belegd bij de managers.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Ja, hiervoor is kortgeleden een procedure opgezet specifiek voor de afdeling ERP. Hierop staan actiepunten zoals het dichtzetten van accounts, blokkeren van toegangspassen, retouneren van devices etc. De eindverantwoordelijke is de manager echter is de controle gedelegeerd naar teammanagers binnen de afdeling.

Uitwerking interview 4:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Solution architect. Belast met wijzigingen op de verschillende systemen binnen de organisatie.

2. Hoeveel jaar werkt u in uw huidige functie?
1,5 jaar binnen de huidige functie

3. Aan hoeveel medewerkers geeft u leiding?
0, stuurt wel mensen aan bij wijzigingen maar geen medewerkers onder zich.

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
De leidinggevende van de organisatie hebben de mogelijkheid tot het aanvragen van een A, B of C screening voor sollicitanten. Hiernaast wordt gecontroleerd of de sollicitant de juiste diploma's heeft. Dit is een fysieke controle van de diploma's, er wordt geen navraag gedaan bij de instantie welke het diploma heeft uitgegeven. Elke medewerker dient een VOG verklaring te overhandigen.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, vanuit de functie is toegang tot verschillende informatiesystemen waar vertrouwelijke informatie in aanwezig is.

Informatie beveiligingsbeleid
6. Hoe wordt binnen het BLAUW omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
De Baseline Informatie Rijk is leidend en wordt uitgedragen door een informatie beveiligings coördinator. Ook wordt veel op de ondersteunde IT dienstverlener gesteund voor certificeringen en de beveiliging. Voor compliancy aan de BIR wordt gewerkt via het "comply or explain" beleid.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is? Er is geen lijst/systeem bekend bij de informant waarop de verschillende informatiebronnen met de vertrouwelijkheid is opgesomd. De medewerkers weten van hun eigen afdeling wel wat de vertrouwelijke informatie is en hoe hier mee dient te worden omgegaan. De directeur van de afdeling is op de hoogte van de verschillende soorten vertrouwelijke informatie.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De BIR is leidend binnen de organisatie. Hiernaast is de organisatie gecertificeerd voor verschillende ISO certificaten, waaronder ISO 27001.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? De informant is alleen op de hoofdlijnen bekend met de BIR, hij is niet op de hoogte of social engineering wordt behandeld/aanwezig is in de BIR. Wel is bekend dat voortvloeiend uit de BIR penetratie testen plaatsvinden in een gecontroleerde setting.

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid. De leidinggevende binnen de organisatie/afdeling zijn verantwoordelijk voor het navolgen van het informatiebeveiligingsbeleid. Het beleid wordt echter op hoger niveau bepaald en afgestemd.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Het is de taak van de manager van een afdeling om ervoor te zorgen dat het informatiebeveiligingsbeleid goed wordt uitgevoerd en uitgedragen. De uitvoering is echter wel gedelegeerd naar een beveiligingscoördinator. Met regelmaat vindt een onderling overleg plaatst om bij te praten.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt? Bij elke melding die binnenkomt op de servicedesk wordt aangegeven of het om een beveiligingsrisico gaat of niet. Hiervoor kan op elke melding een vinkje worden gezet. Als het vinkje wordt gezet komt de melding automatisch bij het team security terecht welke vervolgens de risico analyse maakt en ook rapporteert over de risico's binnen de organisatie. Het team van de informant maakt zelf niet de risico analyses. Het is wel mogelijk om over een bepaalde periode alle bekende/gemelde beveiligingsincidenten op te vragen.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk? Beveiligingsincidenten worden gemeld bij de leidinggevende en de servicedesk van de IT-dienstverlener. De afhandeling van informatiebeveiligingsincidenten worden vervolgens aangestuurd vanuit de IT-dienstverlener.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen? De informant heeft hier geen ervaring mee en weet dan ook niet of dit wel of niet zo is.

Social engineering
15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering? Een groep mensen die niet van de organisatie zijn

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.* De informant geeft aan hier geen ervaring mee te hebben en zou het dan ook niet weten.

17. Welke motieven zou een social engineer kunnen hebben?
Kwaadwillend of goedwillend. Financieel en zichzelf bewijzen (ego strelen) worden genoemd.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Phishing, trojans, backdoors, exploits worden genoemd.

19. Waar maakt een social engineer misbruik van? Menselijke eigenschappen: Jaloezie, hebzucht en nieuwschierigheid worden genoemd.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Op bepaalde momenten lopen er zeer veel externen rond binnen de organisatie. Deze externen dienen ook een VOG aan te leveren echter het risico lijkt groter met deze medewerkers.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
1. Phising mails

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email.

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Nee, de bewustwording en kennis van social engineering dienen beiden te worden vergroot.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Nee, er zijn veel medewerkers waarbij IT niet hun werk is. IT is ondersteunend.
Verbeteringen welke kunnen worden doorgevoerd zijn: training/bewustwording, hand-outs met daadwerkelijke voorbeelden, informatiemails.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Dit kan zeer grote gevolgen hebben voor de organisatie, IT dienstverlener en zelfs de verantwoordelijke minister. Als het uitlekt naar de pers kan dit tot Kamervragen leiden. De minister kan in het uiterste geval uit zijn functie worden gezet.

Audit:

27. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten?
Alle medewerkers maken gebruik van flexplekken. Hierdoor is aan het eind van elke dag elke werkplek schoon. Op de afdelingen staan papierbakken welke op slot zitten. Ook is een papierbak aanwezig met een schredder erop waardoor documenten versnipperd kunnen worden. Steeds meer medewerkers werken digitaal waardoor er steeds minder fysieke documenten aanwezig zijn. Tablets en telefoons worden na inlevering vernietigd en dus niet doorverkocht.

28. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
Jaarlijks vinden audits plaats op verschillende systemen en de autorisatie structuur binnen de systemen. Daarnaast is de organisatie voor verschillende ISO certificaten gecertificeerd welke worden bijgehouden.

29. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt. De kans dat het geprobeerd wordt is groot. De usb poorten staan echter uit waardoor er geen mogelijkheid is de data container uit te lezen. Als de datacontainer op de netwerkschijf wordt geplaatst met een aantrekkelijke naam is de kans groot dat deze wordt geopend door medewerkers mits deze in de root directory staat.

30. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is zeer laag. Er is een pas benodigd om binnen te komen. Alle bezoekers dienen te worden aangemeld. Zelfs als de persoon binnen kan komen kan deze niet veel, de belangrijke ruimtes zijn alleen toegankelijk door geautoriseerde medewerkers. USB poorten staan dicht en werken niet. Alle werkplekken zijn virtueel waarbij de medewerkers geen rechten hebben om executabel uit te voeren. Alle executabel dienen geautoriseerd te zijn door de IT dienstverlener.

31. Weet je welke trends er spelen op het gebied van social engineering.
Nee niet persoonlijk. Binnen de organisatie is een specifieke afdeling verantwoordelijk voor het bijhouden van de trends op alle vlakken van informatiebeveiliging.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
Nee, grote organisaties hebben het kenmerk om log te zijn. Als nieuwe ontwikkelingen worden aangekaart duurt dit een tijd voordat deze door alle lagen van de organisatie zijn doorgevoerd.

33. Is er bij het bereidingen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Binnen de afdeling is een medewerker hiervoor verantwoordelijk. Deze medewerker beëindigd dienstcontracten in het PMS systeem. Hier kunnen rijkspassen en ad accounts worden geblokkeerd. Ook houd deze medewerker bij welke devices een medewerker in zijn bezit heeft.

34. Hoe groot is de kans dat een medewerker in een phishing mailt trapt?
Laag.

Uitwerking interview 5:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Informatie manager van het team informatiemanagement. Houd zich bezig met activiteiten om te zorgen dat de systemen in de lucht blijven en dat het systeem aan blijft sluiten bij de wensen van de klanten.

2. Hoeveel jaar werkt u in uw huidige functie?
8 jaar.

3. Aan hoeveel medewerkers geeft u leiding?
geen

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Er wordt een VOG verklaring gevraagd.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van uw functie?
Niet in de systemen zelf. Ik heb wel autorisaties met toegang tot met SLS beveiligde gegevens van de BD. Wel veel vertrouwelijke documenten.

Informatie beveiligingsbeleid
6. Hoe wordt binnen Blauw omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
De baseline informatiebeveiliging rijk (BIR) is leidend voor informatiebeveiliging . Hiervoor is binnen de organisatie een in control traject uitgevoerd. Er is een CISO overleg met de CISO's van alle sectoren. Daarnaast gaat in feite niet over IBis er ook de baseline informatie huishouding rijk. Hier staat in hoe om wordt gegaan met informatie, hoe deze wordt gearchiveerd en/of vernietigd etc.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat?
Is er binnen de organisatie bekend welke informatie het belangrijkst is?
Er is een rubricering aanwezig met de verschillende classificeringen van informatie.departementvertrouwelijke (depV), staatsgeheim etc.

Het blijft een persoonlijke inschatting in veel van de gevallen, bij sommige documenten wordt aangegeven hoe vertrouwelijk ze zijn. De rest van de informatie/documenten dient de medewerkers zelf goed over na te denken. De inschatting is dat de medewerkers weten welke informatie wel en niet verspreid mag worden intern en aan wie en extern.

Nieuwe medewerkers worden niet actief bekend gemaakt met het informatiebeveiligingsbeleid.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De BIR is leidend voor de organisatie. ISO is de basis van de BIR.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven?
Ja hier staan maatregelen voor op ingenomen. Het gaat hier maatregelen m.b.t. de awareness.

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid.
Hij beoordeelt de ICV en de explains en ik bespreek onderwerpen op IB gebied met het afdelingshoofd.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid.
De lijnmanagers zijn verantwoordelijk voor het informatiebeveiligingsbeleid. Zowel voor het invoeren als uitvoeren hiervan. Dit staat uitgebreid beschreven en aangegeven binnen de BIR. Veel van het werk wordt gedaan door de chief information security officer (ciso). De verschillende sectoren binnen het ministerie hebben allen een ciso. De ciso's hebben regelmatig onderling overleg.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?

Risico analyses worden gemaakt door de lijnorganisatie ! niet de ciso en de IT dienstverlener (wel voor hun eigen organisatie!). Hoe vaak deze worden gemaakt is wel bekend, nl. elke 3 jaar en voor elk nieuw informatie systeem

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?
Er wordt een melding gemaakt bij de ondersteunende IT dienstverlener. Daarnaast wordt de manager en de ciso op de hoogte gebracht. Er is een organisatiebrede procedure voor, het proces hiervan is niet precies bekend bij de informant. Het proces zal niet bij alle medewerkers bekend zijn.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?
Binnen het intranet is een informatiepagina aanwezig als men inlogt. Het beleid wordt niet actief uitgedragen binnen de organisatie en afdeling. Zo worden nieuwe medewerkers niet op de hoogte gebracht van het informatiebeveiligingsbeleid.

Social engineering
15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering?
Het via de zachte kant, de mensen toegang verkrijgen tot informatie of bedrijfsmiddelen. De mensen factor is hierbij leiden.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.*
Als eerste wordt informatie ontfutselt of opgezocht via sociale media, documenten etc. Vervolgens wordt deze informatie gebruikt om een aanval uit te voeren binnen de organisatie of op een persoon.

17. Welke motieven zou een social engineer kunnen hebben?
Wraak en financieel worden genoemd.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Phishing, man in the middle (jezelf voordoen als iemand anders), office snooping (diefstal van documenten), namen noemen worden genoemd.

19. Waar maakt een social engineer misbruik van?
Van het menselijke aspect, niet de techniek.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Dezelfde als bij elke organisatie, zie hierboven. Werkzaamheden worden alleen uitgevoerd door Blauw. Deze besteed niet verder uit.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
Ja, phishing aanvallen. Tientallen per jaar.

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website.
Vooral Email.

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?

Er zijn bewustwording campagnes geweest o.a. via intranet Er is dan ook wel iets aan gedaan echter het kan een stuk beter. Trainingen kunnen niet voor alles worden gegeven, echter memo's, korte informatiesessies etc kunnen worden ingezet.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Redelijk, transparanter zijn over aantal aanvallen, casussen en aantalen presenteren in werkoverleggen.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?
Dit kan vergaande gevolgen hebben, het ligt aan de soort informatie. Niet !Alle data lekken zie website Autoriteit Persoonsgegevens dienen gemeld te worden, als dit niet wordt gemeld staat hier een boete op voor de organisatie. Het kan gevolgen hebben voor de directeur, managers, lekkende medewerker etc.

26. Hoe groot is de kans dat een medewerker in een phishing mailt trapt?
De informant (aha, ik ben informant!, ik zou zeggen respondent of geinterviewde denkt dat deze kans klein is.

27. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is klein, je hebt een pasje nodig en je dient langs de beveiliging te komen. Bij elke ingang staan beveiligers. Er kan daarnaast maar 1 persoon door de deur.

28. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt.
De kans is klein aangezien de usb poorten dicht staan. Hier kunnen alleen beveiligde usb sticks in. Niet alle medewerkers zullen zich echter realiseren dat dit een aanval kan zijn.

Als het om een file op de netwerkschijf gaat met een aantrekkelijke naam dan is de kans groot dat medewerkers dit zullen openen. De gedachte is dat alle bestanden op deze schijf publiekelijk toegankelijk zijn en daarom veilig zijn aangezien er technische beveiliging aan ten grondslag ligt om deze schijf te beveiligen.

Audit:
29. Hoe gaat men binnen de organisatie om met het verwijderen van vetrouwelijke documenten?
Op elke afdeling is een schredder aanwezig. Daarnaast zijn normale papierbakken en een afgesloten papierbak met schredder aanwezig. Medewerkers kunnen zelf kiezen hoe ze hun documenten verwijderen. Harde schrijven worden na afschrijving vernietigd, mobiele devices worden ook vernietigd.

30. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
Ja, er is een in controle verklaring onderzoek uitgevoerd op de BIR. Hierbij is gekeken of de organisatie compliant aan de BIR is.

31. Weet je welke trends er spelen op het gebied van social engineering.
de phishing mails worden steeds geavanceerder. .

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling? Wel nieuwe vormen. Ik denk niet genoeg, het zijn vooral IB ers die er mee bezig zijn.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Hier zijn procedures voor; zo worden nu de autorisaties van oud Blauw medewerkers voor het ERP systeem beëindigd!

Uitwerking interview 6:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
Senior Security adviseur: Alle takken van sport met betrekking tot de technische beveiliging binnen de organisatie, hieronder valt ook de fysieke beveiliging. Hiernaast valt er ook een stukje van het aspect business continuïteit onder zijn functie. Hierbij dient gedacht te worden aan wat er gebeurd als het pand niet meer beschikbaar is om te werken voor welke reden dan ook. Ook is de informant jaarlijks verantwoordelijk voor de ISO 27001 certificering welke wordt uitgevoerd door de DEKRA. Voor zijn huidige functie was de informant team coördinator van kantoorautomatisering/netwerken.

2. Hoeveel jaar werkt u in uw huidige functie?
8 jaar.

3. Aan hoeveel medewerkers geeft u leiding?
In de dagelijkse werkzaamheden niet. Bij het uitvoeren van projecten wel aan 1 of meerdere medewerkers.

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Niet alle medewerkers. Dit is afhankelijk van de functie waarop wordt gesolliciteerd. De screenings worden uitgevoerd door de AIVD en zijn verdeeld in de niveaus A, B en C screenings, waarvan A het hoogste is. De meeste medewerkers worden niet gescreend. Bij vertrouwensfuncties die te maken hebben met cryptologie of staatsgeheimen wordt een A screening uitgevoerd, security medewerkers ondergaan een B screening. In een A screening wordt je hele financiële situatie doorgelicht, ook de familie en vriendenkring wordt bekeken. Een A screening moet zijn voltooid voor een medewerker mag beginnen, in de praktijk wordt hier echter wel eens van afgeweken.
Voor zover bekend is bij de informant worden referenties en diploma's niet gecontroleerd.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Niet tot vertrouwelijke klantinformatie, wel tot persoonlijke informatie van medewerkers. De informant is voor zijn huidige functie gescreend

Informatie beveiligingsbeleid
6. Hoe wordt binnen het BLAUW omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
Als organisatie is er een leidraad waar volgens wordt gewerkt. Er is een classificering aanwezig voor de verschillende soorten informatiesystemen. Denk hierbij aan departement vertrouwelijk, staatsgeheim etc. Op de interne website staan informatiebeveiliging richtlijnen welke bij alle medewerkers bekend zouden moeten zijn. Deels van de richtlijnen worden opgelegd door de departementen vanuit een hoger niveau binnen de organisatie. Hiernaast zijn voor de organisatie zelf deels aanvullende richtlijnen.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?
De informant is op de hoogte van wat de waardevolle informatie voor de organisatie is. Het is niet vastgelegd in een systeem maar zit in de hoofden van de medewerkers en de informant. De informant is op de hoogte van wat elke afdeling doet, welke systemen deze hebben en welke informatie het hier om gaat. Het huidige MT is waarschijnlijk niet volledig op de hoogte van welke vertrouwelijke informatie aanwezig is binnen de organisatie.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De BIR is een document met informatiebeveiligingsrichtlijnen waar de gehele rijksoverheid aan moet voldoen. Er vind jaarlijks een audit plaats vanuit de Audit Dienst Rijk (ADR) of de organisatie aan de BIR voldoet. Uit de audit komen bevindingen waaraan voldaan dient te worden. Voor de BIR geld een "comply or explain", per punt kan worden aangegeven waarom de organisatie niet aan dat punt kan of wil voldoen. Deze punten worden getekend door het management. De BIR is van toepassing op alle aspecten binnen de informatiebeveiliging van de rijksoverheid. In principe is de BIR tactisch normenkader (TnK) leidend voor de jaarlijkse audit. Na de audit wordt een "in controle verklaren" afgegeven.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? '
Ja directe informatiebeveiligingsmaatregelen, in de BIR staat in hoofdstuk 8 paragraaf 2.2 wat hiervoor geregeld dient te worden.
Bewustzijn, management/directiebetrokkenheid, screenings, geheimhoudingsovereenkomsten etc.
Tevens staan in de BIR richtlijnen voor disciplinaire maatregelen(8,3).

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid.
Volledig, de manager van de informant heeft de functie chief information officer en is dan ook verantwoordelijk voor het informatiebeveiligingsbeleid binnen de organisatie. De directeur is eindverantwoordelijk maar wordt alleen geïnformeerd door de CIO over audits en beveiliging aandachtspunten.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid.
Dit is afhankelijk van het soort incident. De afdeling security neemt de leiding en schakelt waar nodig met de afdelingsmanagers en afdelingsbeveiligingscoördinatoren.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?
Ja, hier worden jaarlijks analyses van opgesteld. Voor elk incident wordt een melding gelogd welke wordt meegenomen in de rapportages. Deze worden opgesteld door het security team en gedeeld met het MT.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?
Incidenten worden gemeld bij de servicedesk, welke een melding hiervoor aanmaakt en deze vervolgens doorzet naar het security team. Per melding wordt dan bekeken in samenwerking met de betrokken partijen/afdelingen welke acties er genomen dienen te worden, tevens is een escalatie team ingericht waarvan gebruik gemaakt kan worden. Tevens is een security operation center ingericht (soc) welke de systemen proactief monitord. Veel aanvallen worden afgevangen door de serviceprovider, hiervan worden geen meldingen gemaakt. Als de serviceprovider echter merkt dat de organisatie doelgericht wordt aangevallen wordt de organisatie hiervan geïnformeerd.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?

Ja, alle afdelingen dienen aan de BIR te voldoen. Daarnaast heeft elke afdeling een beveiligingscoördinator welke binnen de afdeling het beleid wat op hoger niveau wordt bepaald uitdraagt.

Social engineering

15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering?
Proberen gegevens te ontfutselen waarmee schade kan worden aangericht tegen de organisatie waarvan de gegevens zijn ontfutselt.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.* Nee, de informant is niet bekend met de typische aanvalscyclus welke wordt doorlopen bij een social engineeringsaanval. Het verzamelen van informatie en het uitvoeren van de aanval worden wel genoemd.

17. Welke motieven zou een social engineer kunnen hebben?
Wraak en financieel worden genoemd.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
Shoulder surfing, phishing, met iemand meelopen om de security te omzeilen (piggyback) en het bemachtigen van documentatie (dumpster diving/office snooping) worden genoemd.

19. Waar maakt een social engineer misbruik van?
Op de bereidwilligheid/behulpzaamheid van de collega's om te helpen.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Er bestaat altijd de mogelijkheid dat medewerkers worden gechanteerd. Dit is echter bijna niet af te vangen als de medewerker zich niet anders gedraagt.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
Ja, phishing mails, informatie opvragen via de telefoon en een mysterie guest.

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email, telefoon, fysiek.

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Ja, er wordt door collega's uit het security team regelmatig actie ondernomen op verschillende aspecten van social engineering. Denk hierbij aan clean desk policy, het locken van computers etc. Voor de medewerkers in zijn algemeenheid ook ja, er valt wel een verbeterslag te maken bij nieuwe medewerkers en externen.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Ja en nee. Je kan nooit voorkomen dat een medewerker iets lekt naar de media. Voor aanvallen van buitenaf zijn we als organisatie voldoende beschermd.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?

Dan hebben we als organisatie flink wat uit te leggen. In het extreme geval hebben we als organisatie een uitdaging om het bestaan ervan te kunnen verdedigen. Verschillende medewerkers kan het de functie kosten. Denk hierbij aan de directeur, CIO, verantwoordelijke minister.

26. Hoe groot is de kans dat een medewerker in een phishing mailt trapt?
Klein, de medewerkers zijn goed op de hoogte van het fenomeen phishing.

27. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is klein, er is fysieke beveiliging aanwezig bij de hoofdingangen waarbij een toegangspas benodigd is. Ook de afdelingen zelf zijn beveiligd en medewerkers dienen geautoriseerd te zijn. De kans bij de achterdeur is groter aangezien hier geen fysieke beveiliging aanwezig is (wel camerabewaking) . De kans is dus wel aanwezig maar wordt klein geacht. Bezoekers dienen zich aan te melden en krijgen een bezoekerspas. Tevens dienen zijn begeleid te worden door een medewerker.

28. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt.
Klein, de usb poorten zijn alleen toegankelijk met iron keys(beveiligde usb sticks) en niet toegankelijk voor andere usb sticks.

Audit:
29. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten?
Op alle afdelingen staan containers welke op slot zitten. Met een speciale vrachtwagen worden de containers opgehaald waarna de inhoud wort vernietigd. Na het vernietigen wordt een rapport ontvangen. Op elke afdeling is daarnaast een schredder aanwezig. Afgeschreven hardware, harde schijven, mobiele apparaten worden vernietigd.

30. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?
Ja, jaarlijks vindt een ISO 27001 audit plaats door de DEKRA. Daarnaast wordt jaarlijks een audit op de doorvoering van de BIR uitgevoerd. De afdeling kwaliteit voert zelf ook audits uit, denk hierbij aan clean desk policy etc.

31. Weet je welke trends er spelen op het gebied van social engineering.
Niet persoonlijk. Vanuit andere sectoren worden echter weekrapportages rondgestuurd naar het security team omtrent nieuwe informatiebeveiligingsontwikkelingen, hieronder valt ook social engineering. Tevens is het security team geabonneerd op verschillende security tijdschriften waarin ook social engineering wordt behandeld.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
Ja, de organisatie heeft een SOC wat dagelijks monitort op mogelijke aanvallen. Daarnaast wordt vanuit andere sectoren de BIR bijgewerkt waaraan de organisatie dient te voldoen.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Dit is de verantwoordelijkheid van de verantwoordelijke lijnmanager. Hiervoor zijn richtlijnen aanwezig. Er vindt geen controle plaats vanuit het team security hierop, in de toekomst is het wel de bedoeling dat deze controles gaan plaatsvinden.

Uitwerking interview 7:

1. Wat is uw functie en kunt u deze in het kort omschrijven?

Manager van de afdeling Customer Services en Procesmanagement(CSP).
Het team CSP bestaat uit het cluster Servicedesk en het cluster Procesmanagement.
De Servicedesk is het centrale loket voor onze klanten voor vragen over onze dienstverlening, het melden van verstoringen en voor het aanvragen van producten en diensten.
Het cluster Procesmanagement heeft als doel het optimaliseren en aansturen van de ICT-beheerprocessen. Het gaat hierbij om het incident management, problem management, change management, configuration management en het software asset management.

2. Hoeveel jaar werkt u in uw huidige functie?
3 jaar als manager van de afdeling CSP, daarvoor 13 jaar als IT beheerder.

3. Aan hoeveel medewerkers geeft u leiding?
+- 50 medewerkers

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Alle interne en externe medewerkers dienen een Verklaring Omtrent Gedrag aan te leveren. Voor interne medewerkers wordt gecontroleerd of de medewerker de juiste papieren heeft bij het sollicitatiegesprek. Bij externe medewerkers is het de verantwoordelijkheid van de broker/detacheerder om te controleren of de juiste papieren aanwezig zijn. Binnen de overheid bestaat daarnaast de mogelijkheid om een A of B screening uit te voeren. Deze screenings worden alleen uitgevoerd wanneer men een vertrouwensfunctie dient uit te voeren. *Een veiligheidsonderzoek hoort bij een sollicitatieprocedure voor een vertrouwensfunctie. Voor een vertrouwensfunctie heeft u een Verklaring van Geen Bezwaar (VGB) nodig. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) doet eerst een veiligheidsonderzoek. Daarna geeft de minister van Binnenlandse Zaken en Koninkrijksrelaties of de minister van Defensie een VGB.*
Referenties worden niet altijd nagetrokken, als het gevoel goed is dan is het prima.

Vanuit HR worden managers geïnformeerd over medewerkers met financiële problemen. Er bestaat de mogelijkheid om leningen te bieden aan deze medewerkers.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, vertrouwelijke informatie van medewerkers uit het team CSP, informatie m.b.t. MT verslagen, inzage in financiële rapportages + tarieven van externe consultants. In zijn vorige functie was er meer toegang tot vetrouwelijke informatie in de verschillende systemen.

Informatie beveiligingsbeleid
6. Hoe wordt binnen het BLAUW omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
De Baseline informatiebeveiliging rijk (BIR) is van toepassing binnen de organisatie. De inhoud van de BIR is alleen op grote lijnen bekend bij de informant. Naast de BIR is een handleiding uitgedeeld aan de medewerkers waarin een aantal belangrijke informatiebeveiligingstaken staan vermeld. Zoals clean desk beleid, locken van schermen, wees alert op mensen die men niet kent etc.

Niet alle medewerkers dienen bewust te zijn van het gehele informatie beleid. Voor de meeste medewerkers is een hand-out, folder met de highlights uit het beleid voldoende. De belangrijkste punten dienen regelmatig worden genoemd en behandeld.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?
Voor concurrenten kan het gewenst zijn om te weten waar het bedrijf in investeert en wat voor de dienstverlening wordt berekend. Er is geen lijst binnen de organisatie waarop de verschillende informatiebronnen geclassificeerd zijn. Vertrouwelijke informatie is dan ook vooral bekend bij de

medewerkers van bepaalde afdelingen. Of alle medewerkers het evengoed weten en beseffen durft de informant zijn hand niet voor in het vuur te steken.
Daarnaast zijn contactgegevens van bijvoorbeeld bewindspersonen (voor bepaalde personen) waardevolle informatie.
Ook technische informatie, zoals IP-adressen, gebruikte hard- en software en beveiligingsmaatregelen worden als waardevol gezien.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De Baseline informatiebeveiliging rijk (BIR) is van toepassing binnen de organisatie. Hiernaast is er beleid op data lekken. Alle data lekken dienen gemeld te worden, de medewerkers van de servicedesk dienen ook altijd te overwegen of een melding een informatiebeveiligingsincident is of kan zijn. De organisatie is daarnaast gecertificeerd in ISO 27001. ISO 27001 dient als basis voor de BIR. De exacte punten uit ISO en BIR zijn niet puntsgewijs bekend. In de tool MAVIM worden alle procesbeschrijvingen vastgelegd en beheerd.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven? Social engineering wordt niet direct benoemd in de BIR, wel kort in ISO 27001. Indirect wordt wel aangegeven dat de awareness van het personeel inzake informatiebeveiliging moet worden aangeleerd.

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid. Deze is niet direct betrokken. Het wordt van bovenaf in de organisatie gedelegeerd naar operationeel niveau. Bij audits wordt wel stilgestaan door de lijnverantwoordelijke dat het belangrijk is. Ook is informatiebeveiliging een vast onderwerp op de agenda van een aantal overleggen.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Het is de taak van de manager van een afdeling om ervoor te zorgen dat het informatiebeveiligingsbeleid goed wordt uitgevoerd en uitgedragen. De uitvoering is echter wel gedelegeerd naar een beveiligingscoördinator. Bij audits krijgt de informant te horen of er wordt voldaan. Daarnaast vindt er regelmatig een onderling overleg plaatst om bij te praten. De informant is vrij om vanuit zijn leidinggevende rol meer of minder tijd aan informatiebeveiliging of de awareness van informatiebeveiliging te besteden.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt? Bij elke melding die binnenkomt op de servicedesk wordt aangegeven of het om een beveiligingsrisico gaat of niet. Hiervoor kan op elke melding een vinkje worden gezet. Als het vinkje wordt gezet komt de melding automatisch bij het team security terecht welke vervolgens de risico analyse maakt en ook rapporteert over de risico's binnen de organisatie. Het team van de informant maakt zelf niet de risico analyses. Het is wel mogelijk om over een bepaalde periode alle bekende/gemelde beveiligingsincidenten op te vragen.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk? Beveiligingsincidenten worden afgewikkeld door het team security. De afdeling CSP maakt alleen de meldingen aan waarna deze worden doorgezet.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen? Het beleid is niet op alle afdelingen hetzelfde. Op sommigen afdelingen geldt dat mensen een A screening dienen te ondergaan, alleen deze medewerkers hebben dan ook toegang tot deze afdeling. De afdeling is afgeschermd met

gesloten deuren waarvoor een pasje benodigd is. De informant is vanuit zijn functie verantwoordelijk voor het uitdragen van het beleid binnen zijn afdeling. Informatie zoals de hand-outs worden wel verspreid over alle afdelingen.

Social engineering

15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering? Er kan vanuit de techniek of vanuit het menselijke aspect toegang worden verkregen tot vertrouwelijk informatie. Social engineering betreft het verkrijgen van toegang tot informatie vanuit het menselijke aspect d.m.v. misleiding en manipulatie.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? ***Als vervolg het aanvalsschema doorlopen.*** Als eerste wordt informatie verzameld over het bedrijf of de persoon op social media of internet, dit kan zijn het vinden van mail adressen, namen, functies. Vervolgens wordt deze informatie gebruikt om het slachtoffer te misleiden om tot het gewenste resultaat te komen.

17. Welke motieven zou een social engineer kunnen hebben? Financieel, concurrentievoordeel, spionage, terrorisme, chantage om imagoschade te voorkomen.

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
De aanvallen die worden genoemd zijn: Phishing, jezelf voordoen als iemand anders, shoulder surfing.

19. Waar maakt een social engineer misbruik van? Van het menselijke aspect. Manipulatie, verleiding, nieuwsgierigheid, angst, chantage en misleiding worden genoemd.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Er zullen altijd bedreigingen blijven, het is haast niet uit te sluiten. Er werken binnen de organisatie velen verschillende nationaliteiten, wie weet hebben deze medewerkers nog nauwe contacten met hun vaderland.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
1. Phising mails om inloggegevens van applicaties te bemachtigen.
2. Devices welke zijn gestolen. Het gaat hier om tablets en telefoons.

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email.

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Nee, het kan beter binnen de organisatie.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?
Nee, medewerkers worden wel geïnformeerd via hand-outs en de email.
Een presentatie m.b.t. social engineering is zeer gewenst om de medewerkers hiervan meer bewust te maken en zo de beveiliging te vergroten.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Als financiële gegevens op straat komen te liggen kunnen journalisten deze gegevens uit hun verband trekken of het vergelijken met andere bedrijven waardoor verkeerde conclusie**s** getrokken kunnen worden. Dit kan tot Kamervragen lijden.

Audit:

27. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten? Op alle afdelingen zijn schredders en gesloten papierbakken aanwezig. Alle documenten worden dan ook vernietigd of afgeschermd weggegooid.

28. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten? Er wordt jaarlijks geaudit (DEKRA), de auditor kiest echter zelf de onderdelen welke dat jaar onder de loep worden genomen. Van te voren is echter niet bekend welke punten worden bekeken waardoor de organisatie wel alle punten zelf dient af te dekken.
Hierdoor worden niet alle punten elk jaar behandeld.
Elke drie jaar vindt controle op BIR plaats, door de ADR. Puntsgewijs wordt dan gekeken of de afdeling nog voldoet aan de BIR. Als dat punt is gecontroleerd en is afgedekt wordt het niet opnieuw bekeken bij een ongewijzigde situatie. De audits dienen er ook voor om weer stil te staan bij het beveiligingsbeleid, er wordt niet pro actief gekeken.
Ook wordt er gebruik gemaakt van interne audits, welke worden uitgevoerd vanuit het cluster Kwaliteit.
Tot slot vinden er ook audits en/of penetratietesten plaats op verzoek van systeemeigenaren, gericht op 1 systeem of 1 keten van systemen.

29. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt. Binnen de organisatie staan alle USB poorten dicht, deze kunnen niet worden gebruikt. De kans is hiervoor dan klein.
De kans is groot als een bestand op de G schijf wordt geplaatst met een aantrekkelijke naam: Bijvoorbeeld het salaris van de directeur. Hiervoor dient dan wel eerst toegang worden gekregen tot het netwerk van de organisatie.

30. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is niet heel groot, er dient via een pas toegang verkregen te worden tot het gebouw. Daarnaast is er fysieke beveiliging aanwezig welke controleert of alle personen gemachtigd zijn.

Niet alle medewerkers zijn zich bewust dat hun ook dienen op te letten dat een ander persoon niet met hun meeloopt. Bij ontruimingen wordt er niet gecontroleerd wie er na het gebouw weer binnenkomt, mensen klokken niet uit bij een ontruiming waarna de deur wordt opengezet om na de ontruiming iedereen weer binnen te laten. De kans is niet groot echter kan de awareness worden verhoogt bij de medewerkers om hierop te letten.

31. Weet je welke trends er spelen op het gebied van social engineering.
Phising mails worden steeds professioneler, geen spelfouten meer. Hiernaast meerchantage mails en praktijken. Ook proberen journalisten steeds vaker om gegevens te achterhalen via social engineering praktijken.
De bewustwording wordt wel hoger, documenten worden niet meer gedeeld d.m.v. dropboxaccounts, medewerkers geven dit aan als het afwijkt. Er wordt ook nagedacht over bedrijven in het buitenland, denk aan apple tablets. Is deze informatie wel echt beveiligd of kan apple dit inzien? Hier wordt over nagedacht en acties op genomen.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
De organisatie wordt regelmatig geïnformeerd over nieuwe ontwikkelingen. Nieuwe ontwikkelingen krijgen hierdoor dan ook voldoende aandacht. De organisatie is geen absolute koploper maar loopt zeker niet achter de feiten aan.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
In het Personeel Management Systeem(PMS) worden de dienstverbanden bijgehouden. Bij het beëindigen van een dienstverband wordt in PMS een uit dienst datum gezet. Hierna wordt automatisch op de ingevulde datum de toegangspas geblokkeerd en de active directory account geblokkeerd. Maandelijks wordt een document naar alle managers gestuurd met de huidige werknemers, deze lijst dient ter extra controle om zeker te zijn dat alle medewerkers correct zijn beëindigd, zijn toegevoegd of zijn verlengt. Er vindt een terugmelding plaats vanuit PMS dat een medewerkers ook daadwerkelijk is verwerkt, dit gebeurd echter niet op detailniveau. De manager dient zelf bij te houden welke medewerker een device heeft. De manager is dan ook verantwoordelijk voor het terugkrijgen van de devices, deze lijst is op te vragen in het systeem.

Uitwerking interview 8:

1. Wat is uw functie en kunt u deze in het kort omschrijven?
IT specialist

2. Hoeveel jaar werkt u in uw huidige functie?
17 jaar

3. Aan hoeveel medewerkers geeft u leiding?
0

4. Worden medewerkers gescreend voordat deze aangenomen, welke zaken?
Alle interne en externe medewerkers dienen een Verklaring Omtrent Gedrag aan te leveren.

5. Heeft u toegang tot vertrouwelijk informatie tijdens het uitvoeren van u functie?
Ja, vertrouwelijke informatie uit klantsystemen.

Informatie beveiligingsbeleid
6. Hoe wordt binnen Blauw omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?
De Baseline informatiebeveiliging rijk (BIR) is van toepassing binnen de organisatie. De inhoud van de BIR is alleen op grote lijnen bekend bij de informant. Naast de BIR is een handleiding uitgedeeld aan de medewerkers waarin een aantal belangrijke informatiebeveiligingstaken staan vermeld. Zoals clean desk beleid, locken van schermen, wees alert op mensen die men niet kent etc.

7. Wat is waardevolle informatie voor uw organisatie? Weet uw baas en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?
De informant weet alleen wat voor hem vanuit zijn functie waardevolle informatie is. Hij denkt niet dat zijn baas op de hoogte is van alle informatie en hun classificering.

8. Hoe verhoud de informatiebeveiliging zich tot de BIR en ISO 27001.
De Baseline informatiebeveiliging rijk (BIR) is van toepassing binnen de organisatie. De exacte punten uit ISO en BIR zijn niet puntsgewijs bekend.

9. Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie (BIR en ISO). Kunt u hiervan een voorbeeld geven. Is niet bekend bij de informant

10. In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid. Deze is niet direct betrokken. Het wordt van bovenaf in de organisatie gedelegeerd naar operationeel niveau.

11. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Het is de taak van de manager van een afdeling om ervoor te zorgen dat het informatiebeveiligingsbeleid goed wordt uitgevoerd en uitgedragen. De uitvoering is echter wel gedelegeerd naar een beveiligingscoördinator.

12. Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt? Is niet bekend bij de informant.

13. Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk? Beveiligingsincidenten worden gemeld bij de servicedesk. Wat er vervolgens mee gebeurd is niet bekend bij de informant.

14. Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen? Nee, dit ligt verschilt per afdeling.

Social engineering
15. Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in mijn definitie van social engineering? Social engineering betreft het verkrijgen van toegang tot informatie vanuit het menselijke aspect i.p.v. via de techniek. Verleiding en manipulatie spelen hierbij een grote rol.

16. Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat? *Als vervolg het aanvalsschema doorlopen.* Als eerste wordt informatie verzameld over het bedrijf of de persoon op social media of internet. Vervolgens wordt deze informatie gebruikt om het slachtoffer te misleiden om tot het gewenste resultaat te komen.

17. Welke motieven zou een social engineer kunnen hebben? Financieel, concurrentievoordeel

18. Bent u in staat om een aantal verschillende socialengineeringsaanvallen te beschrijven?
De aanvallen die worden genoemd zijn: Phishing, shoulder surfing.

19. Waar maakt een social engineer misbruik van? Manipulatie, verleiding worden genoemd.

20. Ziet u vanuit uw eigen personeel en externe partijen bedreigingen binnen de organisatie?
Er zullen altijd bedreigingen blijven, het is haast niet uit te sluiten.

21. Zijn er recent incidenten geweest rondom socialengineeringsaanvallen?
Phising mails om inloggegevens van applicaties te bemachtigen.

22. Via welk kanaal werd deze poging ondernomen? Email, Instant messaging, telefoon, sociaal netwerk, cloud, website. Email.

23. Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?
Nee, het kan beter binnen de organisatie.

24. Is naar uw mening uw organisatie momenteel voldoende beschermd tegen socialengineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?

Nee, medewerkers worden wel geïnformeerd via hand-outs en de email.

25. Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen? Dit kan zeer grote gevolgen hebben voor de organisatie. Meerdere mensen kunnen hun functie verliezen en klanten zouden kunnen opstappen.

Audit:
27. Hoe gaat men binnen het BLAUW om met het verwijderen van vetrouwelijke documenten? Op alle afdelingen zijn schredders en gesloten papierbakken aanwezig. Alle documenten worden dan ook vernietigd of afgeschermd weggegooid.

28. Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten? Er Weet ik niet

29. Hoe groot is de kans dat wanneer een medewerker een data container vind deze ook daadwerkelijk bekijkt. Binnen de organisatie staan alle USB poorten dicht, deze kunnen niet worden gebruikt. De kans is hiervoor dan klein.

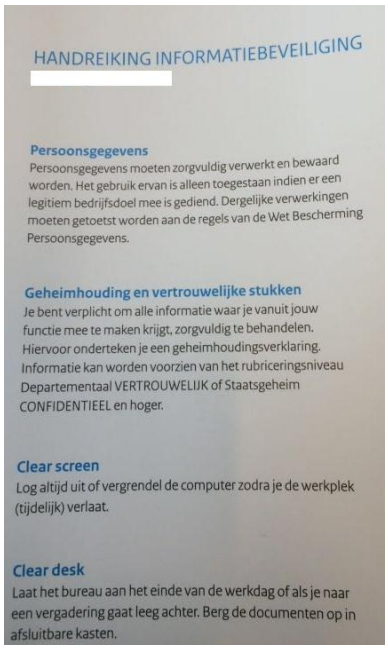
30. Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft.
De kans is niet heel groot, er dient via een pas toegang verkregen te worden tot het gebouw. Daarnaast is er fysieke beveiliging aanwezig welke controleert of alle personen gemachtigd zijn.

31. Weet je welke trends er spelen op het gebied van social engineering.
Nee, is niet bekend.

32. Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering.
Misschien op de achtergrond. De informatie wordt echter niet actief verspreid binnen de organisatie.

33. Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?
Ja, er vindt controle plaats op het retourneren van goederen en het dichtzetten van inlogaccounts/toegangspassen.

Bijlagen 3: Handreiking Informatiebeveiliging



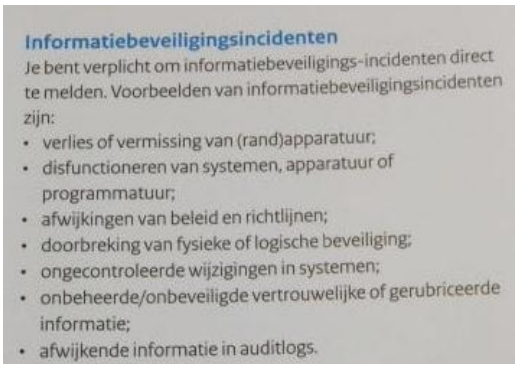
HANDREIKING INFORMATIEBEVEILIGING

Persoonsgegevens
Persoonsgegevens moeten zorgvuldig verwerkt en bewaard worden. Het gebruik ervan is alleen toegestaan indien er een legitiem bedrijfsdoel mee is gediend. Dergelijke verwerkingen moeten getoetst worden aan de regels van de Wet Bescherming Persoonsgegevens.

Geheimhouding en vertrouwelijke stukken
Je bent verplicht om alle informatie waar je vanuit jouw functie mee te maken krijgt, zorgvuldig te behandelen. Hiervoor onderteken je een geheimhoudingsverklaring. Informatie kan worden voorzien van het rubriceringsniveau Departementaal VERTROUWELIJK of Staatsgeheim CONFIDENTIEEL en hoger.

Clear screen
Log altijd uit of vergrendel de computer zodra je de werkplek (tijdelijk) verlaat.

Clear desk
Laat het bureau aan het einde van de werkdag of als je naar een vergadering gaat leeg achter. Berg de documenten op in afsluitbare kasten.



Informatiebeveiligingsincidenten
Je bent verplicht om informatiebeveiligings-incidenten direct te melden. Voorbeelden van informatiebeveiligingsincidenten zijn:

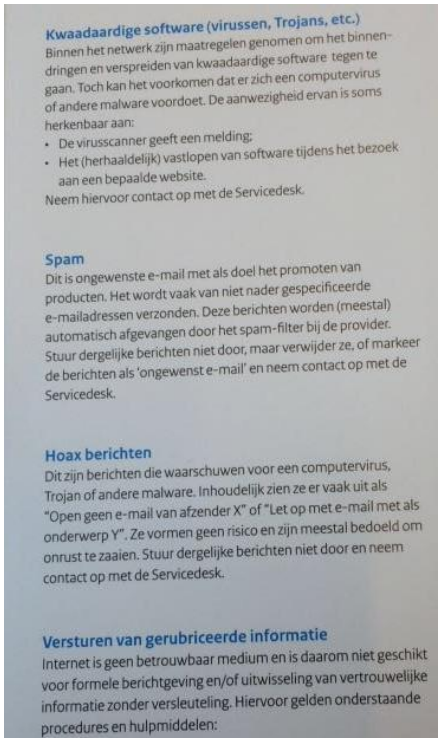
- verlies of vermissing van (rand)apparatuur;
- disfunctioneren van systemen, apparatuur of programmatuur;
- afwijkingen van beleid en richtlijnen;
- doorbreking van fysieke of logische beveiliging;
- ongecontroleerde wijzigingen in systemen;
- onbeheerde/onbeveiligde vertrouwelijke of gerubriceerde informatie;
- afwijkende informatie in auditlogs.

Papiervernietiging
Voor vertrouwelijke informatie en documenten die je wilt weggooien, gebruik je de hiervoor bestemde papiervernietiger. Voor grote hoeveelheden kan gebruik worden gemaakt van de afgesloten stalen bakken.

Gedragscode e-mail en internet
Uitgangspunt is dat iedere medewerker zelf verantwoordelijk is voor zijn gedrag als het gaat om het gebruik van e-mail en internet. E-mail en internet zijn bedoeld voor zakelijk gebruik en voor het uitvoeren van de opgedragen taken.

Bezoekers
Bezoekers worden altijd opgehaald en teruggebracht naar de receptie en mogen zich niet onbegeleid door de panden begeven. Spreek mensen aan die je niet kent om zeker te zijn van hun bedoelingen.

Wachtwoorden
Gebruikersnaam en wachtwoord zijn persoonlijk. Laat collega's dus nooit met jouw gebruikersnaam en wachtwoord werken. Hierdoor krijgt men inzage in bijvoorbeeld e-mailberichten, kan men gegevens wijzigen of op basis van 'Single Sign-on' persoonsgegevens inzien (bijvoorbeeld P-Direkt). Kies en gebruik je wachtwoord daarom zorgvuldig en verander dit regelmatig, ook het netwerk vraagt hier automatisch om. Verander initiële wachtwoorden direct na ontvangst of als het vermoeden bestaat dat deze bekend zijn bij anderen. Je bent en blijft te allen tijde zelf verantwoordelijk.



Kwaadaardige software (virussen, Trojans, etc.)
Binnen het netwerk zijn maatregelen genomen om het binnendringen en verspreiden van kwaadaardige software tegen te gaan. Toch kan het voorkomen dat er zich een computervirus of andere malware voordoet. De aanwezigheid ervan is soms herkenbaar aan:

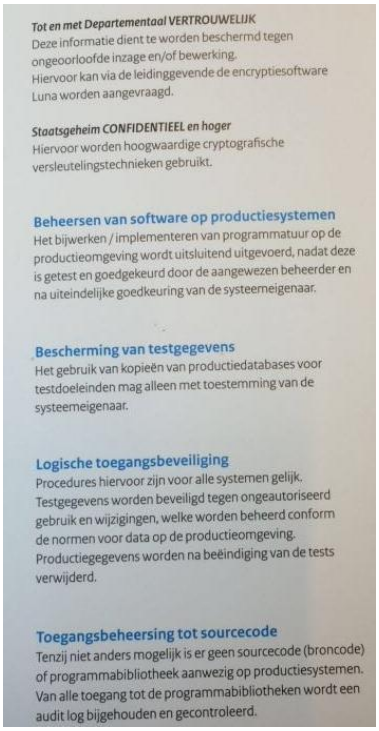
- De virusscanner geeft een melding;
- Het (herhaaldelijk) vastlopen van software tijdens het bezoek aan een bepaalde website.

Neem hiervoor contact op met de Servicedesk.

Spam
Dit is ongewenste e-mail met als doel het promoten van producten. Het wordt vaak van niet nader gespecificeerde e-mailadressen verzonden. Deze berichten worden (meestal) automatisch afgevangen door het spam-filter bij de provider. Stuur dergelijke berichten niet door, maar verwijder ze, of markeer de berichten als 'ongewenst e-mail' en neem contact op met de Servicedesk.

Hoax berichten
Dit zijn berichten die waarschuwen voor een computervirus, Trojan of andere malware. Inhoudelijk zien ze er vaak uit als "Open geen e-mail van afzender X" of "Let op met e-mail met als onderwerp Y". Ze vormen geen risico en zijn meestal bedoeld om onrust te zaaien. Stuur dergelijke berichten niet door en neem contact op met de Servicedesk.

Versturen van gerubriceerde informatie
Internet is geen betrouwbaar medium en is daarom niet geschikt voor formele berichtgeving en/of uitwisseling van vertrouwelijke informatie zonder versleuteling. Hiervoor gelden onderstaande procedures en hulpmiddelen:



Tot en met Departementaal **VERTROUWELIJK**
Deze informatie dient te worden beschermd tegen ongeoorloofde inzage en/of bewerking.
Hiervoor kan via de leidinggevende de encryptiesoftware Luna worden aangevraagd.

Staatsgeheim **CONFIDENTIEEL** *en hoger*
Hiervoor worden hoogwaardige cryptografische versleutelingstechnieken gebruikt.

Beheersen van software op productiesystemen
Het bijwerken / implementeren van programmatuur op de productieomgeving wordt uitsluitend uitgevoerd, nadat deze is getest en goedgekeurd door de aangewezen beheerder en na uiteindelijke goedkeuring van de systeemeigenaar.

Bescherming van testgegevens
Het gebruik van kopieën van productiedatabases voor testdoeleinden mag alleen met toestemming van de systeemeigenaar.

Logische toegangsbeveiliging
Procedures hiervoor zijn voor alle systemen gelijk. Testgegevens worden beveiligd tegen ongeautoriseerd gebruik en wijzigingen, welke worden beheerd conform de normen voor data op de productieomgeving. Productiegegevens worden na beëindiging van de tests verwijderd.

Toegangsbeheersing tot sourcecode
Tenzij niet anders mogelijk is er geen sourcecode (broncode) of programmabibliotheek aanwezig op productiesystemen. Van alle toegang tot de programmabibliotheken wordt een audit log bijgehouden en gecontroleerd.

Bijlagen 4: Literatuuronderzoek

Literatuuronderzoek naar risicomanagement op het gebied van social engineering

Naam:	Krijn van der Laan
Studentnummer:	851212445
Datum:	28-12-2015
Eerste begeleider / Examinator:	dr.ir. H.L Jonker
Tweede begeleider:	dr.ir. H.P.E. Franken

Inhoudsopgave

Het doel van het literatuuronderzoek

Het voornaamste doel van dit literatuuronderzoek is om mij en de lezer te helpen bij het ontwikkelen
van een goed begrip van en inzicht in relevant onderzoek op het gebied van risicomanagement met betrekking tot social engineering. Hieronder vallen: het identificeren en definiëren van de kernbegrippen uit het gebied social engineering en risicomanagement met betrekking tot social engineering zodat het op een later tijdstip uit te voeren empirische onderzoek op basis van een eenduidig en expliciet begrippenkader kan plaatsvinden.

Verder heeft het literatuuronderzoek een aantal overige doelen:

- Het verfijnen en verder uitwerken van de onderzoeksvragen ter voorbereiding op het empirische onderzoek
- Expliciete aanbevelingen vinden voor verder onderzoek
- Inzicht krijgen in methoden van onderzoek en strategieën en technieken voor onderzoek die geschikt zijn binnen het afstudeertraject.

Het literatuuronderzoek is deductief van aard. De literatuur wordt gebruikt om theorieën en ideeën te vinden die in een theoretisch kader of een conceptueel raamwerk worden geplaatst. In het empirische vervolgonderzoek zal dit theoretisch kader of conceptueel raamwerk worden uitgebreid en worden getest.

Het resultaat van het literatuuronderzoek is een omschrijving van het onderzoeksgebied social engineering en een beschrijving van het onderzoeksgebied risicomanagement van social engineering, aangevuld met de definities van een aantal kernbegrippen.
Deze resultaten worden gepresenteerd in een door mij te ontwikkelen referentiemodel. Het referentiemodel wordt als input gebruikt voor het empirische vervolgonderzoek (praktijkonderzoek).

Ook heb ik nog een aantal persoonlijke doelstellingen die ik wil bereiken tijdens het uitvoeren van dit literatuuronderzoek, te weten:

- Het kunnen opzetten en uitwerken van een literatuuronderzoek op een wetenschappelijk verantwoorde wijze.
- Mijn kritische lezen verbeteren, hieronder vallen:
    1. Previewing van literatuur: literatuur in grote lijnen doornemen om een snelle effectieve selectie te maken op relevantie
    2. Annotating: een dialoog voeren met mijzelf om intensief over de inhoud na te denken
    3. Comparing en contrasting: het vergelijken en tegen elkaar afzetten van de literatuurstof met als doel om na te gaan of nog op dezelfde manier over de stof wordt gedacht.

Onderzoeksvragen

Hoofdvraag literatuuronderzoek:

1. Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarop, waarmee, wat ontbeekt?

Deelvragen literatuuronderzoek social engineering:

1. Wat is social engineering?

2. De social engineer, wie is hij en welke motieven kan hij hebben?

3. Welk proces wordt doorlopen bij social engineering?

4. Welke menselijke factoren worden door de social engineers uitgebuit?

5. Welke soorten aanvallen worden geclassificeerd als social engineering?

Deelvragen literatuuronderzoek risicomanagement

1. Wat is risicomanagement?

2. Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
3. Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?

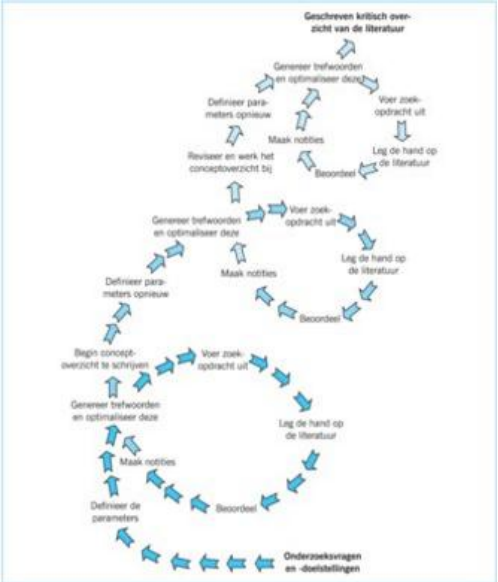
Deelvragen literatuuronderzoek organisaties

1. Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties?
2. Hoe vaak komen socialengineeringaanvallen voor bij organisaties?

3. Hoe gaan verzekeringsmaatschappijen en banken om met risicomanagement met betrekking tot uitkeringen na een socialengineeringaanval?

De methode van onderzoek

In dit literatuuronderzoek worden drie fasen doorlopen. De fasen hebben echter overlap met elkaar waardoor de fasen alle drie meerdere keren worden doorlopen. In figuur 1 zijn de drie fasen weergegeven in een model dat het proces en het doel van de literatuurstudie weergeeft. Ook kunnen de onderzoeksvragen worden bijgesteld naar aanleiding van de gevonden literatuur.



Figuur 44: Het proces van literatuurstudie

Fase 1: oriënterende fase

In deze fase wordt het zoekterrein afgebakend, wordt het begrippenkader vastgesteld en worden onderwerpspecifieke secundaire publicaties gezocht en globaal doorgenomen.

Parameter	Gebied
Taal	Nederlands en Engels
Onderzoeksgebied	Risicomanagement + social engineering + IT security
Bedrijfstak	Information Technology
Geografisch gebied	Internationaal
Publicatieperiode	Afgelopen 15 jaar
Soort literatuur	Wetenschappelijke artikelen/tijdschriften en boeken. De wetenschappelijke artikelen dienen peer reviewed te zijn. Peer review verwijst naar het onderling feedback geven tussen gelijken (peers) met als doel kwaliteitsverbetering (De Bruin et al., 2013)
Begrippenkader	Social engineering, risicomanagement.
Referentiestijl	APA versie 6

Tabel 16: Afbakening zoekterrein

Fase 2: systematisch zoeken van geschikte literatuur

In fase 2 wordt het onderzoek definitief gepland en wordt de literatuur gezocht, vastgelegd en beoordeeld.

Zoekmethoden:

In het zoeken naar geschikte literatuur wordt gebruikgemaakt van de citation-indexmethode, trechtermethode, sneeuwbalmethode en het opstellen van de initiële zoekopdracht. Hieronder worden de methoden toegelicht:

- Citation index: met behulp van een citation index (Web of Science) naar meer recente literatuur zoeken, gebruikmakend van geschikte, reeds gevonden literatuur.
- Sneeuwbalmethode: het zoeken van literatuur uit een verder verleden via de literatuurverwijzingen in de reeds gevonden geschikte literatuur.
- Trechtermethode: van een breed onderwerp naar een klein aspect daarvan. Denk hierbij aan een trechter die van breed naar smal gaat.
- Initiële zoekopdracht samenstellen.

Initieel is gezocht naar artikelen waarbij de gebruikte zoekterm ergens in het artikel voorkomt.

Zoekterm	OU Bibliotheek	Sciencedirect	Google Scholar
Social engineering	1.225.819	192.826	3.440.000
Social engineering threats	128.832	31.540	390.000
Social engineering attacks	81.074	22.985	440.000
Social engineering security threats	53.122	23.778	220.000
Social engineering techniques	312.936	103.523	3.010.000
Risk management	3.659.927	941.443	3290.000
Risk management AND Social Engineering	254.887	60.492	2.250.000
Social engineering AND Risk Management	254.877	60.492	2.220.000
Social engineering risk management	254.887	60.492	2.290.000
Social engineering risicomanagement	1	3	514
Information security risk management	498.498	97.122	2.580.000
Information security risk management framework	156.683	48.603	1
Enterprise risk management	431.494	65.744	2.010.000
Enterprise risk management framework	136.500	37.345	2.150.000

Tabel 2: Initiële zoekopdracht

Vervolgens is een tweede schifting gemaakt waarbij de gebruikte zoekterm in de titel voorkomt.

Zoekterm	OU Bibliotheek	Sciencedirect	Google Scholar
Social engineering	825	18	4080
Social engineering threats	16	2	28
Social engineering attacks	33	3	74
Social engineering security threats	9	0	4
Social engineering techniques	24	0	41
Risk management	19.937	4228	95.200
Risk management AND Social Engineering	6	1	5
Social engineering AND Risk Management	6	1	5
Social engineering risk management	6	1	6
Social engineering risicomanagement	0	0	0
Information security risk management	96	1	388
Information security risk management framework	12	15	1
Enterprise risk management	637	55	2390
Enterprise risk management framework	30	2	142

Tabel 3: Verfijnde zoekopdracht

Zowel uit de 1e schifting als 2e schifting zijn artikelen bekeken. De zoekresultaten zijn gesorteerd op datum als ook op relevantie. Tevens is gekeken hoe vaak de artikelen zijn geciteerd in andere artikelen.

Bij artikelen gevonden via de initiële zoekopdracht die relevante informatie bevatten om één of een gedeelte van een onderzoeksvraag te beantwoorden is in de referentielijst gekeken of daar geschikte/relevante artikelen in stonden. Figuur 01 is een voorbeeld van de referentielijst van het artikel: *A means to violate a computer system*. Het artikel van Sarah Granger is door middel van deze sneeuwbalmethode gevonden en gebruikt in het literatuuronderzoek.

References

Allan, Ant, Noakes-Fry, Kristen, Mogull, Rich. "Business Update: How Businesses Can Defend Against Social Engineering Attacks". Gartner, March 16, 2005.

Arthurs, Wendy. "A Proactive Defence to Social Engineering", August 2, 2001.
URL: http://www.sans.org/rr/whitepapers/engineering/511.php

Bernz. "The Complete Social Engineering FAQ".
URL: http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

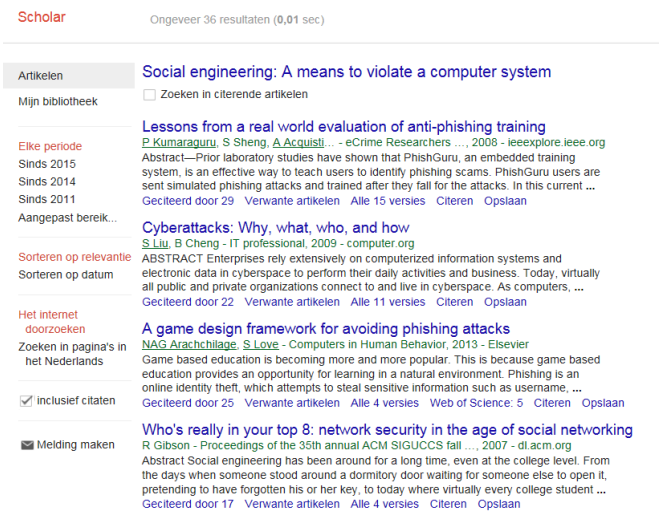
CERT Advisory CA-1991-04. "Social Engineering", Revised September 18, 1997.
URL: http://www.cert.org/advisories/CA-1991-04.html

Frank, John. "Locking Down Data Security", Collections and Credit Risk. March 2006, pg 18.

Granger, Sarah. "Social Engineering Fundamentals, Part I : Hacker Tactics", December 8, 2001
URL: http://www.securityfocus.com/infocus/1527

Figuur 2: Sneeuwbalmethode via referenties in artikelen

Voor een artikel wat via een zoekterm is gevonden kan via een citation index worden bekeken welke artikelen naar dit artikel refereren. Een gedeelte van de citation index (google scholar) van het artikel *A means to violate a computer system* is als voorbeeld weergegeven in figuur 02. Ook via deze methode zijn meerdere artikelen gevonden en gebruikt.



Figuur 3: Citation index methode

Zoektermen:

De volgende zoektermen worden gebruikt: cybercrime, cybercriminaliteit, cyberaanvallen, IT security measures, IT-beveiligingsmaatregelen, Social engineering, Social engineering threats, Social engineering attacks, Social engineering security threats, Social engineering techniques, Risk management, Risk management AND Social Engineering, Social engineering AND Risk Management, Social engineering risk management, Social engineering risicomanagement, Information security risk management, Information security risk management framework, Enterprise risk management, Enterprise risk management framework

De zoektermen worden onderling gecombineerd met de volgende zoekoperatoren:

AND - alleen artikelen met beide zoektermen worden weergegeven

OR - artikelen met ten minste een van de trefwoorden worden weergegeven.

Bronnen/indexen:

De volgende bronnen worden gebruikt: Google Scholar, Google, Web of Science en de Universiteitsbibliotheek van de Open Universiteit (OU).

De gevonden artikelen worden met het softwarepakket Endnote X7 bewaard.

Fase 3: proces en opbrengst evalueren/beoordelen

In fase 3 wordt de waarde van de gevonden publicaties beoordeeld, wordt het proces geëvalueerd en indien nodig worden vervolgacties gepland.

Voor het beoordelen van de artikelen op relevantie en waarde van de literatuur is de volgende checklist gebruikt:

- Is het artikel recent genoeg?
- Is er een nieuw artikel waardoor dit artikel achterhaald is?
- Bevat het artikel relevante referenties voor het literatuuronderzoek?
- Biedt het artikel hulp bij de beantwoording van de onderzoeksvragen?

Voor het onderwerp risicomanagement is gekeken welk(e) model(len) het vaakst voorkomen in de resultaten van de initiële en tweede zoekopdracht per gebied. Dit geld voor Enterprise Risk Management en Information Security Risk Management. Hier is dan ook handmatig geteld/gekeken welk model het vaakst wordt genoemd in de eerste 100 resultaten per zoekopdracht/database. De telling is uitgevoerd op verschillende sorteringen, dit zijn relevantie en datum (descending) van de artikelen.

Hoofdstuk 1: Social engineering

Dit hoofdstuk geeft antwoord op de volgende vijf deelvragen over social engineering:

1. Wat is social engineering?
2. Welk proces wordt doorlopen bij social engineering?
3. De social engineer, wie is hij en welke motieven kan hij hebben?
4. Welke menselijke factoren welke door de social engineers uitgebuit?
5. Welke soorten aanvallen worden geclassificeerd als social engineering?

In de eerste paragraaf staan een inleiding en de definitie van het begrip social engineering. Vervolgens wordt ingegaan op de motieven van een social engineer en welke overeenkomstige eigenschappen social engineers bezitten. Daarna volgt een nadere concretisering naar het proces, de methoden en de technieken van social engineering. De volgende paragraaf behandelt de soorten aanvallen die worden geclassificeerd als social engineering. Hierbij wordt een overzicht gegeven van de aanvallen waarin de volgende gegevens zijn verwerkt: mijn classificatie van aanvalstype, aanvalskanalen en -operatoren, gewilde informatie en welke emoties door social engineers gemanipuleerd worden.
Het hoofdstuk besluit met een conclusie, waarin de hoofdvraag gedeeltelijk kan worden beantwoord. Het gedeelte van de hoofdvraag dat wordt beantwoord is: ‘schiet de literatuur tekort op het gebied van social engineering?

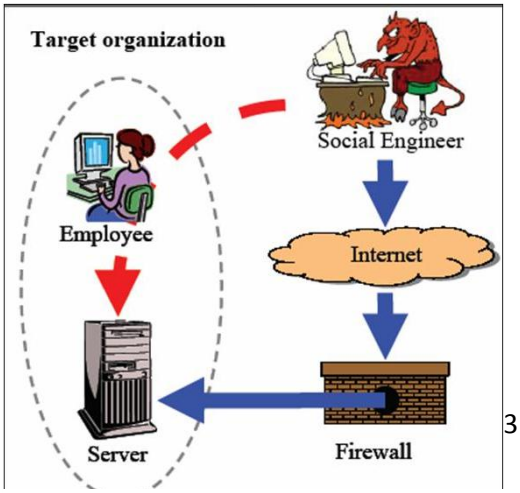
1.1 Inleiding en definitie van social engineering

In deze paragraaf wordt deelvraag 1 m.b.t. social engineering beantwoord: Wat is social engineering?

De hoeveelheid informatie die een individu of organisatie heeft, is evenredig met de macht die een organisatie of individu over anderen kan hebben. Daarom is niet alleen het verwerven van informatie belangrijk maar ook het beschermen van informatie tegen potentiële aanvallen is van belang.

De opkomst van informatiesystemen en beschermingsmechanismen leek de beveiligingsproblemen te hebben opgelost. Echter, het cruciale element blijft het individu en niet de machine. Het installeren van de nieuwste beveiligingsmechanismen staat dan ook niet garant voor een volledige bescherming van het systeem. Het systeem met het beveiligingsmechanisme hoeft niet zelf geïnfiltreerd te worden, het is vaak gemakkelijker om de informatie te krijgen die nodig is met behulp van overtuigingskracht, manipulatie of goede wil. Social engineers vallen dan ook de zwakste schakel aan in de organisatie, namelijk de mensen. Technologie alleen is dan ook weerloos als deze schakel wordt uitgebuit. Dit maakt social engineering aanvallen een van de gevaarlijkste aanvallen voor een organisatie.

De sleutelwoorden zijn hier: social engineering, overtuigingskracht, vertrouwen, risico's, gevoelige informatie, security, zelfvertrouwen en manipulatie.



Figuur 4: The Social Engineer (Hermansson & Ravne, 2005)

Social engineering is op verschillende manieren gedefinieerd in het verleden door vele verschillende personen. Hieronder wordt een aantal definities van social engineering gegeven. Social engineering is:

- Het zich voordoen als iemand/iets anders, met als doel iemand te misleiden zodat hij informatie geeft die hij normaal gesproken niet zou geven en waar normaal geen toegang toe is. Kortom, social engineering is liegen. Iemand noemt zichzelf liever een social engineer dan dat hij van zichzelf zegt dat hij een leugenaar is (Cole & Ring, 2006).

- Social engineering of social hacking is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen. Hij doet dit door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. De aanval is gericht op het verkrijgen van vertrouwelijke of geheime informatie, waarmee de hacker dichter bij het aan te vallen object kan komen (Wikipedia, 2015).

- Op het gebied van informatiebeveiliging is social engineering een term die gebruikt wordt om de niet-technische aard van een inbraak te beschrijven. De inbraak is gebaseerd op het manipuleren van mensen tot het bekendmaken van vertrouwelijke informatie en het uitvoeren van onbewuste acties (Tipton & Henry, 2006).

- De succesvolle of mislukte pogingen om een persoon te beïnvloeden om informatie te onthullen of het handelen op een wijze die zou leiden tot ongeautoriseerde toegang tot, ongeoorloofd gebruik van of ongeoorloofde bekendmaking van een informatiesysteem, een netwerk of van data (Hansche, Berti, & Hare, 2003).

- Op het gebied van computers is social engineering de handeling van het verkrijgen of het proberen te verkrijgen van beveiligde data door een individu te misleiden om beveiligde informatie te onthullen (Webopedia, 2015).

- Social engineering is een methode die een aanvaller in staat stelt technische controles te omzeilen door een aanval op de menselijke factor in een organisatie (Scott, 2009).

- Social engineering maakt gebruik van het beïnvloeden en manipuleren van mensen om hen te misleiden door hen ervan te overtuigen dat de social engineer iemand is die hij niet is. Het resultaat is sociale manipulatie ten gevolge waarvan de social engineer profiteert van mensen om informatie te verkrijgen, met of zonder het gebruik van technologie (Mitnick & Simon, 2003).

Social engineering is een heel breed begrip en uit de bovenstaande definities is op te maken dat er geen eenduidige definitie bestaat van social egineering in zowel de gevonden literatuur als in overige bronnen. De definitie die in dit literatuuronderzoek wordt gebruikt en door mij is opgesteld is ontleend aan de opgesomde definities.

De definitie van social engineering die in dit literatuuronderzoek wordt gebruikt, is:
"Social engineering is een set van methoden waarmee het gedrag van een individu of groep individuen wordt gemanipuleerd zodanig dat dit individu of deze groep toegang verleent tot

bepaalde informatie, met als doel deze informatie te gebruiken om de slachtoffers uit te buiten. Deze techniek maakt gebruik van de intrinsieke aard van de mensheid om slachtoffers uit te buiten, om gevoelige informatie te verkrijgen en hen te manipuleren en van het overtuigen van mensen om deze informatie te onthullen door het inzetten van uitzonderlijk goede communicatieve vaardigheden. Boven alles maakt social engineering gebruik van de zwakste schakel in de beveiliging: de menselijke factor."

1.2 De social engineer; ken je vijand

"Als je weet wie je vijanden zijn en je jezelf kent, kun je honderd gevechten winnen zonder een enkel verlies.
Als je alleen jezelf kent, maar niet je tegenstander, kun je winnen of verliezen.
Als je jezelf noch je vijand kent, zul je altijd in gevaar zijn."
Dit citaat is afkomstig uit het boek 'The Art of War', geschreven door Sun Tzu. In dit hoofdstuk wordt ingegaan op wie de vijand is. In hoofdstuk 2 wordt ingegaan op het jezelf leren kennen.

De eerste stap om de verdediging te versterken is om zo veel mogelijk over de vijand te weten te komen. In paragraaf 1.2 wordt duidelijk wie de vijand is (de social engineer), welke eigenschappen de vijand heeft, in welke groepen de vijand ingedeeld kan worden en welke motieven hij normaliter heeft. Als de vijand bekend is, kan men zich vervolgens specifiek op de vijand richten om aanvallen te voorkomen en te stoppen.
In deze paragraaf 1.2 wordt deelvraag 2 m.b.t. social engineering beantwoord: De social engineer, wie is hij en welke motieven kan hij hebben?

1.2.1 Wie zijn social engineers? (Hinson, 2008; Kirwan & Power, 2011; Zager, 2002)
In het extreme kunnen praktisch alle mensen worden geclassificeerd als social engineers. Menselijke interactie draait om communicatie en leidt vaak tot het overhalen van een persoon om iets te doen voor de ander. Mensen met beroepen zoals verkoper en docent ontwikkelen deze communicatieve vaardigheden voor en op het werk. Social engineers zijn daarentegen getalenteerde personen die deze vaardigheden misbruiken om mensen te misleiden. Deze vaardigheden zetten zij in om menselijke kwetsbaarheden en emoties uit te buiten. Denk hierbij aan onwetendheid, naïviteit en het natuurlijke verlangen aardig gevonden te worden door anderen. Social engineers hacken in wezen mensen om nuttige en gewilde informatie te bemachtigen. Deze nuttige informatie stelt hen in staat om toegang te krijgen tot het einddoel.

1.2.2 Eigenschappen van social engineers (Kirwan & Power, 2011)
De eigenschappen van social engineers zijn:

- Zij hebben het vermogen om andere mensen te overtuigen, te dwingen of te manipuleren
- Geloofwaardigheid en inlevingsvermogen, benodigd om overtuigend te liegen, vertrouwen op te bouwen en mensen op een onverdachte manier informatie te laten onthullen door bijvoorbeeld te flirten of hen een compliment te geven
- Zelfvertrouwen en assertiviteit in combinatie met ervaring om te weten wanneer te pushen of niet verder te vragen.
- Zij zijn goed in luisteren, herinneren, correleren en het gebruik van kleine stukjes informatie
- Focus en vastberadenheid, zij kunnen zich concentreren op het slachtoffer en blijven volhouden tot het doel is bereikt.

1.2.3 Verschillende groepen waarin social engineers ingedeeld kunnen worden
Zager(Zager, 2002) identificeert vier verschillende groepen waarin social engineers kunnen worden ingedeeld. Deze groepen worden vaak in andere literatuur aangehaald. Tevens geeft Zager aan dat de verschillende social engineers per groep verschillende primaire motivaties hebben. Zelf ben ik echter van mening dat in principe een motief door elke groep kan worden gebruikt. Ik ben het er wel mee eens dat de primaire motieven vaak verschillen per groep. De verschillende groepen en de motieven zullen hieronder worden besproken.

- ***Casual social engineers:*** dit is de grootste groep en de meeste individuen zijn niet vakkundig. De belangrijkste motivatie is de uitdaging om in een systeem te komen. Ze zijn gemotiveerd door nieuwsgierigheid of door de kick van succes. Soms hopen ze financieel voordeel te behalen en een aantal zal het puur doen om zich te bewijzen tegenover andere social engineers (Kirwan & Power, 2011; Seebruck, 2015; Zager, 2002).

- ***Politieke social engineers:*** dit is een groep die zeer specifieke doelen heeft. De leden worden ook vaak cyberactivisten genoemd. Zij maken gebruik van hun vaardigheden om politieke organisaties of overheidsorganisaties die belangen hebben die tegengesteld zijn aan hun zaak aan te vallen. De expertise van deze groep varieert sterk, van uiterst bekwaam tot beginnend. Cyberterroristen vallen ook onder deze groep (Kirwan & Power, 2011; Seebruck, 2015; Zager, 2002).

- ***Georganiseerde misdaad social engineers:*** deze hackers worden voornamelijk gemotiveerd door financieel belang. Ze richten zich vaak op banken, creditcardmaatschappijen of grote organisaties met gevoelige informatie. Deze groep is vaak uiterst bekwaam (Kirwan & Power, 2011; Seebruck, 2015; Zager, 2002).

- ***Inside social engineers:*** dit is een groep die voornamelijk gemotiveerd wordt door financieel belang of wraak. Deze groep heeft het grote voordeel dat zij op de hoogte is van de gang van zaken binnen een bedrijf. Deze groep kan dan ook enorme schade veroorzaken door haar plaats in de organisatie (Kirwan & Power, 2011; Seebruck, 2015; Zager, 2002).

1.2.4 Motieven van de social engineer

Wat motiveert een individu om een socialengineeringaanval uit te voeren? Welke verschillende motieven worden erkend in het vakgebied? Malcolm Allen beschrijft vier motieven van een social engineer om een aanval uit te voeren, hij geeft tevens aan dat deze lijst niet allesomvattend is. Naast de vier motieven van Allen zijn er nog drie andere motieven gevonden in andere bronnen.

- ***Financieel voordeel*** (Allen, 2006).

- ***Eigenbelang:*** een individu kan informatie over zichzelf, vrienden, collega's of familie wijzigen of willen inwinnen met als doel hiermee persoonlijk voordeel te behalen (Allen, 2006).

- ***Wraak:*** een individu wil vergelding van het onrecht of het leed dat hem is aangedaan door het slachtoffer (Allen, 2006).

- ***Externe druk:*** een individu kan onder druk worden gezet door vrienden, familie, de overheid of de georganiseerde misdaad om redenen als financieel gewin, eigenbelang en/of wraak (Allen, 2006).

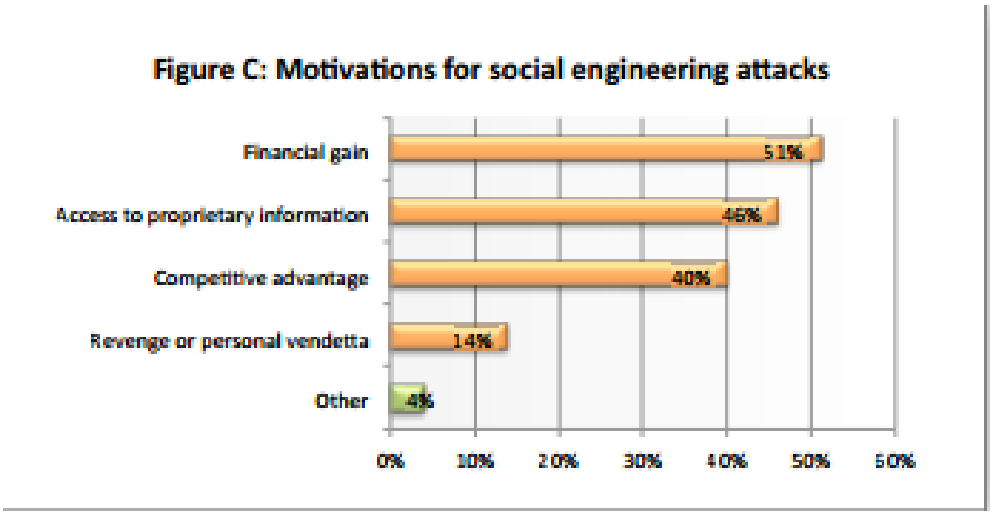
- **Voor de fun:** een individu kan het ook gewoon leuk vinden om socialengineeringaanvallen uit te voeren of om slachtoffers schade toe te brengen (Maurya, 2013).

- **Concurrentievoordeel (**Research, 2011a).

- **Aantonen van vaardigheid:** een individu probeert zijn expertise te bewijzen of zijn ego te vergroten (Government, 2005).

Praktijkonderzoek 1: uitgevoerd door Dimensional Research in 2011 (Research, 2011)
De volgende gegevens zijn gebaseerd op een wereldwijd onderzoek onder 853 IT-professionals dat is uitgevoerd in de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië, Nieuw-Zeeland en Duitsland in de maanden juli en augustus van 2011. Het doel van het onderzoek was het verzamelen van gegevens over de perceptie van socialengineeringaanvallen en hun impact op het bedrijfsleven (Research, 2011).

De deelnemers die hebben aangegeven dat ze het slachtoffer zijn geworden van socialengineeringaanvallen werd gevraagd wat zij geloofden dat de motivaties achter die aanslagen waren. Financieel gewin was de meestvoorkomende reden (51%), gevolgd door de toegang tot vertrouwelijke informatie (46%) en concurrentievoordeel (40%). Wraak was de minst vermoede reden voor een social engineering aanval met slechts 14% (Research, 2011).



Figuur 5: Door slachtoffers genoemde motieven voor socialengineeringaanval

De vermoede motivering voor socialengineeringaanvallen was enigszins gevarieerd in de verschillende landen. Australiërs (61%) en Amerikanen (52%) hebben grotendeels financieel gewin als motief genoemd. Duitsers meldden meer wraakgemotiveerde aanvallen (18%), terwijl de Canadezen meer kans hadden om aanvallen gemotiveerd door concurrentievoordeel (54%) te ervaren (Research, 2011).

Praktijkonderzoek 2: uitgevoerd door de Australische overheid in 2004 (Government, 2005)
In een enquête die is gehouden door de Australische overheid met als naam de 2004 AusCERT computercriminaliteits- en veiligheidsenquête vroeg de overheid de respondenten wat zij dachten wat het motief achter een hackaanval was die heeft plaatsgevonden bij de respondenten in een bepaalde, recente periode (Government, 2005).

De respondenten onderkenden de volgende motieven voor diverse hackaanvallen: het aantonen van vaardigheid (40%), opzettelijke schade (34%), voorbereiding op verdere

aanvallen (26%), financieel gewin (18%), onbekende reden (18%), eigenbelang (14%), politiek belang (9%) en concurrentievoordeel (4%) (Government, 2005).

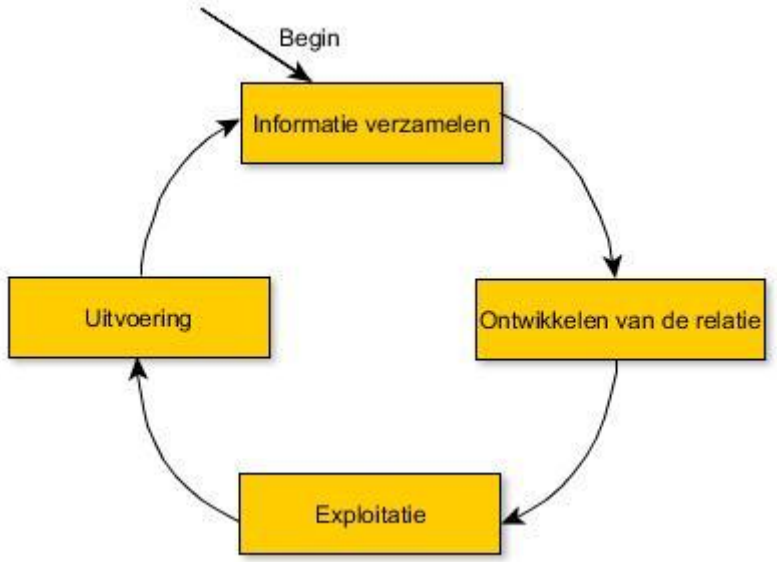
1.3 Het proces van social engineering

In deze paragraaf 1.3 wordt deelvraag 3 m.b.t. social engineering beantwoord: Welk proces wordt doorlopen bij social engineering?
Nu de vijand bekend is, kan worden ingegaan op het aanvalsproces van de vijand.
In deze paragraaf zal dan ook duidelijk worden van welk aanvalsproces de vijand gebruikmaakt. Per fase van de aanvalscyclus wordt inzichtelijk gemaakt wat het doel is van de fase en welke informatie gebruikelijk is om in te winnen voor de vijand van die fase. Als het aanvalsproces bekend is, kan de verdediging ter hand worden genomen.

Volgens Malcolm Allen (Allen, 2006) is er een gemeenschappelijk patroon dat kan worden gekoppeld aan socialengineeringaanvallen. Dit patroon kan worden aangeduid als 'de aanvalscyclus' zoals weergegeven in figuur 4. Deze cyclus van social engineering bestaat uit de volgende vier fasen: informatie verzamelen, relatieontwikkeling, exploitatie en uitvoering.

Elke individuele socialengineeringaanval is uniek en kan zich herhalende fasen, meerdere cycli of de integratie en mix van meer traditionele aanslagen bevatten. Elke fase heeft een of meerdere doelen en elke aanval heeft een of meerdere motieven, zoals besproken in paragraaf 1.2.

Dit model met de bijbehorende fasen wordt vaak aangehaald in de gevonden en gebruikte literatuur. Naast dit model heb ik geen andere modellen kunnen vinden die ingaan op de aanvalscyclus van social engineering.



Figuur 6: Aanvalscyclus social engineering (Allen, 2006).

1.3.1 Informatie verzamelen (Allen, 2006; Mitnick & Simon, 2003; Tipton & Henry, 2006; Zulkurnain, Hamidy, Husain, & Chizari, 2015)

Informatie verzamelen is de fase waarin aanvallers de aanval voorbereiden en het doelwit identificeren voor de lancering van een aanval. De eerste fase omvat niet alleen het verzamelen van doelgerelateerde informatie maar ook andere (fysieke) eigenschappen die nodig zijn in de volgende fasen van de aanval. Een voorbeeld hiervan is het namaken van briefhoofden van officiële documenten van het doelwit.

De aanvallers kunnen verschillende technieken gebruiken om informatie te verzamelen over hun doelgroep. Deze informatie kan vervolgens worden gebruikt om een relatie op te bouwen met het doelwit of een belangrijke persoon die kan helpen bij het succesvol uitvoeren van de aanval.

Voorbeelden van socialengineeringtechnieken die specifiek in deze fase worden gebruikt om informatie te verzamelen zijn[1]:

- Physical reconnaissance
- Dumpster diving
- Phreaking
- Mail-outs
- Profiling
- People spotting
- Forensic analysis
- Phishing
- Web search

Deze technieken hebben gemeen dat het personeel dat de informatie aanlevert niet weet wat de waarde van de informatie voor de social engineer of hacker is.

Voorbeelden van informatie die specifiek in deze fase ingewonnen wordt, zijn:

- Organisatiestructuur
- Medewerkersfuncties
- Kalenders
- E-mailadressen
- Lingo
- Organisatielogo's
- Wachtwoorden
- Namen van medewerkers
- Nieuwe medewerkers
- Interne telefoonnummers
- Organisatieprocessen en -richtlijnen
- IT-infrastructuur
- Gebruikersnamen

1.3.2 Ontwikkelen van de relatie (Allen, 2006; Krombholz, Hobel, Huber, & Weippl, 2015; Mitnick & Simon, 2003)

In de fase 'relatieontwikkeling' maakt een aanvaller gebruik van de natuurlijke bereidheid van een doelwit om zijn vertrouwen te winnen en een relatie te ontwikkelen. Bij de ontwikkeling van deze relatie zal de aanvaller het doelwit in een positie van vertrouwen manoeuvreren die hij vervolgens kan exploiteren.
Het vertrouwen en zorgen voor anderen zit in de natuur van mensen. Social engineers exploiteren deze menselijke eigenschappen en manipuleren en beïnvloeden doelwitten om authenticiteit en vertrouwen op te bouwen.

De handeling van manipulatie kan worden gedaan door middel van fysieke of virtuele interactie. Virtuele interactie is een interactie door middel van media zoals telefoon, e-mail of zelfs sociale media. In tabel 2 worden de fundamentele psychologische principes die ten grondslag liggen aan manipulatie weergegeven.[2]

Fundamentele psychologische principes die worden uitgebuit door de social engineer	
- Onvoorzichtigheid	- Spreiding van verantwoordelijkheid
- Overbelasting	- Urgentie
- Angst	- Schaarste
- Wederkerigheid	- Opbouwen van vertrouwen
- Gelijksoortigheid	- Behulpzaamheid
- Integriteit	- Legitimiteit

[1] De socialengineeringtechnieken worden besproken in paragraaf 1.6.
[2] De fundamentele psychologische principes worden besproken in paragraaf 1.4 Menselijke factoren die door social engineers worden uitgebuit.

- Autoriteit	- Conformiteit
- Nieuwsgierigheid	- Sterk effect
- Namen noemen	- Vleierij
- Verankering	- Representativiteit

Tabel 4: Psychologische principes

Het vertrouwen dat is opgebouwd via de psychologische principes leidt tot een situatie waarin het verzoek van de social engineer niet in twijfel wordt getrokken door het slachtoffer. Deze situatie creëert dus kwetsbaarheden in de beveiliging. De social engineer dient over accurate kennis van de doelgroep te beschikken en bereid te zijn om compromissen te sluiten.

Voorbeelden van socialengineeringtechnieken die specifiek zijn fase van de ontwikkeling van de relatie:

- Physical impersonation
- Phishing
- Reverse social engineering

In deze fase wordt geen specifieke informatie verzameld. Het ontwikkelen van de relatie vormt de basis voor de exploitatie in de volgende fase.

1.3.3 Exploitatie (Allen, 2006; Mitnick & Simon, 2003; Tipton & Henry, 2006)

Exploitatie is de handeling om via het slachtoffer informatie te bemachtigen of het slachtoffer handelingen te laten verrichten die de security van een informatiesysteem in gevaar brengen door ongeautoriseerde toegang, ongeoorloofd gebruik of ongeoorloofde onthullingen.
Tijdens deze fase kan informatie die niet beschikbaar was in de eerste fase worden verkregen door gebruik te maken van de relatie en het opgebouwde vertrouwen door middel van manipulatie in de voorafgaande fase. Bijvoorbeeld kan het slachtoffer worden gemanipuleerd door de 'vertrouwde' aanvaller om wachtwoorden te onthullen of acties uit te voeren zoals het verwijderen van een record, wat niet zou gebeuren onder normale omstandigheden.

Voorbeelden van socialengineeringtechnieken die specifiek zijn voor de exploitatiefase zijn[3]:

- Physical impersonation
- Virtual impersonation
- Reverse social engineering
- Tailgating
- Piggybacking
- Office snooping/Desk sniffing
- Baiting
- Data leakage
- Direct approach

Voorbeelden van gegevens die specifiek in deze fase ingewonnen worden:

- Inlognamen
- Wachtwoorden
- Namen van servers
- Namen van applicaties
- IP-adressen
- Firewall, besturingssysteem

1.3.4 Uitvoering (Allen, 2006; Mitnick & Simon, 2003; Tipton & Henry, 2006)

De uitvoeringsfase is de fase waarin de social engineer gebruikmaakt van wat is bereikt tijdens de vorige fase. Deze fase is dan ook niet specifiek gerelateerd aan social engineering noch het begin van een nieuwe cyclus. De acties in deze fase kunnen leiden tot het ultieme doel van de aanval.
Deze acties zijn dan ook vaak van technische aard in plaats van van psychologische aard zoals het geval was in de andere drie fasen. Denk hierbij aan hacking en cracking of diefstal van gegevens. Ook diefstal of vernietiging van fysieke bezittingen kan een einddoel zijn, waarmee

[3] De socialengineeringtechnieken worden besproken in paragraaf 1.6

door social engineering de fysieke locatie achterhaald wordt. Het succes van deze fase hangt af van hoe succesvol de socialengineeringfasen waren (fasen 1, 2 en 3).

Voorbeelden van socialengineeringtechnieken die specifiek zijn voor de uivoeringsfase zijn[4]:

- Mail-outs
- Identity theft
- Malicious software

1.4 Menselijke factoren die door social engineers worden uitgebuit

In deze paragraaf 1.4 wordt deelvraag 4 beantwoord m.b.t. social engineering: Welke menselijke factoren worden door de social engineers uitgebuit?
Mensen zijn interessante wezens. Hoewel veel mensen geloven dat ze bewust onafhankelijke denkers zijn, is het over het algemeen gemakkelijk om hen instructies te laten volgen. Vanaf de vroege kinderjaren, via de school en op de arbeidsmarkt, volgen mensen van nature instructies op (Mann, 2008).

In dit tijdperk van informatietechnologie moeten medewerkers beslissingen nemen of iemand betrouwbaar is, niet alleen face-to-face of via de telefoon, maar ook via het internet. Als mensen echter iedereen zouden wantrouwen dan zouden ze een moeilijk leven leiden (Mitnick & Simon, 2003). Social engineers weten dit en gebruiken deze menselijke eigenschap 'vertrouwen' om medewerkers of klanten van een organisatie te misleiden (Mann, 2008). Dit wordt verder verklaard door een verklaring van psycholoog Robert Cialdini te citeren *"Er kan niet van ons worden verwacht dat we alle aspecten van een persoon, gebeurtenissen of situaties die we op één dag meemaken kunnen herkennen en analyseren. We hebben hier niet de tijd, energie of de capaciteit voor. In plaats daarvan moeten we heel vaak gebruikmaken van bekende stereotypen en vuistregels om zaken te classificeren."*

Een social engineer speelt in op de emoties van een slachtoffer om dit slachtoffer te manipuleren en uit te buiten.
Een emotie is een subjectieve, mentale en fysiologische toestand in de hersenen van een individu en zij wordt geassocieerd met een verscheidenheid van gevoelens, gedrag en gedachten (RS Lazarus & Lazarus, 1996). Emoties kunnen worden onderverdeeld in negatief, positief of neutraal (Gupta & Sharman, 2008). Deze drie categorieën worden hieronder toegelicht.

- Negatieve emoties betreffen onplezierige gevoelens en kunnen een 'fight or flight'-reactie uitlokken. Hierdoor ontstaat een grotere kans dat het slachtoffer het beleid aan zijn laars lapt of gevoelige informatie openbaarmaakt (Gupta & Sharman, 2008).
- Positieve emoties zijn gevoelens die een vertrouwensrelatie tussen de social engineer en het slachtoffer trachten op te bouwen. Hierdoor is het slachtoffer sneller bereid om aan een verzoek te voldoen (Gupta & Sharman, 2008).
- Ten slotte kunnen neutrale emoties ervoor zorgen dat het slachtoffer zich minder verantwoordelijk voelt voor eventuele incidenten. Neutrale emoties kunnen zowel positieve als neutrale emoties uitbuiten (Gupta & Sharman, 2008).

[4] De socialengineeringtechnieken worden besproken in paragraaf 1.6

Wanneer de social engineer het slachtoffer manipuleert en bedriegt door gebruik te maken van emoties wordt hiervoor een bepaalde techniek gebruikt. Er zijn verschillende technieken die kunnen worden gebruikt om emoties uit te buiten. Deze technieken kunnen worden gecategoriseerd door de soort emotie die de techniek uitbuit. Hieronder staan de technieken opgesomd en deze zullen vervolgens inhoudelijk worden besproken.

Fundamentele psychologische principes die worden uitgebuit: negatieve emoties	
- Onvoorzichtigheid	- Spreiding van verantwoordelijkheid
- Overbelasting	- Urgentie
- Angst	- Schaarste

Tabel 5: Negatieve emoties

Fundamentele psychologische principes die worden uitgebuit: positieve emoties	
- Wederkerigheid	- Opbouwen van vertrouwen
- Gelijksoortigheid	- Behulpzaamheid
- Integriteit	- Legitimiteit
- Autoriteit	- Conformiteit
- Nieuwsgierigheid	

Tabel 6: Positieve emoties

Fundamentele psychologische principes die worden uitgebuit: neutrale emoties	
- Sterk effect	- Namen noemen
- Vleierij	- Verankering
- Representativiteit	

Tabel 7: Neutrale emoties

1.4.1 Uitbuitingstechnieken met betrekking tot negatieve emoties

- ***Onvoorzichtigheid:*** de social engineer maakt gebruik van het gebrek aan waakzaamheid van het slachtoffer (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Spreiding van verantwoordelijkheid:*** de social engineer maakt het slachtoffer wijs dat een incident niet zijn schuld is of dat de schuld nooit alsnog bij het slachtoffer kan worden neergelegd. In een organisatie is het gemakkelijk voor de eindgebruikers om te geloven dat veiligheid niet hun verantwoordelijkheid is (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Overbelasting:*** door een slachtoffer te overladen met nieuwe informatie voor eerdere informatie is verwerkt, kan het vermogen van het slachtoffer om een argument goed te wegen aangetast worden (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Urgentie:*** tijdens een noodsituatie omzeilen werknemers vaak het beleid en procedures. Dit schept voor de social engineer een uitstekende gelegenheid om anders bijna onmogelijke aanvragen goedgekeurd te krijgen (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Angst:*** veel werknemers hebben ervaring met negatieve reacties vanuit het management omdat een verificatie van een belangrijke persoon te lang duurde of een belangrijke persoon te langs moest wachten op zijn verzoek (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Schaarste:*** wanneer wordt aangenomen dat iets alleen voor bepaalde tijd beschikbaar of geldig is. Door deze schaarste is het gemakkelijker om mensen te manipuleren (Mitnick & Simon, 2003).

1.4.2 Uitbuitingstechnieken met betrekking tot positieve emoties

- **Wederkerigheid:** deze techniek is gebaseerd op de sociale regel dat als iemand een belofte doet of een actie onderneemt om iemand een plezier te doen, die persoon de behoefte krijgt om iets terug te doen (Gragg, 2002; Gupta & Sharman, 2008; Mann, 2008).

- ***Opbouwen van vertrouwen:*** het opbouwen van een vertrouwensrelatie met het slachtoffer. Dit kan geruime tijd in beslag nemen en wordt gerealiseerd door regelmatig contact te onderhouden met dezelfde persoon (Mitnick & Simon, 2003).

- ***Gelijksoortigheid:*** mensen in dezelfde situatie geloven dat ze gelijksoortig zijn met de ander en hierdoor ook geloofwaardig zijn (Mann, 2008). Als het slachtoffer dezelfde gedachten, hobby's, interessegebieden of dezelfde doelen in het leven heeft als de social engineer kan het slachtoffer hier een positief gevoel door krijgen waardoor het sneller aan een verzoek zal voldoen (Mitnick & Simon, 2003).

- ***Behulpzaamheid:*** mensen willen over het algemeen andere mensen helpen (Mitnick & Simon, 2003). Behulpzaamheid kan dan ook positieve emoties oproepen en zo kan het slachtoffer gemotiveerd raken om te helpen omdat het slachtoffer zich in de geschetste situatie van de social engineer kan inleven (Gupta & Sharman, 2008).

- ***Integriteit:*** mensen hebben een sterke neiging om aan verzoeken te voldoen waarin wordt beweerd dat deze door een collega zijn toegezegd, waardoor de verplichting reeds is aangegaan. Het slachtoffer kan hierdoor gemotiveerd zijn tot het uitvoeren van de aanvraag (Gragg, 2002).

- ***Legitimiteit:*** als de bron geloofwaardig en legitiem overkomt op het slachtoffer is het slachtoffer sneller geneigd een verzoek of actie uit te voeren (Gupta & Sharman, 2008).

- ***Autoriteit:*** mensen hebben de neiging om te voldoen aan een verzoek wanneer dat wordt gedaan door een persoon met autoriteit (Gupta & Sharman, 2008; Mitnick & Simon, 2003).

- ***Conformiteit:*** slachtoffers voelen zich minder verantwoordelijk voor zaken als de beslissing en verantwoordelijkheid voor het uitwerken van een verzoek door een andere persoon/collega is goedgekeurd (Gupta & Sharman, 2008).

- ***Nieuwsgierigheid:*** het verleiden van het slachtoffer door het verlangen op te wekken om iets te weten of iets te zien (Gupta & Sharman, 2008).

1.4.3 Uitbuitingstechnieken met betrekking tot neutrale emoties

- ***Sterk effect:*** veroorzaakt een verhoogde emotionele toestand waardoor het slachtoffer een sterk gevoel van verbazing, anticipatie of woede ervaart (Gupta & Sharman, 2008). Sterk effect kan positieve of negatieve emoties uitbuiten (Gragg, 2002).

- ***Namen noemen:*** het beïnvloeden van het slachtoffer om het te laten geloven dat de social engineer iemand kent die het slachtoffer ook kent door de naam van die persoon te noemen (Mitnick & Simon, 2003). Individuen kunnen zowel negatieve als positieve gevoelens ten opzichte van die andere persoon ervaren. Hierdoor kunnen zowel negatieve als positieve emoties worden uitgebuit (Gupta & Sharman, 2008).

- ***Vleierij:*** het beïnvloeden van het slachtoffer zodat dit zich speciaal voelt. Als een persoon wordt gevleid, zal hij twee mogelijke reacties hebben. De persoon zal of denken dat de vleier liegt met negatieve emoties tot gevolg of denken dat het oprecht wordt gemeend, wat positieve emoties tot gevolg heeft. Daarom kan een social engineer vleierij gebruiken om zowel negatieve als positieve emoties uit te buiten (Gupta & Sharman, 2008).

- ***Verankering:*** het slachtoffer krijgt eerst een extreem verzoek en daarna een gematigd verzoek. Dit zorgt ervoor dat het extreme verzoek als baseline wordt gezien en het vervolgverzoek als aanvaardbaar ten opzichte van de baseline (Gupta & Sharman, 2008).

- ***Representativiteit:*** wanneer verhalen details bevatten lijken ze meer geloofwaardig. Door gebruik te maken van details die alleen een medewerker zou kennen, ontstaat een grotere kans dat het slachtoffer de social engineer gelooft (Gupta & Sharman, 2008).

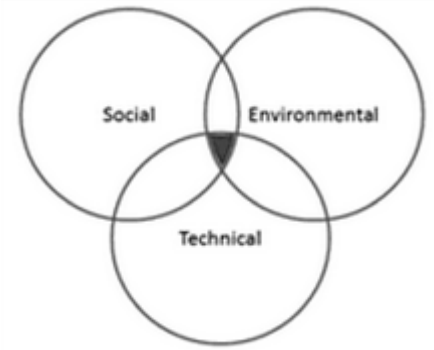
1.5 Soorten aanvallen van social engineering

In deze paragraaf 1.5 wordt deelvraag 5 m.b.t. social engineering beantwoord: Welke soorten aanvallen worden geclassificeerd als social engineering?
Socialengineeringaanvallen zijn veelzijdig en omvatten fysieke, sociale, technische of socio-technische aspecten. Deze aspecten worden gebruikt in verschillende stadia van de aanval. In deze paragraaf worden de verschillende benaderingen van social engineers beschreven. Als eerste komen de verschillende typen van aanvallen aan bod. Vervolgens worden de verschillende operatoren en kanalen besproken. Als laatste komen de verschillende aanvallen aan de orde.
Dit is een overzicht dat ik op basis van de gevonden literatuur heb opgesteld. Het is dan ook niet een allesomvattend overzicht, het is naar mijn mening echter wel een zo goed als compleet overzicht. In de aankomende jaren kan dit overzicht echter snel incompleet raken door de snel veranderende technologie en de creativiteit van de mensen die deze aanvallen uitvoeren en de benaderingen toepassen.
Met deze informatie wordt inzichtelijk tegen welke aanvallen er reeds verdedigingsmechanismen in stelling zijn gebracht en tegen welke aanvallen nog stappen gezet dienen te worden om deze af te dekken en de organisatie te beschermen.

Directe benadering: een aanvaller kan face-to-face een doelwit vragen om een taak uit te voeren. Hoewel dit de eenvoudigste en meest ongecompliceerde benadering is, zal zij waarschijnlijk niet de meest succesvolle zijn (Allen, 2006).

Sociale aanpak: het belangrijkste aspect van een succesvolle socialengineeringaanval is de sociale benadering. Hierbij vertrouwen aanvallers op sociaalpsychologische technieken, zoals eerder in sectie 1.4 is besproken (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Socio-technische benadering: deze aanvallen zijn vaak een combinatie van enkele of alle verschillende benaderingen die hierboven zijn beschreven. Socio-technische benaderingen zijn de krachtigste wapens van de social engineers en zijn het meest succesvol (Krombholz et al., 2015). In het onderzoek van Jagatic en anderen (Jagatic, Johnson, Jakobsson, & Menczer, 2007) werden socialenetwerkwebsites gebruikt om gegevens over studenten te bemachtigen. Met deze informatie stelden de onderzoekers een bericht op dat er uitzag alsof het door een van de vrienden van de studenten verstuurd was. Door het gebruik van dergelijke "sociale gegevens" wist Jagatic het slagingspercentage van zijn social phishing-aanval van 16 naar 72 procent te verhogen.



Figuur 7: Socio-technische benadering

Technische benadering: technische aanvallen worden voornamelijk uitgevoerd via het internet (Krombholz et al., 2015). Granger (Granger, 2010) merkt op dat het internet vooral interessant is voor social engineers om wahctwoorden te verzamelen. Individuen gebruiken vaak hetzelfde (eenvoudige) wachtwoord voor verschillende accounts en applicaties.

1.5.1 Verschillende aanvalskanalen

E-mail is het meestgebruikte kanaal voor phishing- en reverse socialengineeringaanvallen (Krombholz et al., 2015). Er zijn twee gebruikelijke vormen. De eerste betreft kwaadaardige code, zoals een virus of trojan. Deze code wordt meestal verborgen in een bestand en als bijlage meegestuurd met een e-mail. De tweede – even effectieve – aanpak hanteert oplichting, kettingmails en nepvirussen (Allen, 2006).

Telefoon en Voice over IP zijn gemeenschappelijke aanvalskanalen voor social engineers om hun slachtoffer gevoelige informatie te laten onthullen (Granger, 2010; Krombholz et al., 2015).

Instant messaging-toepassingen winnen aan populariteit onder de social engineers als instrumenten voor phishing- en reverse socialengineeringaanvallen (Krombholz et al., 2015).

Sociale netwerken bieden een verscheidenheid aan mogelijkheden voor socialengineeringaanvallen. Gezien hun potentieel om valse identiteiten te creëren in combinatie met hun complexe informatie-uitwisselingsmodel, maken ze het eenvoudig voor aanvallers om hun identiteit te verbergen en gevoelige informatie te verzamelen (Krombholz et al., 2015).

Cloud-diensten worden gebruikt om kennis over samenwerkingsscenario's te krijgen. Aanvallers kunnen een bestand of software plaatsen in een gedeelde map met als doel het slachtoffer informatie te ontfutselen (Krombholz et al., 2015).

Websites worden meestal gebruikt om waterholing-aanvallen (beschreven in paragraaf 1.5.4) uit te voeren. Bovendien kunnen ze worden gebruikt in combinatie met e-mails om phishing-aanvallen uit te voeren (Allen, 2006; Krombholz et al., 2015).

1.5.2 Verschillende operatoren

Er kunnen twee operatoren worden benoemd, te weten mensen en software. Deze operatoren worden hieronder toegelicht.
Mensen: indien de aanval direct wordt uitgevoerd door een persoon wordt deze persoon de operator genoemd. Het aantal doelen is beperkt vanwege de lagere capaciteit vergeleken met een aanslag uitgevoerd door software (Krombholz et al., 2015).
Software: Bepaalde typen aanvallen kunnen worden geautomatiseerd met software. Een voorbeeld hiervan is de Social Engineering Toolkit (SET), die ingezet kan worden voor spearfishing-e-mailaanvallen (Krombholz et al., 2015).

1.5.3 Aanvalstechnieken

Er kunnen vervolgens verschillende manieren worden benoemd waarop de aanval kan worden uitgevoerd. Deze termen zijn bewust niet vertaald aangezien dit de gangbare termen zijn in het vakjargon inzake social engineering.

Socialengineeringtechnieken	
- Phishing	- Dumpster diving
- Shoulder surfing	- Reverse social engineering
- Waterholing	- Advanced persistent threat
- Baiting	- Fake profiles
- Mail-outs	- Web search
- Identity theft	- People spotting
- Impersonatie	- Piggybacking/ Tailgating
- Phreaking	- Office Snooping/Desk sniffing
- Prextexting	- Malicious software
- Data leakage	- Direct approach

Tabel 8: Socialengineeringtechnieken

Baiting is een aanval waarbij een met malware geïnfecteerd opslagmedium wordt achtergelaten op een plaats waar het beoogde slachtoffer dit zal vinden (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Phishing is de poging om gevoelige informatie te verwerven of om iemand te laten handelen op een gewenste manier door zich voor te doen als een betrouwbare entiteit. De aanvallen zijn meestal gericht op grote groepen mensen. Phishing-aanvallen kunnen worden uitgevoerd op bijna elk kanaal, van websites, fysieke benadering, sociale netwerken tot zelfs cloud-diensten. Aanvallen gericht op specifieke personen of bedrijven worden aangeduid als spear phishing. Als een phishing-aanval is gericht op high-profile doelen in ondernemingen, wordt de aanval aangeduid als de whale fishing (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Dumpster diving is het doorzoeken van de prullenbak/afvalcontainer van particulieren of bedrijven met als doel weggegooide items te vinden met gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Shoulder surfing verwijst naar het gebruik van directe-observatietechnieken om informatie te krijgen, zoals meekijken over iemands schouder naar zijn scherm of toetsenbord (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Reverse social engineering is een aanval waarbij eerst een vertrouwensrelatie tot stand wordt gebracht tussen de aanvaller en het slachtoffer. De aanvaller creëert een situatie waarin het slachtoffer hulp nodig heeft waarna hij zichzelf presenteert als de persoon die de situatie kan oplossen. Dit zorgt ervoor dat het slachtoffer hem vertrouwt en eerder op zijn verzoeken zal ingaan (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Waterholing beschrijft een gerichte aanval waarin de aanvallers een website overnemen die waarschijnlijk bezocht gaat worden door het gekozen slachtoffer. De aanvallers wachten vervolgens ‘bij de waterpoel’ op hun slachtoffer (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Advanced persistent threat verwijst naar op de lange termijn gerichte, meestal internetgebaseerde spionageaanvallen. Deze aanvallen worden uitgevoerd door een aanvaller die de mogelijkheden en intentie heeft om permanent in het systeem in te breken (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Fake profiles is het opzetten van onechte profielen met het doel informatie van de slachtoffers te bemachtigen (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Web search is het zoeken naar online informatie over het slachtoffer of de organisatie. Hiermee wordt het voorwerk gedaan voor een verdere aanval (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

People spotting is het bestuderen en observeren van een slachtoffer of een groep slachtoffers om na te gaan wat hun gewoontes zijn (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Impersonatie is het zich voordoen als een werknemer met als doel de slachtoffers te misleiden. De meeste mensen zijn sneller bereid te helpen of regels te omzeilen als het om een collega gaat (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Piggybacking of ***tailgating*** is een aanval waarmee met een andere persoon wordt meegelopen om in een besloten gebied te komen. De persoon met wie wordt meegelopen heeft wel de juiste autorisatie (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Office snooping/Desk sniffing is het doorzoeken van een kantoor en de werkplekken binnen het kantoor van bedrijven met als doel het vinden van gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).
Pretexting is wanneer een social engineer een verhaal ontwikkelt dat hem in staat stelt om zich een beeld te verwerven van de doelgroep. Het biedt de rechtvaardiging voor de vragen die bij de echte aanval gesteld kunnen worden (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Data leakage is het met opzet achterlaten van een bestand op een systeem of in de cloud met de bedoeling dat andere individuen dit bestand openen. Op het moment van openen, kan kwaadaardige software worden geïnstalleerd (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Direct approach is de directe benadering van slachtoffers om informatie te bemachtigen die nodig is voor de daadwerkelijke aanval. Dit kan door simpelweg te bellen en te vragen naar informatie (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Identity theft is het gebruiken van informatie van een persoon zonder diens medeweten, zoals zijn naam, bankrekeningnummer, geboortedatum of zijn BSN-nummer. Dit kan op verschillende wijzen worden bewerkstelligd, variërend van het dragen van een uniform, phishing-aanvallen tot het aanpassen van de DNS-setting (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Malicious software is kwaadaardige software die door een social engineer wordt geïnstalleerd of wordt aangeboden. Als de software eenmaal op het systeem van de slachtoffer is geïnstalleerd, kan vaak de controle op het systeem worden overgenomen of wordt bepaalde informatie verzameld en opgehaald (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

1.6 Conclusie hoofdstuk 1

Social engineering leeft in de literatuur. De literatuur over social engineering is dan ook naar mijn mening goed op de hoogte van de laatste ontwikkelingen en zeer compleet. Het is alleen jammer dat de informatie niet compleet in één model of op één plek is vastgelegd. Het doel van hoofdstuk 1 is om een goed inzicht te creëren in social engineering en inzichtelijk te maken wie de vijand is, wat de aanvalscyclus is van de vijand, welke emoties worden uitgebuit en welke aanvallen kunnen worden gebruikt.
Dit inzicht in de belangrijkste begrippen en onderdelen is verkregen door de beantwoording van de vijf deelvragen. De deelvragen die zijn beantwoord zijn, waren:

1. Wat is social engineering?

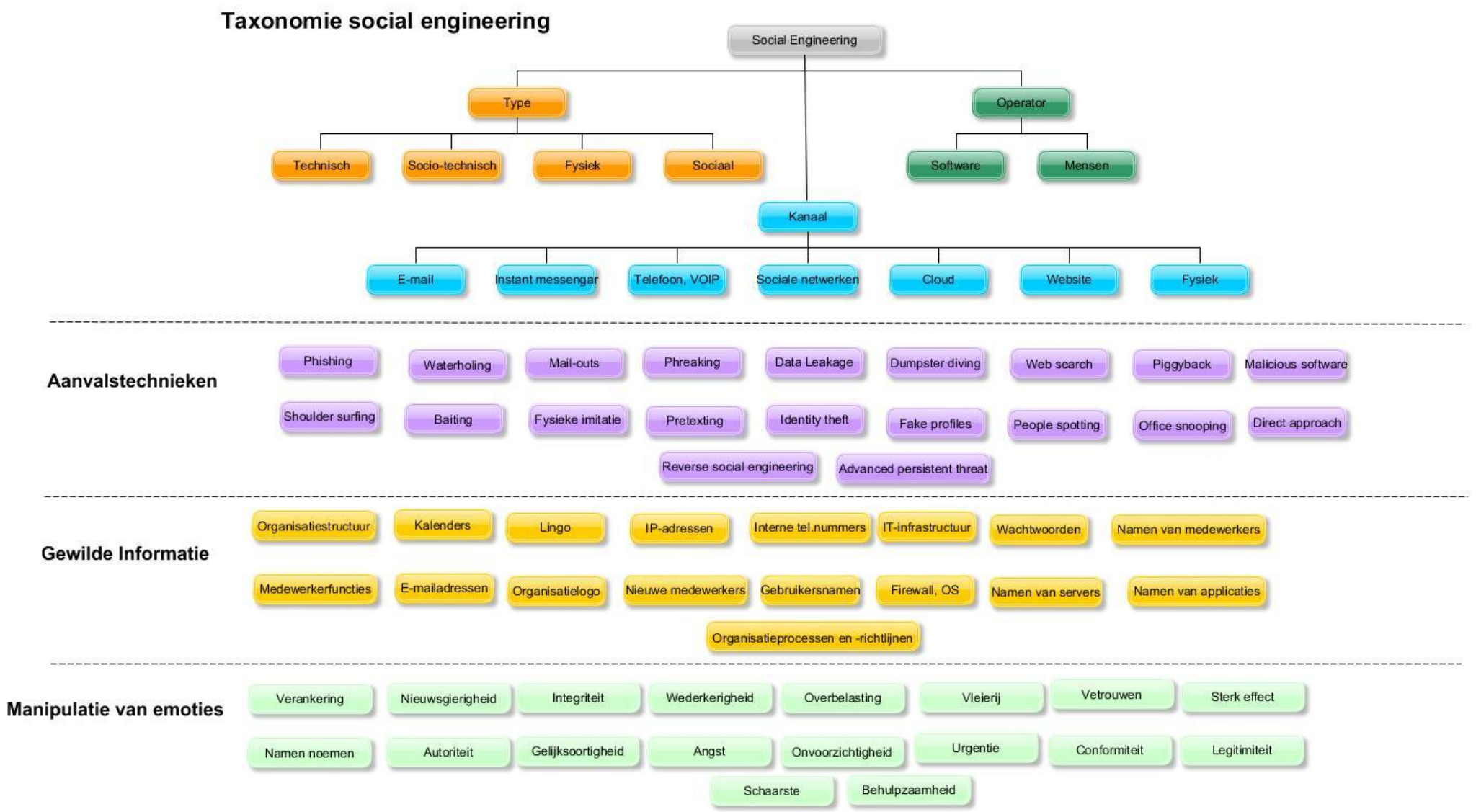
2. Welk proces wordt doorlopen bij social engineering?

3. De social engineer, wie is hij en welke motieven kan hij hebben?

4. Welke menselijke factoren worden door de social engineers uitgebuit?

5. Welke soorten aanvallen worden geclassificeerd als social engineering?

Naast het beantwoorden van de deelvragen heb ik een classificatie gemaakt die als input dient voor het empirisch vervolgonderzoek dat dient plaats te vinden voor mijn afstudeeropdracht. De classificatie maakt inzichtelijk welke typen socialengineeringaanvallen er zijn, welke operatoren gebruikt kunnen worden, de kanalen waardoor een aanval kan plaatsvinden, de gevonden aanvalstechnieken, de gewilde informatie en welke emoties van mensen worden gemanipuleerd door social engineers. Het overzicht maakt dan ook inzichtelijk welke risico's afgedekt dienen te worden om een organisatie zo goed mogelijk te beschermen tegen socialengineeringaanvallen. Dit classificatieoverzicht zal dan ook dienen als belangrijke input en is een van de uitgangspunten voor het komende empirische onderzoek.



Overzicht van mijn classificatie van aanvalstypen, - kanalen en - operatoren, gewilde infomatie en welke emoties gemanipuleeerd worden

Figuur 8: Classificatie van aanvalstypen, -kanalen en -operatoren, gewilde informatie en welke emoties die gemanipuleerd worden

Hoofdstuk 2 Risicomanagement inzake social engineering

Dit hoofdstuk geeft antwoord op de hoofdvraag van het literatuuronderzoek en de vijf deelvragen over risicomanagement met betrekking tot social engineering.

1. Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarop, waarmee, wat ontbeekt?

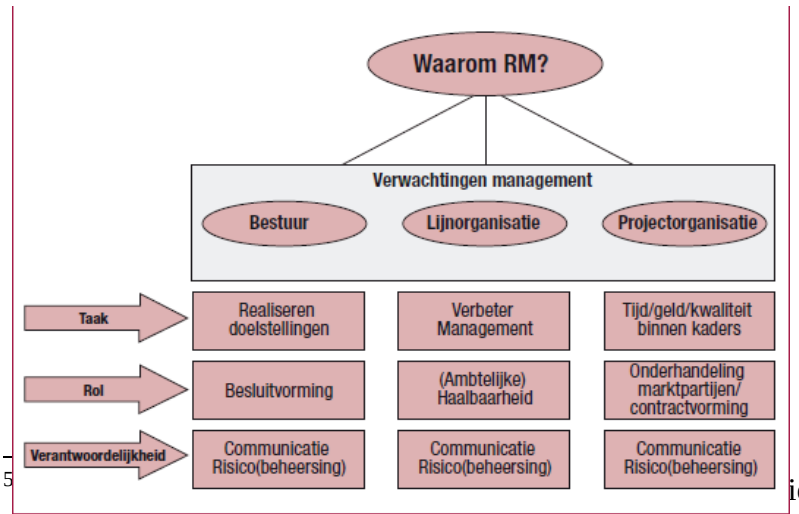
1. Wat is risicomanagement?
2. Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
3. Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?

In de eerste paragraaf staan een inleiding en de definitie van het begrip risicomanagement. Hier wordt als eerste naar gekeken om een goede indruk te krijgen van wat risicomanagement precies inhoudt. Vervolgens wordt ingegaan op risicomanagement specifiek gericht op social engineering. Daarna volgen twee paragrafen over technieken en modellen voor informatiebeveiligingsrisicomanagement en enterprise-risicomanagementmodellen en -technieken. Er wordt naar deze deelgebieden van risicomanagement gekeken aangezien tijdens de literatuurstudie bleek dat er geen risicomanagementmodellen specifiek voor social engineering bestaan. Daarna volgt een analyse van welke modellen geschikt zijn of uitgebreid kunnen worden specifiek voor social engineering.

Het hoofdstuk besluit met een conclusie waarin de hoofdvraag wordt beantwoord.

2.1 Wat is risicomanagement

In deze paragraaf 2.1 wordt deelvraag 1 m.b.t. risicomanagement beantwoord: Wat is risicomanagement?



De ISO 27002[5] definieert risico als een "combinatie van de waarschijnlijkheid van een gebeurtenis en het gevolg ervan". Deze verklaring bevat de volgende twee variabelen: een kans dat een gebeurtenis zal plaatsvinden en de gevolgen (impact) van deze gebeurtenis op de organisatie. De combinatie van deze twee

5 ...ionale standaard die richtlijnen en principes geeft voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie.

variabelen geeft de grootte van het risico.

Risico's kunnen afkomstig zijn uit verschillende bronnen: bijvoorbeeld de onzekerheid op de financiële markten, bedreigingen uit mislukte projecten, verstoring van de dienstverlening, ongevallen, natuurlijke oorzaken en rampen of opzettelijke aanvallen door social engineering.

Figuur 9. Waarom risicomanagement (Merle & Hiasma, 2009)

De ISO 31000-norm stelt dat een raamwerk noodzakelijk is voor een succesvolle implementatie. Het raamwerk is de basis voor het inbedden van risicomanagement in de organisatie, op alle niveaus. Dit raamwerk vormt het beleidskader en daarmee het mandaat voor de aansturing van alle risicomanagementprocessen in de organisatie (Merle & Hiasma, 2009)

Er zijn vele soorten risicomanagement, bijvoorbeeld informatiebeveiligingsrisicomanagement, enterprise-risicomanagement, projectrisicomanagement en risicomanagement op bouwprojecten.

2.2 Risicomanagement specifiek gericht op social engineering

In paragraaf wordt een gedeelte van deelvraag 2 m.b.t. risicomanagement beantwoord: Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
Malcom Allen schrijft het volgende over risicomanagement met betrekking tot social engineering (Allen, 2006).
Is er een effectieve manier om een organisatie volledig te beschermen tegen socialengineeringaanvallen? Het antwoord is 'nee', om de eenvoudige reden dat het niet uitmaakt welke controles worden uitgevoerd, er zal altijd de mogelijkheid zijn om de 'menselijke factor' te beïnvloeden door een sociale, politieke en/of cultureel gebeurtenis. Niettemin, zoals bij elke bedreiging, zijn er manieren om de kans op succes te verminderen. Dit kan worden bereikt door een analyse van de bedreiging en door kennis te hebben van zowel de technieken die kunnen worden gebruikt als de tegenmaatregelen die kunnen worden toegepast (Allen, 2006).

Tijdens mijn literatuuronderzoek ben ik op dezelfde conclusie uitgekomen. Er is naar mijn weten geen generiek model voor organisaties om zich te beveiligen tegen social engineering. Er zijn wel best practices, criteria, maatregelen, controles en richtlijnen gericht op risicomanagement met betrekking tot social engineering. Deze punten, die gevonden zijn in de literatuur en elders, worden in deze paragraaf doorgenomen.

Omdat er geen specifiek risicomanagementmodel bestaat op het gebied van social engineering heb ik gekeken naar op welke soortgelijke gebieden er wel risicomanagementmodellen bestaan. Zo bestaan wel modellen gericht op informatiebeveiligings- en enterprise-risicomanagement. Deze modellen zijn echter op een hoger niveau opgesteld en geven alleen een model/richtlijn hoe om te gaan met risico's binnen informatiebeveiliging en organisaties. Ze gaan niet specifiek in op een deelgebied als social engineering. Social engineering is wel een van de aspecten die informatiebeveiligings en enterprise-risicomanagement zouden moeten afdekken en naar mijn verwachting kan een van de modellen of een combinatie ervan worden gebruikt of uitgebreid om tot risicomanagement met betrekking tot social engineering te komen.

In de volgende paragrafen wordt ingegaan op deze risicomanagementmodellen om vervolgens te analyseren welk van deze modellen het meest geschikt is om te gebruiken of uit te breiden voor social engineering.

2.3 Informatiebeveiligingsmaatregelen tegen social engineering volgens NEN/ISO

In paragraaf wordt een gedeelte van deelvraag 2 m.b.t. risicomanagement beantwoord: Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
De Code voor Informatiebeveiliging NEN-ISO/IEC 27002 en 27005 beschrijft de volgende informatiebeveiligingsmaatregelen tegen social engineering (Disterer, 2013; Humphreys, 2008).

Voorafgaand aan het dienstverband:

- Vastleggen rollen en verantwoordelijkheden
- Screening
- Arbeidsvoorwaarden

Tijdens het dienstverband:

- Directieverantwoordelijkheid
- Bewustzijn, opleiding en training
- Disciplinaire maatregelen
- Zorg voor doeltreffende procedures voor het helpen van het personeel om met dit soort aanvallen om te gaan
- Zorg ervoor dat controles plaatsvinden en procedures aanwezig zijn en gevolgd worden om gevoelige en waardevolle informatie beschermen

Bij beëindiging of wijziging van het dienstverband:

- Beëindiging van verantwoordelijkheden
- Retournering van bedrijfsmiddelen
- Blokkering van toegangsrechten.

De Code voor Informatiebeveiliging geeft echter slechts een richtlijn en beschrijft niet wat de inhoud zou moeten zijn van een opleiding of training. De beschreven maatregelen vanuit NEN-ISO zijn dan ook verre van volledig.

2.4 Essentiële controles tegen social engineering

In paragraaf wordt een gedeelte van deelvraag 2 m.b.t. risicomanagement beantwoord: Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
Hieronder is een lijst van essentiële controles opgenomen die kunnen worden uitgevoerd door organisaties om zich te beschermen tegen een aanval. Deze lijst is samengesteld op basis van de verschillende wetenschappelijke bronnen die ik heb doorgenomen.

Essentiële controles	
Management buy-in	Fysieke beveiliging
Opleiding en bewustwording	Beveiligingsarchitectuur
Het beperken van datalekken	Incidentafhandelingsstrategie
Beveiligingscultuur	Beveiligingsbeleid

Tabel 9: Essentiële controles

Fysieke beveiliging	
Foto-identificatiepasjes	Biometrische toegangsdeuren
Beveiligingscamera's	Bezoekerspasjes
Aanmeldformulieren	

Tabel 10: Fysieke beveiliging

Beveiligingsbeleid

Wachtwoordmanagement	Twee-ogenprincipe
Anti-virus/-phishing	Verandermanagement
Informatieclassificatie	Documentafhandeling/-vernietiging
Clean desk	Locken van computer
Firewall-regels	E-mail-filtering
Encryptie	

Tabel 11: Beveiligingsbeleid

Management buy-In: managers moeten een duidelijk begrip krijgen van wat hun rol is in het definiëren van de benodigde beveiligingsmaatregelen. Dit inzicht moet ervoor zorgen dat de juiste beschermende maatregelen worden getroffen met betrekking tot de risico's van social engineering (Allen, 2006).

Fysieke beveiliging: een essentieel controlemiddel voor het beperken van de fysieke toegang van medewerkers, aannemers en bezoekers tot computerfaciliteiten en -systemen (Allen, 2006; Hinson, 2008). De organisatie moet effectieve fysieke beveiligingsmaatregelen nemen, zoals bezoekerslogs, begeleide toegang en antecedentenonderzoek (Gulati, 2003). Hier vallen onder:

- Foto-identificatiepasjes
- Biometrische toegangsdeuren
- Beveiligingscamera's
- Bezoekerspasjes
- Aanmeldformulieren

Opleiding en bewustwording: een eenvoudige oplossing die kan worden gebruikt om dergelijke aanvallen te voorkomen. Een goed opgezet programma voor opleiding en bewustwording zal zichzelf ongetwijfeld terugbetalen (Allen, 2006; Gulati, 2003; Hinson, 2008).

Beveiligingsarchitectuur: een goede en slim opgezette infrastructuurarchitectuur stelt het personeel in staat om zich te concentreren op belangrijke taken. De medewerkers weten met een goede architectuur precies hoe deze in elkaar zit en hoe de omgeving zal reageren bij incidenten. De oplostijd van incidenten zal hierdoor drastisch korter worden (Allen, 2006; Hinson, 2008).

Het beperken van datalekken: het verminderen van de hoeveelheid beschikbare specifieke gegevens zorgt ervoor dat een aanval niet de moeite waard is. Websites, openbare databases, internetregisters en andere publiek toegankelijke bronnen dienen alleen algemene informatie te bevatten (Allen, 2006).

Incidentafhandelingsstrategie: een gedocumenteerde incidentreactiestrategie zal ervoor zorgen dat een gebruiker onder druk precies weet welke procedures hij dient te volgen (Allen, 2006; Hinson, 2008).

Beveiligingscultuur: het bouwen van een informatiebeveiligingscultuur binnen een organisatie begint met mensen bewust te maken van veiligheid, hen te voorzien van instrumenten om te reageren en het stimuleren van de communicatie over en weer tussen beveiligingspersoneel, managers en medewerkers (Allen, 2006; Gulati, 2003; Hinson, 2008).

Beveiligingsbeleid: een gedegen veiligheidsbeleid zorgt voor een duidelijke richting waar medewerkers zich aan dienen te houden binnen een organisatie (Allen, 2006; Gulati, 2003). Er dienen richtlijnen en procedures te zijn voor:

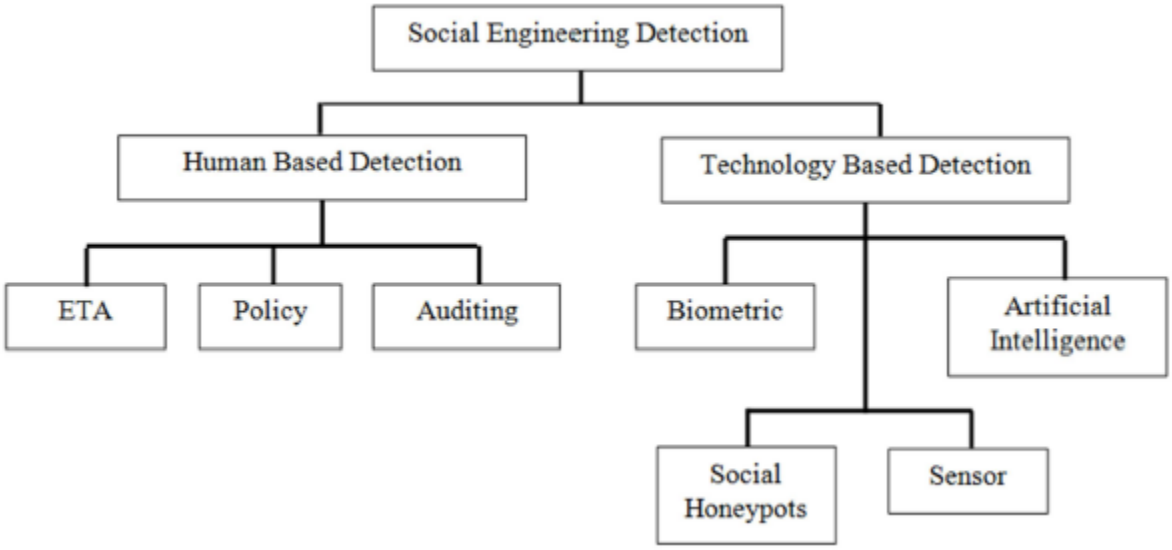
- ***Wachtwoordmanagement:*** richtlijnen zoals het aantal karakters dat en de aard daarvan die elk wachtwoord moet bevatten, hoe vaak een wachtwoord moet worden gewijzigd en zelfs een eenvoudige verklaring dat de medewerkers geen wachtwoorden moeten bekendmaken aan anderen (Gulati, 2003; Hinson, 2008).
- ***Twee-ogenprincipe:*** authenticatie voor hoog-risico-netwerkdiensten, zoals modem pools en VPN's, dienen een twee-ogenauthenticatie te gebruiken in plaats van vaste wachtwoorden (Hinson, 2008).
- ***Anti-virus/-phishing:*** meerdere lagen van virusafweer, zoals bij e-mailgateways en eindgebruiker-desktop, kunnen de dreiging van phishing- en andere socialengineeringaanvallen minimaliseren (Hinson, 2008).
- ***Verandermanagement:*** een gedocumenteerd verandermanagementproces is veiliger dan een ad-hocproces. Een ad-hocproces is gemakkelijker te misbruiken door een aanvaller (Hinson, 2008).
- ***Informatieclassificatie:*** een classificatiebeleid dient duidelijk te beschrijven welke informatie als gevoelig wordt beschouwd en hoe met deze informatie om moet worden gegaan (Gulati, 2003).
- ***Documentafhandeling/-vernietiging:*** gevoelige documenten en media moeten veilig worden afgevoerd/vernietigd en niet gewoon worden weggegooid in de reguliere kantoorprullenbak (Hinson, 2008).
- ***Clean desk:*** documenten dienen niet open en bloot op de bureaus van medewerkers te liggen. De documenten dienen veilig in kasten, achter slot en grendel, te worden opgeborgen (Gulati, 2003; Hinson, 2008).
- ***Locken van computer:*** als een medewerker niet in de buurt van zijn computer is, dient hij de computer te locken zodat andere personen hier geen gebruik van kunnen maken (Gulati, 2003; Hinson, 2008).
- ***Firewall-regels:*** het configureren en onderhouden van strenge firewallregels helpt om een aanvaller buiten de deur te houden. Tevens kunnen websites worden geblokkeerd die niet benodigd zijn tijdens en voor het werk (Zulkurnain et al., 2015).
- ***E-mailfiltering:*** opzetten en onderhouden van e-mail-spamfilters zal ervoor zorgen dat gebruikers minder snel ten prooi vallen aan phishing-aanvallen, ketting-e-mails, virussen of wormen die schade zouden kunnen veroorzaken (Zulkurnain et al., 2015).
- ***Encryptie:*** het beschermen van gevoelige informatie met sterke encryptietechnologie van ten minste 128 bits (Zulkurnain et al., 2015).

Verzekeringsbeleid: een organisatie kan een verzekering tegen cyberaanvallen en socialengineeringaanvallen afsluiten. De meeste verzekeraars zullen echter eisen dat het bedrijf richtlijnen en procedures implementeert om de dreiging van social engineering te verkleinen (Gulati, 2003).

Auditbeleid en -controles: als procedures, richtlijnen en beleid zijn opgesteld binnen een organisatie maar niemand zich hier aan houdt, dan levert dit beleid weinig toegevoegde waarde aan het verminderen van de risico's met betrekking tot socialengineeringaanvallen (Gulati, 2003).

2.5 Taxonomie aanvalsdetectie volgens Zulkurnain en anderen (Zulkurnain et al., 2015)

In paragraaf wordt een gedeelte van deelvraag 2 m.b.t. risicomanagement beantwoord: Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
Zulkurnain en anderen (Zulkurnain et al., 2015) hebben begin 2015 een taxonomie voor het detecteren van socialengineeringaanvallen opgesteld en gedeeld in het 'International Journal of Mathematics and Computational Science'. Dit schema ziet er als volgt uit.



Figuur 10: Taxonomie van de detectie van socialengineeringaanvallen

Volgens dit schema zijn er twee manieren waarop een aanval kan worden gedetecteerd, namelijk door mensen en door technologie. Vervolgens is de menselijke detectie opgedeeld in education, training and awareness (ETA), richtlijnen en auditing. De technologie is onderverdeeld in biometrisch, artificial intelligence, sensoren en social honeypots. Ik zal een aantal onderdelen kort toelichten, een groot aantal is eerder al aan bod gekomen en zal niet worden herhaald.

- ***Social honeypots:*** honeypot is een systeem dat is ontworpen om bestaande systemen te imiteren en aanvallers te verleiden om deze aan te vallen met als doel om de aanvalspatronen te leren herkennen. Een traditionele honeypot kan een website, netwerk of een computer zijn. Traditionele typen aanvallen zijn meestal: malware-aanvallen, database-aanvallen, en spam-aanvallen op een systeem. Niet-traditionele honeypotaanvallen richten zich op sociale media, phishing en identiteitsdiefstal (Zulkurnain et al., 2015)
- ***Sensoren:*** hiermee wordt de technologie bedoeld die in staat is om toegangspasjes, paspoorten en uniformen te herkennen en goed te keuren (Zulkurnain et al., 2015).
- ***Artificial intelligence (AI):*** dit zijn systemen die bestaande gegevens analyseren en beoordelen, denk hierbij aan het herkennen van phishing mails via headerinformatie of inhoud. Deze techniek staat nog in de kinderschoenen maar er wordt verwacht dat deze zich in de toekomst snel zal ontwikkelen (Zulkurnain et al., 2015).
- ***Biometrisch:*** biometrische technologie herkent iemand met behulp van zijn unieke biologische kenmerken, zoals vingerafdrukken, stem en gezicht (Zulkurnain et al., 2015).

2.6 Informatiebeveiligingsrisicomanagement (ISRM)

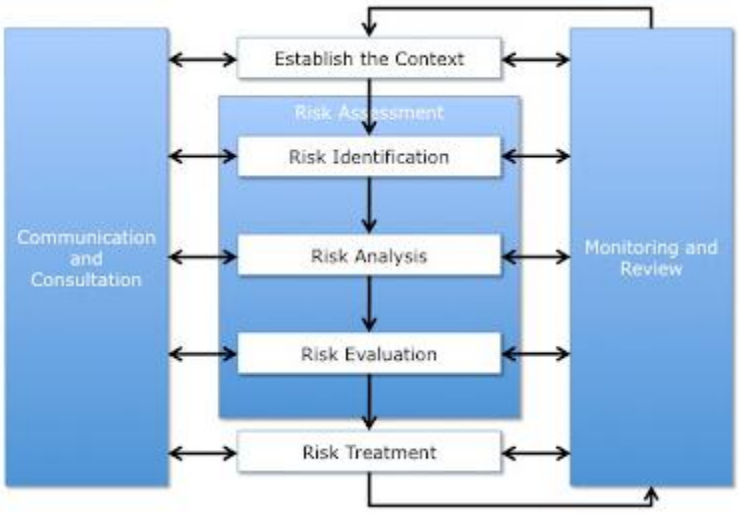
In deze paragraaf wordt een gedeelte van deelvraag 3 m.b.t. risicomanagement beantwoord: Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?
De bescherming van informatiebronnen tegen complexe en snel evoluerende bedreigingen is een belangrijke uitdaging voor de moderne organisatie. De belangrijkste aandachtspunten voor organisaties zijn de lekkage of wijziging van gevoelige informatie en de verstoring of vernietiging van bedrijfskritische IT-services.

In principe maakt het proces van informatiebeveiligingsrisicomanagement (ISRM) het mogelijk voor organisaties om te bepalen of ze hun informatie(systemen) op de meest effectieve en kostenefficiënte manier beschermen. De risico's zijn de potentiële gevolgen die bedreigingen en kwetsbaarheden van informatiesystemen kunnen veroorzaken waardoor schade wordt toegebracht aan de organisatie (Webb, Ahmad, Maynard, & Shanks, 2014).

De definitie van ISRM die in dit literatuuronderzoek wordt gebruikt, is: informatiebeveiligingsrisicomanagement is het belangrijkste middel waarmee organisaties de vertrouwelijkheid, integriteit en beschikbaarheid van informatiebronnen behouden (Webb et al., 2014).

Volgens Whitman en Mattord (Whitman & Mattord, 2004) en de internationale standaard ISO 31000 risicomanagementproces bestaan de kernactiviteiten van het ISRM-proces uit de volgende fasen.

1. ***Vaststellen van de context:*** opstellen van de contextgerelateerde programmadoelen en -activiteiten.
2. ***Risico-identificatie:*** het identificeren van de veiligheidsrisico's.
3. ***Risicoanalyse:*** analyseren van de risico's.
4. ***Risico-evaluatie:*** prioriteren van de geïdentificeerde risico's.
5. ***Risicobehandeling:*** bepalen van de meest kosteneffectieve manier van het beheersen van het risico (bijvoorbeeld vermijding, mitigatie, overdracht, negeren).
6. ***Risico-reviewing:*** het monitoren van veranderingen in het risicobeheersysteem.
7. **Communicatie en consultatie**: het communiceren met de betrokken partijen over de risico's.



Figuur 11: Risicomanagementmodel

2.7 PDCA-model

In deze paragraaf wordt een gedeelte van deelvraag 3 m.b.t. risicomanagement beantwoord: Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?
In de jaren dertig van de vorige eeuw ontwikkelde de Amerikaan Walter Shewhart de PDCA-cirkel.
Deze 'plan-do-check-act'-cirkel is een instrument om een proces te verbeteren. De PDCA-cirkel is wellicht de bekendste checklist voor 'continu verbeteren' (Terhurne, 2005). De cirkel bestaat uit vier fasen (Humphreys, 2008; Terhurne, 2005):

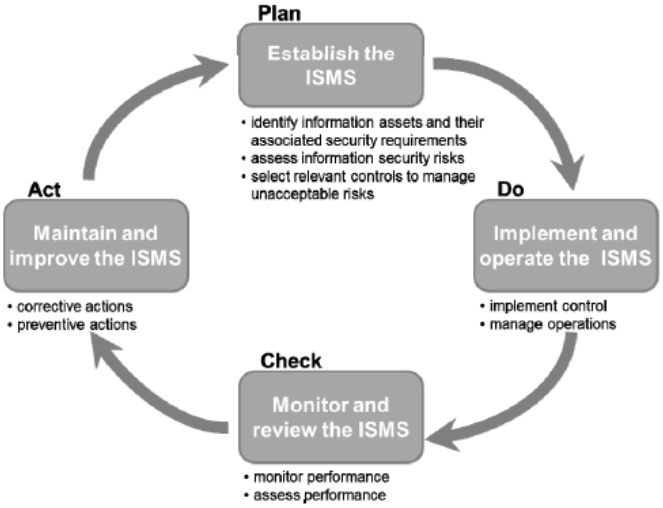
Plan: wat gaat er verkeerd? Bepaal de echte oorzaak van een probleem, genereer mogelijke oplossingen en plan een verandering of een test gericht op verbetering.

Do: voer de verandering in of voer de test uit.

Check: controleer of het beoogde resultaat bereikt is. Ga na of er iets verkeerd ging en zo ja, wat ging er dan verkeerd? Wat is het leereffect?

Act: als de test succesvol was, implementeer dan de verandering in de breedte. Was de test geen succes, herhaal dan deze stap met behulp van hetgeen geleerd is in de vorige stap.

ISO/IEC 27002 heeft de PDCA-cirkel overgenomen en opgenomen in de standaard. Daarnaast geeft ISO nog een uitgewerkt controlegebied 'proces' erbij (Humphreys, 2008).



Figuur 13: PDCA-cirkel (Disterer, 2013)

Figuur 12. Controlegebieden van informatiebeveiliging (Humphreys, 2008)

Volgens Humphreys (Humphreys, 2008) gaat het voor een organisatie bij het beoordelen van de risico's om het identificeren van de activa, de bedreigingen, de kwetsbaarheden en het berekenen van het:

- Risico van blootstelling = de waarschijnlijkheid dat een beveiligingslek (risico) echt wordt uitgebuit voor één of meer activa van de organisatie (Humphreys, 2008).
- Risiconiveau = (risico van blootstelling) x (de gevolgen van dit risico als het zich voordoet, oftewel de impact op de organisatie) (Humphreys, 2008).

2.8 Risicomanagement ISO/Humphreys

In deze paragraaf wordt een gedeelte van deelvraag 3 m.b.t. risicomanagement beantwoord: Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?
Het proces van risicomanagement dat volgens Humphreys (Humphreys, 2008) gevolgd dient te worden is weergegeven in figuur 14 en bestaat uit de volgende vier stappen:

1. Schat de risico's in en prioriteer deze
2. Behandel de risico's
3. Selecteer en implementeer controlemechanismen zodat deze risico's worden afgedekt
4. Monitor de risico's en schat deze opnieuw in en review ze.

Figuur 14: Risicomanagementproces (Humphreys, 2008)

De impact kan zijn: een financieel verlies, diefstal of beschadiging van informatie, verlies van imago en reputatie, etc.
Zodra de risico's zijn geïdentificeerd, dient een risicoregister te worden samengesteld dat deze risico's in de volgorde van hun ernst registreert en prioriteert. Daarnaast kunnen details van de aard van de risico's, de impactinschatting en andere gegevens die nuttig zijn voor het opbouwen van een risicoprofiel voor organisatie worden opgenomen (Humphreys, 2008).

Het is zeer belangrijk dat een organisatie beschikt over een uitgebreid incidentafhandelingsmanagementproces. Dit is een van de eisen van de ISO/IEC 27001-certificering (Humphreys, 2008). Dit proces omvat (Humphreys, 2008):

- Identificatie, detectie en rapportage van incidenten
- Analyse en evaluatie van het incident
- Reageren op het incident
- Herstel en sanering van het incident
- Leren van het incident.

2.9 Enterprise-risicomanagement/COSO

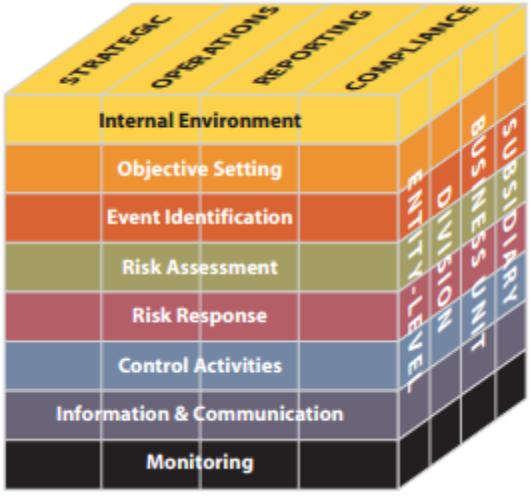
In deze paragraaf wordt een gedeelte van deelvraag 3 m.b.t. risicomanagement beantwoord: Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?
Een ander veelgebruikt model is het model van het Committee of Sponsoring Organizations of the Treadway Commission (COSO). ***Dit model wordt aangeduid als een enterprise-risicomanagementmodel*** en is dus niet specifiek ontworpen voor informatiebeveiliging of social engineering. Desalniettemin is het een model dat door veel organisaties wordt ingezet voor risicomanagement en daarom zal het kort worden besproken (Steinberg, Everson, Martens, & Nottingham, 2004).

Dit model kan ook worden gebruikt voor informatiebeveiligingsrisicomanagement.

De achterliggende gedachte van enterprise-risicomanagement is dat iedere onderneming bestaat om waarde te creëren voor haar aandeelhouders. Alle ondernemingen worden geconfronteerd met onzekerheden en de uitdaging voor het management is om vast te stellen hoeveel onzekerheid acceptabel is, terwijl er gestreefd wordt naar groei van de aandeelhouderswaarde. Onzekerheid biedt zowel risico's als kansen, met de potentie om zowel waarde te verhogen als deze uit te hollen. Enterprise-risicomanagement stelt het management in staat om op een efficiënte wijze met deze onzekerheid en de hieraan verbonden risico's en kansen om te gaan en daarbij de capaciteit om waarde te creëren te versterken (Steinberg et al., 2004).

De verschillende fasen van het COSO model:

- Enterprise-risicomanagement is een proces dat voortdurend stroomt door de gehele onderneming
- Het wordt bewerkstelligd door mensen op elk niveau in een organisatie
- Het wordt toegepast bij de formulering van strategische doelstellingen
- Het wordt toegepast in de hele onderneming, op elk niveau en in elk onderdeel en omvat een portfoliovisie op risico op het niveau van de onderneming
- Het is ontworpen om potentiële gebeurtenissen te herkennen die, als ze voorkomen, van invloed zijn op de onderneming en zodoende het risico te beheersen binnen de risicoacceptatiegraad
- Het stelt het management van een onderneming en de raad van bestuur in staat om een redelijke zekerheid aan te bieden
- Het zorgt ervoor dat de onderneming ingericht is om de doelstelling te behalen in een of meer afzonderlijke maar wel overlappende categorieën.



Figuur 15: Het COSO-model

Enterprise-risicomanagement bestaat uit acht met elkaar verbonden componenten. Deze componenten zijn afgeleid van de wijze waarop het management een onderneming runt en zijn verbonden met het managementproces. De componenten zijn (Steinberg et al., 2004):

- ***Interne omgeving:*** de interne omgeving omvat de

toon van een organisatie en legt de basis voor de wijze waarop risico's worden beschouwd en aangepakt door de mensen van een onderneming, inclusief risicobeheer en risicoacceptatiegraad, integriteit, ethische normen en waarden en de omgeving waarin zij opereren (Steinberg et al., 2004).

- ***Formuleren van doelstellingen:*** doelstellingen moeten bestaan voordat het management potentiële gebeurtenissen die invloed hebben op het behalen van deze doelen kan erkennen. Enterprise-risicomanagement bewerkstelligt dat het management over een proces beschikt dat doelstellingen vastlegt, dat ervoor zorgt dat gekozen doelstellingen afgestemd zijn op de missie en de missie ondersteunen en consistent zijn met de risicoacceptatiegraad (Steinberg et al., 2004).

- ***Identificeren van gebeurtenissen***: interne en externe gebeurtenissen die invloed hebben op het behalen van de doelstellingen van de ondernemingen moeten worden geïdentificeerd, daarbij onderscheid makend tussen risico's en kansen. Kansen worden teruggekoppeld naar het strategie- en/of doelstellingenformuleringsproces (Steinberg et al., 2004).

- ***Risicobeoordeling:*** risico's worden geanalyseerd, rekening houdend met hun waarschijnlijkheid en impact, als basis voor het vaststellen hoe deze zouden moeten worden beheerst. De inherente risico's en restrisico's worden ingeschat (Steinberg et al., 2004).

- ***Reactie op risico:*** het management selecteert de reacties op het vermijden, accepteren, verminderen of delen van risico's waarbij een set acties wordt ontwikkeld om risico's af te stemmen op de risicotolerantie en risicoacceptatiegraad (Steinberg et al., 2004).

- ***Beheersingsactiviteiten:*** richtlijnen en procedures worden geformuleerd en geïmplementeerd om te waarborgen dat de reacties op risico's effectief worden uitgevoerd (Steinberg et al., 2004).

- ***Informatie en communicatie:*** relevante informatie wordt geïdentificeerd, verzameld en gecommuniceerd in een vorm die en tijdsbestek dat mensen in staat stellen hun verantwoordelijkheden

uit te voeren. Effectieve communicatie vindt ook in ruimere zin plaats, horizontaal, verticaal en bilateraal binnen een onderneming (Steinberg et al., 2004).

- ***Bewaking:*** de totaliteit van het enterprise-risicomanagement wordt bewaakt en wijzigingen worden waar nodig aangebracht. Bewaking wordt mogelijk gemaakt door voortdurende managementactiviteiten, afzonderlijke evaluaties of beide (Steinberg et al., 2004).

2.10 Vergelijking en beoordeling van de modellen voor hergebruik met betrekking tot social engineering

In deze paragraaf wordt een gedeelte van deelvraag 3 m.b.t. risicomanagement beantwoord: Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?
De volgende modellen zijn behandeld in de vorige paragrafen:

- Model 1: COSO, enterprise-risicomanagementmodel (Steinberg et al., 2004)
- Model 2: Risicomanagementmodel (Humphreys, 2008)
- Model 3: PDCA-cirkel-model (Humphreys, 2008)
- Model 4: Informatierisicomanagementmodel (Whitman & Mattord, 2004) en ISO 31000.

De vraag die beantwoord dient te worden in deze paragraaf is welk model of welke combinatie van modellen kan worden gebruikt en het meest geschikt is voor risicomanagement op het gebied van social engineering.

De methode om deze vraag te beantwoorden is het vergelijken van de modellen. Ik ben namelijk van mening dat drie van de vier modellen voldoen en gebruikt kunnen worden voor risicomanagement op het gebied van social engineering. Door de modellen met elkaar te vergelijken kan inzichtelijk worden gemaakt wat de verschillen zijn tussen de modellen en welk model voor dit literatuuronderzoek en het empirische vervolgonderzoek het meest geschikt is.

In principe dekken de modellen vrijwel dezelfde gebieden af. Echter, de modellen 1 en 4 zijn iets uitgebreider met relevante additionele stappen dan de modellen 2 en 3. Model 3 wordt in de praktijk voornamelijk gebruikt als incidentenafhandelingsmodel, terwijl de modellen 1, 2 en 3 risicomanagementmodellen zijn.
Zowel model 2 als 3 vallen als eerste af aangezien de modellen 1 en 4 net iets completer zijn. De stappen interne-omgevingsanalyse, opstellen van doelstellingen en informatie en communicatie zijn naar mijn mening relevante stappen om te gebruiken binnen een organisatie.

Het COSO-model 1 heeft één extra stap ten opzichte van het ISO-model 4. Deze stap houdt het volgende in. De interne omgeving omvat de toon van een organisatie en legt de basis voor hoe risico's worden beschouwd en aangepakt door de mensen in een onderneming, inclusief risicobeheer en risicoacceptatiegraad, integriteit, ethische normen en waarden en de omgeving waarin zij opereren.

Deze extra stap is naar mijn mening wel een heel belangrijke stap, aangezien hier wordt vastgesteld hoe binnen de organisatie met risico's wordt omgegaan en waar de verschillende verantwoordelijkheden voor het afdekken van de risico's liggen binnen de organisatie.

Model 1 is dan ook net iets uitgebreider dan model 4 vanwege de extra stap van de interne-omgevingsanalyse. In dit literatuuronderzoek wordt dan ook model 1 in combinatie met model 3 aanbevolen als modellen die kunnen worden gebruikt om risicomanagement op het gebied van social engineering inzichtelijk te maken. In het empirisch vervolgonderzoek zullen de modellen 1 en 3 daadwerkelijk worden gebruikt om de gevonden risico's uit hoofdstuk 1 af te dekken met de gevonden best practices, criteria, maatregelen, controles en richtlijnen die zijn gevonden in hoofdstuk 2, gericht op risicomanagement op het gebied van social engineering. Binnen het ministerie van Veiligheid en Justitie en dat van Binnenlandse Zaken en Koninkrijksrelaties zal dit model vervolgens worden toegepast en wordt bekeken hoe deze ministeries met social engineering omgaan.

Model 1 COSO	**Model 2 risicomanagement**	**Model 3 PDCA**	**Model 4 ISO**
Interne-omgevingsanalyse	X	X	X
Formuleren van doelstellingen	X	X	Vaststellen van de context
Identificeren van gebeurtenissen	Schat de risico's in en prioriteer deze	Plan	Risico-identificatie
Risicobeoordeling	Schat de risico's in en prioriteer deze	Plan	Risicoanalyse, Risico-evaluatie
Reactie op risico	Behandel de risico's	Do, Act	Risicobehandeling
Beheersingsactiviteiten, bewaking	Monitor de risico’s en schat deze opnieuw in en review ze regelmatig. Selecteer en implementeer controlemechanismen zodat deze risico's worden afgedekt	Check, Act	Risico-reviewing en monitoren van de risico’s
Informatie en communicatie	X	X	Communicatie en consultatie

Tabel 2: Vergelijking modellen

2.11 Conclusie hoofdstuk 2

In hoofdstuk 2 is besproken wat risicomanagement in het algemeen inhoudt, welke risicomanagementmodellen specifiek voor social engineering aanwezig zijn en welke andere risicomanagementmodellen als basis kunnen dienen voor een risicomanagementmodel dat specifiek is voor social engineering.

De volgende drie deelvragen zijn beantwoord in dit hoofdstuk:

1. Wat is risicomanagement?

2. Welke risicomanagementmodellen zijn ontwikkeld voor social engineering?
3. Welke risicomanagementtechnieken/-modellen kunnen goed worden toegepast met betrekking tot social engineering?

Uit dit onderzoek kwam naar voren dat er weinig literatuur beschikbaar is over risicomanagement op het gebied van social engineering.
Er is geen generiek model voor organisaties om zich te beveiligen tegen social engineering. Er zijn wel best practices, criteria, maatregelen, controles en richtlijnen gericht op risicomanagement met betrekking tot social engineering. Deze zaken zijn echter nergens volledig en allesomvattend in de praktijk, literatuur of een model vastgelegd. Er ontbreekt dan ook een gevalideerd overzicht/model waarmee iedere organisatie overweg kan en zich kan verdedigen tegen social engineering.

De hoofdvraag van dit literatuuronderzoek *'Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarop, waarmee, wat ontbeekt?'* kan dan ook volmondig met 'ja' worden beantwoord. Er ontbreekt een risicomanagementmodel dat specifiek social engineering aangaat. Ook ontbreekt een totaaloverzicht van alle essentiële controles en welke aanvallen/technieken/emoties worden afgedekt door gebruik te maken van deze controles.

Na de analyse van vier generieke risicomanagementmodellen ben ik van mening dat het COSO-model het meest in aanmerking komt als basis voor een generiek socialengineeringrisicomodel.

Hoofdstuk 3 De gevolgen van social engineering voor organisaties

In dit hoofdstuk worden de volgende deelvragen beantwoord:

- Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties?
- Hoe vaak komen socialengineeringaanvallen voor bij organisaties?
- Hoe gaan verzekeringsmaatschappijen en banken om met risicomanagement met betrekking tot uitkeringen na een socialengineeringaanval?

De vragen worden beantwoord door een aantal recente onderzoeken die zijn uitgevoerd door verschillende organisaties te analyseren. Ik focus in die onderzoeken op aanvallen die mensen ervaren als social engineering en die bedrijven veel geld kosten. De onderzoeken gaan over de impact van social engineering voor het onderzochte bedrijf. In de onderzoeken wordt hetzelfde verstaan onder en bedoeld met social engineering als in hoofdstuk 1 is besproken.

De dreiging van op technologie gebaseerde beveiligingsaanvallen is bekend bij veel IT-professionals en IT security-specialisten van hedendaagse mkb-bedrijven, grote organisaties en multinationals. Organisaties maken gebruik van de expertise van medewerkers, instrumenten en processen om de risico's van deze dreiging te beheersen. De risico's van socialengineeringaanvallen zijn echter een grote uitdaging voor alle organisaties, aangezien de aanvallen afhankelijk zijn van menselijk gedrag en zich richten op kwetsbare werknemers in plaats van op technologie.

3.1 Onderzoek 1: Dimensional research

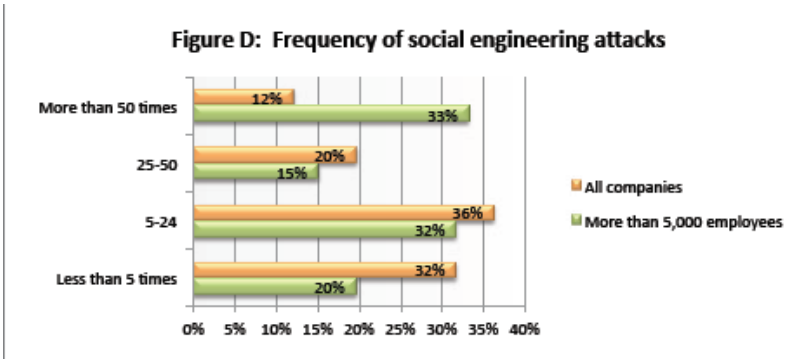
In deze paragraaf wordt een gedeelte van deelvraag 1 en 2 m.b.t. organisaties beantwoord: 1.Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties? 2. Hoe vaak komen socialengineeringaanvallen voor bij organisaties?

Het volgende verslag, opgesteld door Dimensional Research, is gebaseerd op een wereldwijd onderzoek onder 853 IT-professionals in de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië, Nieuw-Zeeland en Duitsland tijdens de maanden juli en augustus van 2011. Het doel van het onderzoek was tweeledig (Research, 2011):

- Het verzamelen van gegevens over de perceptie van socialengineeringaanvallen
- De impact van deze socialengineeringaanvallen op het bedrijfsleven analyseren.

De belangrijkste uitkomsten uit het onderzoek zijn:
Socialengineeringaanvallen komen vaak voor en kosten organisaties veel geld (Research, 2011)

- 48% van de grote bedrijven (>5000 medewerkers) en 32% van de bedrijven van alle groottes hebben in de periode van 2009-2011 meer dan 25 socialengineeringaanvallen ondervonden.

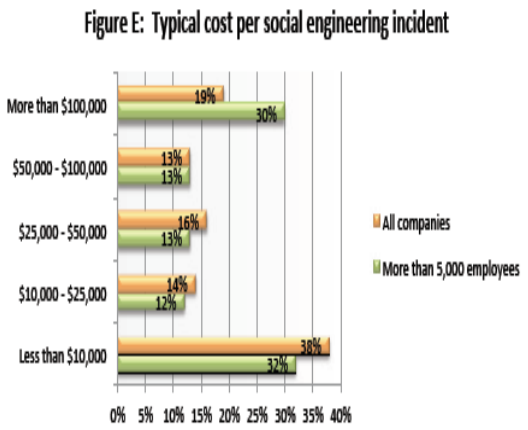


- 48% van alle deelnemers noemt een gemiddelde kostprijs per incident van meer dan $25.000 USD.
- 30% van de grote bedrijven noemt een kostprijs per incident van meer dan $100.000 USD.

Figuur 16: Frequentie van socialengineeringaanvallen

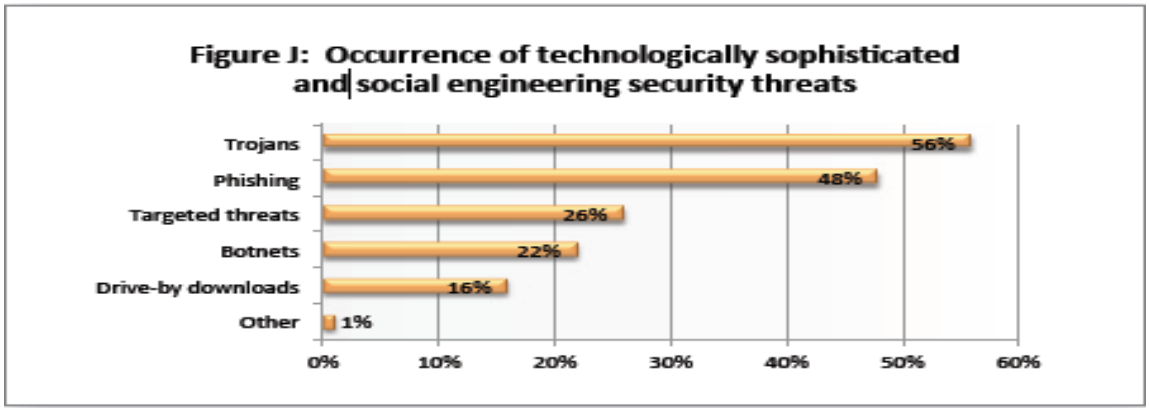
Nieuwe medewerkers zijn het meest vatbaar voor socialengineeringtechnieken/-aanvallen ([Research, 2011](#))

Nieuwe medewerkers hebben 60%, externen 44%, managers 38%, human research 33% en IT-personeel 22% kans om ten prooi te vallen aan socialengineeringtechnieken/-aanvallen.



Figuur 17: Kosten per socialengineeringaanval

Verder concludeerde Dimensional Research dat organisaties in alle sectoren en van alle groottes een verscheidenheid van zowel technologische aanvallen als socialengineeringaanvallen ervoeren. Dit wijst volgens Dimensional Research op een duidelijke behoefte om zowel de technologische als de socialengineeringrisico's te kunnen beheersen/controleren. Figuur 18 laat zien wat de meestvoorkomende aanvallen waren bij de onderzochte organisaties ([Research, 2011](#)).



Figuur 18: Voorvallen van technologische en socialengineeringaanvallen ingedeeld naar soort

3.2 Onderzoek 2: Ponemon en IBM

In deze paragraaf wordt een gedeelte van deelvraag 1 en 2 m.b.t. organisaties beantwoord: 1.Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties? 2. Hoe vaak komen socialengineeringaanvallen voor bij organisaties?

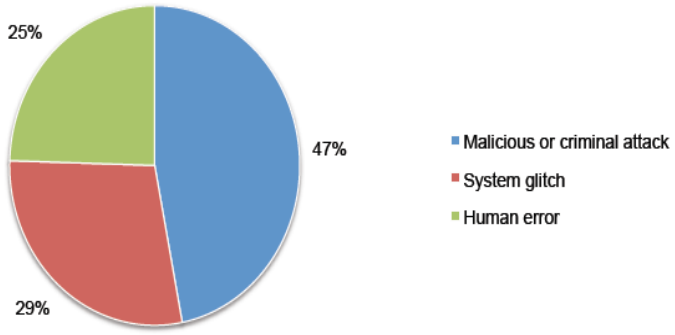
Een ander interessant onderzoek dat ik heb gevonden gaat over data-inbreuken[6]. Dat onderzoek is uitgevoerd in 2014 en gepubliceerd in 2015 door de organisaties Ponemon en

[6] Een data-inbreuk (data breach) wordt gedefinieerd als een gebeurtenis waarin de naam en het medisch dossier en/of een financieel record of betaalkaart van een individu mogelijk onder ogen of in het bezit is gekomen van personen die daar geen recht toe hebben, in elektronische of papieren vorm.

IBM. 350 bedrijven zijn onderzocht afkomstig uit de volgende 11 landen: de Verenigde Staten, het Verenigd Koninkrijk, Duitsland, Australië, Frankrijk, Brazilië, Japan, Italië, India, Verenigde Arabische Emiraten, Saoedi-Arabië en Canada. Alle deelnemende organisaties ervoeren een data-inbreuk variërend van circa 2200 tot iets meer dan 101.000 gecompromitteerde records[7] (Institute, 2015).

De belangrijkste resultaten van dit onderzoek zullen wederom worden besproken (Institute, 2015).

1. Het verlies van klanten verhoogt de kosten van data-inbreuken. Van 1,45 miljoen USD in 2014 naar 1,57 miljoen in 2015.
2. 47% van alle inbreuken werd veroorzaakt door kwaadaardige of criminele aanvallen.
3. De gemiddelde kosten om een kwaadaardige/criminele aanval op te lossen is $170 USD per record.
4. De gemiddelde kosten van een data-inbreuk zijn $3,79 miljoen USD.

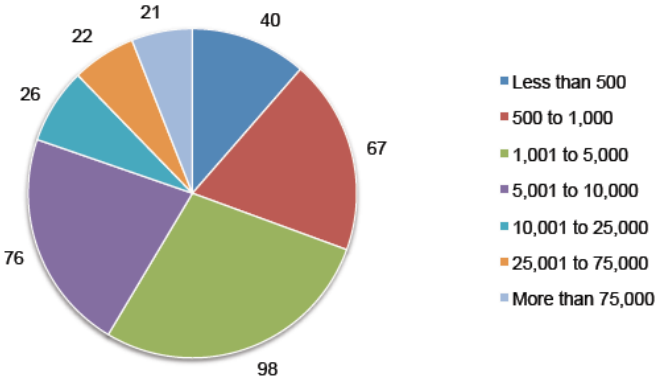


Figuur 19: Percentage aanvallen

De meestvoorkomende kwaadaardige/criminele aanvallen waren: malware infections, criminal insiders, phishing/social engineering en SQL injection (Institute, 2015).

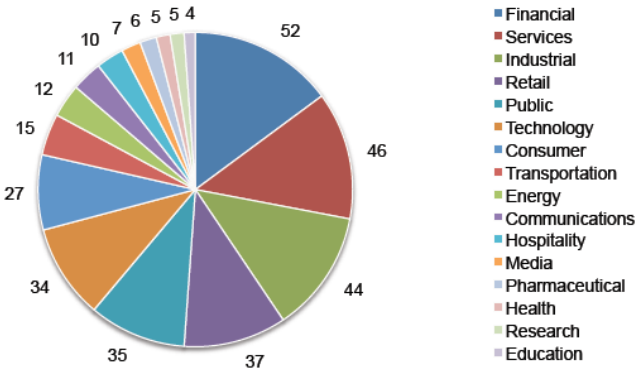
3.3 Onderzoek 3: Ponemon en Hewlett Packard

In deze paragraaf wordt een gedeelte van deelvraag 1 en 2 m.b.t. organisaties beantwoord: 1.Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties? 2. Hoe vaak komen socialengineeringaanvallen voor bij organisaties?
Een ander onderzoek is uitgevoerd wederom door de organisatie Ponemon, echter ditmaal in samenwerking met Hewlett Packard.
De studie focust zich op de kosten van cybercrime voor organisaties en is uitgevoerd in 2014. Voor dit literatuuronderzoek is uiteraard het gedeelte over social engineering belangrijk.
De studie werd uitgevoerd bij 257 organisaties. De organisaties kwamen uit de volgende landen: de Verenigde Staten, het Verenigd Koninkrijk, Duitsland, Australië, Japan, Frankrijk en de Russische Federatie (Institute, 2014). De sector en grootte van de deelnemende organisaties zijn te zien in de figuren 18 en 19.



Figuur 21: Grootte van de bedrijven

[7] Een gecompromitteerd record is een record waarvan de ve

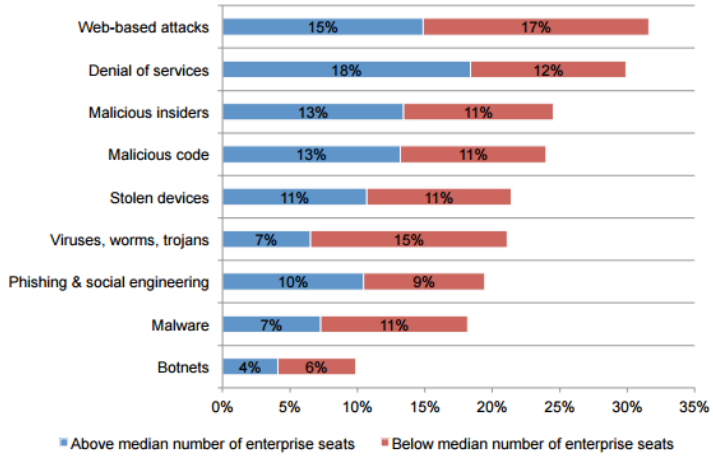


Figuur 20: Verdeling van organisaties naar sector

De belangrijkste resultaten van dit onderzoek worden hieronder beschreven.

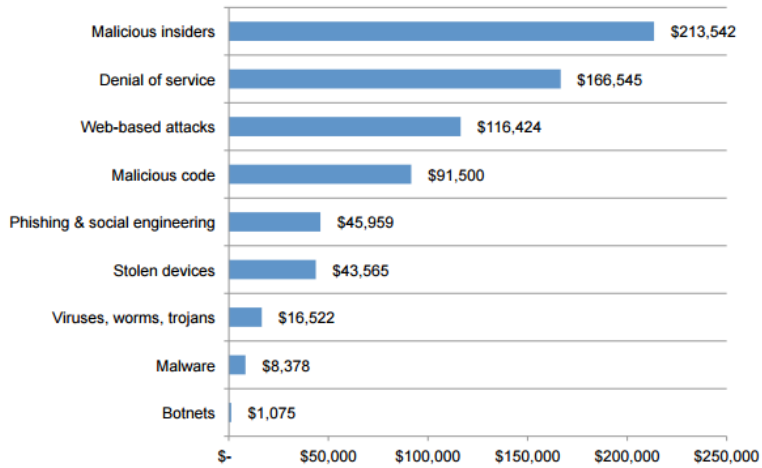
Een van de constateringen uit de studie (die te zien is in figuur 21) is dat er een verschil is tussen grote en kleine organisaties betreffende de kosten die zij moeten maken naar aanleiding van aanvallen die deze organisaties hebben ervaren. De mediaan is 5800 medewerkers, blauw zijn grote organisaties en rood zijn kleine organisaties. Voor socialengineeringaanvallen ligt dit percentage vrijwel gelijk (Institute, 2014).

De vraag is echter wat precies onder social engineering wordt verstaan in de studie, dit wordt niet verduidelijkt. Malicious insiders, stolen devices, viruses, worms en trojans kunnen bijvoorbeeld met behulp van social engineering zijn bewerkstelligd.



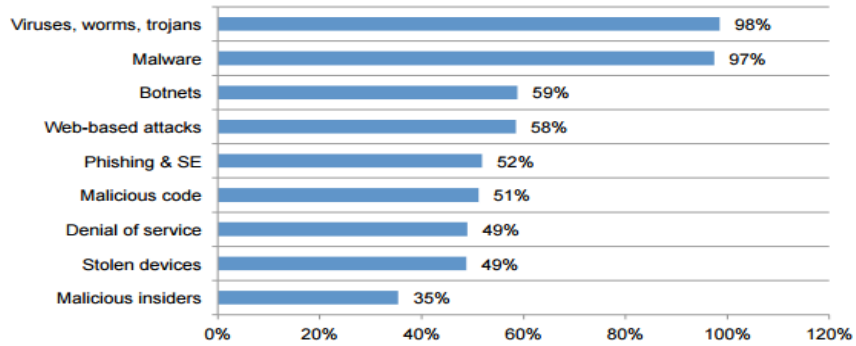
Figuur 22: Organisatorische omvang beïnvloedt de kosten van soorten aanvallen

Figuur 23 (hieronder) toont de gemiddelde kosten per soort aanval. Voor social engineering wordt aangegeven dat de gemiddelde kosten per aanval op $45.959 USD uitkomen. Dit is plek vijf uit negen van de onderzochte aanvallen. De kosten van een aanval bestaan uit directe en indirecte kosten. Directe kosten zijn kosten die meteen worden gemaakt, zoals het inhuren van forensisch deskundigen, een advocatenkantoor of het aanbieden van schadevergoedingen. Indirecte kosten omvatten de tijd, moeite, capaciteit en andere organisatorische hulpmiddelen die de organisatie besteed tijdens het oplossen van de data-inbreuk. Indirecte kosten omvatten ook het verlies van goodwill, imagoschade en klantverloop.



Figuur 23: Gemiddelde kosten per soort aanval

Ook werd aan alle 257 organisaties gevraagd welke soorten aanvallen zij hadden ondervonden in de onderzochte periode. 52% van de onderzochte organisaties gaf aan slachtoffer te zijn geweest van socialengineeringaanvallen (phishing en social engineering). De resultaten staan in figuur 24 (Institute, 2014).



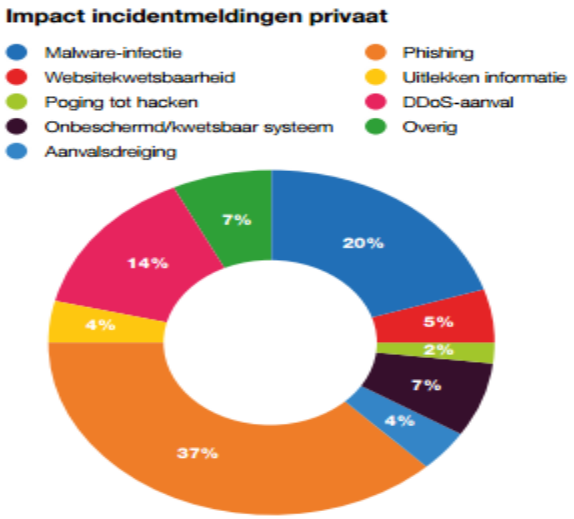
Figuur 24: Percentage organisaties die zijn aangevallen, naar soort aanval

3.4 Onderzoek 4: Capgemini

In deze paragraaf wordt een gedeelte van deelvraag 1, 2 en 3 m.b.t. organisaties beantwoord: 1.Welke risico's zijn verbonden aan socialengineeringaanvallen voor organisaties? 2. Hoe vaak komen socialengineeringaanvallen voor bij organisaties? 3. Hoe gaan verzekeringsmaatschappijen en banken om met risicomanagement met betrekking tot uitkeringen na een socialengineeringaanval?

Uit een onderzoek dat Capgemini in opdracht van verzekeringsmaatschappij Interpolis in Nederland heeft uitgevoerd, blijkt dat 37% van de onderzochte organisaties een phishing-aanval had ondervonden. Phishing valt onder social engineering (Capgemini, 2015).

Socialengineeringaanvallen komen dus vaak voor en kosten ook veel geld per incident. De vraag is dan ook hoe



Figuur 25: Impact incidentmeldingen

verzekeringsmaatschappijen hiermee omgaan. Hiervoor heb ik op verschillende sites van verzekeringsmaatschappijen gekeken. Bijna alle verzekeraars bieden aparte cybersecurity-verzekeringen aan. Hier valt social engineering ook onder. Het Verbond van Verzekeraars heeft in 2013 het volgende persbericht opgesteld (Verzekeraars, 2013):

"De cybermarkt brengt nieuwe verzekeringsvragen met zich mee. Materiële schade – zoals een brand in de serverruimte – wordt via traditionele verzekeringen gedekt. Schade aan data wordt echter zelden gezien als materiële schade. Reguliere aansprakelijkheidsverzekeringen bieden doorgaans ook alleen dekking voor zaak- en letselschade, niet voor financieel nadeel als gevolg van een digitaal incident. In het position paper constateert het Verbond dat geen enkele traditionele verzekering een goede dekking biedt voor cyberincidenten."
(Verzekeraars, 2013)

Verzekeraars zijn dan ook handig ingesprongen op de cybermarkt en verdienen hier goed aan. De cyberpolissen lossen het probleem rond risicomanagement op het gebied van social engineering niet op. De verzekeringen en verzekeraars dragen echter wel bij aan risicomanagement met betrekking tot social engineering. De verzekeringsmaatschappijen laten namelijk een quickscan uitvoeren bij de organisaties en eisen dat de organisaties de punten die uit de quickscan komen oplossen of afdekken. Hier kan worden gedacht aan het doorvoeren van cybersecurity-maatregelen en het opstellen en invoeren van beleid en richtlijnen binnen de organisaties. Ik heb niet kunnen achterhalen op welke punten wordt gecontroleerd in de quickscan.

3.5 Conclusie hoofdstuk 3

Uit de besproken studies blijkt dat een groot deel van de organisaties te maken krijgt met social engineering. Uit de eerste studie blijkt dat 48% van de grote bedrijven en 32% van de kleine bedrijven socialengineeringaanvallen hadden ondervonden. De tweede studie onderzocht alleen bedrijven die ook daadwerkelijk een data-inbreuk hadden ondervonden. Uit de derde studie blijkt dat 52% van de organisaties een socialengineeringaanval heeft ondervonden. De gemiddelde kostprijs van een aanval is $25.000 USD in de eerste studie en in de derde studie $46.000 USD. Dit verschil kan worden verklaard doordat de eerste studie in de periode 2099-2011 is uitgevoerd en de derde studie in 2014. Uit het onderzoek dat in Nederland is gedaan, blijkt dat 37% van de bedrijven met socialengineeringaanvallen te maken heeft gehad.

Informatiebeveiliging is dan ook essentieel voor alle organisaties. Als geen prioriteit aan informatiebeveiliging wordt gegeven, kan zelfs een klein gat in de beveiliging de organisatie te gronde richten. Organisaties hebben niet alleen te maken met directe kosten maar ook met indirecte kosten. Indirecte kosten in de vorm van imagoschade kunnen een organisatie jarenlang achtervolgen. Cybersecurity-verzekeringen kunnen de directe kosten en een gedeelte van de indirecte kosten afdekken. De aanbieders van deze verzekeringen eisen wel dat deelnemende organisaties een quickscan ondergaan en de punten uit de quickscan oppakken en doorvoeren. Hierdoor hebben de cybersecurity-verzekeringen een positieve invloed op risicomanagement op het gebied van cybersecurity en social engineering.

Hoofdstuk 4: Eindconclusie

Social engineering leeft in de literatuur. De literatuur over social engineering is dan ook naar mijn mening goed op de hoogte van de laatste ontwikkelingen en zeer compleet. Het is alleen jammer dat de informatie niet compleet in één model of op één plek is vastgelegd.

Vervolgens blijkt uit de besproken studies in hoofdstuk 3 dat een groot deel van de organisaties te maken krijgt met social engineering. Uit de eerste studie blijkt dat 48% van de grote bedrijven en 32% van de kleine bedrijven socialengineeringaanvallen hadden ondervonden. Uit de derde studie blijkt dat 52% van de organisaties een socialengineeringaanval heeft ondervonden. De gemiddelde kostprijs van een aanval is $25.000 USD in de eerste studie en in de derde studie $46.000 USD. Uit het onderzoek dat in Nederland is gedaan, blijkt dat 37% van de bedrijven met socialengineeringaanvallen te maken heeft gehad.

De hoofdvraag van dit literatuuronderzoek '*Schiet de literatuur over risicomanagement met betrekking tot social engineering tekort? Zo ja, waarop, waarmee, wat ontbeekt?'* kan volmondig met 'ja' worden beantwoord. Er ontbreekt een risicomanagementmodel dat specifiek social engineering aangaat. Ook ontbreekt een totaaloverzicht van alle essentiële controles en welke aanvallen/technieken/emoties worden afgedekt door gebruik te maken van deze controles.

Naar mijn mening is het vreemd dat er geen risicomanagementmodel specifiek voor social engineering aanwezig is als zoveel organisaties te maken krijgen met aanvallen en de gemiddelde kostprijs van een aanval zo hoog is. In mijn empirisch onderzoek wil ik dan ook de gegevens uit dit literatuuronderzoek gebruiken om een risicomanagement model specifiek voor social engineering te ontwikkelen.

Het gemaakte classificatieoverzicht in hoofdstuk 1 zal dan ook dienen als belangrijke input en is een van de uitgangspunten voor het komende empirische onderzoek. De classificatie maakt inzichtelijk welke typen socialengineeringaanvallen er zijn, welke operatoren gebruikt kunnen worden, de kanalen waardoor een aanval kan plaatsvinden, de gevonden aanvalstechnieken, de gewilde informatie en welke emoties van mensen worden gemanipuleerd door social engineers. Het overzicht maakt dan ook inzichtelijk welke risico's afgedekt dienen te worden om een organisatie zo goed mogelijk te beschermen tegen socialengineeringaanvallen.

Na de analyse van vier generieke risicomanagementmodellen in hoofdstuk 2 ben ik van mening dat het COSO-model het meest in aanmerking komt als basis voor een generiek socialengineeringrisicomodel. Het COSO model zal dan ook dienen als belangrijke input en is een van de uitgangspunten voor het komende empirische onderzoek.

Bibliografie

Peer-reviewed

Allen, M. (2006). *Social engineering a means to violate a computer system (white paper)*: SANS Institute Reading Room site.

Capgemini. (2015). *Cybersecurity in het MKB (techreport)* (Interpolis Ed.): Interpolis.

Cole, E., & Ring, S. (2006). *Insider Threat: Protecting the enterprise from sabotage, Spying, and Theft*. Canada: Syngress Publishing, Inc.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information Security Management. *Journal of information security and applications, 4*, 92-100.

Government, A. (2005). *Hacking motives*. Australie: Australian Institue of Criminology (white paper) Retrieved from http://www.aic.gov.au/media_library/publications/htcb/htcb006.pdf.

Gragg, D. (2002). *A multilevel defense against social engineering (white paper)*: SANS Institute InfoSec Reading Room.

Granger, S. (2010). *Social engineering fundamentals, Part I: hacker tactics (white paper)*: Symantec.

Gulati, R. (2003). *The Threat of social engineering and Your Defense Against It (white paper)*: SANS Institute InfoSec Reading Room.

Gupta, M., & Sharman, R. (2008). *Handbook of Research on Social and Organizational Liabilities in Information Security*. New York: Hershey.

Hansche, S., Berti, J., & Hare, C. (2003). *Official (ISC)² guide to the CISSP exam* Auerbach Publications: Boca Raton.

Hinson, G. (2008). Social engineering Techniques, Risks, and Controls. *EDPACS, 37*(4-5), 32-46. doi:10.1080/07366980801907540

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information security technical report, 13*(4), 247-255.

Institute, P. (2014). *2014 Global Report on the Cost of Cyber Crime*: Ponemon Institute.

Institute, P. (2015). *2015 Cost of Data Breach Study: Global Analysis (techreport)*: IBM.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50,* 94-100.

Kirwan, G., & Power, A. (2011). *The Psychology of Cyber Crime: Concepts and Principles*. United States: Hershey.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of information security and applications, 22*, 113-122.

Mann, I. (2008). *Hacking the human: Social engineering Techniques and Security Measures*. Burlington USA: Gower publishing limited.

Merle, E. v., & Hiasma, G. (2009). ISO 31000 stimuleert integraal risicomanagement. *TPC*.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception*: John Wiley &Amp Sons Inc.

Research, D. (2011). *THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS (techreport)*: Grey Castle Security.

Scott, D. (2009). Social engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective, 18*(1).

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeance using eighted arc cirumplex model. *Elsevier, 14*, 36-45.

Steinberg, R., Everson, M., Martens, F., & Nottingham, L. (2004). *Enterprise Risk Management - Integrated Framework (techreport)*: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Tipton, H. F., & Henry, K. (2006). *Official (ISC)2 Guide to the CISSP CBK*. Florida: Auerbach Publication.

Verzekeraars, V. v. (2013). Vraag naar cyberverzekering gaat hoge vlucht nemen. Retrieved from https://www.verzekeraars.nl/actueel/nieuwsberichten/Paginas/Vraag-naar-cyberverzekering-gaat-hoge-vlucht-ne-men.aspx

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Elsevier, 44*, 1-15.

Whitman, M., & Mattord, H. (2004). *Management of information security*.

Zulkurnain, A. U., Hamidy, A. K. B. K., Husain, A. B., & Chizari, H. (2015). Social engineering Attack Mitigation. *International Journal of Mathematics and Computational Science, 1*(4), 188-198.

Niet-peer-reviewed

Hermansson, M., & Ravne, R. (2005). Fighting social engineering: University of Stockholm: Royal Institute of Technology.

Terhurne, H. (2005). De PDCA cirkel in 7 stappen. *Management Tools, 3*.

Webopedia. (2015). Social engineering. Retrieved from http://www.webopedia.com/TERM/S/social_engineering.html

Wikipedia. (2015). Social engineering. Retrieved from https://nl.wikipedia.org/wiki/Social_engineering_(informatica)

Zager, M. (2002). Who are the hackers? . *Infosec News,* 3.